HAL
open science

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

José Grimm

To cite this version:

José Grimm. Implementation of Bourbaki's Elements of Mathematics in Coq: Part Two; Ordered Sets, Cardinals, Integers. [Research Report] RR-7150, 2009, pp.263. inria-00440786v1

HAL Id: inria-00440786

https://inria.hal.science/inria-00440786v1

Submitted on 11 Dec 2009 (v1), last revised 5 Dec 2018 (v10)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

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

José Grimm

N° 7150

December 2009

Domaine Mathématiques appliquées, calcul et simulation

Rapport de recherche

ISSN 0249-6399 ISRN INRIA/RR--7150--FR+ENG

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

INRIA

centre de recherche SOPHIA ANTIPOLIS - MÉDITERRANÉE

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

José Grimm*

Domaine Mathématiques appliquées, calcul et simulation —

Équipe-Projet Apics

Rapport de recherche n° 7150 — December 2009 — 263 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

Centre de recherche INRIA Sophia Antipolis – Méditerranée
2004, route des Lucioles, BP 93, 06902 Sophia Antipolis Cedex
Téléphone : +33 4 92 38 77 77 — Télécopie : +33 4 92 38 77 65

Implémentation de la théorie des ensembles de Bourbaki dans Coq partie 2
Ensembles Ordonnés, cardinaux, nombres entiers

Résumé : Nous pensons qu'il est possible de mettre dans un ordinateur l'ensemble de l'œuvre de Bourbaki. L'un des objectifs du projet Gaia concerne l'algèbre homologique (théorie et algorithmes); dans une première étape nous voulons implémenter les neuf chapitres du livre Algèbre. Au préalable, il faut implémenter la théorie des ensembles. Nous utilisons l'Assistant de Preuve Coq; les choix fondamentaux et axiomes sont ceux proposées par Carlos Simpson. Ce rapport liste et commente toutes les définitions et théorèmes du Chapitre "Ensembles ordonnés, cardinaux, nombres entiers". Une petite partie des exercises a été résolue. Le code est disponible sur le site Web http://www-sop.inria.fr/apics/gaia.

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

Introduction

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.

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 x 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 $\mathrm{E} \cup \{\mathrm{E}\}$ has cardinal $x+1$. As a consequence, one can define a mapping $n \mapsto \mathrm{E}_n$ 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. 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** containg 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 $\mathbf{N} \mapsto$ E, it is also the number of orderings on E (see Exercices).

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?).

Terminology

Chapter III is much less formal that 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 "$(\mathbf{R}, \leq)$ 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 $x \leq_{\mathbf{R}} y$; an alternative would be $x \leq y \pmod{\mathbf{R}}$ as in [7].

Bourbaki says: "a well-ordered set is totally ordered". This is a short-hand for: for every (E, Γ), if Γ is a well-ordering on E, then Γ 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 Γ 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).

Chapter 1

Order relations. Ordered sets

1.1 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 $x \in \mathrm{E}$ 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 transitive. The opposite relation of $\prec$, denoted by $\succ$, is such that $x \prec y$ and $y \succ x$ are equivalent.

```
Definition antisymmetric_r (r:EEP) :=
  forall x y, r x y -> r y x -> x = y.
Definition is_antisymmetric (r:Bset) :=
  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).
```

```
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. A correspondence $\Gamma = (\mathrm{G}, \mathrm{E}, \mathrm{E})$, whose graph G is an order on E, is also called an order by Bourbaki (this definition is in fact never used).

```
Definition order (r: Bset) :=
  is_graph r & is_reflexive r & is_transitive r & is_antisymmetric r.
Definition preorder (r: Bset) :=
  is_graph r & is_reflexive r & is_transitive r.
Definition opposite_order := inverse_graph.
Definition order_c r :=
  is_correspondence r & source r = target r & source r = substrate (graph r)
  & order (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).
```

We give here some simple properties of orders.

```
Lemma order_reflexivity_pr: forall  r x u v,
  order_re r x -> r u v -> (inc u x & inc v x).
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 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 $\mathfrak{P}$(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:Bset) :=
  graph_on (fun u v => sub u a & sub v a & sub u v) (powerset a).
Definition inclusion_suborder (b:Bset) :=
  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) 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 Φ(E, F) of functions from a subset of E to F and the extension relation. Remember that $x \in \Phi$(E, F) if an 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 Φ(E, F), they have the same target, namely F.

We can now define *extends_in* on the set Φ(E, F), and simplify the definition: g extends f if and only if $\mathrm{pr}_1 f \subset \mathrm{pr}_1 g$. This is an order; the only non trivial point is antisymmetry. If

$\mathrm{pr}_1 x = \mathrm{pr}_1 y$, we have $x = y$ since the source of a function depends only on its graph $\mathrm{pr}_1 x$. We then define *extension_order*. This is an order on $\Phi(\mathrm{E},\mathrm{F})$. Note that Bourbaki considers "g extends f" as a relation between f and g. In our definition g comes before f.

```
Definition extends_in x y:=
  fun g f=> inc f (set_of_sub_functions x y) & inc g (set_of_sub_functions x y)
    & extends (inv_corr_value g) (inv_corr_value f).
Definition extension_order x y :=
  graph_on (extends_in x y) (set_of_sub_functions x y).

Lemma extends_in_pr: forall x y g f,
  extends_in x y g f =
  (inc f (set_of_sub_functions x y) & inc g (set_of_sub_functions x y) &
  sub (P f) (P g)).
Lemma extends_refl: forall f,
  is_function f -> extends f f.
Lemma extends_antisymmetric: forall x y f g,
  inc f (set_of_sub_functions x y) ->
  inc g (set_of_sub_functions x y) ->
  P f = P g -> f = g.
Lemma extends_order: forall x y,
  order_re(extends_in x y) (set_of_sub_functions x y).
Lemma extension_is_order: forall x y,
  order (extension_order x y).
Lemma extension_order_rw: forall x y u v ,
  related (extension_order x y) u v = (extends_in x y u v).
Lemma substrate_extension_order:forall x y,
  substrate (extension_order x y) = (set_of_sub_functions x y).
```

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

```
Definition set_of_partition_set x :=
  Zo(powerset(powerset x)) (fun z => partition z x).

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 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 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 ϖ be a partition; consider the set formed of all $A \times A$ with $A \in \varpi$; let $\tilde{\varpi}$ be the union of all these sets. We pretend that this set is the graph of the equivalence associated to the partition. The relation "ϖ coarser than ϖ'" is equivalent to $\tilde{\varpi} \supset \tilde{\varpi}'$. Bourbaki says that this shows that coarser is an order. The nontrivial point is antisymmetry: we must show that $\tilde{\varpi} = \tilde{\varpi}'$ implies $\varpi = \varpi'$. 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 ϖ and in A and B for ϖ', the pair (a, b) is in $\tilde{\varpi}$, hence in $\tilde{\varpi}'$, 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 $\Delta \subset G$ and $G \circ G \subset G$ then $G \circ G = G$. The two assumptions say that G is reflexive and transitive, this a preorder. Antisymmetry is $G \cap G^{-1} \subset \Delta$. Since Δ is symmetric (i.e., it is its inverse), reflexivity is also $\Delta \subset G^{-1}$, so that G is an order if and only $G \circ G = G$, and $G \cap G^{-1} = \Delta$ (we know that G is an equivalence if and only $G \circ G = G$ and $G \cap G^{-1} = \Delta$). Proposition 1 of Bourbaki [2, p. 132] considers the case of a correspondence.

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

1.2 Preorder relations

Consider the relation "R is coarser than R′" in the set of all coverings of E. This is a preorder relation, since it is reflexive and transitive; it is not antisymmetric, for if R is a covering, $R' = R \cup \{X\}$ with $X \subset E$, then R′ is a covering which is coarser then R. Now, R is coarser than R′ if there is a $Y \in R$ such that $X \subset Y$. It can happen that $X \notin R$; 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 r ->
  equivalence_r (fun x y => r x y & r y x).
Lemma compatible_equivalence_preorder: forall r,
  let s := (fun x y => r x y & r y x) in
  preorder_r r -> forall x y x' y', r x y -> s x x' -> s y y' -> r x' y'.
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_pre_order: forall r,
  let s := (fun x y => r x y & r y x) in
  preorder_r r -> forall x y x' y', r x y -> s x x' -> s y y' -> r x' y'.
Lemma compatible_equivalence_preorder1: forall r u v x y,
  preorder r -> related r x y ->
  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 π 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 π. This set is also $(\pi \times \pi)\langle G \rangle$, 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 *associated* with $\prec$.

```
Definition order_associated (r:Bset) :=
  let s := (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,
  is_graph s -> is_graph r ->
  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.   (* 41 *)
```

1.3 Notation and terminology

For simplicity, we shall write $x \leq y$ instead of $x \prec y$, 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 *gle*, *gge*, *ggt* and *glt*. These are functions with three arguments: an order and two elements to be compared.

```
Definition gle (r x y:Bset) := related r x y.
Definition gge (r x y:Bset) := related r y x.
Definition glt (r x y:Bset) := gle r x y &  x <> y.
Definition ggt (r x y:Bset) := gge r x y &  x <> y.
```

For Bourbaki an order on E satisfies

(RO_I) The relation "$x \leq y$ and $y \leq z$" implies $x \leq z$.
(RO_{II}) The relation "$x \leq y$ and $y \leq x$" implies $x = y$.
(RO_{III}) The relation $x \leq y$ implies "$x \leq x$ and $y \leq y$".
(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, $P\{\!\{x\}\!\}$ is equivalent to $(\forall x)(P\{\!\{x\}\!\})$. 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:Bset) :=
  (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 $\leq_{\mathrm{E}}$ or $\leq_{\mathrm{F}}$ on E and F if f is a function from E to F compatible with the orders (this means the obvious: if $x \leq_{\mathrm{E}} y$ then $f(x) \leq_{\mathrm{F}} f(y)$ 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)).
```

1.4 Ordered subsets. Product of ordered sets

Let G be a graph, A a set. Define $\mathrm{G}_{\mathrm{A}} = \mathrm{G} \cap (\mathrm{A} \times \mathrm{A})$. This is a graph, whose substrate is a subset of A. If G is reflexive, with substrate E and $\mathrm{A} \subset \mathrm{E}$, 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 $x \leq y$ instead of $x \leq_{\mathrm{A}} y$. The first three lemmas here say that $x \leq_{\mathrm{A}} y$ implies $x \leq y$, and $x <_{\mathrm{A}} y$ implies $x < y$; moreover if $x \in \mathrm{A}$ and $y \in \mathrm{A}$, then $x \leq_{\mathrm{A}} y$ is equivalent to $x \leq y$.

```
Definition induced_order (r a:Bset):=
  intersection2 r (coarse a).

Lemma related_induced_order: forall r a x y,
  inc x a -> inc y a ->
  related (induced_order r a) x y = related r x y.
Lemma related_induced_order1: forall r a x y,
  gle (induced_order r a) x y -> gle r x y.
Lemma related_induced_order2: forall r a x y,
  glt (induced_order r a) x y -> glt r x y.

Lemma relation_induced_order :forall r a,
  is_graph r -> is_graph (induced_order r a).

Lemma substrate_induced_order1 :forall r a,
```

```
  is_reflexive r ->
  sub a (substrate r) ->  substrate (induced_order r a) = a.
Lemma substrate_induced_order :forall r a,
  order r ->
  sub a (substrate r) ->  substrate (induced_order r a) = a.
Lemma reflexive_induced_order: forall r a,
  sub a (substrate r) ->
  is_reflexive r -> is_reflexive (induced_order r a).
Lemma transitive_induced_order: forall r a,
  sub a (substrate r) ->
  is_transitive r -> is_transitive (induced_order r a).
Lemma preorder_induced_order: forall r a,
  sub a (substrate r) ->
  preorder r -> preorder (induced_order r a).
Lemma order_induced_order: forall r a,
  sub a (substrate r) ->
  order r -> order (induced_order r a).
Lemma sub_graph_coarse_substrate: forall r,
  is_graph r -> sub r (coarse (substrate r)).
Lemma induced_order_substrate: forall r,
  order r -> (* OK if r is graph *)
  induced_order r (substrate r) = r.
```

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 $\Gamma \mapsto G$ 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 :Bset):=
  (Zo(powerset (product x y)) (fun z => functional_graph z)).

Definition graph_of_function (x y:Bset):=
  BL (fun g => (P g)) (set_of_sub_functions x y)
  (set_of_graphs x y).

Lemma sub_graph_of_function: forall x y z,
  inc z (set_of_sub_functions x y) -> sub (P z) (product x y).
Lemma set_of_graphs_pr: forall x y z,
  inc z (set_of_sub_functions x y) -> inc (P z) (set_of_graphs x y).
Lemma axioms_graph_of_function: forall x y,
  transf_axioms(fun g => (P g)) (set_of_sub_functions x y)
  (set_of_graphs x y).
Lemma fonction_graph_of_function: forall x y,
  is_function (graph_of_function x y).
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 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 $\varpi \mapsto \tilde{\varpi}$, that maps a partition to the graph of the associated equivalence. We know that "ϖ coarser than ϖ'" 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 $\mathfrak{P}(E \times E)$.

```
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 target_gop: forall x,
  target(graph_of_partition 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 $s \subset t$; 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 =
  (preorder u & preorder v & substrate u = x & substrate v = x & sub 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_ι, a family of orders Γ_ι with graphs G_ι. Denote the relation associated to G_ι by $\leq_\iota$. On the product $\prod E_\iota$ we can consider the relation: $\forall \iota,\ x_\iota \leq_\iota x'_\iota$ between

$(x_\iota)_\iota$ and $(x'_\iota)_\iota$. 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:Bset): EEP :=
  fun 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').

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 &
  (forall i, inc i (domain f) -> order (V i g)) &
  (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 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 $f(x) \leq g(x)$. This is not an order because we cannot consider the set of all functions. However, this gives a natural order on $\mathscr{F}(E;F)$ via *sof_value*. Note.

The function that associates to a triple of $\mathscr{F}(E;F)$ its graph in F^E is an isomorphism.

```
Definition graph_order_r(x y g:Bset): EEP :=
  fun z z' =>
    inc z (set_of_gfunctions x y) & inc z' (set_of_gfunctions x y) &
    forall i, inc i x-> related g (V i z)(V i z').
Definition function_order_r x y r f g :=
  is_function f & is_function g &  source f = x & target f = y
  & source g =x & target g = y &
  forall i, inc i x -> related r (W i f) (W i g).
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 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 order_graph_order: forall x y g, order g -> substrate g = y ->
  order (graph_order x y g).
Lemma substrate_graph_order: forall x y g, order g -> substrate g = y ->
  substrate (graph_order x y g) = set_of_gfunctions x y.
Lemma reflexive_function_order: forall x y r u,
  order r -> substrate r = y ->
  inc u (set_of_functions x y) -> related (function_order x y r) u u.
Lemma substrate_function_order: forall x y r,
  order r -> substrate r = y ->
  substrate (function_order x y r) =set_of_functions x y.
Lemma order_function_order: forall x y r,
  order r -> substrate r = y -> order (function_order x y r).
Lemma function_order_pr: forall x y r f f',
  order r -> substrate r = y ->
  related (function_order x y r) f f' =
  (inc f (set_of_functions x y) &
    inc f' (set_of_functions x y) &
    forall i, inc i x ->
      related r (W i (sof_value x y f)) (W i (sof_value x y f'))).
Lemma isomorphism_function_order: forall x y r,
  order r -> substrate r = y ->
  order_isomorphism (BL P (set_of_functions x y)(set_of_gfunctions x y))
  (function_order x y r)(graph_order x y r). (* 15 *)
```

¶ 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).
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).
```

1.5 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*.

```
Definition 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 consequence 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 then one element. Let E be set, f the function that maps $X \subset E$ to its complementary. 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 r:=
  Zo (substrate r)(fun y => related r x y).
```

```
Lemma set_of_majorants1_pr: forall x y r,
  order r -> inc x (substrate r) -> inc y (substrate r) ->
  (related r x y = sub (set_of_majorants1 y r) (set_of_majorants1 x r)).
Lemma set_of_majorants1_decreasing: forall r, (* 15 *)
 order r ->
 strict_decreasing_fun(BL (fun x=> (set_of_majorants1 x r))
   (substrate r)(powerset (substrate r))) r  (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 opposite are increasing.

```
Lemma strict_increasing_from_injective: forall f r r',
  injective f -> increasing_fun f r r' -> strict_increasing_fun f r r'.
Lemma strict_decreasing_from_injective: forall f r r',
  injective f ->decreasing_fun f r r' -> strict_decreasing_fun f r r'.
Lemma strict_monotone_from_injective: forall f r r',
  injective f -> monotone_fun f r r' -> strict_monotone_fun f r r'.
Lemma order_isomorphism_increasing: forall f r r',
  order_isomorphism f r r' ->
  strict_increasing_fun f r r'.
Lemma order_morphism_increasing: forall f r r',
  order_morphism f r r' ->
  strict_increasing_fun f r r'.
Lemma order_isomorphism_pr: forall f r r',
  order r -> order r' ->
  bijective f -> substrate r = source f -> substrate r' = target f ->
  (order_isomorphism f r r' =
    (increasing_fun f r r' & increasing_fun (inverse_fun f) r' 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',
  decreasing_fun u r r' -> decreasing_fun v r' r ->
  (forall x, inc x (substrate r) -> related r (W (W x u) v) x) ->
  (forall x', inc x' (substrate r') -> related r' (W (W x' v) u) x') ->
  (compose u (compose v u) = u & compose v (compose u v) = v).  (* 21 *)
```

1.6 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 to 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,
  surjective 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 $\mathfrak{P}(E)$, the empty set is the smallest 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, (* 43 *)
  nonempty F -> inc x (set_of_sub_functions E F) ->
  maximal_element (opposite_order (extension_order E F)) x = (P (Q x) = E).
```

1.7 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 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.

```
Definition greatest_element r a:=
  inc a (substrate r) & forall x, inc x (substrate r) -> gle r x a.
Definition least_element r a:=
  inc a (substrate r) & forall x, inc x (substrate r) -> gle r a x.

Lemma unique_greatest: forall a b r,
```

```
  order r -> greatest_element r a -> greatest_element r b  -> a = b.
Lemma unique_least: forall a b r,
  order r -> least_element r a -> least_element r b -> a = b.
Lemma greatest_reverse: forall a r,
  order r -> greatest_element r a -> least_element (opposite_order r) a.
Lemma least_reverse: forall a r,
  order r -> least_element r a -> greatest_element (opposite_order r) a.
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 $\mathfrak{S}$ is a subset of $\mathfrak{P}(E)$, then the upper and lower bounds of $\mathfrak{S}$ 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 $\mathfrak{S}$. 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 $\mathfrak{P}(E)$, 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. In fact, two constant functions defined on the whole of E are maximal. Hence all constant functions are the same. If E is empty there is a unique partial function, the empty function, otherwise constants $x \mapsto u$ and $x \mapsto v$ are the same only if $u = v$.

```
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, Δ the diagonal of E, then Δ is the smallest of equivalences or preorders on E (for the inclusion order induced on $\mathfrak{P}(E \times E)$). 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 $(f \times f)\langle G\rangle$ is an order, its substrate is $f\langle E\rangle$, namely $\bar{E}$, and there is a unique order on $\bar{E} \cup \{a'\}$, extending $(f \times f)\langle G\rangle$ 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 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
  bijective f -> order r -> substrate r = source f ->
  (order r' & substrate r' = target f). (* 47 *)
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 *cofinal* (or *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).
```

1.8 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 :=
  inc x (substrate r) & forall y, inc y X -> gle r y x.
Definition lower_bound r X x :=
  inc x (substrate r) & forall y, inc y X -> 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 ->
  upper_bound r X x = lower_bound (opposite_order r) X x.
Lemma opposite_lower_bound: forall x X r, order r ->
  lower_bound r X x = upper_bound  (opposite_order r) X x.
Lemma smaller_lower_bound: forall x y X r, preorder r ->
  lower_bound r X x -> gle r y x -> lower_bound r X y.
Lemma greater_upper_bound: forall x y X r, preorder r ->
  upper_bound r X x -> gle r x y -> upper_bound r X y.
Lemma sub_lower_bound: forall x X Y r,
  lower_bound r X x -> sub Y X-> lower_bound r Y x.
Lemma sub_upper_bound: forall x X Y r,
  upper_bound r X x -> sub Y X -> upper_bound r Y x.
Lemma least_element_pr: forall X r, order r -> sub X (substrate r) ->
  (exists a, least_element (induced_order r X) a) =
  (exists x, lower_bound r X x & inc x X).
Lemma greatest_element_pr: forall X r, order r -> sub X (substrate r) ->
  (exists a, greatest_element (induced_order r X) a) =
  (exists x, upper_bound r X x & 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 ->bounded_above r X  -> bounded_above r Y.
Lemma bounded_below_sub: forall X Y r,
  sub Y X ->bounded_below r X  -> bounded_below r Y.
Lemma bounded_both_sub: forall X Y r,
```

```
  sub Y X ->bounded_both r X  -> bounded_both r Y.
Lemma singleton_bounded:forall x r,
  is_singleton x -> order r -> sub x (substrate r) -> bounded_both r x.
```

1.9 Least upper bound and greatest lower bound

The Bourbaki definition is: *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 *least upper bound* of X is an upper bound x such that if z is another upper bound, then $x \leq z$.

```
Definition greatest_lower_bound r X x :=
  greatest_element (induced_order r (Zo (substrate r)
    (fun z => lower_bound r X z))) x.
Definition least_upper_bound r X x :=
  least_element (induced_order r (Zo (substrate r)
    (fun z => upper_bound r X z))).

Lemma greatest_lower_bound_pr: forall r X x,
  order r -> sub X (substrate r) ->
  greatest_lower_bound r X x = (lower_bound r X x
    & forall z, lower_bound r X z -> gle r z x).
Lemma least_upper_bound_pr: forall r X x,
  order r -> sub X (substrate r) ->
  least_upper_bound r X x = (upper_bound r X x
    & forall z, upper_bound r X z -> gle r x z).
```

The greatest lower bound and least upper bound are also called supremum and infimum and denoted by $\sup_E X$ and $\inf_E X$. 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 $\sup(x, y)$ and $\inf(x, y)$. 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.

```
Lemma supremum_unique: forall x y X r, order r ->
  least_upper_bound r X x  -> least_upper_bound r X y  -> x = y.
Lemma infimum_unique: forall x y X r, order r ->
  greatest_lower_bound r X x  -> greatest_lower_bound r X y  -> x = y.

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

Lemma supremum_pr1: forall X r,
  order r -> sub X (substrate r) -> has_supremum r X ->
  least_upper_bound r X (supremum r X).
Lemma infimum_pr1: forall X r,
```

```
  order r -> sub X (substrate r) -> has_infimum r X ->
  greatest_lower_bound r X (infimum r X).
Lemma inc_supremum_substrate : forall X r,
  order r -> sub X (substrate r) -> has_supremum r X ->
  inc (supremum r X) (substrate r).
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 z (inf r a b)).
Lemma least_upper_bound_doubleton: forall r x y z,
  order r -> gle r x z -> gle r y z ->
  (forall t, gle r x t -> gle r y t -> gle r z t) ->
  least_upper_bound r (doubleton x y) z.
Lemma greatest_lower_bound_doubleton: forall r x y z,
  order r -> gle r z x  -> gle r z y ->
  (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 $\mathfrak{S}$ is a subset of $\mathfrak{P}(\mathrm{E})$, then the upper and lower bounds of $\mathfrak{S}$ 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.

```
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).
```

Third example. If u is in $\Phi(\mathrm{E},\mathrm{F})$, the set of partial functions from E to F, we denote its domain by $\mathrm{D}(u)$. If Θ is subset of $\Phi(\mathrm{E},\mathrm{F})$, it has a least upper bound if and only if for all u and v in the family, for all $x \in \mathrm{D}(u) \cap \mathrm{D}(v)$ we have $u(x) = v(x)$. Denote this property by $\mathrm{P}(u, v)$. We use an auxiliary result: if $u \leq w$, the condition $x \in \mathrm{D}(u) \cap \mathrm{D}(w)$ is equivalent to $x \in \mathrm{D}(u)$, and $\mathrm{P}(u, w)$ is true. Thus, if u and v are bounded by w, $\mathrm{P}(u, v)$ is true. Conversely, we know that if P is true on T there is a f function defined on the union of the $\mathrm{D}(u)$ 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)) ->  W x (inv_corr_value f) =  W 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 (P (Q u)) ->  inc x (P (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 (P (Q u)) ->  inc x (P (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 $f\langle\mathrm{A}\rangle$ is denoted by $\sup\limits_{x\in\mathrm{A}} f(x)$. The infimum is denoted by $\inf\limits_{x\in\mathrm{A}} f(x)$. For typographical reasons, for in-text formulas, the notations $\sup_{x\in\mathrm{A}} f(x)$, $\inf_{x\in\mathrm{A}} f(x)$ are preferred. If f is the identity function, one can write $\sup\limits_{x\in\mathrm{A}} x$ or $\inf\limits_{x\in\mathrm{A}} x$. We give a characterization of the sup and inf of a function.

```
Definition is_sup_fun r f x := least_upper_bound r (image_of_fun f) x.
Definition is_inf_fun r f x := greatest_lower_bound r (image_of_fun f) x.
```

```
Lemma is_sup_fun_pr: forall r f x, order r -> substrate r = target f ->
  is_function f ->
 is_sup_fun r f x = (inc x (target f)
   & (forall a, inc a (source f) -> gle r (W a f) x)
   & forall z, inc z (target f) -> (forall a, inc a (source f)
     -> gle r (W a f) z) -> gle r x z).
Lemma is_inf_fun_pr: forall r f x, order r -> substrate r = target f ->
  is_function f ->
  is_inf_fun r f x = (inc x (target f)
   & (forall a, inc a (source f) -> gle r x (W a f))
   & forall z, inc z (target f) -> (forall a, inc a (source f)
     -> gle r z (W a f)) -> gle r z x).
```

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

```
Definition is_sup_graph r f x := least_upper_bound r (range f) x.
Definition is_inf_graph r f x := greatest_lower_bound r (range f) x.
Definition has_sup_graph r  f := has_supremum r (range f).
Definition has_inf_graph r  f := has_infimum r (range f).
Definition sup_graph r f := supremum r (range f).
Definition inf_graph r f := infimum r (range f).
```

Here are the characteristic properties.

```
Lemma is_sup_graph_pr1: forall r f,
  order r -> sub (range f) (substrate r) -> has_sup_graph r f ->
  least_upper_bound r (range f) (sup_graph r f).
Lemma is_inf_graph_pr1: forall r f,
  order r -> sub (range f) (substrate r) -> has_inf_graph r f ->
  greatest_lower_bound r (range f) (inf_graph r f).

Lemma is_sup_graph_pr: forall r f x, order r -> sub (range f) (substrate r) ->
  fgraph f ->
  is_sup_graph r f x = (inc x (substrate r)
   & (forall a, inc a (domain f) -> gle r (V a f) x)
   & forall z, inc z (substrate r) -> (forall a, inc a (domain f)
     -> gle r (V a f) z) -> gle r x z).
Lemma is_inf_graph_pr: forall r f x, order r -> sub (range f) (substrate r) ->
  fgraph f ->
  is_inf_graph r f x = (inc x (substrate r)
   & (forall a, inc a (domain f) -> gle r x (V a f))
   & forall z, inc z (substrate r) -> (forall a, inc a (domain f)
     -> gle r z (V a f)) -> 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 $\mathfrak{P}(E)$ into E, where $\mathfrak{P}$ is ordered by inclusion). Of course, these are only partial functions. As a corollary, consider a family $(x_\iota)_{\iota\in I}$ and $J \subset I$; we have $\sup_{\iota\in J} x_\iota \leq \sup_{\iota\in I} x_\iota$ if both quantities 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 $F \to E$, 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 $\iota \in I$ we have $x_\iota \leq y_\iota$, then $\sup_{\iota\in I} x_\iota \leq \sup_{\iota\in I} y_\iota$, and $\inf_{\iota\in I} x_\iota \leq \inf_{\iota\in I} y_\iota$.

```
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 $(x_\iota)_{\iota\in I}$, and let $(J_\lambda)_{\lambda\in L}$ be a covering of I. The family $(x_\iota)_{\iota\in J_\lambda}$ is the restriction of (x_ι) to J_λ; we assume that it has a supremum $\sup_{\iota\in J_\lambda} x_\iota$, and we consider the family $(\sup_{\iota\in J_\lambda} x_\iota)_{\lambda\in L}$. This family has a supremum if and only if $(x_\iota)_{\iota\in I}$ has one, and the values are the same; the second equality in (1) is true under similar conditions.

$$\sup_{\iota\in I} x_\iota = \sup_{\lambda\in L}\big(\sup_{\iota\in J_\lambda} x_\iota\big), \qquad \inf_{\iota\in I} x_\iota = \inf_{\lambda\in L}\big(\inf_{\iota\in J_\lambda} x_\iota\big). \tag{1}$$

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, (* 58 *)
  order r -> fgraph f ->  sub (range f) (substrate r) ->
  covering c (domain f) ->
  (forall l, inc l (domain c) -> has_sup_graph r (restr f (V l c))) ->
  is_sup_graph r f x =
  is_sup_graph r (L (domain c) (fun l => sup_graph r (restr f (V l c)))) x.
Lemma inf_distributive: forall r f c x,  (* 58 *)
  order r -> fgraph f ->  sub (range f) (substrate r) ->
  covering c (domain f) ->
  (forall l, inc l (domain c) -> has_inf_graph r (restr f (V l c))) ->
  is_inf_graph r f x =
  is_inf_graph r (L (domain c) (fun l => inf_graph r (restr f (V l c)))) x.
Lemma sup_distributive1: forall r f c,
  order r -> fgraph f ->  sub (range f) (substrate r) ->
  covering c (domain f) ->
  (forall l, inc l (domain c) -> has_sup_graph r (restr f (V l c))) ->
  has_sup_graph r f =
  has_sup_graph r (L (domain c) (fun l => sup_graph r (restr f (V l c)))) .
Lemma inf_distributive1: forall r f c,
  order r -> fgraph f ->  sub (range f) (substrate r) ->
  covering c (domain f) ->
  (forall l, inc l (domain c) -> has_inf_graph r (restr f (V l c))) ->
  has_inf_graph r f =
  has_inf_graph r (L (domain c) (fun l => inf_graph r (restr f (V l c)))) .

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

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

$$\sup_{(\lambda,\mu)\in L\times M} x_{\lambda\mu} = \sup_{\mu\in M}\big(\sup_{\lambda\in L} x_{\lambda\mu}\big), \qquad \inf_{(\lambda,\mu)\in L\times M} x_{\lambda\mu} = \inf_{\mu\in M}\big(\inf_{\lambda\in L} x_{\lambda\mu}\big). \tag{2}$$

```
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_ι, a subset A of $\prod E_\iota$, and if $A_\iota = \mathrm{pr}_\iota A$, then A has a least upper bound of the form $(x_\iota)_\iota$ if and only if each A_ι has one, and there is equality; a similar property holds for the greatest lower bound.

$$\sup A = (\sup A_\iota)_{\iota\in I} = \big(\sup_{x\in A} \mathrm{pr}_\iota x\big)_{\iota\in I}, \qquad \inf A = (\inf A_\iota)_{\iota\in I} = \big(\inf_{x\in A} \mathrm{pr}_\iota x\big)_{\iota\in I}.$$

```
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

$$\sup_E A \le \sup_F A, \qquad \inf_E \ge \inf_F A \qquad (F \subset E).$$

If $\sup_E A$ exists and is in F, it is $\sup_F A$.

```
Theorem sup_induced1: forall r A F, order r -> sub F (substrate r) -> sub A F ->
  has_supremum r A -> has_supremum (induced_order r F) A ->
  gle r (supremum r A) (supremum (induced_order r F) A).
Theorem inf_induced1: forall r A F, order r -> sub F (substrate r) -> sub A F ->
  has_infimum r A -> has_infimum (induced_order r F) A ->
  gge r (infimum r A) (infimum (induced_order r F) A).
Theorem sup_induced2: forall r A F, order r -> sub F (substrate r) -> sub A F ->
```

```
  has_supremum r A -> inc (supremum r A)  F ->
  (has_supremum (induced_order r F) A &
    supremum r A = supremum (induced_order r F) A).
Theorem inf_induced2: forall r A F, order r -> sub F (substrate r) -> sub A F ->
  has_infimum r A -> inc (infimum r A)  F ->
  (has_infimum (induced_order r F) A &
    infimum r A = infimum (induced_order r F) A).
```

1.10 Directed sets

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

```
Definition right_directed r :=
  order r & forall x, forall y, inc x (substrate r) -> inc y (substrate r) ->
    bounded_above r (doubleton x y).
Definition left_directed r :=
  order r & forall x, forall y, inc x (substrate r) -> inc y (substrate r) ->
    bounded_below r (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,
  right_directed r = (order r &
    forall x, forall y, inc x (substrate r) -> inc y (substrate r) -> exists z,
      inc z (substrate r) & gle r x z  & gle r y z).
Lemma left_directed_pr: forall r,
  left_directed r = (order r &
    forall x, forall y, inc x (substrate r) -> inc y (substrate r) -> exists z,
      inc z (substrate r) & gle r z x  & gle r z y).

Lemma greatest_right_directed : forall r, order r ->
  (exists a, greatest_element r a )  -> right_directed r .
Lemma least_left_directed : forall r, order r ->
  (exists a, least_element r a )  -> left_directed r.
Lemma opposite_right_directed : forall r, is_graph r ->
  right_directed r = left_directed(opposite_order r).
Lemma opposite_left_directed : forall r, is_graph r ->
  left_directed r = right_directed(opposite_order r).
Lemma product_right_directed: forall f g, (* 14 *)
  axioms_product_order f g ->
  (forall i, inc i (domain f) -> right_directed (V i g))
  -> right_directed (product_order f g).
Lemma product_left_directed: forall f g,  (* 14 *)
  axioms_product_order f g ->
  (forall i, inc i (domain f) -> left_directed (V i g))
  -> 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 coinitial_left_directed: forall r A,
  left_directed r -> coinitial_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_mimimal: forall r x,
  left_directed r -> minimal_element r x -> least_element r x.
```

1.11 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 -> 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 $\mathrm{pr}_\iota A$ 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).
```

1.12 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 is is ordered and if any two elements of E are comparable.

```
Definition total_order r :=
  order r & forall x y, inc x (substrate r) -> inc y (substrate r) ->
    (gle r x y \/ 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 $x > y$ or $x = y$. 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,
  total_order r =
    (compose_graph r r = r &
    intersection2 r (opposite_order r) = diagonal (substrate r)&
    union2 r (opposite_order r) =  coarse (substrate r)).
Lemma total_order_pr1 : forall r x y,
  total_order r ->  inc x (substrate r) -> inc y (substrate r) ->
    (glt r x y \/ ggt r x y \/ x = y).
Lemma total_order_sub : forall r x,
  total_order r ->  sub x (substrate r) -> total_order (induced_order r x).
Lemma total_order_conterexample:
  ~ (total_order (inclusion_order two_points)).
Lemma total_order_opposite: forall r,
 total_order r -> total_order (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, gle r x y ->
  order r -> least_upper_bound r (doubleton x y) y.
Lemma inf_comparable: forall r x y, gle r x y ->
  order r -> greatest_lower_bound r (doubleton x y) x.
Lemma sup_comparable1: forall r x y, order r -> gle r x y -> sup r x y = y.
Lemma inf_comparable1: forall r x y, order r -> gle r x y -> inf r x y = x.
Lemma doubleton_sym: forall x y, doubleton x y = doubleton y x.
Lemma total_order_lattice: forall r,  total_order r -> lattice r.
Lemma total_order_directed: forall r,
  total_order r -> (right_directed r & 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',
  strict_increasing_fun f r r' -> increasing_fun f r r'.
Lemma decreasing_fun_from_strict: forall f r r',
  strict_decreasing_fun f r r' -> 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 $z \leq x$. We first show that in a totally order set we have $x \leq y$ or $y < x$.

```
Lemma compare_dichot: forall r x y,
```

```
  total_order r -> inc x (substrate r) -> inc y (substrate r)
  -> (gle r x y \/ glt r y 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)).
```

1.13 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 $]\leftarrow, b[$, 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_cc r a b := Zo(substrate r)(fun z => gle r a z & gle 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 b := Zo (substrate r) (fun z => gle r  z b).
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 := is_closed_interval r x \/
  is_open_interval r x \/ is_semi_open_interval r x.
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_ou r 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 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. There are 81 cases to consider. By symmetry, we have to consider only 45 cases. We further simplify the proof by considering reverse order.

```
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 ->
  is_bounded_interval r x -> is_bounded_interval (opposite_order r) x.

Lemma opposite_interval_uu: forall r,
  order r -> interval_uu r = interval_uu (opposite_order r).
Lemma opposite_interval_uo: forall r a,
  order r -> interval_uo r a = interval_ou (opposite_order r) a.
Lemma opposite_interval_ou: forall r a,
  order r -> interval_ou r a = interval_uo (opposite_order r) a.
Lemma opposite_interval_cu: forall r a,
  order r -> interval_cu r a = interval_uc (opposite_order r) a.
Lemma opposite_interval_uc: forall r a,
  order r -> interval_uc r a = interval_cu (opposite_order r) a.
Lemma opposite_unbounded_interval: forall r x, order r ->
  is_unbounded_interval r x -> is_unbounded_interval (opposite_order r) x.
Lemma opposite_interval: forall r x, order r ->
  is_interval r x -> is_interval (opposite_order r) x.
```

Note the the intersection of two closed intervals is either empty or is a closed interval.

The intersection of two open intervals may be closed: let a and b two non-comparable elements and $c = \sup(a,b)$. Then $c > a$ and $c > b$, so that the intersection of $]a, \rightarrow[$ and $]b, \rightarrow[$ is $[c, \rightarrow[$. We start with lemmas about bounded intervals.

```
Lemma intersection_interval1: forall r x y,
  lattice r ->is_closed_interval r x -> is_closed_interval r y  ->
    is_bounded_interval r (intersection2 x y).   (* 24 *)
Lemma intersection_interval2: forall r x y,
  lattice r ->is_open_interval r x -> is_open_interval r y  ->
  is_bounded_interval r (intersection2 x y).     (* 102 *)
Lemma intersection_interval3: 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_co r a' b')) (* 43 *)
Lemma intersection_interval4: 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_oc r a b)(interval_oc r a' b')).
Lemma intersection_interval5: 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_oc r a' b')). (* 72 *)
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')). (* 68 *)
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')). (* 38 *)
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')). (* 79 *)
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_cc r a b)(interval_co 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).  (* 58 *)
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). (* 33 *)
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). (* 195 *)
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 theorem is trivial, its proof has three lines; however, if we count all previous lemmas, this gives a total of 841.

```
Theorem intersection_interval: forall r x y,
  lattice r -> is_interval r x -> is_interval r y ->
  is_interval r (intersection2 x y).
```

Chapter 2

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.

2.1 Segments of a well-ordered set

A relation $\mathrm{R}\{\!\{x, y\}\!\}$ 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 $\mathrm{R}\{\!\{x, y\}\!\}$ induces an order relation, E, ordered by this relation, has a least element. A set E ordered by an ordering Γ is said to be *well-ordered* if the relation $y \in \Gamma\langle x\rangle$ is a well ordering between x and y; Γ is then said to be a well-ordering on E. The definition that follows corresponds to Γ.

```
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:
```

```
  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 $x < y$ means $x \leq y$ and $x \neq y$. Thus $x < x$ is false and $x < y$ implies that x and y are in E. If we have a total order on E, if $x \in$ E and $y \in$ E then $x < y$ or $y \leq x$; 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 total_order_pr2 : forall r x y,
  total_order r ->  inc x (substrate r) -> inc y (substrate r) ->
    (glt r x y \/ gle r y x).
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' -> worder 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 $]\leftarrow, x[$ is a segment; it will be denoted by S_x, and is called the *segment with endpoint* x. The interval $]\leftarrow, x]$ 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.
```

The 20-some following lemmas sometimes assume that we have an order $\leq$ on E, and that S is a segment. We assume $x' \in \mathrm{E}$. They state that if $x \in \mathrm{S}$ and $y < x$ then $y \in \mathrm{S}$. If $y \in]\leftarrow, x[$ then $y < x$. We have $\mathrm{S} \subset \mathrm{E}$. We have $]\leftarrow, x[\subset \mathrm{E}$, $]\leftarrow, x]x \subset \mathrm{E}$. We have $x \notin]\leftarrow, x[$ and $x' \in]\leftarrow, x']]$. We have $y < x'$ if and only if $y \in]\leftarrow, x['$ and $y \leq x'$ if and only if $y \in]\leftarrow, x']$. We have $]\leftarrow, x'] =]\leftarrow, x[\cup \{x\}'$. We have $]\leftarrow, x[_{\mathrm{F}} \subset \mathrm{F}$, where the notation W_{F} 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 $]\leftarrow, x'[$ is a segment.

```
Lemma lt_in_segment: forall r s x y,
  is_segment r s ->  inc x s -> glt r y x -> inc y s.
Lemma inc_segment: forall r x y, inc y (segment r x) -> glt r y x.
Lemma not_in_segment : forall r x,  inc x (segment r x) -> False.
Lemma sub_segment: forall r x, sub (segment r x) (substrate r).
Lemma sub_segment1: forall r s,  is_segment r s -> sub s (substrate r).
Lemma sub_segment2: forall r x y,
  sub (segment (induced_order r x) y) x.
Lemma segment_inc: forall r x y, inc x (substrate r) ->
  glt r y x -> inc y (segment r x).
Lemma segment_rw: forall r x y, inc x (substrate r) ->
  inc y (segment r x) = glt r y x.
Lemma segmentc_rw: forall r x y, inc x (substrate r) ->
  inc y (segment_c r x) = gle r y x.
Lemma inc_bound_segmentc: forall r x, order r -> inc x (substrate r) ->
  inc x (segment_c r x).
Lemma sub_segmentc: forall r x, sub (segment_c r x) (substrate r).
Lemma segment_c_pr: forall r x, order r -> inc x (substrate r) ->
  tack_on (segment r x) x = segment_c r x.
Lemma empty_is_segment: forall r, is_segment r emptyset.
Lemma substrate_is_segment: forall r, order r -> is_segment r (substrate r).
Lemma intersection_is_segment: forall r s , order r -> nonempty s ->
  (forall x, inc x s -> is_segment r x) -> is_segment r (intersection s).
Lemma union_is_segment: forall r s , order r ->
  (forall x, inc x s -> is_segment r x) -> is_segment r (union s).
Lemma unionf_is_segment: forall r j s, order r ->
  (forall x, inc x j -> is_segment r (s x)) -> is_segment r (unionf j s).
Lemma subsegment_is_segment: forall r s s', order r ->
  is_segment r s -> is_segment (induced_order r s) s' -> is_segment r s'.
Lemma segment_is_segment: forall r x, order r ->
  inc x (substrate r) -> is_segment r (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. If an ordered set has a least element a, then $\mathrm{S}_x = [a, x[$; 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 $\mathrm{S} = [a, x[$.

```
Theorem well_ordered_segment: forall r s, worder r -> is_segment r s ->
  s = substrate r \/ (exists x,  inc x (substrate r) &  s = segment r x). (* 15 *)
Lemma segment_alt: forall r x a, order r -> least_element r a ->
```

```
  segment r x = interval_co r a x.
Lemma segment_alt1: forall r s, worder r -> is_segment r s ->
  s = substrate r \/ (exists x, exists a, s = interval_co  r a x).
```

Some useful lemmas. We consider a well-ordered set. If S and S′ are segments, then $S \subset S'$ or $S' \subset S$. If $S \subset S'$, 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 $]\leftarrow, x]$ is a segment. If S is a segment $x \in S$, 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 $]\leftarrow, y]$ or $]\leftarrow, y[$ if $x < y$.

```
Lemma segment_dichot_sub: forall r x y,
  worder r -> is_segment r x -> is_segment r y ->
 (sub x y \/ sub y x).
Lemma segments_induced_order: forall r s' s'' x,
  worder r -> is_segment r s' -> is_segment r s'' -> sub s' s'' -> inc x s' ->
  segment (induced_order r s') x = segment (induced_order r s'') x.
Lemma segment_monotone: forall r x y, order r -> gle r x y ->
  sub (segment r x)  (segment r y).
Lemma le_in_segment: forall r x y z, worder r -> inc x (substrate r) ->
  inc y (segment r x) -> gle r z y -> inc z (segment r x).
Lemma coarse_segment_monotone: forall r x y, worder r -> gle r x y ->
  sub (coarse (segment r x)) (coarse (segment r y)).
Lemma tack_on_segment: forall r x,
  worder r -> inc x (substrate r) ->
  is_segment r (segment_c r x).
Lemma segment_induced_a: forall r s x,
  worder r -> is_segment r s -> inc x s ->
  segment (induced_order r s) x = segment r x.
Lemma segment_induced: forall r x x0, worder r ->  glt r x0 x ->
  segment (induced_order r (segment r x)) x0 = segment r x0.
Lemma segment_induced1: forall r x x0, worder r ->  glt r x0 x ->
  segment (induced_order r (segment_c r x)) x0 = segment r x0.
```

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 ->         (* 18 *)
  let E := substrate r in
    let A := union (fun_image E (fun x => (segment r x))) in
      ( (forall x, ~ (greatest_element r x)) -> A = E)
      & (forall x, greatest_element r x -> A = complement E (singleton x)).
```

If $]\leftarrow, x[=]\leftarrow, y[$ then $x = y$ (if $x < y$, then $x \in]\leftarrow, y[$ et $x \notin]\leftarrow, x[$).

```
Lemma segment_injective: forall r x y, total_order r ->
  inc x (substrate r) ->  inc y (substrate r) -> segment r x = segment r y ->
  x = y.
Lemma segment_injective1: forall r x y, worder r ->
  inc x (substrate r) ->  inc y (substrate r) -> segment r x = segment r y ->
  x = y.
```

Assume that E is well-ordered. The mapping $x \mapsto S_x$ 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:=
  fun_image (substrate r) (fun x => (segment r x)).
Definition set_of_segments r:=
  tack_on (set_of_segments_strict r) (substrate r).
Definition  set_of_segments_iso r:=
  BL(segment r) (substrate r) (set_of_segments_strict r).

Lemma inc_set_of_segments: forall r x, worder r ->
  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* (α,β) *such that* $X_\alpha \subset X_\beta$, *the ordering induced on* X_α *by that of* X_β *is identical with the given ordering on* X_α. *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_α. In the lemma that follows, g is the family of orders (G_α) 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 *Let* $(X_\iota)_{\iota\in I}$ *be a family of well-ordered sets such that for each pair of indices* (ι,κ) *one of the sets* X_ι, X_κ *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_ι. *Endowed with this ordering,* E *is a well-ordered set. Every segment of* X_ι *is a segment of* E*; for each* $x \in X_\iota$, *the segment with endpoint* x *in* X *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_ι. Note that if $X_\alpha = X_\beta$, then each

set is a segment of the other; the orderings G_α and G_β 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 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 *)
```

2.2 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 $\mathfrak{S}$ of segments of E, all segments are in $\mathfrak{S}$ if $\mathfrak{S}$ is stable by union and by adjunction of a greatest element (i.e., if the segment S_x belongs to $\mathfrak{S}$ then $S_x \cup \{x\}$ belongs to $\mathfrak{S}$). As a consequence, the substrate of the order is in $\mathfrak{S}$.

```
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 $\mathrm{H}(x)$ be the assumption: "$x \in \mathrm{E}$, and for all $y \in \mathrm{E}$ such that $y < x$, then $p(y)$ is true". Assume that $\leq$ is a well-ordering on E. Assume that, for all x, $\mathrm{H}(x)$ is true; then $p(x)$ is true. This is C59 ("Principle of transfinite induction"), [2, p. 151].

```
Theorem transfinite_principle: forall r (p:EP),
  worder r ->
  (forall x, inc x (substrate r) ->
       (forall y, inc y (substrate r) -> glt r y x -> p y)
     -> p x)
   ->  forall x, inc x (substrate r) -> p x.
```

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

```
Definition restriction_to_segment r x g :=
  restriction2 g (segment r x) (image_by_fun g (segment r x)).
Definition restriction_to_segment_axiom r x g :=
  worder r & inc x (substrate r) & is_function g & sub (segment r x) (source g).


Lemma sub_image_target: forall g x, is_function g ->
  sub (image_by_fun g x) (target g).
Lemma source_rts: forall r x g,
  source (restriction_to_segment r x g) = (segment r x).
Lemma target_rts:forall r x g,
  target (restriction_to_segment r x g) = image_by_fun g (segment r x).
Lemma axioms_rts: forall r x g,  restriction_to_segment_axiom r x g  ->
  restriction2_axioms g (segment r x) (image_by_fun g (segment r x)).
Lemma function_rts: forall r x g,  restriction_to_segment_axiom r x g  ->
  is_function (restriction_to_segment r x g).
Lemma W_rts: forall r x g a,  restriction_to_segment_axiom r x g  ->
  glt r a x -> W a  (restriction_to_segment r x g) = W a g.
Lemma surjective_rts: forall r x g,  restriction_to_segment_axiom r x g  ->
  surjective(restriction_to_segment r x g).

Lemma rts_extensionality: forall r s x f g,
  worder r -> inc x (substrate r) -> worder s -> inc x (substrate s) ->
  segment r x = segment s x ->
  is_function f -> sub (segment r x) (source f) ->
  is_function g -> sub (segment s x) (source g) ->
  (forall a , inc a (segment r x) -> W a f = W a g) ->
  restriction_to_segment r x f = restriction_to_segment s x g.
```

We can now state Criterion C60 (Definition of a mapping by transfinite induction) [2, p. 151]: *Let u be a letter,* $\mathrm{T}\{u\}$ *a term in the theory* $\mathscr{T}$ *(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* $x \in \mathrm{E}$ *we have* $f(x) = \mathrm{T}\{f^{(x)}\}$*. Furthermore the set* U *and the mapping* f *are uniquely determined by these conditions.*

We shall denote by $f_{\mathrm{S}}^{(x)}$ 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 $\mathscr{I}(\mathrm{S}, \mathrm{T}, f)$ the property of the criterion, namely, that f is a surjective function defined on S such that $f(x) = \mathrm{T}\{f_{\mathrm{S}}^{(x)}\}$ for every $x \in \mathrm{S}$.

Assume that $\mathscr{I}(\mathrm{E}, \mathrm{T}, f)$ and $\mathscr{I}(\mathrm{E}, \mathrm{T}, f')$ are true. Assume $x \in \mathrm{E}$, f and f' agree on S_x. Then $f_{\mathrm{E}}^{(x)} = f_{\mathrm{E}}^{\prime(x)}$ (the functions have the same target, because they are surjective, and take the

same value). By assumption, $\mathrm{T}\{\!\{f_{\mathrm{E}}^{(x)}\}\!\} = \mathrm{T}\{\!\{f_{\mathrm{E}}'^{(x)}\}\!\}$, so that f and f' agree on $\mathrm{S}_x \cup \{x\}$ (this *transfinite_unique1*). We consider the set of all segments $\mathfrak{S}$ 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 $\mathrm{S}_x \cup \{x\}$. Hence it contains E. Since f and f' agree on E, they are equal (same reasoning as above).

Assume now that $\mathscr{I}(\mathrm{S}', \mathrm{T}, f')$ and $\mathscr{I}(\mathrm{S}'', \mathrm{T}, f'')$ are true, and S' and S'' are segments such that $\mathrm{S}' \subset \mathrm{S}''$. Let f be the restriction of f'' on S'. This is a surjective function. We have $f_{\mathrm{S}'}^{(x)} = f_{\mathrm{S}'}''^{(x)}$ (because the functions are surjective and take the same values on S'). We have $f_{\mathrm{S}'}''^{(x)} = f_{\mathrm{S}''}''^{(x)}$ because these are two restrictions to identical segments. We have $f(x) = f''(x)$. Assumption $\mathscr{I}(\mathrm{S}'', \mathrm{T}, f'')$ gives thus $f(x) = \mathrm{T}\{\!\{f_{\mathrm{S}'}^{(x)}\}\!\}$, in other words, $\mathscr{I}(\mathrm{S}', \mathrm{T}, f)$, hence $f = f'$ by uniqueness. This is *transfinite_aux1*.

Assume we have a set of segments $\mathfrak{S}$ and, for $\mathrm{S} \in \mathfrak{S}$, we have a function f_s such that $\mathscr{I}(s, \mathrm{T}, f_s)$. We use our axiom of choice to select such a function f_s. Let t be the union of the targets of the f_s, and let g_s 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_s and $g_{s'}$ agree on s (previous result). By symmetry g_s and $g_{s'}$ agree on s' in the other case. Using *prolongation_covering*, we get a function g that coincides with every g_s. The target of this function is t, so that the function is surjective. Assume $x \in \mathrm{S}$ and $\mathrm{S} \in \mathfrak{S}$. We have $g(x) = f_{\mathrm{S}}(x)$ because $f_{\mathrm{S}}(x) = g_{\mathrm{S}}(x)$. Thus the quantities $g_t^{(x)}$ and $f_{\mathrm{S}t}^{(x)}$ are well defined and equal. We have $f_{\mathrm{S}t}^{(x)} = f_{\mathrm{SS}}^{(x)}$ 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 $x \in \mathrm{S} \subset t$). We have $f_{\mathrm{S}}(x) = \mathrm{T}\{\!\{f_{\mathrm{SS}}^{(x)}\}\!\}$ by assumption. Thus $g(x) = \mathrm{T}\{\!\{g_t^{(x)}\}\!\}$. This means that $\mathscr{I}(t, \mathrm{T}, g)$ is true. This is *transfinite_aux2*. We changed a bit the theorem; initially it was: if, for $\mathrm{S} \in \mathfrak{S}$, there exists a function f such that $\mathscr{I}(s, \mathrm{T}, f)$, there is a function g such that $\mathscr{I}(t, \mathrm{T}, g)$. It is now: given functions f_s such that $\mathscr{I}(s, \mathrm{T}, f_s)$, there exists a function g such that $\mathscr{I}(t, \mathrm{T}, g)$ 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 $\mathscr{I}(\mathrm{S}_y, \mathrm{T}, f)$. Let's extend f to f' via to $\mathrm{S}_y \cup \{y\}$ via the formula $f'(y) = \mathrm{T}\{\!\{f^{(y)}\}\!\}$. This function takes the same values as f on subsets of S_y hence $f'(x) = \mathrm{T}\{\!\{f_{\mathrm{S}_y}'^{(x)}\}\!\}$ for every $x \in \mathrm{S}_y$. The formula is also true for $y = x$, hence $\mathscr{I}(\mathrm{S}_y \cup \{y\}, \mathrm{T}, f')$. 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 $\mathrm{T}\{\!\{u\}\!\} \in \mathrm{F}$. If we change the definition of $\mathscr{I}(\mathrm{S}, \mathrm{T}, f)$ 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) -> 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 : Bset, inc x (segment r z) -> W x f = 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' = restriction2 f'' s' (image_by_fun f'' s').  (* 26 *)

(* old version
Lemma transfinite_aux2: forall r p s, worder r -> (* 70 *)
  (forall z, inc z s -> is_segment r z) ->
  (forall z, inc z s -> (exists f : correspondenceC,
                transfinite_def (induced_order r z) p f)) ->
  exists f : correspondenceC, transfinite_def (induced_order r (union s)) p f.
*)

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).

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 *)
```

2.3 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, Γ and Γ' on E and E$'$; denote by S_x and S'_x the segments with endpoints x in Γ and Γ' (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 Γ and Γ' induce the same ordering on S_x. This set is a segment for Γ and Γ', 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' v, worder r ->  worder r' ->
  v = common_ordering_set r r' ->  is_segment r v.    (* 28 *)
```

```
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(Γ) denote the following property: Γ is a well-ordering of a subset of E, and if S_x denotes the segment of Γ with endpoint x, we have $S_x \in \mathfrak{S}$ and $p(S_x) = x$.

```
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 Γ and Γ′, then $E \subset E'$, E is a segment of Γ′, and Γ is the ordering induced by Γ′ on E. We pretend that if Q(Γ) and Q(Γ′) 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 Γ and Γ′). 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 Γ be a well-ordering and x an element not in the substrate. We can extend Γ as Γ′ by adjoining x as greatest element. This is a well-ordering, a segment of this order is either the substrate of Γ′, the substrate of Γ, or a segment S_x of Γ.

```
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, $\mathfrak{S}$ a part of $\mathfrak{P}(E)$ and p a function from $\mathfrak{S}$ into E such that $p(X) \notin X$. Consider $\mathfrak{M}$, the set of orderings Γ that satisfy property Q; by virtue of *Zermelo_aux3*, there is a well-ordering Γ (the unions of the elements of $\mathfrak{M}$) that extends the orderings of $\mathfrak{M}$. It satisfies Q. Its substrate M is not in $\mathfrak{S}$. Proof: if $M \in \mathfrak{S}$, and $a = p(M)$, we know $a \notin M$, so that we can extend Γ to Γ′ by adjoining a as greatest element. This new order satisfies Q (for all y, $S_y \in \mathfrak{S}$ and $p(S_y) = y$; this is true if y is in the support of Γ, otherwise $y = a$ and $S_a = M \in \mathfrak{S}$, $p(S_a) = p(M) = a$). This means that the new order is in $\mathfrak{M}$, 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 $\mathfrak{S}$ 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 $\mathfrak{P}(E) - \mathfrak{S}$. 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 *)
```

2.4 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 146.

```
Definition inductive_set r :=
  forall X, sub X (substrate r) -> total_order (induced_order r X) ->
    exists x, upper_bound r X x.

Lemma inductive_graphs: forall a b,
  inductive_set (opposite_order (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 $\mathfrak{S}$ be the set of sets $S \subset E$ for such a $p(S)$ exists. By *Zermelo_aux*, there is Γ that satisfies Q, i.e. Γ is a well-ordering of a subset M of E, and if S_x denotes the segment of Γ with endpoint x, we have $S_x \in \mathfrak{S}$ and $p(S_x) = x$. This last condition says that if $y < x$ for Γ, it is true for the ordering on E; hence Γ 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 Zorn_aux: forall r, order  r ->
  (forall s, sub s (substrate r) -> worder (restriction_order r s) ->
    (bounded_above r s)) ->
  exists a, maximal_element r a.  (* 35 *)
Theorem Zorn_lemma: forall r, order  r -> inductive_set  r ->
  exists a, 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 $\mathfrak{F}$ is a subset of the powerset of E such that for every subset $\mathfrak{G}$ of $\mathfrak{F}$ which is totally ordered by inclusion, the union (resp. intersection) of the sets of $\mathfrak{G}$ belongs to $\mathfrak{F}$, then $\mathfrak{F}$ has a maximal or minimal element. The trick with the intersection is that the intersection is not defined if $\mathfrak{G}$ is empty. The set is nevertheless inductive, provided that $\mathfrak{F}$ is not empty (in the case of the union, it contains the empty set).

```
Lemma inductive_max_greater: forall r a, order r ->  inductive_set r ->
  inc a (substrate r) ->
  exists m, maximal_element r m & gle r a m. (* 26 *)
Lemma inductive_powerset: forall A F, sub A (powerset F) ->
  (forall S, (forall x y, inc x S -> inc y S -> sub x y \/ sub y x) ->
    sub S A ->inc (union S) A) ->
  inductive_set (inclusion_suborder A).
Lemma maximal_in_powerset: forall A F, sub A (powerset F) ->
  (forall So, (forall x y, inc x So -> inc y So -> sub x y \/ sub y x) ->
    sub So A -> inc (union So) A) ->
  exists a, maximal_element (inclusion_suborder A) a.
Lemma minimal_in_powerset: forall A F, sub A (powerset F) -> nonempty A ->
```

```
  (forall So, (forall x y, inc x So -> inc y So -> sub x y \/ sub y x) ->
    sub So A -> inc (intersection So) A) ->
  exists a, minimal_element (inclusion_suborder A) a.
```

2.5 Isomorphisms of well-ordered sets

Assume that E and F are two well-ordered sets. We show Theorem 3 [2, p. 155]: Let $\mathrm{I}(u, v, f)$ 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 $\mathrm{I}(\mathrm{E}, \mathrm{F}, f)$, or there exists a unique f such that $\mathrm{I}(\mathrm{F}, \mathrm{E}, f)$. Note: The two cases are not excluded; in that case, f is surjective.

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 $\mathfrak{F}$ of triples $(\mathrm{A}, \mathrm{B}, \mathrm{C})$ 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',
  order r -> order r' -> is_function 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))
  -> 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,
  worder r -> worder r' ->
  increasing_fun f r r' -> strict_increasing_fun g r r'->
  is_segment r' (range (graph f)) ->
  forall x, inc x (source f) -> gle r' (W x f) (W x g).  (* 31 *)
Lemma isomorphism_worder_unique: forall r r' x y,
  worder r -> worder r' ->  is_segment r' (range (graph x)) ->
  is_segment r' (range (graph y)) ->
  order_morphism x r r' -> order_morphism y r r'
  ->  x = y.
Lemma induced_order_trans: forall a b c, sub c b ->
  induced_order (induced_order a b) c = induced_order a c.
```

Given a totally ordered subset X of $\mathfrak{F}$, 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 $\mathrm{I}(\mathrm{E}, \mathrm{F}, f)$

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 $\mathfrak{F}$. 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) ->
  exists w, exists f, is_segment r w &
    order_isomorphism f (induced_order r a) (induced_order r w). (* 46 *)
```

2.6 Lexicographic products

Consider the follow definition. We assume that $(X_\iota)_{\iota\in I}$ is a family of sets, with domain I, g is a family of orderings (for each ι, g_ι is an ordering on f_ι) and r is a well-ordering in I. Denote the order relation associated to r by $\leq$, and the order relation associated to g_ι by $\leq_\iota$. The *lexicographic product* is the order associated to the relation: x and y are elements of the

product $\prod X_\iota$, and either $x = y$, or, if ι is the smallest index (for the relation $\leq$) such that $x_\iota \neq y_\iota$ then $x_\iota \leq_\iota y_\iota$.

```
Definition lexicographic_order_r (r f g:Bset): 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,   (* 67 *)
  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 *)
```

2.7 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 $(X_\iota)_{\iota\in I}$ is the union of the sets $X_\iota \times \{\iota\}$. If x is in the union, it has the form (y, λ), 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 $\leq_\iota$ on each X_ι. 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_λ. 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:Bset): 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 $\sum_{\iota\in I} X_\iota$. As is customary, this notation hides the relations $\leq$ and $\leq_\iota$. 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 disjoint_union_pr: 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 ordinal_sum2 r r' :=
  ordinal_sum (canonical_doubleton_order)
  (Lvariantc (substrate r) (substrate r'))
  (Lvariantc r r').

Lemma ordinal_sum2_axioms: forall r r', order r -> order r' ->
  ordinal_sum_axioms canonical_doubleton_order
  (Lvariantc (substrate r) (substrate r')) (Lvariantc r r').

Lemma order_ordinal_sum2: forall r r', order r -> order r' ->
  order (ordinal_sum2 r r').

Lemma substrate_ordinal_sum2: forall  r r',  order r -> order r' ->
  substrate (ordinal_sum2 r r') = canonical_du2 (substrate r) (substrate r').
```

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

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 related_ordinal_sum2_order: forall r r' x x',  order r -> order r' ->
  related (ordinal_sum2 r r') x x' =
  (inc x (canonical_du2 (substrate r) (substrate r')) &
    inc x' (canonical_du2 (substrate r) (substrate r')) &
    ((Q x = TPa & Q x' = TPa & gle r (P x) (P x'))
      \/ (Q x <> TPa & Q x' <> TPa & gle r' (P x) (P x'))
      \/ (Q x = TPa & Q x' <> TPa))).
Lemma related_ordinal_sum2_order_spec: forall r r' x x',  order r -> order r' ->
  inc x (substrate r) -> inc x' (substrate r') ->
  glt (ordinal_sum2 r r') (J x TPa) (J x' TPb).
Lemma ordinal_sum_totalorder: forall r f g,
  ordinal_sum_axioms1 r f g ->
  total_order (ordinal_sum r f g) = (total_order r &
    forall i, inc i (domain f) -> total_order (V i g)).  (* 17 *)
```

We want to show the associativity of the ordinal sum.

$$\sum_{\iota \in I} E_\iota = \sum_{\lambda \in L} \Big(\sum_{\iota \in J_\lambda} E_\iota \Big), \qquad I = \sum_{\lambda \in L} J_\lambda.$$

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

Assume that $E = \sum E_\iota$ is the sum associated to the triple (r, f, g) (where f is the family E_ι, g the family of orderings and r and ordering on the index set I). Assume $I = \sum J_\lambda$. 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, ι) with $\iota \in I$ and $x \in f(\iota)$. Since I is a disjoint union, ι is a pair, hence our element has the form

$$(*) \qquad y = (x, (\iota, \lambda)), \quad \lambda \in L, \quad \iota \in f'(\lambda), \quad x \in f(\iota, \lambda).$$

Let F_λ be the ordinal sum of the sets E_ι for $\iota \in J_\lambda$. It is the ordinal sum of $(r_\lambda, f_\lambda, g_\lambda)$, where $f_\lambda(\iota) = f((\iota, \lambda))$ and $g_\lambda(\iota) = g((\iota, \lambda))$ (composition of $\iota \mapsto (\iota, \lambda)$ and the restrictions of f and g). Moreover r_λ is the obvious ordering on J_λ, 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, λ), where $\lambda \in L$, and $x \in F(\lambda)$. This means that x has the form (y, ι) where $\iota \in J_\lambda$ and $y \in f_\lambda(\iota)$. Thus, an element in the substrate of E' has the form $((y, \iota), \lambda)$ $\lambda \in L$, $\iota \in f'(\lambda)$. Compare this with (*). This gives a natural bijection between E and E'. It is an order isomorphism since $(x, \iota, \lambda) \leq (x', \iota', \lambda')$ if and only if either $\lambda < \lambda'$ or ($\lambda = \lambda'$ and either $\iota < \iota'$ or ($\iota = \iota'$ and $x \leq x'$)).

```
Section Ordinal_assoc.
  Variables r f g r' f' g':Bset.
  Hypothesis oa_axiom : ordinal_sum_axioms r f g.
  Hypothesis oa_axiom' : ordinal_sum_axioms r' f' g'.
  Hypothesis oa_link : r = ordinal_sum r' f' g'.
Definition ordinal_sum_assoc_aux l:=
  ordinal_sum (V l g') (L (V l f') (fun i => V (J i l) f))
  (L (V l f') (fun i => V (J i l) g)).
Definition ordinal_sum_assoc :=
  ordinal_sum r'
  (L (domain f') (fun l=> disjoint_union (L (V l f') (fun i => V (J i l) f))))
  (L (domain f') (fun l=> ordinal_sum_assoc_aux l)).

Lemma ordinal_sum_assoc_aux1 :forall l,
  inc l (substrate r') ->
  ordinal_sum_axioms  (V l g') (L (V l f') (fun i => V (J i l) f))
  (L (V l f') (fun i => V (J i l) g)).
Lemma ordinal_sum_assoc_aux2 :forall l,
  inc l (domain f') -> order (ordinal_sum_assoc_aux l).
Lemma ordinal_sum_assoc_aux3 :
  ordinal_sum_axioms r'
  (L (domain f') (fun l=> disjoint_union (L (V l f') (fun i => V (J i l) f))))
  (L (domain f') (fun l=> ordinal_sum_assoc_aux l)).
Lemma ordinal_sum_assoc1:  order ordinal_sum_assoc. (* 70 *)
Lemma ordinal_sum_assoc_iso:
  order_isomorphism (BL (fun x=> J (J (P x) (P (Q x))) (Q (Q x)))
    (disjoint_union f) (substrate (ordinal_sum_assoc)))
  (ordinal_sum r f g) (ordinal_sum_assoc).  (* 70 *)
End Ordinal_assoc.
```

Chapter 3

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 $\tau_Z(\mathrm{Eq}(X, Z))$. 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 $\mathfrak{a}^{\mathfrak{b}}$ 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 $\mathfrak{P}(\mathbf{N})$ (where $\mathbf{N}$ is the set of natural integers, defined in Chapter 6). For us, the term "power" will only be used to denote $\mathfrak{a}^{\mathfrak{b}}$.

Bourbaki does not define "a cardinal". The only possible interpretation of "$\mathfrak{r}$ is a cardinal" is "the object $\mathfrak{r}$ is of the form 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 $\mathfrak{a}$ denotes the cardinal of A, it is impossible to prove $\mathfrak{a} = A$ or $\mathfrak{a} \neq A$ (non-uniqueness of τ). 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 $\mathfrak{a}.\mathfrak{a} = \mathrm{Card}(A \times A)$ is $\mathfrak{a}$ (if A is the set given above). This makes sense because $\mathrm{Card}(A \times B)$ is left unchanged when A is replaced by A' with $\mathrm{Card}(A) = \mathrm{Card}(A')$. 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 $\mathfrak{P}(I) \to C$. 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 $\mathfrak{a}.\mathfrak{b} = \mathfrak{b}.\mathfrak{a}$, valid for two cardinals, is 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 $\mathfrak{a}.1 = \mathfrak{a}$ is true only if $\mathfrak{a}$ is a cardinal. The relation $\mathfrak{a} \leq \mathfrak{a}\mathfrak{b}$ is true if $\mathfrak{b} \neq 0$; in order for $\leq$ to be antisymmetric we impose that its arguments are cardinals, so that we need $\mathfrak{a}$ to be a cardinal. Our proof uses $1 \leq \mathfrak{b}$ which is valid only if $\mathfrak{b}$ is a cardinal. Thus our theorem assumes that both arguments are cardinals. This is a case where assumptions are not minimal.

3.1 The cardinal of a set

We denote by Eq(X, Y) the property that there is a bijection between X and Y. This is *equipotent* in Coq. We know that this relation is reflexive, symmetric and transitive (but is not an equivalence, because it has no graph). Singletons are equipotent, as well as sets with two distinct elements.

```
Lemma singletons_equipotent: forall x y,
  equipotent (singleton x) (singleton y).
Lemma doubleton_equipotent: forall x y x' y',
  let f:= corresp (doubleton x x') (doubleton y y')
    (doubleton (J x y) (J x' y')) in
    x <> x' -> y <> y' ->
    (bijective f & source f = doubleton x x' & target f = doubleton y y' &
      W x f = y & W x' f = y').  (* 26 *)
Lemma doubleton_equipotent1: forall x y x' y',
  x <> x' -> y <> y' -> equipotent (doubleton x x')(doubleton y y').
```

Products of equipotent sets are equipotent. We first consider the case of *productb* since we have theorems that say that *ext_prod_map* from $\prod E_\iota$ to $\prod F_\iota$ is injective or surjective (See Part I, section 6.7). We also consider the case of the product of two sets (the bijection is *ext_to_prodC*).

```
Lemma equipotent_productf:  forall In p1 p2,
  (forall i, inc i In -> equipotent (p1 i) (p2 i)) ->
   equipotent (productf In p1)(productf In p2).
Lemma equipotent_productb:  forall x y, fgraph x -> fgraph y ->
  domain x = domain y ->
  (forall i, inc i (domain x) -> equipotent (V i x) (V i y)) ->
  equipotent (productb x) (productb y).
Lemma equipotent_product: forall a b a' b',
  equipotent a a' -> equipotent b b' ->
  equipotent (product a b) (product a' b').
```

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.

```
Lemma equipotent_product_sym: forall a b,
  equipotent (product a b)(product b a).
Lemma product2associative : forall a b c,
  equipotent (product a (product b c)) (product (product a b) c).
Lemma distrib_inter_prod2: forall a b c,
  product (union2 a b) c = union2 (product a c) (product b c).
Lemma distrib_inter_prod3: forall a b c,
  product c (union2 a b) = union2 (product c a) (product c b).
Lemma equipotent_a_times_singl: forall a b,
  equipotent a  (product a (singleton b)).
```

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, inc u a -> inc u b -> False) -> disjoint a b.
Lemma disjoint_union2_pr0: forall a b x y,
  disjoint x y -> disjoint (product a x) (product b y).
Lemma disjoint_union2_pr1: forall x y,
  x <> y -> disjoint (singleton x) (singleton y).
Lemma disjoint_union2_pr: forall a b x y,
  x <> y -> disjoint (product a (singleton x)) (product b (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_ι is a function from X_ι into Y_ι, 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_ι (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 ι such that $x \in X_\iota$ and $y \in X_\iota$, hence $f_\iota(x) = f_\iota(y)$. Thus f is injective if each f_ι is injective.

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

```
Lemma equipotent_disjoint_union: forall X Y,
  fgraph X -> fgraph Y ->  domain X = domain Y ->
  (forall i, inc i (domain X) -> equipotent (V i X) (V i Y)) ->
  mutually_disjoint X ->  mutually_disjoint Y ->
  equipotent (unionb X) (unionb Y).  (* 38 *)
Lemma equipotent_disjoint_union1: forall X Y,
  fgraph X -> fgraph Y ->  domain X = domain Y ->
  (forall i, inc i (domain X) -> equipotent (V i X) (V i Y)) ->
  equipotent (disjoint_union X) (disjoint_union  Y).
```

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 $(X_\iota)_{\iota \in I}$ such that such that $A = X_\alpha$ and $B = X_\beta$. This family is *Lvariant*. We shall denote it by $X_{\alpha\beta}(A, B)$. We show here uniqueness of the family. We will use for J the set *two_points*, and denote the family by $X(A, B)$. If g is the function that maps α and β to *TPa* and *TPb* it is a bijection from I to J, so that very every family of two sets is, modulo a change of variables, a family on J.

```
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 ->
  range f  =  doubleton a b -> f = Lvariant x y a b.
Lemma two_terms_bij: forall a b x y f,
  x <> y -> fgraph f -> domain f = doubleton x y -> V x f = a -> V y f = b ->
  exists g, (bijective g & target g = two_points
    & source g = doubleton x y &
    f= gcompose (Lvariantc a b) (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 α and β; 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 disjoint_commutative: forall a b,
  disjoint a b -> disjoint b a.
Lemma union_of_twosets_aux1: forall a b,
  union2 a b = unionb (Lvariantc a b).
Lemma equipotent_disjoint_union2: forall a b a' b',
  disjoint a b -> disjoint a' b' -> equipotent a a' -> equipotent b b' ->
  equipotent (union2 a b) (union2 a' b').
```

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

```
Definition cardinal x := choose (fun z => equipotent x z).
Definition card_zero := cardinal emptyset.
Definition card_one := cardinal (singleton emptyset).
Definition card_two := cardinal (doubleton (singleton emptyset) emptyset).
```

Proposition 1 [2, p. 158] states that X and Y are equipotent if and only if they have the same cardinal. The cardinal of the empty set is the empty set. A nonempty set has non-zero cardinal.

```
Lemma cardinal_pr: forall x, equipotent (cardinal x) x.
Lemma cardinal_pr0: forall x, equipotent x (cardinal x).

Theorem cardinal_equipotent: forall x y,
  (cardinal x = cardinal y) = (equipotent x y).

Lemma cardinal_zero: cardinal emptyset = emptyset.
Lemma zero_is_emptyset: card_zero = emptyset.
Lemma cardinal_emptyset: cardinal emptyset = card_zero.
Lemma cardinal_nonemptyset: forall x,
  cardinal x = card_zero -> x = emptyset.
Lemma cardinal_nonemptyset1: forall x,
  nonempty x -> cardinal x <> card_zero.
Lemma cardinal_one_is_singleton: is_singleton(card_one).
```

The cardinal of a singleton is one, the cardinal of a doubleton with two distinct elements is two.

```
Lemma cardinal_singleton: forall x, cardinal(singleton x) = card_one.
Lemma cardinal_doubleton: forall x x',
  x <> x' ->  cardinal(doubleton  x x') = card_two.
```

3.2 Order relation between cardinals

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 $x \in \mathrm{E}$ implies $x \prec x$, there exists a well-ordering, denoted by $\leq$, whose substrate is E, such that $x \leq y$ is equivalent to "$x \in \mathrm{E}$ and $y \in \mathrm{E}$ and $x \prec y$."

```
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 related_graph_on1: forall r x a b,
  related  (graph_on r x) a b = (inc a x & inc b x & r a b).
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 $\mathfrak{r}$ is a *cardinal* if it is of the form Card(y). We say that $\mathfrak{r} \leq_{\text{Card}} \mathfrak{n}$ if $\mathfrak{r}$ and $\mathfrak{n}$ are cardinals, and $\mathfrak{r}$ is equipotent to a subset of $\mathfrak{n}$. The notation is often simplified to $\mathfrak{r} \leq \mathfrak{n}$. We also introduce the notation $\mathfrak{r} >_{\text{Card}} \mathfrak{n}$

```
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, Card(x) is a cardinal. Then A is equipotent to a subset of B if and only if there is an injection from A into B. Since the composition of two injections is an injection, and bijections are injections, we get some interesting results. For instance 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). Thus A $\leq$ B if and only if Card(A) $\leq$ Card(B). If $\mathfrak{a}$ is a cardinal, then Card($\mathfrak{a}$) = $\mathfrak{a}$ and $\mathfrak{a} \leq \mathfrak{a}$. We have Card(Card(A)) = Card(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 inj_compose1: forall f f',
  injective f-> injective f' -> source f' = target f ->
  injective (compose f' f).
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_le 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).
```

We show here that 0, 1 and 2 are cardinals.

```
Lemma cardinal0: is_cardinal card_zero.
Lemma cardinal1: is_cardinal card_one.
Lemma cardinal2: is_cardinal card_two.
```

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 ϕ 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 $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{c}$, are cardinals, then $\mathfrak{a} \leq_{\text{Card}} \mathfrak{b}$ and $\mathfrak{b} \leq_{\text{Card}} \mathfrak{c}$ implies $\mathfrak{a} \leq_{\text{Card}} \mathfrak{c}$ (this is easy). Either $\mathfrak{a} \leq_{\text{Card}} \mathfrak{b}$ or $\mathfrak{b} \leq_{\text{Card}} \mathfrak{a}$; but if both relations hold, then $\mathfrak{a} = \mathfrak{b}$. 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.

```
Lemma cardinal_antisymmetry1: forall x y,
  cardinal_le x y -> cardinal_le y x -> x = y.
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.
Lemma cardinal_le_total_order1: forall a b,
  is_cardinal a -> is_cardinal b ->
  a = b \/ cardinal_lt a b \/ cardinal_lt b a.
Lemma cardinal_le_total_order2: forall a b,
  is_cardinal a -> is_cardinal b ->
  cardinal_le a b \/ cardinal_lt b a.
```

We have $0 \leq \mathfrak{a}$ for every cardinal $\mathfrak{a}$, and $1 \leq \mathfrak{a}$ if moreover $\mathfrak{a} \neq 0$.

```
Lemma zero_smallest: forall x, is_cardinal x -> cardinal_le card_zero x.
Lemma zero_smallest1: forall x, cardinal_lt x card_zero -> False.
Lemma one_small_cardinal: forall x, is_cardinal x -> x <> card_zero ->
  cardinal_le card_one x.
Lemma one_small_cardinal1: forall x, cardinal_lt card_zero x ->
   cardinal_le card_one x.
```

For every cardinal $\mathfrak{a}$, the set of objects of the form $\text{Card}(b)$ for $b \in \mathfrak{P}(\mathfrak{a})$ is the set of cardinals $\leq \mathfrak{a}$. Given a family of cardinals $(\mathfrak{a}_\iota)_{\iota \in I}$, we can find a cardinal $\mathfrak{b}$ greater than all $\mathfrak{a}_\iota$ (for

instance the union) and consider the set E of cardinals $\leq \mathfrak{b}$. The family, being bounded in a well-ordered set, has a supremum $\mathfrak{c}$. If $\mathfrak{d}$ is another upper bound, either $\mathfrak{d} \geq \mathfrak{b}$ hence $\mathfrak{d} \geq \mathfrak{c}$, or $\mathfrak{d} \leq \mathfrak{b}$, hence is in E and $\mathfrak{d} \geq \mathfrak{c}$. 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 Card(Y) ≤ Card(X) if there is a surjection of X onto Y.

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

3.3 Operations on cardinals

Given a family of cardinals $(\mathfrak{a}_\iota)_{\iota\in I}$, the cardinal of the sum of these sets is called the *cardinal sum* and denoted by $\sum_{\iota\in I}\mathfrak{a}_\iota$; the cardinal of the product is called the *cardinal product* and denoted $\mathsf{P}_{\iota\in I}\mathfrak{a}_\iota$. The standard notation is $\prod_{\iota\in I}\mathfrak{a}_\iota$ and will be used in the next chapter. The qualificative "cardinal" will also be omitted in "cardinal sum" and "cardinal product". . Bourbaki introduces a new notation (for this chapter only), in order to avoid ambiguities. 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 $\mathrm{Card}(E_\iota)$ is the cardinal of the sum or the product of the sets E_ι. In other terms, if $\mathfrak{a}_\iota = \mathrm{Card}(E_\iota)$ then $\mathrm{Card}(\prod E_\iota) = \mathsf{P}\mathfrak{a}_\iota$ and $\mathrm{Card}(\mathsf{S}E_\iota) = \sum \mathfrak{a}_\iota$. 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)))).
```

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

$$\sum_{\kappa\in K}\mathfrak{a}_{f(\kappa)}=\sum_{\iota\in I}\mathfrak{a}_\iota,\qquad \mathop{\mathsf{P}}_{\kappa\in K}\mathfrak{a}_{f(\kappa)}=\mathop{\mathsf{P}}_{\iota\in I}\mathfrak{a}_\iota.$$

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

$$\sum_{\iota\in I}\mathfrak{a}_\iota=\sum_{\lambda\in L}\Big(\sum_{\iota\in J_\lambda}\mathfrak{a}_\iota\Big),\qquad \mathop{\mathsf{P}}_{\iota\in I}\mathfrak{a}_\iota=\mathop{\mathsf{P}}_{\lambda\in L}\Big(\mathop{\mathsf{P}}_{\iota\in J_\lambda}\mathfrak{a}_\iota\Big).$$

Let $((\mathfrak{a}_{\lambda,\iota})_{\iota\in J_\lambda})_{\lambda\in L}$ be a family of families of cardinals. Let $I=\prod J_\lambda$. Distributivity of product over sum is

$$\mathop{\mathsf{P}}_{\lambda\in L}\Big(\sum_{\iota\in J_\lambda}\mathfrak{a}_{\lambda,\iota}\Big)=\sum_{f\in I}\Big(\mathop{\mathsf{P}}_{\lambda\in L}\mathfrak{a}_{\lambda,f(\lambda)}\Big).$$

Note that we do not need $\mathfrak{a}_\iota$ 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 the families are disjoint.

```
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 *)
  fgraph f ->
  (forall l, inc l (domain f) -> fgraph (V l f)) ->
  cardinal_prod (L (domain f) (fun l => cardinal_sum (V l f))) =
  cardinal_sum (L (productf (domain f) (fun l => (domain (V l f))))
    (fun g => (cardinal_prod (L (domain f) (fun l => V (V l g) (V l f)))))).
```

Given two sets $\mathfrak{a}$ and $\mathfrak{b}$, we can consider a family of two elements whose range is the doubleton $\{\mathfrak{a},\mathfrak{b}\}$ (for instance $X_{xy}(\mathfrak{a},\mathfrak{b})$, see page 59). The cardinal product of this family is the cardinal of the product, it is denoted by $\mathfrak{a}\mathfrak{b}$ or $\mathfrak{a}.\mathfrak{b}$. The cardinal sum of the family is the cardinal of the disjoint union, namely $\mathfrak{a}\times\{x\}\cup\mathfrak{b}\times\{y\}$. We shall sometimes denote this as $\mathfrak{a}_x\cup\mathfrak{b}_y$. The cardinal sum of this family is independent of the pair (x,y) by commutativity. It will be denoted by $\mathfrak{a}+\mathfrak{b}$. 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 card_plus a b :=
  cardinal_sum (Lvariantc a b).
Definition card_mult a b :=
  cardinal_prod (Lvariantc a b).
Definition doubleton_fam f a b :=
  exists x, exists y, x<>y & fgraph f &  domain f = doubleton x y &
    V x f = a &   V y f = b.

Lemma card_plus_is_cardinal: forall a b, is_cardinal (card_plus a b).
Lemma card_mult_is_cardinal: forall a b, is_cardinal (card_mult a b).

Lemma card_mult_pr1:forall a b,
  card_mult a b = cardinal (product a b).

Lemma card_plus_pr: forall a b f,
  doubleton_fam f a b ->  card_plus a b = cardinal_sum f.
Lemma card_mult_pr: forall a b f,
  doubleton_fam f a b ->  card_mult a b = cardinal_prod f.

Lemma disjoint_union2_pr3: forall a b  x y, y <> x ->
  equipotent (card_plus a b)
    (union2 (product a (singleton x)) (product b (singleton y))).
Lemma disjoint_union2_pr4: forall a b,
  equipotent (card_plus a b)
   (union2 (product a (singleton TPa)) (product b (singleton TPb))).
Lemma card_plus_pr1: forall a b a' b',
  disjoint a b -> equipotent a a' -> equipotent b b' ->
  cardinal (union2 a b) = card_plus a' b'.
Lemma cardinal_sum_pr2: forall a b a' b', equipotent a a' -> equipotent b b' ->
  card_plus a b = card_plus a' b'.
Lemma card_mult_pr2: forall a b a' b',
  cardinal a = cardinal a' -> cardinal b = cardinal b' ->
  card_mult a b = card_mult a' b'.

Lemma doubleton_fam_canon: forall (f:EE),
  doubleton_fam (L two_points f) (f TPa) (f TPb).
Lemma card_commutative_aux: forall a b,
  doubleton_fam (Lvariantc b a) 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).
```

The proof of the associativity of the sum needs three distinct sets. We may chose 0, 1 and 2.

```
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.
```

As a corollary, if $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$ are cardinals we have

(1) $$\mathfrak{a}+\mathfrak{b}=\mathfrak{b}+\mathfrak{a} \quad \text{and} \quad \mathfrak{a}\mathfrak{b}=\mathfrak{b}\mathfrak{a},$$

(2) $$\mathfrak{a}+(\mathfrak{b}+\mathfrak{c})=(\mathfrak{a}+\mathfrak{b})+\mathfrak{c} \quad \text{and} \quad \mathfrak{a}(\mathfrak{b}\mathfrak{c})=(\mathfrak{a}\mathfrak{b})\mathfrak{c},$$

(3) $$\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{a}\mathfrak{b}+\mathfrak{a}\mathfrak{c}.$$

Note that the formulas are true even if $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$ are not cardinals. In the case of (1), we use $\mathrm{X}_{xy}(a,b) = \mathrm{X}_{yx}(b,a)$. Associativity of the product is a consequence of equipotency of $\mathrm{A}\times(\mathrm{B}\times\mathrm{C})$ and $(\mathrm{A}\times\mathrm{B})\times\mathrm{C}$. In the case of a sum, the situation is a bit more complicated. Using the same notations as before, $\mathfrak{a}(\mathfrak{b}+\mathfrak{c})$ is equipotent to $\mathfrak{a}_i \cup (\mathfrak{b}_j \cup \mathfrak{c}_k)_l)$. Using distributivity of the product and union, it is equipotent to $\mathfrak{a}_i \cup \mathfrak{b}_{jl} \cup \mathfrak{c}_{kl}$. One can replace double indices by single ones, and this is equipotent to $\mathfrak{a}_i \cup \mathfrak{b}_j \cup \mathfrak{c}_k$. The same idea can be used for (3). The quantity $\mathfrak{a}(\mathfrak{b}+\mathfrak{c})$ is equipotent to $\mathfrak{a}\times(\mathfrak{b}_i \cup \mathfrak{c}_j)$ hence to $(\mathfrak{a}\times\mathfrak{b}_i)\cup(\mathfrak{a}\times\mathfrak{c}_j)$, and $(\mathfrak{a}\times\mathfrak{b})_i \cup (\mathfrak{a}\times\mathfrak{c})_j$, by associativity of the product. We show in fact $(\mathfrak{b}+\mathfrak{c})\mathfrak{a} = \mathfrak{b}\mathfrak{a}+\mathfrak{c}\mathfrak{a}$, because, basically we use equipotency of $(\mathrm{A}\cup\mathrm{B})\times\mathrm{C}$ and $(\mathrm{A}\times\mathrm{C})\cup(\mathrm{B}\times\mathrm{C})$. We have $\mathfrak{a}\sum_\iota \mathfrak{b}_\iota = \sum_\iota \mathfrak{a}\mathfrak{b}_\iota$. We use the same techniques as above (rather the use general distributivity).

```
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, (* 75 *)
  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)))).
```

3.4 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_card_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 $0_i = \emptyset$ (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 one_unit_prodr: forall a, is_cardinal a ->
  card_mult a card_one = a.
Lemma one_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 $\mathfrak{a}$ and $\mathfrak{b}$ be two cardinals; consider a set I equipotent to $\mathfrak{b}$ and the two families $\mathfrak{a}_\iota = \mathfrak{a}$ and $\mathfrak{c}_\iota = 1$. Then

$$\mathfrak{a}\mathfrak{b} = \sum_{\iota\in I} \mathfrak{a}_\iota; \qquad \mathfrak{b} = \sum_{\iota\in I} \mathfrak{c}_\iota.$$

The first formula is obtained from the second after multiplication by $\mathfrak{a}$, 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 $\mathfrak{a}$ and $\mathfrak{b}$ are two cardinals such that $\mathfrak{a}+1 = \mathfrak{b}+1$ then $\mathfrak{a} = \mathfrak{b}$. In effect, there exists X equipotent to $\mathfrak{a}$, Y equipotent to $\mathfrak{b}$, 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 $\mathfrak{c} = \mathrm{Card}(Z)$ we have $\mathfrak{a} = \mathfrak{b} = \mathfrak{c}+1$.

```
Lemma disjoint_with_singleton: forall a b,
  ~ (inc b a) -> disjoint a (singleton b).
Theorem zero_cardinal_product: forall f,
  fgraph f ->  (forall i, inc i (domain f) -> V i f <> card_zero) =
```

```
  (cardinal_prod f <> card_zero).
Lemma zero_cardinal_product2: forall a b, a <> card_zero  -> b <> card_zero ->
  card_mult a b <> card_zero.
Theorem succ_injective: forall a b, is_cardinal a ->
  is_cardinal b -> card_plus a card_one = card_plus b card_one ->
  a = b.    (* 73 *)
```

3.5 Exponentiation of cardinals

If $\mathfrak{a}$ and $\mathfrak{b}$ are two cardinals, the cardinal of the set of functions from $\mathfrak{b}$ to $\mathfrak{a}$ is denoted $\mathfrak{a}^{\mathfrak{b}}$, by abuse of notations[1]. Proposition 9 [2, p. 163] says that we can replace $\mathfrak{a}$ and $\mathfrak{b}$ by equipotent sets.

```
Definition card_pow a b := cardinal (set_of_functions b a).
Lemma card_pow_pr: forall a b a' b',
  equipotent a a' -> equipotent b b' ->
  card_pow a b = card_pow a' b'.
Theorem card_pow_pr1: forall x y,
  cardinal (set_of_functions y x) = card_pow (cardinal x) (cardinal y).
```

Proposition 10 [2, p. 163] says that if $\mathfrak{a}$ and $\mathfrak{b}$ are two cardinals, I is a set with cardinal $\mathfrak{b}$ and $\mathfrak{a}_\iota$ is the constant family $\mathfrak{a}$, then $\mathfrak{a}^{\mathfrak{b}} = \mathop{\mathsf{P}}_{\iota\in I} \mathfrak{a}_\iota$. 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 $\mathfrak{a}$ and $\mathfrak{b}$ to be cardinals. Note also that Card(I) = $\mathfrak{b}$ implies that $\mathfrak{b}$ is a cardinal, hence, we give also another version of the theorem.

A consequence is that, if $\mathfrak{a}$ and $\mathfrak{b}$ are cardinals, $(\mathfrak{a}_\iota)_{\iota\in I}$ and $(\mathfrak{b}_\iota)_{\iota\in I}$ are families of cardinals we have

$$\mathfrak{a}^{\sum_{\iota\in I}\mathfrak{b}_\iota} = \mathop{\mathsf{P}}_{\iota\in I} \mathfrak{a}^{\mathfrak{b}_\iota}, \qquad \Big(\mathop{\mathsf{P}}_{\iota\in I} \mathfrak{a}_\iota\Big)^{\mathfrak{b}} = \mathop{\mathsf{P}}_{\iota\in I} \mathfrak{a}_\iota^{\mathfrak{b}}.$$

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 $\mathfrak{a}_\iota = \mathfrak{a}$. We have $\mathfrak{a}^{\sum_{\iota\in I}\mathfrak{b}_\iota} = \mathop{\mathsf{P}}_{J} \mathfrak{a}_\iota$, where J is any set whose cardinal is $\sum_{\iota\in I}\mathfrak{b}_\iota$; we chose the disjoint union of the sets $\mathfrak{b}_\iota$. We have a natural partition of J and we can apply the associativity of the product. For the second formula, let $\mathfrak{a}_{\iota\beta} = \mathfrak{a}_\iota$ for $\iota \in I$ and $\beta \in \mathfrak{b}$. This is a family defined on the product $I \times \mathfrak{b}$, for which we have have two natural partitions (all elements with the same ι, or all elements with the same β); we can apply associativity of the product twice. We also have

$$\mathfrak{a}^{\mathfrak{b}+\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}}\mathfrak{a}^{\mathfrak{c}}, \qquad (\mathfrak{a}\mathfrak{b})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{c}}\mathfrak{b}^{\mathfrak{c}}, \qquad \mathfrak{a}^{\mathfrak{b}\mathfrak{c}} = (\mathfrak{a}^{\mathfrak{b}})^{\mathfrak{c}}.$$

```
Lemma card_pow_pr2: forall a b,
  cardinal_prod (cst_graph b a) = card_pow a b.
Theorem card_pow_pr3: forall a b j, cardinal j = b ->
  cardinal_prod (cst_graph j a) = card_pow a b.
Lemma power_of_sum: forall a f, fgraph f ->
  card_pow a (cardinal_sum f) =
  cardinal_prod (L (domain f) (fun i => card_pow a (V i f))).  (* 18 *)
Lemma power_of_prod: forall b f, fgraph f ->
  card_pow (cardinal_prod f) b =
```

[1] 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 120

```
  cardinal_prod (L (domain f) (fun i => card_pow (V i f) b)). (* 65 *)
Lemma power_of_sum2: forall a b c,
  card_pow a (card_plus b c) =
  card_mult (card_pow a b) (card_pow a c).
Lemma power_of_prod2: forall a b c,
  card_pow (card_mult a b) c =
  card_mult (card_pow a c) (card_pow b c).
```

Proposition 11 [2, p. 164] states $\mathfrak{a}^0 = 1$ (Bourbaki says that there is a unique function from the empty set into an another one. We use the fact that 0 is the empty sum, and rewrite $\mathfrak{a}^0$ as a product). We have $\mathfrak{a}^1 = \mathfrak{a}$ (Bourbaki says that this is a consequence of *bijective_product1_canon*, a lemma that says that E^F is equipotent to E if F has a single element; we replace the power by a product with a single factor, then simplify). One has $1^{\mathfrak{a}} = 1$ (Bourbaki says that there exists a unique function from a set into a singleton; here we rewrite 1 as an empty product, rewrite the power as an (empty) product). Finally, if $\mathfrak{a}$ is not zero, then $0^{\mathfrak{a}} = 0$ since there is no function from a non-empty set into the empty set.

```
Lemma power_x_0: forall a, card_pow a card_zero =  card_one.
Lemma power_0_0: card_pow card_zero card_zero =  card_one.
Lemma power_x_1: forall a, is_cardinal a -> card_pow a card_one = a.
Lemma power_1_x: forall a, card_pow  card_one  a = card_one.
Lemma power_0_x: forall a, a <> card_zero ->
  card_pow  card_zero  a = card_zero.
```

We have $1+1 = 2$; this can be shown by proving the the LHS is the sum of a family containing only ones, hence is the number of elements in the family; the family has two elements; all sets with two distinct elements are equipotent. A consequence is $\mathfrak{a}^2 = \mathfrak{a}.\mathfrak{a}$.

```
Lemma equipotent2_two_points: equipotent card_two two_points.
Lemma card_two_pr: card_two = card_plus card_one card_one.
Lemma power_x_2: forall a, is_cardinal a ->
   card_pow a card_two = card_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: forall X,
  cardinal (powerset X) = card_pow card_two X. (* 80 *)
```

3.6 Order relation and operations on cardinals

Proposition 13 [2, p. 164] states that $\mathfrak{a} \geq \mathfrak{b}$ if and only if there exists $\mathfrak{c}$ such that $\mathfrak{a} = \mathfrak{b} + \mathfrak{c}$ (for simplicity, we assume all three quantities to be cardinals, although $\mathfrak{c}$ could be any set, and both relations $\mathfrak{a} \geq \mathfrak{b}$ and $\mathfrak{a} = \mathfrak{b} + \mathfrak{c}$ imply that $\mathfrak{a}$ 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 $B_1 \cup C_2 \to A$, and by restriction an injection $B_1 \to A$, and by composition, an injection $B \to A$.

```
Theorem cardinal_le_when_complement: forall a b, (* 36 *)
  is_cardinal a -> is_cardinal b ->
  (cardinal_le b a) = (exists c, is_cardinal c & card_plus b c = a).
```

Proposition 14 [2, p. 165] says that is $\mathfrak{a}_\iota \geq \mathfrak{b}_\iota$ (for two families of cardinals) we have

$$\sum_{\iota\in I} \mathfrak{a}_\iota \geq \sum_{\iota\in I} \mathfrak{b}_\iota, \qquad \mathop{\mathsf{P}}_{\iota\in I} \mathfrak{a}_\iota \geq \mathop{\mathsf{P}}_{\iota\in I} \mathfrak{b}_\iota$$

The first formula is shown as follows. We have a bijection from $\mathfrak{b}_\iota$ into a subset E_ι of $\mathfrak{a}_\iota$, hence a bijection from $\mathfrak{b}_\iota \times \{\iota\}$ into a subset $E_\iota \times \{\iota\}$ of $\mathfrak{a}_\iota \times \{\iota\}$. This gives a bijection from the disjoint union $\bigcup \mathfrak{b}_\iota \times \{\iota\}$ into a subset $\bigcup E_\iota \times \{\iota\}$ of $\bigcup \mathfrak{a}_\iota \times \{\iota\}$. The proof of the second formula is similar: we get a bijection from $\prod \mathfrak{b}_\iota$ into a subset $\prod E_\iota$ of $\prod \mathfrak{a}_\iota$. 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 -> fgraph g -> domain f = domain g ->
  (forall x, inc x (domain f) -> cardinal_le (V x f) (V x g)) ->
  cardinal_le (cardinal_sum f) (cardinal_sum g).  (* 24 *)
Theorem product_increasing: forall f g,
  fgraph f -> fgraph g -> domain f = domain g ->
  (forall x, inc x (domain f) -> cardinal_le (V x f) (V x g)) ->
  cardinal_le (cardinal_prod f) (cardinal_prod g).

Lemma sum_increasing1: forall f j, fgraph f ->
  (forall x, inc x (domain f) -> is_cardinal (V x f)) ->
  sub j (domain f) -> cardinal_le (cardinal_sum (restr f j)) (cardinal_sum f).
Lemma product_increasing1: 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) ->
  sub j (domain f) -> cardinal_le (cardinal_prod (restr f j)) (cardinal_prod f).
Lemma sum_increasing2: forall a b a' b',
  cardinal_le a a' -> cardinal_le b b' ->
  cardinal_le (card_plus a b)  (card_plus a' b').
Lemma product_increasing2: forall a b a' b',
  cardinal_le a a' -> cardinal_le b b' ->
  cardinal_le (card_mult a b)  (card_mult a' b').
Lemma sum_increasing3: forall a b, is_cardinal a ->is_cardinal b ->
  cardinal_le a (card_plus a b).
Lemma product_increasing3: forall a b, is_cardinal a ->is_cardinal b ->
  b <> card_zero ->
  cardinal_le a (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 $2^{\mathfrak{a}} > \mathfrak{a}$ for every cardinal $\mathfrak{a}$, 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 4

Natural integers. Finite sets

There are two kinds of sets and cardinals: the finite ones and the infinite ones. There is a set $\mathbf{N}$ containing all finite cardinals, so that we have statements of the form: if $n \in \mathbf{N}$ then $n \neq n+1$, and no special font is required. Moreover, we think of elements of $\mathbf{N}$ 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) sequence of letters S followed by a single O. The five axioms are

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

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 $\forall a, a = \mathrm{O} + a$, 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 $a = \mathrm{O} + a$, 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 $\mathrm{X}\{u\}$ is a well-formed formula in which u occurs free. If both $\forall u : \langle \mathrm{X}\{u\} \supset \mathrm{X}\{\mathrm{S}u/u\} \rangle$ and $\mathrm{X}\{0/u\}$ are theorems, then $\forall u : \mathrm{X}\{u\}$ is also a theorem." This is built-in in Coq, under the form

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

```
  : forall P : nat -> Prop,
    P 0 -> (forall n : nat, P n -> P (S n)) -> forall n : nat, P n.
```

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

```
Lemma cardinal_c_induction_v: forall r:EP,
  (r card_zero) -> (forall n, inc n  Bnat-> r n -> r (succ n))
  ->  (forall n, inc n Bnat -> 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 of element not satisfying a property (if the set is non-empty) is not either O or Sa. This is a consequence of the fact that **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 $f_m : \mathbf{N} \to \mathrm{E}_m$, which is the unique surjective function satisfying the two axioms, show that $\mathrm{E}_m \subset \mathbf{N}$, extend the function $f'_m : \mathbf{N} \to \mathbf{N}$, then merge all these functions to get $f : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$. 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 $n \in \mathbf{N}$ 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" it is something that associates an ordinal to a pair of ordinals.

4.1 Definition of integers

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

```
Definition succ x := card_plus x card_one.
Definition is_finite_c x :=  is_cardinal x & x <> succ x.
Definition is_finite_set x := is_finite_c (cardinal x).
Definition card_three := succ card_two.
Definition card_four := succ card_three.
```

If $\mathfrak{a}$ is finite, so is $\mathfrak{a} + 1$, by injectivity of the successor function. The converse is obvious. This is Proposition 1 [2, p. 166].

```
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.
```

4.2 Inequalities between integers

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

```
Definition prec n := choose (fun m => is_finite_c m & n = succ m).

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).
Theorem le_int_is_int: forall a b, is_finite_c b ->
  cardinal_le a b -> is_finite_c a.
Lemma is_finite_in_sum: forall a b, is_cardinal b ->
  is_finite_c (card_plus a b) -> is_finite_c b.
Theorem exists_prec: forall n, is_finite_c n -> n <> card_zero ->
  exists_unique (fun m => is_finite_c m & n = succ m).
Lemma prec_pr: forall n, is_finite_c n -> n <> card_zero ->
  (is_finite_c (prec n) &  n = succ (prec n)).
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.
```

As a corollary, every subset of a finite set is finite. If $X \subset Y$, $X \neq Y$ and Y is finite, then $\mathrm{Card}(X) < \mathrm{Card}(Y)$. Bourbaki says that the converse is true by definition. In fact, if Y is empty, it is finite, otherwise there is $x \in Y$, and if X is the complement of $\{x\}$ in Y, then $\mathrm{Card}(Y) = \mathrm{Card}(X) + 1$. The relation $\mathrm{Card}(X) < \mathrm{Card}(Y)$ implies that $\mathrm{Card}(X)$ is finite, hence $\mathrm{Card}(X) + 1$ 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 equipotent_singleton_one: forall a, equipotent (singleton a) card_one.
Lemma cardinal_succ_pr: forall a b, ~ (inc b a) ->
  cardinal (tack_on a b) = succ a.
Lemma not_inc_complement_singleton: forall a b,
  ~ (inc b (complement a (singleton b))).
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. If f is a function from E to F that are finite and equipotent, then f is injective if and only f is surjective if and only f is bijective.

```
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).
Lemma image_smaller_cardinal: forall f, is_function f ->
  cardinal_le (cardinal (image_of_fun f))(cardinal (source f)).
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_fun_image: forall a f, is_finite_set a ->
  is_finite_set  (fun_image a 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) ->
  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) -> is_finite_set (source f) ->
  surjective f -> bijective f. (* 38 *)
```

4.3 The set of natural integers

Bourbaki introduces the set **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 $x \in \mathbf{N}$ and $y \in \mathbf{N}$ we have $x+y \in \mathbf{N}$.

Remember that $\mathbb{N}$ is the set of all $\mathrm{S}^k\mathrm{O}$, i.e., the set that contains O, SO, SSO, SSSO, etc. The mapping $x \mapsto \mathrm{S}x$ 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 $\mathfrak{a}$ is an *infinite cardinal* if it is a cardinal, but not a finite cardinal, and we set that E is an *infinite set* it it is not finite, i.e., when its cardinal is infinite. If $\mathfrak{a}$ is finite and $\mathfrak{b}$ is infinite, then $\mathfrak{a} < \mathfrak{b}$ thus $\mathfrak{a} \leq \mathfrak{b}$. As a consequence, the set of all finite cardinals $\leq \mathfrak{b}$ it is the set of all finite cardinals. This gives a set $\mathbf{N}$ such that $x \in \mathbf{N} \iff x$ 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 $x \leq_{\mathbf{N}} y$ to be "$x \in \mathbf{N}$ and $y \in \mathbf{N}$ and $x \leq_{\mathrm{Card}} y$". This is a well-ordering on $\mathbf{N}$.

```
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 $x \in \mathbf{N}$.

```
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.
```

4.4 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 $a \leq n$ (respectively $a \leq n < b$) implies R($n+1$), then for all n such that $a \leq n$ (respectively $a \leq n \leq b$), 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 = ¬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_lt 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_lt n b -> r n -> r (succ n))
  ->  (forall n, cardinal_le a n  -> cardinal_le n b -> 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_lt n b -> r (succ n) -> r n)
  ->  (forall n, cardinal_le a n  -> cardinal_le n b -> r n).
```

We rewrite our induction principle with $x \in \mathbf{N}$ 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 $a \leq_{\mathbf{N}} n \leq_{\mathbf{N}} b$ then as $a \leq_{\text{Card}} n \leq_{\text{Card}} b$. The trick is that $n \leq_{\text{Card}} b$ implies $n \in \mathbf{N}$.

```
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).
```

```
Lemma cardinal_c_induction_v: forall r:EP,
  (r card_zero) -> (forall n, inc n  Bnat-> r n -> r (succ n))
  ->  (forall n, inc n Bnat -> r n).
Lemma cardinal_c_induction3_v:  forall (r:EP) a b,
  inc a Bnat -> inc b Bnat ->  r a ->
  (forall n, inc n (interval_co Bnat_order a b) -> r n -> r (succ n))
  ->  (forall n, inc n (interval_cc Bnat_order a b) -> r n).
Lemma cardinal_c_induction4_v:  forall (r:EP) a b,
  inc a Bnat -> inc b Bnat ->  r b ->
  (forall n, inc n (interval_co Bnat_order a b) -> r (succ n) -> r n)
  ->  (forall n, inc n (interval_cc Bnat_order a b) -> r n).
```

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 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 succ_nonzero1:forall n, cardinal_le card_one (succ n).
Lemma succ_nonzero:forall n, succ n <> card_zero.
Lemma prec_pr0: forall n, inc n Bnat -> prec (succ n) = n.
Lemma succ_positive: forall a, cardinal_lt card_zero (succ a).
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,
  (forall a, A (singleton a) -> B (singleton a))
  -> (forall a b, (A a -> nonempty a -> B a) ->
    nonempty a -> A(tack_on a b) -> B(tack_on a b))
  -> is_finite_set x -> A x -> nonempty x -> B x.
```

The next lemmas correspond to Exercise 4.1. If we denote by $\mathfrak{F}(E)$ the set of finite subsets of E, and by $P(E,\mathfrak{G})$ the property: (i) $\emptyset \in \mathfrak{G}$; (ii) the relation $X \in \mathfrak{G}$ and $x \in E$ imply $X \cup \{x\} \in \mathfrak{G}$, then $P(E,\mathfrak{F})$ is true; by induction, $P(E,\mathfrak{G})$ implies $\mathfrak{F} \subset \mathfrak{G}$. As a consequence, the union of two finite sets is finite. The powerset of a finite set is finite (proof by induction: $\mathfrak{P}(X \cup \{x\})$ is the union of $\mathfrak{P}(X)$ and the image of $\mathfrak{P}(X)$ by the mapping $Y \mapsto (Y \cup \{x\})$; if $x \notin X$, the union is disjoint, and the cardinal is twice the cardinal of $\mathfrak{P}(X)$).

```
Definition set_of_finite_subsets E := Zo(powerset E)(fun X => is_finite_set X).
Definition set_of_finite_subsets_prop E F:=
  inc emptyset  F & forall x X, inc x E -> inc X F -> inc (tack_on X x) F.

Lemma set_of_finite_subsets_pr: forall E,
  set_of_finite_subsets_prop E (set_of_finite_subsets E) &
  (forall F, set_of_finite_subsets_prop E F -> sub (set_of_finite_subsets E) F)
Lemma set_of_finite_subsets_pr: forall E,
  set_of_finite_subsets_prop E (set_of_finite_subsets E) &
  (forall F, set_of_finite_subsets_prop E F -> sub (set_of_finite_subsets E) F).
Lemma finite_union2: forall x y, is_finite_set x -> is_finite_set y ->
  is_finite_set (union2 x y).
Lemma finite_powerset: forall x,
  is_finite_set x -> is_finite_set (powerset x).  (* 36 *)
```

4.5 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: forall (p:EEP) E X,
  (forall a b, inc a E -> inc b E -> exists y, p (doubleton a b) y) ->
  (forall a b x y, sub a E -> inc b E -> p a x -> p (doubleton x b) y->
    p (tack_on a b) y) ->
  (forall X x, sub X E -> nonempty X -> p X x -> inc x E) ->
  nonempty X -> is_finite_set X -> sub X E -> exists x, p X x.

Lemma finite_subset_directed_bounded: forall r X,
  right_directed r ->is_finite_set X -> sub X (substrate r) -> nonempty X
  -> bounded_above r X.
Lemma finite_subset_lattice_inf: forall r X,
  lattice r ->is_finite_set X -> sub X (substrate r) -> nonempty X
  -> exists x, greatest_lower_bound r X x.
Lemma finite_subset_lattice_sup: forall r X,
  lattice r ->is_finite_set X -> sub X (substrate r) -> nonempty X
  -> exists x, least_upper_bound r X x.
Lemma finite_subset_torder_greatest: forall r X,
  total_order r ->is_finite_set X -> sub X (substrate r) -> nonempty X
  -> exists x, greatest_element (induced_order r X) x. (* 20 *)
Lemma finite_subset_torder_least: forall r X,
  total_order r ->is_finite_set X -> sub X (substrate r) -> nonempty X
  -> exists x, least_element (induced_order r X) x.
```

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.

```
Lemma finite_set_torder_greatest: forall r,
  total_order r ->is_finite_set (substrate r) -> nonempty (substrate r)
  -> exists x, greatest_element r x.
Lemma finite_set_torder_worder: forall r,
  total_order r ->is_finite_set (substrate r) -> worder r.
Lemma finite_set_maximal: forall r,
  order r ->is_finite_set (substrate r) -> nonempty (substrate r) ->
  exists x, maximal_element r x.
```

4.6 Properties of finite character

If E is a set, a property P⦃X⦄ (where X is a subset of E) is said to be of *finite character* if the set $\mathfrak{S}$ of all X satisfying P is of finite character; this means $X \in \mathfrak{S}$ if and only if every finite subset Y of X satisfies $Y \in \mathfrak{S}$. Example: the set of totally ordered subsets of an ordered set. Theorem 1 [2, p. 171] states: Every set $\mathfrak{S}$ 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 $X \in \mathfrak{S}$, then $\emptyset$ is a finite subset of X; hence $\emptyset \in \mathfrak{S}$. But the empty set is of finite character.

```
Definition of_finite_character s:=
  forall x, (inc x s) = (forall y, (sub y x & is_finite_set y) -> inc y s).

Lemma of_finite_character_example: forall r, order r ->
  of_finite_character(Zo (powerset (substrate r)) (fun z =>
    total_order (induced_order r z))).
Lemma maximal_inclusion: forall s, of_finite_character s -> nonempty s ->
  exists x, maximal_element (inclusion_suborder s) x.
```

4.7 Finite cardinals and the type nat

4.7.1 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 "$x \in E$ and $y \in E$ and ($x = y$ 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 $y \in x$. 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 $x \subset X$. 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 transitive_set X:= forall x, inc x X -> sub x X.
Definition pseudo_ordinal X:= forall Y, sub Y X -> transitive_set Y ->
  Y <> X -> inc Y X.
Definition decent_set x := forall y, inc y x -> ~ (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 transitive_tack_on_itself: forall y,
  transitive_set y -> transitive_set (tack_on y y).
Lemma transitive_union: forall x, (forall y, inc y x -> transitive_set y)
  -> transitive_set (union x).
Lemma transitive_intersection: forall x, (forall y, inc y x -> transitive_set y)
  -> nonempty x -> transitive_set (intersection x).
Lemma pseudo_ordinal_transitive1: forall x,
  pseudo_ordinal x -> (transitive_set x & decent_set x). (* 17*)
Lemma pseudo_ordinal_transitive: forall x,
  pseudo_ordinal x -> transitive_set x.
Lemma pseudo_ordinal_tack_on: forall x,
  pseudo_ordinal x ->  pseudo_ordinal (tack_on x x).
Lemma pseudo_ordinal_emptyset:  pseudo_ordinal emptyset.
Lemma pseudo_not_inc_itself: forall x, pseudo_ordinal x -> ~(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 pseudo_ordinal_dichotomy : forall x y,
  pseudo_ordinal x -> pseudo_ordinal y ->
  (inc x y \/ inc y x \/ x = y).
Lemma pseudo_ordinal_pr: forall x, transitive_set x ->
  (forall y, inc y x -> pseudo_ordinal y) ->
  pseudo_ordinal x.
Lemma pseudo_ordinal_empty: pseudo_ordinal emptyset.
Lemma inc_pseudo_pseudo: forall x y, pseudo_ordinal x -> inc y x ->
  pseudo_ordinal y.
Lemma intersection_of_pseudo_ordinals: forall x, nonempty x ->
  (forall a, inc a x -> pseudo_ordinal a) -> inc (intersection x) x.
Lemma worder_sub_ordinal: forall x, pseudo_ordinal x ->
  worder (inclusion_suborder x).
```

The conclusion of Exercise 20 is: for every ordinal α there exists a unique pseudo-ordinal E_α such that $\mathrm{Ord}(E_\alpha) = \alpha$. Exercise 2.13 defines $\mathrm{Is}(\Gamma, \Gamma')$ as the property that Γ and Γ' are two orderings and there is an isomorphism between the two orderings (compare with $\mathrm{Eq}(E, E')$, that says that there a bijection between the two set), and $\mathrm{Ord}(\Gamma)$ to be $\tau_\Delta(\mathrm{Is}(\Gamma, \Delta))$ (compare with $\mathrm{Card}(E)$). 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 $a \in$ X and $b \in$ X then $a \subset b$ is equivalent to $f(a) \subset f(b)$. Since a, b, $f(a)$ and $f(b)$ are pseudo ordinals, $a \in b$ is equivalent to $f(a) \in f(b)$. Let A be the subset of X formed of all a such that $f(a) \neq a$. If A is not empty, it has a smallest element b (because X is well-ordered). If $c \in b$, then $c \subset b$ and $c \neq b$, hence $c \notin$ A and $f(c) = c$. On the other hand, if $u \in f(b)$, then $u \in$ Y by transitivity of Y, so that $u = f(v)$ for some $v \in$ X. From $f(v) \in f(b)$ we deduce $v \in b$, hence $v = f((v) = u\ f(b) \subset b$. Since $f(b)$ is a pseudo-ordinal distinct from b we deduce $f(b) \in b$, hence $f(f(b)) = f(b)$ hence $f(b) = b$ by injectivity, absurd. Thus A is empty, and $f(a) = a$ for all $a \in$ X. This implies X $\subset$ Y; by surjectivity we have X = Y.

Let $p(f, x)$ be the set $f\langle x\rangle$, namely the set of all $f(y)$ for $y \in x$. Assume that $\leq$ 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 $x \in$ E, we have $f(x) = f\langle]\leftarrow, x[\rangle$, where $]\leftarrow, x[$ is the set of all b such that $b < x$. From the definition we get $f(a) \in f(b)$ if $a < b$ and $f(a) \subset f(b)$ if $a \leq b$. Assume $f(a) \in f(a)$; every $w \in f(a)$ is of the form $f(v)$ for $v < a$; if $w = f(a)$, we find $v < a$ such that $f(v) \in f(v)$. The set of all a such that $f(a) \in f(a)$ 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 $x \in f(a)$, then $x = f(b)$ for some $b < a$, thus $f(b) \subset f(a)$ 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 $\in$ Y, then Z $\in$ X by transitivity of X; by definition of Y we have Y $\subset$ Z, absurd. Thus Y $\subset$ 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).
```

4.7.2 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, $a \in$ B means $a = \mathscr{R}b$ for some b of type B (where $\mathscr{R}$ denotes *Ro*). This is an abstract construction. If we define a type A with two constructors B and C, then $\mathscr{R}$B $\in$ A and $\mathscr{R}$C $\in$ A. We assume $\mathscr{R}$ injective; since B $\neq$ C by construction, the set A has two distinct elements $\mathscr{R}$B and $\mathscr{R}$C. The only property of $\mathscr{R}$B is that it is one of the two elements of A. A property of the form $\mathscr{R}$B = $\emptyset$ 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 $\mathrm{S}x$ 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 $\mathbf{N}$, the set of finite cardinals. It satisfies the principle of induction (see section 4.4), and functions can be defined by induction (Chapter six, section 6.2), as a variant of definition by transfinite induction of the well-ordered set $\mathbf{N}$. In the next section, we shall show that $\mathbb{N}$ and $\mathbf{N}$ 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 $\mathrm{S}n$ is of type $\mathbb{N}$ whenever n is of type $\mathbb{N}$, we can define a function s such that $s(a) \in \mathbf{N}$ whenever $a \in \mathbb{N}$: if $a \in \mathbb{N}$ and $a = \mathscr{R}(b)$ then $s(a) = \mathscr{R}(\mathrm{S}(b))$. As noted above, a property of the form $\mathscr{R}\mathrm{O} = \emptyset$ is undecidable. Although the exact value of $s(\mathscr{R}\mathrm{O})$ 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 $\mathrm{S}x$ is never O and $\mathrm{S}x = \mathrm{S}y$ 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 $\mathbf{0}$, $\mathbf{1}$ and $\mathbf{2}$ for the cardinals (note that $\mathbf{0} = \emptyset$).

Let's define by induction a function f by $f(\mathbf{0}) = \mathscr{R}\mathrm{O}$ and $f(n+\mathbf{1}) = \mathscr{R}(\mathrm{S}(\mathscr{B}(f(n)))$ where $a = \mathscr{B}(f(n))$ is defined by $\mathscr{R}a = f(n)$. For instance $f(\mathbf{1}) = \mathscr{R}(1)$. The property "$f$ is the identity function" (more precisely $f = \mathscr{R}$) 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 $\mathbf{N}$ and $\mathbb{N}$. Given that $\emptyset = f(\mathbf{0}) = \mathscr{R}0 = \mathscr{R}\mathrm{O}$, we may assume $\mathscr{R}\mathrm{O} = \emptyset$. The relation $f(\mathbf{1}) = \mathscr{R}(1)$ suggest that $\mathscr{R}(1)$ should be $\mathbf{1}$, 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 $\mathscr{R}(\mathrm{SO}) = \{\emptyset\}$ as axiom. As a consequence $\mathscr{R}(\mathrm{SO})$ is unlikely to be a cardinal, but it will allow us to construct a function card, such that $\mathrm{card}(x) = 1$ whenever x is a singleton, i.e., whenever $\mathrm{Card}(x) = \mathbf{1}$. The two axioms relating $\mathscr{R}$, S and O have been introduced by Carlos Simpson in the following way:

```
(*
   Axiom nat_realization_O : forall x : Bset, ~ inc x (Ro 0).
   Axiom nat_realization_S :
          forall (n : nat) (x : Bset),
          inc x (Ro (S n)) = (inc x (Ro n) \/ x = Ro n).
   Lemma nat_zero_emptyset : 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 $\mathscr{R}0$ that contains no element, hence is the emptyset. The second axioms defines $\mathscr{R}(\mathrm{S}n)$, that is equal (by extensionality) to $\mathrm{T}(\mathscr{R}n)$. Thus, we define *natR* denoted by $\mathscr{R}_{\mathbb{N}}$, via $\mathscr{R}_{\mathbb{N}}0 = \emptyset$ and $\mathscr{R}_{\mathbb{N}}(\mathrm{S}n) = \mathrm{T}(\mathscr{R}_{\mathbb{N}}n)$.

```
Fixpoint natR (n:nat) :=
  match n with 0 =>  emptyset
             | S p => tack_on (natR p) (natR p)
  end.
```

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*

$$\emptyset, \quad \{\emptyset\}, \quad \{\emptyset,\{\emptyset\}\}, \quad \{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\}.$$

```
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
  natR 3 = tripleton (doubleton (singleton emptyset) emptyset)
  (singleton emptyset) emptyset.
```

If a is a pseudo-ordinal, then so is $\mathrm{T}(a)$. By induction, we deduce that if n is of type *nat*, $\mathscr{R}_{\mathbb{N}} n$ 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 *nat* by the properties: $\forall x, x \leq x$ and $\forall xy,\ x \leq y \implies x \leq \mathrm{S}(y)$. 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 $\mathrm{S}x \leq y$, is equivalent to $x \leq y$ and $x \neq y$.

It is clear by induction that if $x \leq y$ then $\mathscr{R}_{\mathbb{N}} x \subset \mathscr{R}_{\mathbb{N}} y$. If $x < y$ then $\mathscr{R}_{\mathbb{N}}(\mathrm{S}x) \subset \mathscr{R}_{\mathbb{N}} y$ hence $\mathscr{R}_{\mathbb{N}} x \in \mathscr{R}_{\mathbb{N}} y$. If $\mathscr{R}_{\mathbb{N}} x \subset \mathscr{R}_{\mathbb{N}} y$, then $x \leq y$, for otherwise we would have $y < x$, hence $\mathscr{R}_{\mathbb{N}} y \in \mathscr{R}_{\mathbb{N}} x$, hence $\mathscr{R}_{\mathbb{N}} x \in \mathscr{R}_{\mathbb{N}} x$, absurd. In the same fashion, $x < y$ is equivalent to $\mathscr{R}_{\mathbb{N}}(\mathrm{S}x) \subset \mathscr{R}_{\mathbb{N}} y$. Note that, if $\mathscr{R}_{\mathbb{N}} i = \mathscr{R}_{\mathbb{N}} j$, then $\mathscr{R}_{\mathbb{N}} i \subset \mathscr{R}_{\mathbb{N}} j$ and $\mathscr{R}_{\mathbb{N}} j \subset \mathscr{R} i$, this $i \leq j$ and $j \leq i$; hence $i = j$. This shows injectivity of $\mathscr{R}_{\mathbb{N}}$.

```
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 Rnat_sub_le : forall i j,  sub (natR i) (natR j) = (i <= 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 $\mathrm{Card}(\mathscr{R}_{\mathbb{N}} i) <_{\mathrm{Card}} \mathrm{Card}(\mathscr{R}_{\mathbb{N}} j)$, and if $\mathrm{Card}(\mathscr{R}_{\mathbb{N}} i) = \mathrm{Card}(\mathscr{R}_{\mathbb{N}} j)$, then $i = j$. From this, we deduce that each finite cardinal is of the form $\mathrm{Card}(\mathscr{R}_{\mathbb{N}}(i))$ 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 define here a new variant of the axiom of choice: *choosenat p*, or $\mathscr{C}_{\mathbb{N}}(p)$, will be a natural number satisfying p, or zero otherwise.

```
Definition refined_prnat (p:nat -> Prop) u :=
  (ex p -> p u)  &  ~(ex p) -> u = 0.
Lemma exists_refined_prnat : forall p , exists u, (refined_prnat p u).
Definition choosenat p := chooseT (refined_prnat p)  (nonemptyT_intro 0).
Lemma choosenat_pr : forall p, (ex p) -> p (choosenat p).
```

We can now introduce a function card(n) making the following diagram commutative

(Finite cardinals)

$$\begin{tikzcd} \mathrm{Set} \arrow[r, "\mathrm{Card}"] \arrow[d, "\mathrm{card}"] & \mathbf{N} \\ \mathbb{N} \arrow[r, "\mathscr{R}_{\mathbb{N}}"'] & \mathrm{Set} \arrow[u, "\mathrm{Card}"'] \end{tikzcd}$$

In this diagram, $\mathbb{N}$, Set and $\mathbf{N}$ are types; $\mathbb{N}$ is the set of natural numbers (as a Coq type), and $\mathbf{N}$ 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 $\mathbf{N}$ 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 card(x) to be 0, in this case the diagram does not commute. If however n is finite we have $\mathrm{Card}(\mathscr{R}_{\mathbb{N}}(\mathrm{card}(n))) = \mathrm{Card}(n)$. By uniqueness, we have $\mathrm{card}(\mathscr{R}_{\mathbb{N}}(i)) = i$ for every nat i. If A is a finite set, then Card A = Card B implies card A = card B. The converse is true if both sets are finite.

```
Definition cardinal_nat x := choosenat(fun i => cardinal (natR i) = x).
Lemma cardinal_nat_cardinal: forall x,
  cardinal_nat (cardinal x) = cardinal_nat x.
Lemma cardinal_nat_pr: forall x, is_finite_set x ->
  cardinal (natR (cardinal_nat x)) = cardinal x.
Lemma cardinal_nat_pr1: forall i, cardinal_nat(natR i) = i.
Lemma cardinal_nat_finite_eq: forall a b, is_finite_set a ->
  cardinal a = cardinal b -> cardinal_nat a = cardinal_nat b.
Lemma cardinal_nat_finite_eq1: forall a b,
  is_finite_set a -> is_finite_set b ->
  cardinal_nat a = cardinal_nat b -> cardinal a = cardinal b.
```

We have card $\mathbf{0} = 0$, card $\mathbf{1} = 1$ and card $\mathbf{2} = 2$. Note that, if s is the successor function, then $\mathbf{3} = s(\mathbf{2})$ and $3 = \mathrm{S}2$, this implies card $\mathbf{3} = 3$.

```
Lemma cardinal_nat_emptyset: cardinal_nat emptyset = 0.
Lemma cardinal_nat_singleton: forall x, cardinal_nat (singleton x) = 1.
Lemma cardinal_nat_doubleton: forall x y,
  x <> y -> cardinal_nat (doubleton x y) = 2.
Lemma cardinal_nat_zero: cardinal_nat card_zero = 0.
Lemma cardinal_nat_one: cardinal_nat card_one = 1.
Lemma cardinal_nat_two: cardinal_nat card_two = 2.
```

4.7.3 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,
  card_plus a (succ n) = succ (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 ->
  card_mult a (succ b) = card_plus (card_mult a b) a.
Lemma Bnat_stable_mult: forall a b, inc a Bnat -> inc b Bnat ->
  inc (card_mult a b) Bnat.
```

We define now by induction a function $\mathcal{N}$ that associates a cardinal to each *nat*; by construction $\mathcal{N}(0) = \mathbf{0}$ and $\mathcal{N}(\mathrm{S}n) = s(\mathcal{N}(n))$. This function converts addition and multiplication on *nat* to cardinal sum and cardinal product (induction on $\mathbb{N}$). This function is injective (because *succ* is injective). By induction on $\mathbf{N}$, this function is surjective. More precisely, every finite cardinal has the form $\mathcal{N}(n)$. Assume $a \leq b$; then $\mathcal{N}(a) \leq_{\mathrm{Card}} \mathcal{N}(b)$; 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 $\mathcal{N}(a) <_{\mathrm{Card}} \mathcal{N}(b)$ 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 $\mathrm{card}(\mathcal{N}(x)) = x$ and $\mathcal{N}(\mathrm{card}(x)) = x$.

```
Fixpoint nat_to_B (n:nat) :=
  match n with 0 => card_zero | S m => succ (nat_to_B m) end.

Lemma nat_B_0: nat_to_B 0 = card_zero.
Lemma nat_B_1: nat_to_B 1 = card_one.
Lemma nat_B_2:  nat_to_B 2 = card_two.
Lemma nat_B_S: forall n, nat_to_B (S n) = succ (nat_to_B n).
Lemma inc_nat_to_B: forall n, inc (nat_to_B n) Bnat.
Lemma nat_B_plus: forall a b,
  nat_to_B (a+b) = card_plus (nat_to_B a) (nat_to_B b).
Lemma nat_B_mult: forall a b,
  nat_to_B (a*b) = card_mult (nat_to_B a) (nat_to_B b).

Lemma nat_B_inj: forall a b,
  nat_to_B a = nat_to_B b -> a = b.
Lemma nat_to_B_surjective: forall n, inc n Bnat -> exists m,
  nat_to_B m = n.
Lemma nat_B_le: forall a b,
  (a<= b) =  cardinal_le (nat_to_B a) (nat_to_B b).
Lemma nat_B_lt: forall a b,
  (a< b) =  cardinal_lt (nat_to_B a) (nat_to_B b).
Lemma nat_B_lt: forall a b,
  (a< b) =  cardinal_lt (nat_to_B a) (nat_to_B b).
Lemma nat_B_lt0: forall b,
  (0<b) = cardinal_lt card_zero (nat_to_B b).
Lemma nat_to_B_pr: forall n, inc n Bnat ->
  nat_to_B (cardinal_nat n) = n.
Lemma nat_to_B_pr1: forall n,
  cardinal_nat(nat_to_B n) = n.
```

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 5

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 $x \in \mathbf{N}$. Sometimes, we shall use $x \in \mathbb{N}$ or $x : \mathbb{N}$, where $\mathbf{N}$ is the set of finite cardinals and $\mathbb{N}$ is the type *nat*. The function $\mathcal{N}$ is the natural bijection between $\mathbb{N}$ and $\mathbf{N}$.

5.1 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 $\mathrm{F}(x_1, x_2, \ldots, x_n) = g(x_1, \mathrm{F}(x_2, \ldots, x_n))$. This formula allows us to prove properties by induction on the length n of the sequence (for $n \geq 2$). We may have $\mathrm{F}(x) = x$, 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 5.4.

We show that a finite sum $\sum_{i \in \mathrm{I}} x_i$ of integers is an integer, by considering $f(\mathrm{J}) = \sum_{i \in \mathrm{J}} x_i$. The proof is by induction on the cardinal of J. If $\mathrm{J} = \mathrm{J}' \cup \{j\}$, and $j \notin \mathrm{J}'$, we have a partition of J, with index set $\mathrm{K} = \{1, 2\}$, and we can apply the associativity formula. It says $f(\mathrm{J}) = \sum_{k \in \mathrm{K}} y_k$. 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 $y_1 = f(\mathrm{J}')$ 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 domain_restr: forall f a,
  fgraph  f ->  sub a (domain f) -> domain (restr f a) = a.
Lemma double_restr: forall f a b, fgraph f ->
  sub  (tack_on a b) (domain f) ->
  (restr (restr f (tack_on a b)) a) = (restr f a).
Lemma double_restrb: forall f a b, fgraph f ->
  sub  (tack_on a b) (domain f) ->
  (restr (restr f (tack_on a b)) (singleton b)) = (restr f (singleton b)).
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 $\mathfrak{a}_i$ with sum S and product P we have $\mathfrak{a}_i \leq \mathrm{S}$ and $\mathfrak{a}_i \leq \mathrm{P}$, 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 $i \in \mathrm{I} \mapsto x_i$ where I is finite and each x_i is finite. We may rewrite this as $x_i \in \mathbf{N}$.

```
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 $(a_i)_{i\in\mathrm{I}}$ is a finite family of integers, then $\sum_{i\in\mathrm{I}} a_i$ and $\prod_{i\in\mathrm{I}} a_i$ are integers. As a consequence, if $\mathrm{J} \subset \mathrm{I}$ then $\sum_{i\in\mathrm{J}} a_i$ and $\prod_{i\in\mathrm{J}} a_i$ are integers. As explained above, we first show the result for all J, by induction on the cardinal, then consider the special case $\mathrm{J} = \mathrm{I}$.

```
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 Card(E) ≤ S, so that card(E) is finite. However Card(E) ≤ 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: forall 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: forall 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: forall b, is_finite_c b -> is_finite_set b.
Lemma Bnat_stable_pow: forall a b, inc a Bnat -> inc b Bnat ->
  inc (card_pow a b) Bnat.
Lemma finite_powerset: forall a, is_finite_set a -> is_finite_set (powerset a).
```

5.2 Strict inequalities between integers

We start this section with a list of some definitions and theorems, extracted from the Coq library. Consider for instance *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 *nat*), one of A or B is true. This is summarized by the notation {A} + {B} (certified disjoint union). The *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 *if zerop n then 0 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.

```
(*
  Definition zerop n : {n = 0} + {0 < n}.
  Definition lt_eq_lt_dec n m : {n < m} + {n = m} + {m < n}.
  Definition gt_eq_gt_dec n m : {m > n} + {n = m} + {n > m}.
  Definition le_lt_dec n m : {n <= m} + {m < n}.
  Definition le_le_S_dec n m : {n <= m} + {S m <= n}.
  Definition le_ge_dec n m : {n <= m} + {n >= m}.
  Definition le_gt_dec n m : {n <= m} + {n > m}.
  Definition le_lt_eq_dec n m : n <= m -> {n < m} + {n = m}.

Definition heavyside n := match (zerop n) with left _ => 0 | right _ => 1 end.

  Theorem dec_le : forall n m, decidable (n <= m).
  Theorem dec_lt : forall n m, decidable (n < m).
  Theorem dec_gt : forall n m, decidable (n > m).
  Theorem dec_ge : forall n m, decidable (n >= m).
  Theorem not_eq : forall n m, n <> m -> n < m \/ m < n.
  Theorem not_le : forall n m, ~ n <= m -> n > m.
  Theorem not_gt : forall n m, ~ n > m -> n <= m.
```

```
  Theorem not_ge : forall n m, ~ n >= m -> n < m.
  Theorem not_lt : forall n m, ~ n < m -> n >= 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 $b = \mathrm{S}b'$ and $a \leq b'$. As a consequence $b' = a + c'$, and $b = \mathrm{S}b' = \mathrm{S}(a + c') = a + \mathrm{S}c'$. The first relation says that c' is an integer, so that $\mathrm{S}c'$ is an integer; it is obviously > 0. Conversely, from $a \leq a$ we get $a < \mathrm{S}a$, 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 *nat*.

```
Theorem lt_to_plus: forall a b:nat, a<b = exists c:nat, 0<c & c+a=b.
Theorem cardinal_lt_pr: forall a b, inc a Bnat -> inc b Bnat ->
  (cardinal_lt a b = exists c, is_finite_c c & cardinal_lt card_zero c &
    b =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

  Lemma plus_reg_l : forall n m p, p + n = p + m -> n = m.
  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 plus_le_compat_l : forall n m p, n <= m -> p + n <= p + m.
  Lemma plus_le_compat_r : forall n m p, n <= m -> n + p <= m + p.
  Lemma le_plus_l : forall n m, n <= n + m.
  Lemma le_plus_r : forall n m, m <= n + m.
  Theorem le_plus_trans : forall n m p, n <= m -> n <= m + p.
  Theorem lt_plus_trans : forall n m p, n < m -> n < m + p.
  Lemma plus_lt_compat_l : forall n m p, n < m -> p + n < p + m.
  Lemma plus_lt_compat_r : forall n m p, n < m -> n + p < m + p.
  Lemma plus_le_compat : forall n m p q, n <= m -> p <= q -> n + p <= m + q.
  Lemma plus_le_lt_compat : forall n m p q, n <= m -> p < q -> n + p < m + q.
  Lemma plus_lt_le_compat : forall n m p q, n < m -> p <= q -> n + p < m + q.
  Lemma plus_lt_compat : forall n m p q, n < m -> p < q -> n + p < m + q.

  Lemma mult_O_le : forall n m, m = 0 \/ n <= m * n.
  Lemma mult_le_compat_l : forall n m p, n <= m -> p * n <= p * m.
  Lemma mult_le_compat_r : forall n m p, n <= m -> n * p <= m * p.
  Lemma mult_le_compat :
    forall n m p (q:nat), n <= m -> p <= q -> n * p <= m * q.
  Lemma mult_S_lt_compat_l : forall n m p, m < p -> S n * m < S n * p.
  Lemma mult_lt_compat_r : forall n m p, n < m -> 0 < p -> n * p < m * p.
  Lemma mult_S_le_reg_l : forall n m p, S n * m <= S n * p -> m <= p.
*)

Lemma mult_lt_le_compat : forall n m p q,
  0<q -> n < m -> p <= q -> n * p < m * q.
Lemma mult_le_lt_compat : forall n m p q,
  0< m -> n <= m -> p < q -> n * p < m * q.

Lemma zero_lt_one: cardinal_lt card_zero card_one.
Lemma zero_lt_oneN: 0 < 1.
```

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 $\mathrm{J} \cup \{j\}$ of I. We have $\sum_{i\in\mathrm{I}} a_i = \mathrm{A} + a_j$, where $\mathrm{A} = \sum_{i\in\mathrm{J}} a_i$ (we use the same argument as when showing that the sum is finite). In the same way, $\sum_{i\in\mathrm{I}} b_i = \mathrm{B} + b_j$, and $\mathrm{A} \leq \mathrm{B}$. 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_lt (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_lt a a' ->
  cardinal_lt (card_plus a b) (card_plus a' b).
Lemma not_card_le_lt: forall a b, cardinal_le a b -> cardinal_lt b a -> False.
Lemma lt_n_succ_le: forall a b, inc a Bnat -> inc b Bnat ->
   cardinal_lt a b = cardinal_le (succ 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,  (* 14 *)
  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,  (* 18 *)
  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)) ->
  (forall i, inc i (domain f) -> cardinal_lt card_zero (V i g)) ->
  cardinal_lt (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 $a^b < a^b a^x$. If $b > 1$ we get $a < b^a$.

```
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 *pow* on the type *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_0N:  0 ^ 0 = 1.
Lemma power_x_1N: 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 power_1_xN: forall a,  1 ^ a = 1.
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 finite_power_lt2N: forall a b b',
  b < b' -> 1 < a ->  a^ b < a ^ b'.
```

If $a+b=a+b'$ or if $ab=ab'$ then $b=b'$ (all arguments are integers; $a \neq 0$ in the case of a product).

```
Lemma plus_simplifiable_left: forall a b b',
 inc a  Bnat -> inc b Bnat -> inc b' Bnat ->
  card_plus a b = card_plus a b' -> b = b'.
Lemma plus_simplifiable_right: forall a b b',
 inc a  Bnat -> inc b Bnat -> inc b' Bnat ->
  is_finite_c a ->  is_finite_c b -> is_finite_c b' ->
  card_plus b a = card_plus b' a -> b = b'.
Lemma mult_simplifiable_left: forall a b b',
  inc a  Bnat -> inc b Bnat -> inc b' Bnat -> a <> card_zero ->
  card_mult a b = card_mult a b' -> b = b'.
Lemma mult_simplifiable_right: forall a b b',
  inc a  Bnat -> inc b Bnat -> inc b' Bnat -> a <> card_zero ->
  card_mult b a = card_mult b' a -> b = b'.

Lemma plus_simplifiable_leftN: forall a b b':nat,
  a + b = a + b' -> b = b'.
Lemma plus_simplifiable_rightN: forall a b b':nat,
  b + a = b' + a -> b = b'.
Lemma mult_simplifiable_leftN: forall a b b':nat,
  0 <>a -> a * b = a * b' -> b = b'.
Lemma mult_simplifiable_rightN: forall a b b',
  0 <>a -> b * a = b' * a -> b = b'.
```

If a and b are integers and $a \leq b$ there is a unique integer c such that $b = a + c$, it is called the difference, and denoted by $b - a$. There is a Coq function, denoted by *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 $\mathbf{N}$, 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 $\mathrm{P}(a - b) = a - \mathrm{S}\,b$. If $b \leq a$, then $a - b \leq a$. 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, m <= n -> S (n - m) = S n - m.
   Lemma le_plus_minus : forall n m, n <= m -> m = n + (m - n).
   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.
   Lemma lt_O_minus_lt : forall n m, 0 < n - m -> m < n.
   Theorem not_le_minus_O : 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).
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
  -> prec a = card_sub a card_one.
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 -> prec (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) a).
Lemma double_sub: forall n p, Bnat_le p n ->
  card_sub n (card_sub n p) = p.
Lemma double_subN: forall n p, p <= n -> n - (n- p) = p.
Lemma succ_le_lt: forall a b, inc a Bnat -> is_cardinal b ->
  cardinal_le (succ b) a -> (inc b Bnat & cardinal_lt b a).
```

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.
Lemma zero_smallest2: forall a, cardinal_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

$x = ab$, then $x = x + b$. As a consequence b is integer, and we can simplify by x in $x + 0 = x + b$, thus $b = 0$.

```
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-> a <> card_zero ->
  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-> a <> card_zero ->
  cardinal_lt (card_mult a b)  (card_mult a c) ->  cardinal_lt 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.
```

5.3 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 $\leq_{\mathrm{Card}}$. As a consequence, all isomorphisms are strictly increasing.

We use here a different approach. If $a \in \mathbf{N}$ and $b \in \mathbf{N}$, we can consider $[a, b]$ as an interval for the ordering $\leq_{\mathbf{N}}$ on $\mathbf{N}$ (ordered by $\leq_{\mathbf{N}}$). 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_Bnato 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 $a \leq_{\mathbf{N}} x$ and $x \leq_{\mathbf{N}} b$, where $x \leq_{\mathbf{N}} b$ is the same as $x \in \mathbf{N}$, and $b \in \mathrm{N}n$ and $x \leq b$. Note that $x \leq b$ implies $x \in \mathbf{N}$. Thus we state: $x \in [0, a[$ if and only if $x < a$ and $x \in [0, a]$ if and only if $x \leq a$. These two intervals are subsets of $\mathbf{N}$. We have $[0, a + 1[= [0, \mathrm{A}]$.

```
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,
```

```
  sub (interval_Bnat a b) Bnat.
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_Bnat a b) &
    inc y (interval_Bnat 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 $\mathbf{N}$). 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).
```

```
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 $z \mapsto z+b$, $(z \in [0,a], z+b \in [a,a+b])$, that has $z \mapsto z-b$ 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 ->
  (bijective (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 $\mathbf{N}$ we have $n+1 \leq \mathrm{Card}(\mathbf{N})$, so that $\mathrm{Card}(\mathbf{N})$ 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 $n \geq 1$, 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 (prec a)) = a.
Lemma interval_co_0a_pr: forall a x, inc a Bnat -> a <> card_zero ->
  inc x (interval_Bnat card_zero (prec 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 (prec 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: forall r, total_order r ->
  is_finite_set (substrate r) ->
  exists_unique (fun f => order_isomorphism f r
    (interval_Bnatco  (cardinal (substrate r)))).
```

5.4 Finite sequences

A *finite sequence* is a family $(x_i)_{i \in \mathrm{I}}$ 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 $k \in [1, n]$. It is called the *kth term of the sequence*. If $k = 1$ or $k = n$, it is called the first or last term.

If $\mathrm{P}\{\!\{i\}\!\}$ is equivalent to $i \in \mathrm{I}$, where I is a finite set of integers, then $(x_i)_{i\in\mathrm{I}}$ may be written as $(x_i)_{\mathrm{P}\{\!\{i\}\!\}}$. In fact, such a notation can be used whatever I. As an example one can see $(t_i)_{a\le i\le b}$. 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 $\mathbb{N} \times \mathrm{A}$) 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.
```

5.4.1 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 reverse order: $g(n-1)$ is the head of the list. On the diagram below, the mapping $g \mapsto \mathrm{L}$ is denoted by *fl*. Given a list L of length n, we define a function g that returns the k-th element of the list (in fact, the element in position $n-k-1$, since the list is in reverse order). This construction could be generalized to any type; we must provide a default value for $k \ge n$; we consider only integers and sets, with default values $g(k) = 0$ or $g(k) = \emptyset$. The mapping $\mathrm{L} \mapsto g$ is denoted by *lf* on the diagram below. The composition of these two functions is the identity.

```
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.

Fixpoint fct_to_list (A:Type) (f: nat->A)(n:nat): list A :=
  match n with 0 => nil
    | S m => (f m) ::(fct_to_list f m) end.
Definition list_to_fct (a: list nat) :=
  fun n => nth (length a -n -1) a 0.
Definition list_to_fctB (a: list Bset) :=
  fun n => nth (length a -n -1) a emptyset.
```

```
Lemma fct_to_list_length :   forall A (f:nat->A) n,
  length (fct_to_list f n) = n.
Lemma list_to_fct_pr0: forall a l2 l1,
  list_to_fct (l1 ++ a :: l2)  (length l2) = a.
Lemma list_to_fct_pr0B: forall a l2 l1,
  list_to_fctB (l1 ++ a :: l2)  (length l2) = a.
Lemma list_to_fct_pr: forall (A:Type) (f:nat->A) (u:A) n i,
  i<n -> nth (n-i-1) (fct_to_list f n) u = f i.
Lemma list_to_fct_pr1: forall f n i,
  i<n -> list_to_fct (fct_to_list f n) i = f i.
Lemma list_to_fct_pr1B: forall f n i,
  i<n -> list_to_fctB (fct_to_list f n) i = f i.
Lemma list_to_fct_pr3: forall l2 l1,
  fct_to_list (list_to_fct (l1++l2)) (length l2) = l2.
Lemma list_to_fct_pr4: forall l,
  fct_to_list (list_to_fct l) (length l) = l.
Lemma list_to_fct_pr3B: forall l2 l1,
  fct_to_list (list_to_fctB (l1++l2)) (length l2) = l2.
Lemma list_to_fct_pr4B: forall l,
  fct_to_list (list_to_fctB l) (length l) = l.
```

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 $\mathrm{L}' = a :: \mathrm{L}$, if the associated functions are g and g', then $g'(n) = a$, and g and g' agree on $[0, n-1]$.

```
Lemma fct_to_list_unique: forall (A:Type) (f g: nat-> A) n,
  (forall i, i< n -> f i = g i) -> fct_to_list f n = fct_to_list g n.

Lemma app_nth3 : forall A (a:A),
  forall l' d n, n >= 1 -> nth n (a::l') d = nth (n-1) l' d.
Lemma list_to_fct_cons0: forall a l,
  list_to_fct (a :: l)  (length l) = a.
Lemma list_to_fct_cons1: forall a l2 n, n< length l2 ->
  list_to_fct (a :: l2) n = list_to_fct l2 n.

Lemma list_to_fct_consB0: forall a l,
  list_to_fctB (a :: l)  (length l) = a.
```

Given a list L of elements of $\mathbb{N}$, of length n, if $g = lf(\mathrm{L})$, we construct a function $\mathrm{G} : [0, n[\to \mathbf{N}$ via $g(\mathrm{card}\, i) = \mathrm{card}(\mathrm{G}(i))$. The mapping $\mathrm{L} \mapsto \mathrm{G}$ will be denoted by LF on the diagram below. Similarly, given a list L of sets, we construct $\mathrm{G} : [0, n[\to \mathrm{E}$ via $g(\mathrm{card}\, i) = \mathrm{G}(i)$. This is well-defined if all elements of the list belong to the set E.

```
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 Bset) E:=
  BL (fun n => (list_to_fctB l (cardinal_nat n)))
  (interval_co_0a  (nat_to_B (length l))) E.

Lemma axioms_list_to_f: forall (l: list nat),
  transf_axioms (fun n =>(Ro (nat_to_B (list_to_fct l (cardinal_nat n)))))
  (interval_co_0a (nat_to_B (length l))) Bnat.
Lemma function_list_to_f: forall (l: list nat),
  is_function (list_to_f l).
```

```
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)

$$\begin{tikzcd}
\text{Lists} \arrow[dr, "\mathrm{LF}"] \arrow[d, bend right, "lf"'] & \\
\mathbb{N} \to \mathbb{N} \arrow[u, bend right, "fl"'] & \mathscr{F}(\mathrm{I}, \mathbf{N}) \arrow[l, "\mathrm{BN}"']
\end{tikzcd}$$

Given a function $[0, n[\to \mathbf{N}$, we can construct a function $\mathbb{N} \to \mathbb{N}$, by extending the function with zero, and using the natural isomorphism between $\mathbb{N}$ and $\mathbf{N}$. It will be denoted by *BN* on the diagram. The composition $fl \circ BN$ is the inverse of *LF*.

```
Definition back_to_nat f n:=
  cardinal_nat (Yo (inc (nat_to_B n) (source f))
    (W (nat_to_B n) f) card_zero).

Lemma back_to_nat_pr: forall f n, inc  (nat_to_B n) (source f) ->
  back_to_nat f n =  cardinal_nat (W  (nat_to_B n) f).
Lemma back_to_nat_pr1: forall f n k,
  source f = (interval_co_0a (nat_to_B k)) ->
  n < k -> back_to_nat f n =  cardinal_nat (W (nat_to_B n) f).
Lemma back_to_nat_pr2: forall (l: list nat) n,
  n < (length l) -> back_to_nat (list_to_f l) n = list_to_fct l n.

Lemma list_to_f_pr1: forall f n, is_function f -> target f = Bnat ->
  source f = (interval_co_0a (nat_to_B n)) ->
  f = list_to_f (fct_to_list (back_to_nat f) n).
Lemma list_to_f_pr2: forall l,
  fct_to_list (back_to_nat (list_to_f l)) (length l) = l.
```

Given a list L and a predicate P, we define P(L) to be true if every element of the list satisfies P. Given a predicate with two arguments, we say that the list satisfies the predicate whenever $\mathrm{P}(a, b)$ is true if a comes before b. This means that, if f is the function associated to the list, then $i < j$ implies $\mathrm{P}(f(i), f(j))$.

```
Fixpoint single_list_prop (A:Type) (L: list A) (q: A->Prop) :=
  match L with nil => True | a :: b => q a /\ single_list_prop b q end.

Lemma single_list_prop1: forall A (q: A->Prop),  single_list_prop nil q.
```

```
Lemma single_list_prop2: forall A a b (q: A->Prop),
  q a -> (single_list_prop b q) = (single_list_prop (a::b) q).
Lemma single_list_prop3: forall A a b (q: A->Prop),
  ~ (q a) -> ~(single_list_prop (a::b) q).

Lemma single_list_prop_app: forall A a b (q: A->Prop),
  (single_list_prop a q) -> (single_list_prop b q)
  -> (single_list_prop (a++b) q).

Lemma single_list_prop_refine: forall A L (p q: A->Prop),
  (forall a, p a -> q a) ->  (single_list_prop L p) ->
  (single_list_prop L q).
Lemma simple_list_prop_nth: forall  A (q: A->Prop) L u n,
  single_list_prop L q -> n < length L ->
  q (nth n L u).
Fixpoint double_list_prop (A:Type) (L: list A) (q: A->A->Prop) :=
  match L with nil => True
      | a :: b => single_list_prop b (q a) /\ double_list_prop b q
end.
```

The contraction $\mathrm{C}_{fv}(\mathrm{L})$ of a list L is inductively defined by $\mathrm{C}_{fv}(a :: \mathrm{L}) = f(a, \mathrm{C}_{fv}(\mathrm{L}))$, 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 $r(\mathrm{L})$. We write $\mathrm{L} \subset \mathrm{E}$ if $\mathrm{P}_{\mathrm{E}}(\mathrm{L})$ holds, where $\mathrm{P}_{\mathrm{E}}(x)$ is $x \in \mathrm{E}$; 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 := single_list_prop L (fun x => inc x E).
```

The range of a list is the smallest set E such that $\mathrm{L} \subset \mathrm{E}$. We show $\mathrm{L} \subset r(\mathrm{L})$ by induction. We have $r(\mathrm{L}) \subset r(a :: \mathrm{L})$. We then use the fact that if P implies Q, then P(L) implies Q(L), where P is $x \in r(\mathrm{L})$ and Q is $x \in r(a :: \mathrm{L})$. We can now state: if $\mathrm{L} \subset \mathrm{E}$ is a list of length n, there is an associated function $[0, n[\rightarrow \mathrm{E}$.

```
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 source_list_to_fB:   forall l E,
  source (list_to_fB l E) = (interval_co_0a (nat_to_B (length l))).
Lemma target_list_to_fB: forall l E,
  target (list_to_fB l E) = E.
Lemma W_list_to_fB: forall l E n, list_subset l E ->
  inc n (interval_co_0a (nat_to_B (length l))) ->
  W n (list_to_fB l E) = list_to_fctB l (cardinal_nat n).
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))).
```

If L is a list of size n, and $\mathrm{L}' = a :: \mathrm{L}$, if the associated functions are G and G′, then $\mathrm{G}'(n) = a$, and G and G′ agree on $[0, n-1]$. This is because the same result holds for g and g'. But here we can be more precise: G′ is the function obtained from G by adding the relation $\mathrm{G}'(n) = a$. We have two variants, depending on whether we have lists of integers or lists of sets.

```
Lemma list_to_f_cons0: forall a l,
  W (nat_to_B  (length l)) (list_to_f (a :: l)) = (nat_to_B a).
Lemma list_to_f_cons1: forall a l n, n< length l ->
  W (nat_to_B n) (list_to_f (a :: l)) =  W (nat_to_B n) (list_to_f l).

Lemma list_to_f_cons2: forall a l,
  list_to_f l = restriction_function (list_to_f (a :: l))
              (interval_co_0a (nat_to_B (length l))).
Lemma list_to_f_cons3: forall a l,
  list_to_f (a::l) =
     tack_on_f  (list_to_f l) (nat_to_B (length l))  (nat_to_B a).


Lemma list_subset_cons: forall a l E, list_subset l E -> inc a E ->
  list_subset (a::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 E,
  list_subset l E -> inc a E ->
  list_to_fB l E = restriction_function (list_to_fB (a :: l) E)
              (interval_co_0a (nat_to_B (length l))).
Lemma list_to_f_consB3: forall a l E,
  list_subset l E -> inc a E ->
  list_to_fB (a::l)  E= tack_on_f  (list_to_fB l E) (nat_to_B (length l))  a.
```

5.4.2 Contracting lists

We show here the following. Assume that $f(n)$ is a cardinal for all n. Let $\mathrm{F}(n)$ be the cardinal sum of the family $i \mapsto f(i)$ on $[0, n-1]$. Then $\mathrm{F}(n+1) = f(n) + \mathrm{F}(n)$, and there is a similar relation for the product. The same formula holds if $\mathrm{F}(n+1)$ is the cardinal sum of the graph of the function f and $\mathrm{F}(n)$ 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(a::L)*; its restriction is *LF(L)*, and $f(n) = a$.

```
Lemma induction_on_sum: forall a f,  inc a Bnat ->
  (forall a, inc a Bnat -> is_cardinal (f a)) ->
  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: forall a f,  inc a Bnat ->
  (forall a, inc a Bnat -> is_cardinal (f a)) ->
  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: 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_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).

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 (a::l))).

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 (a::l))).
```

We define here the sum and product of a list of integers as a contraction. We shall denote this by $\Sigma(\mathrm{L})$ and $\Pi(\mathrm{L})$. We have $\Sigma(a :: b) = a + \Sigma(b)$ and $\Pi(a :: b) = a.\Pi(b)$. By induction $\mathcal{N}(\Sigma(\mathrm{L})) = \sum LF(\mathrm{L})$ and $\mathcal{N}(\Pi(\mathrm{L})) = \prod LF(\mathrm{L})$.

```
Definition list_sum l := contraction l plus 0.
Definition list_prod l := contraction 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 $\mathrm{C}_{fv}(a{+}{+}b) = f(\mathrm{C}_{fv}(a), \mathrm{C}_{fv}(b))$ 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 $\Sigma'_{n+1}(f) = f(n) + \Sigma'_n(f)$; the non-trivial one is $\Sigma'_{n+1}(f) = f(0) + \Sigma'_n(f \circ \mathrm{S})$, where $(f \circ \mathrm{S})(i) = f(i+1)$.

```
Lemma contraction_assoc: forall  (A :Type) (L1 L2: list A)
  (f: A-> A->A) (v: A),
  (forall a b c, f a (f b c) = f (f a b) c) ->
  (forall a, 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) = (f n) + (fct_sum f n).
Lemma fct_prod_rec: forall f n, fct_prod f (S n) = (f n) * (fct_prod 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 $i \mapsto f(n-i-1)$.

```
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->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*→*nat*, we construct a function $[0,n[\to \mathbf{N}$. 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 $[0,n+1[\,=[0,n]$.

```
Lemma l_to_fct: forall f n,
  BL (fun p => nat_to_B(f (cardinal_nat p))) (interval_co_0a (nat_to_B n))
  Bnat = list_to_f (fct_to_list f n).
Lemma l_to_fct1: forall f n,
  L (interval_co_0a (nat_to_B n)) (fun p => nat_to_B(f (cardinal_nat p)))
  = graph (list_to_f (fct_to_list f n)).
```

```
Lemma l_to_fct2: forall f n,
  L (interval_Bnat card_zero (nat_to_B n))
  (fun p => nat_to_B(f (cardinal_nat p)))
  = graph (list_to_f (fct_to_list f (S n))).
```

5.5 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.

```
Definition char_fun A B := BL (fun z=> Yo (inc z A) card_one card_zero)
  B (doubleton  card_one card_zero).

Lemma char_fun_axioms: forall A B,
  transf_axioms (fun z=> Yo (inc z A) card_one card_zero)
  B (doubleton  card_one card_zero).
Lemma function_char_fun: forall A B, is_function (char_fun A B).
Lemma source_char_fun:forall A B, source (char_fun A B) = B.
Lemma target_char_fun:forall A B,

Lemma W_char_fun:forall A B x,
  inc x B -> W x (char_fun A B) =  Yo (inc x A) card_one card_zero.
Lemma cardinal_W_char_fun:forall A B x,
  inc x B -> is_cardinal (W x (char_fun A B)).
Lemma W_char_fun_a:forall A B x,  sub A B -> inc x A ->
  W x (char_fun A B) = card_one.
Lemma W_char_fun_b:forall A B x,  sub A B -> inc x (complement B A) ->
  W x (char_fun A B) = card_zero.
```

Now some properties. We have $\phi_A = \phi_B$ if and only if $A = B$. The function ϕ_A (for $A \subset E$) is constant if and only if $A = E$ or $A = \emptyset$. Proposition 7 [2, p. 176] lists additional properties.

$$\phi_{E-A}(x) = 1 - \phi_A(x)$$

$$\phi_{A\cap B}(x) = \phi_A(x)\phi_B(x)$$

$$\phi_{A\cap B}(x) + \phi_{A\cup B}(x) = \phi_A(x) + \phi_B(x)$$

```
Lemma chart_fun_injective: forall A A' B, sub A B -> sub A' B ->
  (A=A') = (char_fun A B = char_fun A' B).

Lemma W_char_fun_aa:forall A x,  inc x A ->
  W x (char_fun A A) = card_one.
Lemma W_char_fun_bb:forall A x,  inc x A ->
  W x (char_fun emptyset A) = card_zero.
Lemma constant_char_fun:forall A B, sub A B ->
  (forall x y, inc x B -> inc y B -> W x (char_fun A B) = W y (char_fun A B))
  -> (A=B \/ A = emptyset).
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)).
```

5.6 Euclidean Division

Assume that $\mathrm{P}\{\!\{x\}\!\}$ 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 $\mathrm{P}(x)$ is false and $\mathrm{P}(x+1)$ is true, unless $\mathrm{P}(0)$ 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 $p(\mathrm{S}n)$ is true for some n, negating the existence of x such that $p(\mathrm{S}x)$ 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,
  (forall x, 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,
  (forall x, 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 $bq \leq a < b(q+1)$ 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 q' r 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 -> b <> card_zero ->
```

```
  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 *the integral part of the quotient of a by b*, since in the set of rational numbers $\mathbf{Q}$, there exists c such that $a = bc$, and q is the integral part of c. He reserves the term *quotient* only to the case where the remainder is zero. Moreover he says "writing a/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 $a \in \mathbf{N}$ and $b \in \mathbf{N}$", 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 $\{x : \mathbb{N} | \exists y : \mathbb{N},\ \ \mathrm{Z}\}$ 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,
      n > 0 ->
      forall m:nat, {r : nat | exists q : nat, m = q * n + r /\ 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 Nquo a b :=
  cardinal_nat (card_quo (Ro (nat_to_B a))
    (Yo (b = 0) card_one (Ro (nat_to_B b)))).
Definition Nrem a b :=
  cardinal_nat (card_rem (Ro (nat_to_B a))
```

```
    (Yo (b = 0) card_one (Ro (nat_to_B b)))).
Definition Ndivides b a:= 0 <> b & Nrem a b = 0.

Lemma Ndivision_exists: forall a b,  0 <> b ->
  (a = b* (Nquo a b) + (Nrem a b) & (Nrem a b < b)).
Lemma Ndivision_pr: forall a b q r, 0 <> b ->
  a = b* q + r -> r < b -> (q = Nquo a b & r = Nrem a b).

Lemma Ndivision_pr_q: forall a b q r, 0 <> b ->
  a = b* q + r -> r < b -> q = Nquo a b.
Lemma Ndivision_pr_r: forall a b q r, 0 <> b ->
  a = b* q + r -> r < b -> r = Nrem a b.
```

All properties true for *Nquo* and *Nrem* are true for *card_quo* and *card_rem*. For this reason, we shall only prove our theorems for the case of type *nat*.

```
Lemma nat_B_division: forall a b, 0 <> b ->
  (nat_to_B (Nquo a b) =  card_quo (nat_to_B a) (nat_to_B b) &
    nat_to_B (Nrem a b) =  card_rem (nat_to_B a) (nat_to_B b)).
Lemma nat_B_quo: forall a b, 0 <> b ->
  nat_to_B (Nquo a b) =  card_quo (nat_to_B a) (nat_to_B b).
Lemma nat_B_rem: forall a b, 0 <> b ->
  nat_to_B (Nrem a b) =  card_rem (nat_to_B a) (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 inc_quotient_bnat:forall a b, inc a Bnat-> inc b Bnat -> b <> card_zero ->
  inc (card_quo a b) Bnat.
Lemma inc_remainder_bnat:forall a b,
    inc a Bnat-> inc b Bnat -> b <> card_zero ->
    inc (card_rem a b) Bnat.

Lemma Ndivides_pr: forall a b,
  Ndivides b a -> a =  b * (Nquo a b).
Lemma Ndivides_pr1: forall a b,  0 <> b ->  Ndivides b (b *a).
Lemma Ndivides_pr2: forall a b q,  0 <> b ->
  a = b * q -> q = Nquo a b.
Lemma one_divides_all: forall a, Ndivides 1 a.
Lemma Ndivides_pr3: forall a b q,
  Ndivides b a -> q = Nquo a b -> a =  b * q.
Lemma Ndivides_pr4: forall b q, 0 <> b ->
  Nquo (b * q) b = q.
Lemma Ndivision_itself: forall a, 0 <> a ->
  (Ndivides a a & Nquo a a = 1).
Lemma Ndivides_itself: forall a, 0 <> a -> Ndivides a a.
Lemma Nquo: forall a, 0 <> a -> Nquo a a = 1.
Lemma Ndivision_of_zero: forall a, 0 <> a ->
  (Ndivides a 0 & Nquo 0 a = 0).
Lemma Ndivides_trans: forall a b a', Ndivides a a'-> Ndivides b  a
  -> Ndivides b a'.
Lemma Ndivides_trans1: forall a b a', Ndivides a a'-> Ndivides b a
  -> Nquo a' b =  (Nquo a' a) *(Nquo a b).
Lemma Ndivides_trans2: forall a b c,
  Ndivides b a-> Ndivides b (a *c).
Lemma non_zero_mult: forall a b, 0 <> a -> 0 <> b -> 0 <> (a*b).
```

```
Lemma Nquo_simplify:  forall a b c, 0 <> b -> 0 <> c ->
  Nquo (a * c) (b * c) = Nquo a b.
```

If b divides a and a', it divides the sum and the difference.

```
Lemma card_quo_simplify:  forall a b c,
  inc a Bnat -> inc b Bnat ->inc c Bnat -> b <> card_zero -> c <> card_zero
  -> card_quo (card_mult a c) (card_mult b c) = card_quo a b.
Lemma divides_and_sum:  forall a a' b,  Ndivides b a ->  Ndivides b a'
  -> (Ndivides b  (a + a') &
    Nquo  (a + a')  b =  (Nquo a b) + (Nquo a' b)).
Lemma distrib_prod2_sub: forall a b c, inc a Bnat -> inc b Bnat -> inc c Bnat
  -> cardinal_le c b ->
  card_mult a (card_sub b c) = card_sub (card_mult a b) (card_mult a c).
Lemma distrib_prod2_subN: forall a b c, c<= b->
  a * (b-c) = (a*b) - (a*c).

Lemma divides_and_difference:  forall a a' b, inc a Bnat-> inc a' Bnat ->
  inc b Bnat -> b <> card_zero -> cardinal_le  a' a ->
  Bnat_divides b a ->  Bnat_divides b a'
  -> (Bnat_divides b  (card_sub a a') &
    cardinal_le (card_quo a' b) (card_quo a b) &
    card_quo  (card_sub a a')  b = card_sub (card_quo a b) (card_quo a' b)).
```

5.7 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 $(\mathrm{J}_h)_{0\le h\le k-1}$ of intervals all identical with $[0, b-1]$; For each $r = (r_0, r_1, \ldots, r_{k-1}) \in \mathrm{E}_k$, 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

$$a = \sum_{h=0}^{k-1} r_h b^{k-h-1} \tag{1}$$

subject to the conditions $0 \le r_h \le b-1$ for $0 \le h \le k-1$ 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 $0 \le r_h$ and $0 \le h$ 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 $0 \le h \le k-1$ is equivalent to $0 \le k-h-1 \le k-1$, 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

$$a = \sum_{h=0}^{k-1} s_h b^h \tag{2}$$

subject to the conditions $0 \le s_h \le b-1$ for $0 \le h \le k-1$ and $s_{k-1} \neq 0$ is the normalization condition. We call this is LE-expansion[1] Associated to $f_k(r)$ is the function $g_k(s)$.

If $\psi(s)$ is the sequence $(s_1, \ldots, s_k)$, then

$$g_{k+1} = s_0 + b.g_k(\psi(s)) \tag{3}$$

(Bourbaki has a similar formula with f and ϕ). 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 $a = \sum_0^{\mathrm{K}-1} \mathrm{S}_h \mathrm{B}^h$, for some B, case where $k \le n\mathrm{K}$ 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 $s_0 + bg \le s_0 + bg'$ if and only if either $g = g'$ and $s_0 \le s'_0$ or $g < g'$. This condition is equivalent to $(g, s_0) \le (g', s'_0)$, where (g, s_0) is in the substrate of some lexicographic product $\mathrm{F}_k \times \mathrm{J}$ 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

$$g_{k+1} = g_k(\Psi(s)) + s_k.b^k. \tag{4}$$

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 print a number in a computer program, the drawback being that one has to compute all b^k in decreasing order). Note that $s_k b^k \le g_{k+1} < (s_k+1)b^k$. This shows that two numbers with distinct leading digits compare as their leading digits, and shows the theorem. We shall use this approach since Ψ 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, $b \ge 2$. 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 $k+1$.

```
Lemma b_power_k_large: forall a b, inc a Bnat ->  inc b Bnat ->
  cardinal_lt card_one b -> a <> card_zero -> exists k,
    inc k Bnat & cardinal_le  (card_pow b k) a
    & cardinal_lt a (card_pow b (succ k)).
```

[1] According to Wikipedia, little-endian storage means: increasing numeric significance with increasing memory addresses; big-endian is its opposite, most-significant byte first.

```
Definition is_expansion f b k :=
  inc b Bnat & inc k Bnat & cardinal_lt card_one b &
  fgraph f & domain f = interval_co_0a k &
  forall i, inc i (domain f) -> cardinal_lt (V i f) b.
  forall i, inc i (domain f) -> cardinal_lt (V i f) b.

Definition expansion_value f b :=
  cardinal_sum (L (domain f) (fun i=> card_mult (V i f) (card_pow b i))).

Lemma is_expansion_prop0: forall f b k i,
  is_expansion f b k -> (inc i (domain f)) = cardinal_lt i k.
Lemma is_expansion_prop1: forall f b k i,
  is_expansion f b k -> cardinal_lt i k -> inc (V i f) Bnat.
Lemma is_expansion_prop2: forall f b k,  is_expansion f b k ->
  finite_int_fam  (L (domain f) (fun i=> card_mult (V i f) (card_pow b i))).
Lemma is_expansion_prop3: forall f b k,  is_expansion f b k ->
  inc (expansion_value f b) Bnat.
Lemma is_expansion_prop4: forall f b k, is_cardinal k ->
  is_expansion f b (succ k) -> inc k Bnat.
Lemma is_expansion_prop5: forall f b k, is_cardinal k ->
  is_expansion f b (succ k) ->
  is_expansion (restr f (interval_co_0a k)) b k.
Lemma is_expansion_prop6: forall f b k,  is_cardinal k ->
  is_expansion f b (succ k) -> inc (V k f) Bnat.
Lemma is_expansion_prop7: forall f b k,  is_expansion f b (succ k) ->
  is_cardinal k ->
  (expansion_value f b) =
  card_plus (expansion_value (restr f (interval_co_0a k)) b)
     (card_mult (V k f) (card_pow b k)).
Lemma is_expansion_prop8: forall f b k x,
  let g:=  L (interval_co_0a (succ k)) (fun i=> Yo (i=k) x (V i f)) in
    is_expansion f b k ->
    inc x Bnat -> cardinal_lt x b ->
    (is_expansion g b (succ k) &
      expansion_value g  b = card_plus (expansion_value f b)
      (card_mult (card_pow b k) x)).  (* 18 *)
```

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 $a < b^a$, there is at least one extension.

```
Lemma is_expansion_prop9: forall f b k,  is_expansion f b k ->
  cardinal_lt (expansion_value f b)  (card_pow b k). (* 22 *)
Lemma is_expansion_prop10: forall f b k,  is_cardinal k ->
  is_expansion f b (succ k) ->
  division_prop (expansion_value f b) (card_pow b k) (V k f)
  (expansion_value (restr f (interval_co_0a k)) b).
Lemma is_expansion_unique: forall f g b k,
  is_expansion f b k -> is_expansion g b k ->
  expansion_value f b = expansion_value g b -> f = g. (* 32 *)
Lemma is_expansion_exists1: forall a b k,  inc a Bnat -> inc b Bnat ->
  cardinal_lt card_one b ->  cardinal_lt a (card_pow b k) ->
  exists f,  (is_expansion f b k & expansion_value f b = a).
Lemma is_expansion_exists: forall a b,  inc a Bnat -> inc b Bnat ->
  cardinal_lt card_one b -> exists k, exists f,
```

```
    (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 ->
  is_expansion f b (succ k) -> is_expansion g b (succ k) ->
  cardinal_lt (V k f) (V k g) ->
  cardinal_lt (expansion_value f b)  (expansion_value g b).
```

5.8 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 $\mathfrak{a}$ onto a set with cardinal $\mathfrak{b}$, and if all set $f^{-1}\langle\{x\}\rangle$ have the same cardinal $\mathfrak{c}$, then $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. Bourbaki assumes f surjective; in fact if x is in the target but not in the range, then $\mathfrak{c} = 0$, and the source is empty.

```
Theorem shepherd_principle: forall f c, is_function f ->
  (forall x, inc x (target f) -> cardinal (inv_image_by_fun f (singleton x))=c)
  -> cardinal (source f) = card_mult (cardinal (target f)) c. (* 27 *)
```

5.8.1 Iterated functions

Note: all useful results of this section have been moved to section 5.4.2. The remaining trivial results are given without comment.

```
Definition function_on_nat f :=
  fun m =>nat_to_B (f (cardinal_nat m)).

Lemma inc_function_on_nat_Bnat : forall f n,
  inc (function_on_nat f n) Bnat.
Lemma function_on_nat_pr : forall f n,
  cardinal_nat(function_on_nat f n) = f (cardinal_nat n).
Lemma function_on_nat_pr1 : forall f n,
  function_on_nat f (nat_to_B n) = nat_to_B (f n).
```

5.8.2 Factorial

Bourbaki defines the *factorial* of n, denoted by $n!$, as $\prod_{i<n}(i+1)$. If S is the successor function, this is $\Pi'_n(\mathrm{S})$, with the notations of page 104; 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).

```
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.
```

5.8.3 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 $\mathrm{A}_{nm} = n!/(n-m)!$. 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 $\mathrm{J} \subset \mathrm{I}$, 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.

```
(*
   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 $f(\mathrm{A})$ in B.

```
Lemma tack_on_nat: forall a b, is_finite_c (cardinal (tack_on a b)) ->
  ~ (inc b a) -> cardinal_nat (tack_on a b) = S (cardinal_nat a).

Lemma cardinal_complement_image: forall f, injective f ->
  is_finite_set (target f) ->
  (cardinal_le (cardinal (source f)) (cardinal (target f)) &
    cardinal (complement (target f) (image_of_fun f)) =
    card_sub (cardinal (target f)) (cardinal (source f))). (* 21 *)
```

We have $\mathrm{A}_{nm}(n-m)! = n!$. From this we deduce $\mathrm{A}_{nm}(n-m) = \mathrm{A}_{n,m+1}$.

```
Definition number_of_injections b a :=
  Nquo (factorial a) (factorial (a - b)).

Lemma number_of_injections_pr: forall a b,  b <= a ->
  (number_of_injections b a)  * (factorial (a - b))
  = factorial a.
Lemma number_of_injections_rec: forall a b,  b<a ->
  (number_of_injections b a) * (a - b) =
  number_of_injections (S b) a.
Lemma number_of_injections_base: forall a,
  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, $f \mapsto f(a)$ is a bijection from $R^{-1}\langle\{f'\}\rangle$ onto the complementary of the range of f' that has $n-m$ elements. Hence $R^{-1}\langle\{f'\}\rangle$ has $n-m$ elements; the conclusion follows from the shepherd's principle.

```
Definition set_of_injections  E F :=
  Zo (set_of_functions E F)(fun z=> injective(inv_corr_value z)).

Lemma number_of_injections_prop: forall E F n m, (* 128 *)
  cardinal E = nat_to_B n -> cardinal F = nat_to_B m -> n <= m ->
  cardinal (set_of_injections E F)  = nat_to_B(number_of_injections n m).
```

An injection from E into itself is a bijection when E is finite. Since $A_{nnn} = n!$, we deduce that $n!$ is the number of *permutations* of E.

```
Definition set_of_permutations E :=
  (Zo (set_of_functions E E)(fun z=> bijective(inv_corr_value z))).

Lemma number_of_permutations: forall E n, cardinal E = nat_to_B n ->
  cardinal (set_of_permutations E)  = nat_to_B (factorial n).
```

5.8.4 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 $(X_i)_i$ of E such that $\mathrm{Card}(X_i) = p_i$ 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 $\mathfrak{P}(\mathfrak{P}(E))$. Here we consider functions, i.e., a subset of $\mathscr{F}(I, \mathfrak{P}(E))$. 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 $B(p_i) = n!/\prod p_i$ is well defined. The quantity $B(p_1, p_2)$ is called the binomial coefficient; it satisfies $B(p+1, q) + B(p, q+1) = B(p+1, q+1)$ hence is an integer (this is Proposition 13), so that $B(p_i)$ 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 $\mathrm{Card}(E) = \sum p_i$. 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 = 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_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_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))
    (domain p) (powerset E).
Lemma number_of_partitions2: forall E p f g,
  inc g  (set_of_permutations E) ->
  (transf_axioms  (fun i  => image_by_fun (inv_corr_value g) (W i f))
    (domain p) (powerset E)).

Lemma number_of_partitions3: forall p E f g,  (* 29 *)
  finite_int_fam p -> cardinal_sum p = cardinal E ->
  partition_with_pi_elements p E f -> inc g  (set_of_permutations E) ->
  inc (corr_value (set_of_partitions_aux p E f g)) (set_of_partitions p E).
```

```
Lemma number_of_partitions4: forall p E f,
  finite_int_fam p -> cardinal_sum p = cardinal E ->
  partition_with_pi_elements p E f ->
  surjective (BL (fun g => corr_value (set_of_partitions_aux p E f g))
    (set_of_permutations E) (set_of_partitions p E)). (* 78 *)
```

This function ϕ 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 w_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 $(w_i)_i$ is an element of the product of the sets $\mathrm{Q}(f(i))$ (this is lemma 6).

Consider now the function Φ that associates to each permutation k of E the family of restrictions to $\mathrm{A}_i = f(i)$. If k leaves A_i invariant, the restriction of k to A_i is a bijection, so that, if we consider as target of Φ the product of the permutations of A_i, Φ is well-defined for $h^{-1} \circ g$, for each $g \in \phi^{-1}(\{h\})$. This is a bijection (lemma 7). The main result follows: the target of Φ has cardinal $\prod p_i!$; the source of Φ 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 p E f g h,
  finite_int_fam p -> cardinal_sum p = cardinal E ->
  partition_with_pi_elements p E f ->
  inc h (set_of_permutations E) -> inc g (set_of_permutations E) ->
  (set_of_partitions_aux p E f g = set_of_partitions_aux p E f h) =
  (forall i, inc i (domain p) -> image_by_fun (compose (inverse_fun
    (inv_corr_value h))(inv_corr_value g)) (W i f) = (W i f)). (* 43 *)

Lemma number_of_partitions6: forall p E f h,  (* 33 *)
  finite_int_fam p -> cardinal_sum p = cardinal E ->
  partition_with_pi_elements p E f ->
  inc h (set_of_permutations E) ->
  transf_axioms (fun g=> L (domain p)(fun i=> corr_value (restriction2
    (compose (inverse_fun (inv_corr_value h))(inv_corr_value g))
    (W i f) (W i f))))
  (Zo  (set_of_permutations E)
    (fun g => (set_of_partitions_aux p E f g = set_of_partitions_aux p E f h)))
  (productb (L (domain p)(fun i=> (set_of_permutations (W i f))))).
Lemma number_of_partitions7: forall p E f h, (* 148 *)
  finite_int_fam p -> cardinal_sum p = cardinal E ->
  partition_with_pi_elements p E f ->
  inc h (set_of_permutations E) ->
  bijective(BL (fun g=> L (domain p)(fun i=> corr_value (restriction2
    (compose (inverse_fun (inv_corr_value h))(inv_corr_value g))
    (W i f) (W i f))))
  (Zo  (set_of_permutations E)
    (fun g => (set_of_partitions_aux p E f g = set_of_partitions_aux p E f h)))
  (productb (L (domain p)(fun i=> (set_of_permutations (W i f)))))).
```

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)))).
```

We now restate our theorem replacing the functional graph p by a list q of integers. Note that p appears four times; so that we must (1) convert our list q into a finite family of integers, (2) relate the sum of q_i with the sum of p_i, (3) relate the product of $q_i!$ with the product of the $p_i!$ and finally (4) define the set of partitions with q_i elements.

Consider point (4). A partition with p_i elements is a function f whose graph F satisfies the property to be a partition, such that that $f(i)$ has p_i elements for each i. Given a list L and a function f, we can define $f(\mathrm{L})$ by induction; if f is the card function, we can consider a list of sets L such that $f(\mathrm{L}) = q$, and call this a list of sets of cardinal q. We can define by induction the union of the list, hence consider L as a covering of E by sets with cardinal q.

5.8.5 The binomial coefficient

We define here by induction a function, called the *binomial coefficient*, satisfying

$$\binom{n}{0} = 1, \quad \binom{0}{p+1} = 0, \qquad \binom{n+1}{p+1} = \binom{n}{p+1} + \binom{n}{p}.$$

We show here

$$\binom{n}{0} = 1, \qquad \binom{n}{1} = n, \qquad \binom{n+1}{2} = \frac{n(n+1)}{2}.$$

```
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 $(n-p)! = \mathrm{if}(p < n, n-p, 1).(n-(p+1))!$. This gives us an induction property for f, from which we deduce $f(n,p) = \mathrm{if}(p \le n, n!, 0)$.

```
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

$$\binom{n}{p} = \binom{n}{n-p} = \frac{n!}{p!(n-p)!} \text{ when } p \le n \qquad \binom{n}{p} = 0 \text{ when } p > n.$$

Moreover division is exact. Proposition 13 [2, p. 181] is the following relation, which is true by definition:

$$\binom{n+1}{p+1} = \binom{n}{p+1} + \binom{n}{p}.$$

```
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+1) (p+1))  =  (binom n (p+1)) + (binom n p).
Lemma binom_symmetric:forall n p, p <=n ->
  binom n p = binom n (n -p).
```

Consider a set E with n elements, and the set of all subsets A of E with p elements; we shall denote this by $\mathrm{Q}_p(\mathrm{E})$, or simply Q_p. If $p > n$ this set is empty. We assume here $p \le n$. If A is a subset of E with p elements, then $\mathrm{E}-\mathrm{A}$ has $n-p$ elements; these two sets form a partition of E with (p_i) elements, where the family $(p_i)_i$ is formed of p and $n-p$. We restate this as: $(\mathrm{X}_i)_i \mapsto \mathrm{X}_1$ 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 $(p_i!)_i$, which is $p!(n-p)!$. Note that $\mathrm{A} \mapsto \mathrm{E}-\mathrm{A}$ 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 $p \le n$, if $\mathrm{Card}(\mathrm{E}) = \mathcal{N}(n)$ and if d is $p!(n-p)!$, then $\mathrm{Q}_{\mathcal{N}(p)}(\mathrm{E})$ is finite, $d \neq 0$ and $n! = d \cdot \mathrm{card}(\mathrm{Q}_{\mathcal{N}(p)}(\mathrm{E}))$.

```
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 ->
  card_plus (cardinal A) (cardinal (complement E A))  = cardinal E.
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 binomial3: forall n p, 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 binomial4: forall n p E, inc n Bnat -> inc p Bnat ->cardinal_le p n ->
  cardinal E = n -> let num:= factorial n in
    let den := card_mult (factorialC p) (factorialC (card_sub n p))
      in (num = card_mult (cardinal (subsets_with_p_elements p E)) den &
        is_finite_c num & is_finite_c den & den <> card_zero &
        is_finite_set (subsets_with_p_elements p E)).
Lemma bijective_complement: forall n p E, inc n Bnat -> inc p Bnat -> (* 25 *)
  cardinal_le p n -> cardinal E = n ->
  bijective(BL (fun z => complement E z)
    (subsets_with_p_elements p E)(subsets_with_p_elements (card_sub n p) E)).

Lemma binomial5: forall n p E, p<= n -> cardinal E = nat_to_B n ->
  let num:= factorial n in
    let den := (factorial p) * (factorial (n - p)) in
      let swp := subsets_with_p_elements (nat_to_B p) E in
        (num = (cardinal_nat swp) *  den &  0 <> den  & is_finite_set swp).
```

We restate the previous result as: if $\mathrm{Q}_p(\mathrm{E})$ is the set of subsets A of E with $\mathrm{Card}\,\mathrm{A} = \mathcal{N}(p)$, then $\mathrm{Card}(\mathrm{Q}_p(\mathrm{E})) = \mathcal{N}(\binom{n}{p})$.

```
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 $\sum_p \binom{n}{p} = 2^n$ (this is Proposition 12 [2, p. 181]). The sum is over all p with $p \le n$; 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 $\sum \mathrm{Card}(\mathrm{Q}_p(\mathrm{E})) = \mathcal{N}(\sum \binom{n}{p})$. The sets $(\mathrm{Q}_p(\mathrm{E})$ 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 $p \le n$). The second proof is by induction on n. Let B_n be the function $p \mapsto \binom{n}{p}$. We have

$$(*) \qquad \sum_{p<n+1} \mathrm{B}_{n+1}(p) = \mathrm{B}_{n+1}(0) + \sum_{p<n} \mathrm{B}_{n+1}(p+1).$$

We have $\sum \mathrm{B}_{n+1}(p+1) = \sum \mathrm{B}_n(p+1) + \sum \mathrm{B}_n(p)$ 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 $\mathrm{B}_{n+1}(0) = \mathrm{B}_n(0)$).

```
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)))) =
  card_pow card_two n. (* 31 *)

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 $2n = n + n$, hence $2 + 2 = 2.2 = 4$ 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.
```

5.8.6 Number of increasing functions

Consider two finite totally ordered sets E and F. Denote by $\mathscr{S}(\mathrm{E},\mathrm{F})$ the set of strictly increasing mappings from E into F. We pretend that

$$\mathrm{Card}(\mathscr{S}(\mathrm{E},\mathrm{F})) = \binom{n}{p} \quad \text{if } \mathrm{Card}(\mathrm{E}) = p \text{ and } \mathrm{Card}(\mathrm{F}) = n.$$

The idea is that the mapping $f \mapsto \mathrm{R}(f)$ is a bijection from $\mathscr{S}(\mathrm{E},\mathrm{F})$ onto the set of subsets with p elements of F, where $\mathrm{R}(f)$ 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 $\mathrm{E} \to \mathrm{F}$. 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'))). (* 87 *)

Lemma cardinal_set_of_increasing_functions: forall r r' n p,
  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 => strict_increasing_fun (inv_corr_value z) r r')) =
  nat_to_B(binom n p).
```

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 $f(x) \in \mathrm{E}$ for $x \leq p$. Assume $f(x) \leq_{\mathrm{E}} f(x+1)$ for $x < p$. Then $f(x) \leq_{\mathrm{E}} f(y)$ whenever $x \leq y \leq p$ (we write $y = x+c$ and use induction on c). Thus, if g is a mapping $[0,p] \to \mathrm{E}$, then g is increasing (resp. strictly increasing and injective) if $g(x) \leq_{\mathrm{E}} g(x+1)$ (resp. $g(x) <_{\mathrm{E}} g(x+1)$) for $x < p$.

```
Lemma increasing_prop1 : forall p f r, inc p Bnat -> order r ->
  (forall i, cardinal_le i p -> inc (f i) (substrate r)) ->
  (forall n,  cardinal_lt n p -> gle r (f n) (f (succ n))) ->
  (forall i j, cardinal_le i j -> cardinal_le j p ->
    gle r (f i) (f j)).

Lemma strict_increasing_prop : forall p f r, inc p Bnat -> is_function f ->
  source f =  interval_co_0a (succ p) -> order r -> substrate r = target f ->
  (forall n,  cardinal_lt n p -> glt r (W n f) (W (succ n) f)) ->
  (injective f &
    strict_increasing_fun f (interval_Bnato card_zero p) r).
```

```
Lemma increasing_prop : forall p f r, inc p Bnat -> is_function f ->
  source f =  interval_co_0a (succ p) -> order r -> substrate r = target f ->
  (forall n,  cardinal_lt n p -> gle r (W n f) (W (succ n) f)) ->
  increasing_fun f (interval_Bnato card_zero p) r.
```

Assume now $f(x)$ is an integer, $f(x) < f(y)$ for $x < y < p$. Then $x \leq f(x)$ for $x < p$, by induction on x. The function $i \mapsto f(i) - i$ 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 $f(i) - i \in \mathrm{I}_{n+1}$.

```
Lemma strict_increasing_prop1: forall f p,
  inc p Bnat ->  (forall i, cardinal_lt i p -> inc (f i) Bnat)
  -> (forall i j, cardinal_lt i j -> cardinal_lt j p ->
    cardinal_lt (f i) (f j)) ->
  (forall i,  cardinal_lt i p -> cardinal_le i (f i)).

Lemma strict_increasing_prop2: forall f p,
  inc p Bnat ->  (forall i, cardinal_lt i p -> inc (f i) Bnat)
  -> (forall i j, cardinal_lt i j -> cardinal_lt j p ->
    cardinal_lt (f i) (f j)) ->
  (forall i j, cardinal_le i j -> cardinal_lt j p ->
    cardinal_le (card_sub (f i) i) (card_sub (f j) j)). (* 31 *)
Lemma strict_increasing_prop3: forall f p n,
  inc p Bnat -> inc n Bnat -> (forall i, cardinal_lt i p -> inc (f i) Bnat)
  -> (forall i j, cardinal_lt i j -> cardinal_lt j p ->
    cardinal_lt (f i) (f j)) ->
  (forall i, cardinal_lt i p -> cardinal_lt (f i) (card_plus n p)) ->
  (forall i, cardinal_lt i p -> cardinal_le (card_sub (f i) i) n).
```

Denote by $\mathscr{A}(\mathrm{E},\mathrm{F})$ the set of increasing mappings from E into F. If f is a mapping, denote by $s(f)$ the mapping $i \mapsto f(i) - i$. We have show that s is a mapping from $\mathscr{S}(\mathrm{I}_p, \mathrm{I}_{n+p})$ into $\mathscr{A}(\mathrm{I}_p, \mathrm{I}_{n+1})$. We pretend that it is a bijection. In fact, it is rather easy to show that the inverse mapping is $a(f) : i \mapsto f(i) + i$. 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

$$\mathrm{Card}(\mathscr{A}(\mathrm{I}_p, \mathrm{I}_{n+1})) = \mathrm{Card}(\mathscr{S}(\mathrm{I}_p, \mathrm{I}_{n+p})) = \binom{n+p}{p}.$$

```
Lemma cardinal_set_of_increasing_functions3: forall n p,
  let r:= interval_Bnatco (nat_to_B p) in
    let r':= interval_Bnato card_zero (nat_to_B n) in
      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) p). (169 *)
```

Consider now two finite totally ordered set E and F. We pretend

$$\mathrm{Card}(\mathscr{A}(\mathrm{E},\mathrm{F})) = \binom{n+p-1}{p} \text{ if } \mathrm{Card}(\mathrm{E}) = p \text{ and } \mathrm{Card}(\mathrm{F}) = n.$$

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 fom E into F. If $n = 0$ and $p > 0$ the binomial coefficient is zero, F is empty, and there is no function $\mathrm{E} \to \mathrm{F}$. 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 $h : \mathrm{E} \to \mathrm{F}$ 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 $\mathscr{A}(\mathrm{E},\mathrm{F})$ and $\mathscr{A}(\mathrm{I}_p,\mathrm{I}_n)$.

```
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
    (inc (corr_value res) (set_of_functions (source f) (target h)) &
      (forall x, inc x (source f) -> W x res = W (W (W x f) g) h) &
      increasing_fun res r 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 $1 \le i \le j \le n$, and the number b_n of pairs satisfying $1 \le i < j \le n$. 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

$$a_n = \frac{n(n+1)}{2} = \binom{n+1}{2}, \qquad b_n = \frac{n(n-1)}{2} = \binom{n}{2}.$$

The Bourbaki proof of these relations (Proposition 14 [2, p. 181]) is different. He notices that $a_n = b_n + n$ since $i \le j$ is equivalent to $i < j$ or $i \le j$. A subset of $[1,n]$ is of cardinal two if and only if it is a doubleton $\{i,j\}$ with $i \ne j$, 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 set_of_card_two: forall x, cardinal x = card_two  ->
  exists u, exists v, u<>v & x = doubleton u v.
Lemma cardinal_pairs_lt: forall n,
  cardinal(Zo (product Bnat Bnat)
    (fun z=> cardinal_le card_one (P z) &
      cardinal_lt (P z) (Q z) & cardinal_le (Q z) (nat_to_B n)))=
```

```
    nat_to_B (binom n 2). (* 56 *)
Lemma cardinal_pairs_le: forall n,
  cardinal(Zo (product Bnat Bnat)
    (fun z=> cardinal_le card_one (P z) &
      cardinal_le (P z) (Q z) & cardinal_le (Q z) (nat_to_B n)))=
    nat_to_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 $s_{n-1} = \Sigma'_n(\mathrm{I})$ where I is the identity function; remember that Σ'_n is the sum for $0 \le i < n$; adding $i = 0$ does not change the sum. The proof by induction fits on a line. We consider then $\overline{\Sigma}'_n$ which is the sum in reverse order. This is $\Sigma'_n(n-i-1)$. Thus $2s_{n-1} = \Sigma'_n(n-1) = n(n-1)$. 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 $1 \le i \le j \le n$, 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,
  cardinal_sum (L (interval_Bnat card_one (nat_to_B n)) (fun i=>i)) =
  nat_to_B(binom (S n) 2).  (* 26 *)
```

5.8.7 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^3yz^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 $\gamma_{ij} = \binom{n}{i}$ if $i + j = n$ (this is the explanation of the term "binomial coefficient"). More generally, $(\sum x_i)^n = \sum_{\mathrm{I} \in \mathrm{S}_n} \Gamma_{\mathrm{I}} x^{\mathrm{I}}$, where I is a mapping $i \mapsto n_i$, 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 $a = b = 1$, gives $\sum_p \binom{n}{p} = 2^n$. Taking $a = -1$ and $b = 1$ gives $\sum_p (-1)^p \binom{n}{p} = 0$ (The first result has already been proved, the second is the object of Exercice 5.2). We have also $\sum_{\mathrm{I} \in \mathrm{S}_n} \Gamma_{\mathrm{I}} = p^n$ (it can be shown, by induction of the number of variables, that Γ_{I} is the number of coverings of a set with n elements by subsets with n_i elements). The cardinal of the set S_n is the object of the next theorem. We compute it by induction on both n and p.

Let E be a set with h elements, $\bar{\mathrm{A}}_n$ and $\bar{\mathrm{B}}_n$ be the sets of functions u with $\sum_{i \in \mathrm{E}} u(i) \le n$ and $\sum_{i \in \mathrm{E}} u(i) = n$ respectively. Let A_{nh} and B_{nh} the cardinals of these sets. Proposition 15 [2, p. 182]) says

$$\mathrm{A}_{nh} = \binom{n+h}{h} \qquad \mathrm{B}_{nh} = \binom{n+h-1}{h-1}.$$

We have $\mathrm{A}_{nh} = \mathrm{B}_{nh} + \mathrm{A}_{n-1,h}$ since $\bar{\mathrm{A}}_n$ is the disjoint union of $\bar{\mathrm{B}}_n$ and $\bar{\mathrm{A}}_{n-1}$ (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 is the interval $[0,n]$, hence $\bar{\mathrm{A}}_{n-1}$ is not a subset of $\bar{\mathrm{A}}_n$; it is nevetheless isomorphic to the complement of $\bar{\mathrm{B}}_n$ in $\bar{\mathrm{A}}_n$). If $x \notin \mathrm{E}$, every function u such that $\sum u(i) \leq n$ can be uniquely extented to $\mathrm{E} \cup \{x\}$ in such a way as $\sum_{i \in \mathrm{E} \cup \{x\}} u(i) = n$. This gives $\mathrm{B}_{n,h+1} = \mathrm{A}_{nh}$. The formulas follows by induction (they are trivial for $h = 0$ 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,
  let intv:= fun h => (interval_co_0a (nat_to_B h)) in
    let sle:= 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 (sle 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[2]. 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 $\mathrm{A}_{n,p+1} = \binom{n+p+1}{p+1}$. 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 $\mathrm{A}_{n,p+1}$ 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 to 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 $\mathfrak{P}([0,n+p])$ formed of sets with $p+1$ elements). The idea is that the function x is stricly increasing, and uniquely defined by its range. Since $\mathrm{A}_{n,p+1}$ is the number of stricly increasing functions

[2]Suggested by Jean-Baptiste Pomet

$[0,p] \to [0,n+p]$; all we have to to is to prove that the mapping $y \mapsto x$ is a bijection (as a function into $\mathscr{S}([0,p],[0,n+p])$.

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 $\mathrm{A}_{n,p+1}$ is the cardinal of $\mathscr{A}([0,p],[0,n])$, the set of increasing functions $[0,p] \to [0,n]$, all we have to do is show that $y \mapsto z$ is a bijection $\mathrm{C}_{pn} \to \mathrm{C}'_{pn}$ where C_{pn} is the set of functions $y : [0,p] \to [0,n]$ such that $\sum y_i \le n$ and $\mathrm{C}'_{pn} = \mathscr{A}([0,p],[0,n])$. We first show that $\mathrm{A}_{n,p+1}$ 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 $\mathrm{R}(f,i)$ denoted the restriction of the function f to the interval $[0,i]$ we have $\mathrm{R}(\mathrm{R}(f,i),j) = \mathrm{R}(f,j)$ if $j \le i$. If $\mathrm{S}(f,i)$ is the sum of the restrition of $\mathrm{R}(f,i)$ we have $\mathrm{S}(f,0) = f(0)$ and $\mathrm{S}(f,i+1) = f(i+1) + \mathrm{S}(f,i)$.

```
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 $z_i = \mathrm{S}(y,i)$. We first show that z maps $[0,p]$ into $[0,n]$, and then that $z \in \mathrm{C}'pn$ if $y \in \mathrm{C}_{pn}$ (nore that $i \mapsto \mathrm{S}(y,i)$ is increasing). We then show that $y \mapsto z$ 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.

```
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)).
```

Chapter 6

Infinite sets

6.1 The set of natural integers

Bourbaki defines an *infinite set* as a set that is not finite. If such a set exists and $\mathfrak{a}$ is its cardinal, then all integers n satisfy $n < \mathfrak{a}$, since otherwise we would have $\mathfrak{a} \leq n$, which implies $\mathfrak{a}$ finite. This means that the set $\mathbf{N}$ of cardinals n such that n is finite contains all integers. By extensionality, it does not depend on $\mathfrak{a}$. Bourbaki has an axiom that asserts the existence of an infinite set, and deduces (Theorem 1, [2, p. 184]) that the set $\mathbf{N}$ 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 $\mathbf{N}$ and $\mathbb{N}$ are isomorphic. In fact, we have defined a function $\mathcal{N}$ from the type *nat* to the set $\mathbf{N}$ that is compatible with successor, addition, multiplication and order. We have shown that it is injective and surjective. This means that $\mathbb{N}$ and $\mathbf{N}$ are equipotent, so that $\mathbf{N}$ is infinite. We have already shown this fact, using the same argument as Bourbaki: assume $\mathbf{N}$ finite, with cardinal n; then the interval $[0, n]$ is a subset of $\mathbf{N}$ hence $s(n) \leq n$, where $s(n)$ is the cardinal of the interval. But we know that $s(n) = n + 1$ and $n < s(n)$.

```
Lemma equipotent_nat_Bnat: equipotent Bnat nat.
Lemma infinite_Bnat: is_infinite_c (cardinal Bnat).
```

Bourbaki defines a *sequence* as a family whose index set I is a subset of $\mathbf{N}$. 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 $\mathbf{N}$.

Let's quote Bourbaki [2, p. 184] "Let $\mathrm{P}\{\!\{n\}\!\}$ be a relation and let I denote the set of integers n such that $\mathrm{P}\{\!\{n\}\!\}$ is true. I is then a subset of $\mathbf{N}$. A sequence $(x_n)_{n\in\mathrm{I}}$ is then sometimes written $(x_n)_{\mathrm{P}\{\!\{n\}\!\}}$, and x_n is called then *nth term* in the sequence." Example. Assume that $\mathrm{P}\{\!\{n\}\!\}$ is the relation $n \in \mathbf{Z}$ where $\mathbf{Z}$ denotes the set of rational integers as a subset of $\mathbf{N}$. According to the quote, $(x_n)_{n\in\mathbf{N}}$ and $(x_n)_{n\in\mathbf{Z}}$ are the same sequences. This may be confusing since they are obviously different families. In section 5.4, Bourbaki assumes that $\mathrm{P}\{\!\{n\}\!\}$ 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 4-ème 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 $(x_n)_{k \leq n}$ or $(x_n)_{n \geq k}$ 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 $(x_n)_{n \in \mathrm{I}}$ and $(y_n)_{n \in \mathrm{I}}$ 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 $n \in \mathrm{I}$. 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 $\mathbf{N}^p$ (p is a integer).

Let f be a bijection of $\mathbb{N}$ onto a set I. For each family $(x_i)_{i \in \mathrm{I}}$, the sequence $n \mapsto x_{f(n)}$ is said to be obtained by *arranging the family* $(x_i)_{i \in \mathrm{I}}$ *in the order defined by* f.

6.2 Definition of mappings by induction

If we instantiate C60 to the well-ordered set $\mathbf{N}$ we get a criterion that says that we can define a function by induction on $\mathbf{N}$. The value of the function at n is of the form $\mathrm{T}\{\!\{ f^{(n)} \}\!\}$ where $g^{(x)}$ denote the restriction of g to $]\leftarrow, x[$ which is the interval $[0, x-1]$. Let $n = m+1$; the least upper bound of $[0, n-1[$ is m, so that the value of the function can be of the form $\mathrm{S}\{\!\{ f(m) \}\!\}$.

There are some technical details. We use the following definitions

```
M := fun f => supremum Bnat_order (source f)
T:= fun u => Yo (u = empty_function) a (s (W (M u) u))
```

Bourbaki first defines

$$\mathrm{D}(u) = \mathscr{E}_x(x \in \mathbf{N} \text{ and } (\exists y)((x, y) \in \mathrm{pr}_1(\mathrm{pr}_1(u)))).$$

He says that, if u is a function defined on a subset of $\mathbf{N}$, then $\mathrm{D}(u)$ is the domain. This is by definition the intersection of the domain of the graph of u and $\mathbf{N}$. If u is a function, it is the intersection of the source and $\mathbf{N}$. In our definition, we use the whole source. Bourbaki defines $\mathrm{M}(u)$ as being the least upper bound of $\mathrm{D}(u)$, 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 $\mathrm{D}(u)$ is unbounded. In fact, one can even change the definition so that $\mathrm{M}(u)$ is defined when $\mathrm{D}(u)$ is not a subset of $\mathbf{N}$ (this avoids taking the intersection with $\mathbf{N}$). Our definition of *supremum* satisfies this condition. We use the property that if a set has a greatest element, it is a least upper bound, and is the supremum by uniqueness. Let ϕ be the empty function, and consider the relation

$$(u = \phi \text{ and } y = a) \text{ or } (u \neq \phi \text{ and } y = \mathrm{S}\{\!\{ u(\mathrm{M}(u)) \}\!\}).$$

Denote this by $\mathrm{R}\{\!\{ y, u \}\!\}$ and let $\mathrm{T}\{\!\{ u \}\!\}$ be the term $\tau_y(\mathrm{R}\{\!\{ y, u \}\!\})$. If $u = \phi$ then $\mathrm{T}\{\!\{ u \}\!\}$ is a, otherwise it is $\mathrm{S}\{\!\{ u(\mathrm{M}(u)) \}\!\}$; our equivalent of the if-then-else construct is *Yo*. 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 ϕ hence $f(0) = a$, and if $n = m+1$, the restriction has source $[0, m]$, whose supremum is m, so that $f(m+1) = \mathrm{S}\{\!\{ f(m) \}\!\}$.

```
Lemma segment_Bnat_order: forall x, inc x Bnat ->
  segment Bnat_order x = interval_co Bnat_order card_zero x.
```

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

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)). (* 30 *)
```

Our theorem says that there exists f such that P. We use the axiom of choice and call this function as *induction_defined*. Thus $f = \mathrm{I}(a, g)$ satisfies $f(0) = a$ and $f(n+1) = g(f(n))$. Bourbaki says that if $g : \mathrm{E} \to \mathrm{E}$ then $f : \mathbf{N} \to \mathrm{E}$. This is not quite correct: the range of f is a subset of E, and by construction, the function is surjective. There is a unique extension of f (with the same source) whose target is E. If h is a function from $\mathbf{N} \times \mathrm{E}$ into E, there exists a unique function $f : \mathbf{N} \to \mathrm{E}$ such that $f(0) = a$ and $f(n+1) = h(n, f(n))$. This function is $\mathrm{pr}_2 g$ where g is defined by induction via $\psi : (n, x) \mapsto (n+1, h(n, x))$. Note that $\mathrm{pr}_1 g$ is the identity function, so that $\mathrm{pr}_2 g(n+1) = \mathrm{pr}_2 \psi(g(n)) = \mathrm{pr}_2(\psi(n, \mathrm{pr}_2 g(n))) = h(n, \mathrm{pr}_2 g(n))$.

```
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)).

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 integer_induction_stable: forall E g  a,
  inc a E -> is_function g -> source g = E -> target g = E ->
  sub (target (induction_defined (fun  n=> W n 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 ->
  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). (* 29 *)
```

We give a variant, where h is a function of two arguments $n \in \mathbf{N}$ and $x \in \mathrm{E}$, rather then a function with source $\mathbf{N} \times \mathrm{E}$. We give a name to this operation. If $f = \mathrm{I}_1(\mathrm{E}, h, a))$, it is the unique function $\mathbf{N} \to \mathrm{E}$ such that $f(0) = a$ and $f(n+1) = h(n, f(n))$. It exists whenever $n \in \mathbf{N}$ and $x \in \mathrm{E}$ implies $h(n, x) \in \mathrm{E}$. We consider a second variant where $n < p$ and $x \in \mathrm{E}$ implies $h(n, x) \in \mathrm{E}$. Bourbaki notes that, in such cases, the function f is always defined and surjective, but the target of f is no more guaranteed to be a subset of E. There exists a unique surjective function (or unique function with target E) defined on $[0, p]$. We can extend it to $\mathbf{N}$ (for instance, by defining $f(n) = a$). We assert here existence of a function $f = \mathrm{I}_2(\mathrm{E}, h, a, p)$, $f : \mathbf{N} \to \mathrm{E}$ such that $f(0) = a$ and $f(n+1) = h(n, f(n))$ for $n < p$. By induction on $[0, p[$, it is obvious that $f(n)$ is uniquely defined for $n \leq p$ (we leave this as an exercise for the reader).

```
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 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 :=  induction_defined1 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).
```

6.3 Properties of infinite cardinals

Bourbaki claims (Lemma 1, [2, p. 186]) that every infinite set E has a subset F equipotent to **N**; the argument being that there exists a well-ordering on E. If E is isomorphic to a segment of **N**, then E is equipotent to **N** since all other segments are of the form $]\leftarrow, x[$, hence $[0, x[$, thus are finite. Otherwise, **N** is isomorphic to segment of E, hence equipotent 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 Bnat.
```

Bourbaki pretends that there is an injection from $\mathbf{N}\times\mathbf{N}$ into **N**. He uses expansion to base 2. Essentially, the function is defined by $f(2n+i, 2m+j) = 4f(n,m)+2i+j$, where i and j are 0 or 1. Injectivity follows from the fact that every integer can be uniquely written as $4a+2i+j$ where i and j are 0 or 1. In fact, the function is bijective. We use here a different function. If $g(k)$ is the binomial coefficient with indices $k+1$ and 2, then g is strictly increasing (this is clear by induction). The difference between two consecutive values is $k+1$. Let $f(n,m) = n+g(n+m)$. This is in the interval $[g(n+m), g(n+m+1)[$. This interval, hence the quantity $n+m$, is uniquely defined by $f(n,m)$. This means that if $f(n,m) = f(n',m')$ then $n+m = n'+m'$,

hence $n = n'$ and $m = m'$. The mapping is surjective: for all x there is an integer k such that $g(k) \leq x < g(k+1)$ because $g(k) \geq k$.

Bourbaki claims that $\mathbf{N} \times \mathbf{N}$ is equipotent to $\mathbf{N}$: the relation $\mathrm{Card}(\mathbf{N}) \leq \mathrm{Card}(\mathbf{N} \times \mathbf{N})$ is a consequence of $\{0\} \times \mathbf{N} \subset (\mathbf{N} \times \mathbf{N})$. Here we prove existence of a bijection (canonically associated to the function f described above).

```
Definition merge_ints (n m: nat) := n + binom (n+m+1) 2.

Lemma lt_plus: forall a b, 0 <>a -> b < b+a.
Lemma binom_monotone: forall n m,  n< m ->binom (S n) 2 < binom (S m) 2.
Lemma binom_monotone1: forall n m,  binom (S n) 2 < binom (S m) 2 -> n<m.
Lemma binom_injective: forall n m, binom (S n) 2 = binom (S m) 2 -> n = m.
Lemma merge_ints1: forall n m,  let k := n+m+1 in
  binom k 2 <= merge_ints n m &  merge_ints n m < binom (S k)2.
Lemma injective_merge_ints: forall a b c d,
  merge_ints a b = merge_ints c d -> (a=c & b = d). (* 19 *)
Lemma surjective_merge_ints:
  forall x, exists n, exists m, merge_ints n m = x. (* 18 *)
Lemma equipotent_N2_N: equipotent (product Bnat Bnat) Bnat.
```

Let E be some set and $\mathfrak{M}$ the set of functions ψ from a subset of E into $E \times E$, such that (a) ψ is injective and (b) its range is $A \times A$, where A is the source of ψ and (c) ψ extends ψ_0. The set is ordered by the prolongation order. Bourbaki says "It is immediately seen that $\mathfrak{M}$ is inductive". (The example in section 2.4 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. If $\psi \in \mathfrak{M}$ and $\mathfrak{b}$ is the cardinal of its source, conditions (a) and (b) assert that $\mathfrak{b} = \mathfrak{b}^2$ while (c) says $\mathfrak{b} \geq \mathfrak{b}_0$.

Consider now an infinite set E with cardinal $\mathfrak{a}$. There exists a subset D equipotent to $\mathbf{N}$, hence a bijection ψ between D and $D \times D$. This implies that there exists a function ψ_0 that satisfies conditions (a) and (b) above. This function will be used for the definition of $\mathfrak{M}$. Consider a maximal element ψ, whose source F has cardinal $\mathfrak{b}$. The assumption $\mathfrak{b} \geq \mathfrak{b}_0$ says that this cardinal is infinite, so $2\mathfrak{b} \leq \mathfrak{b}^2$ hence $\mathfrak{b} = 2\mathfrak{b}$. Assume $\mathfrak{b} < \mathfrak{a}$. There exists a subset Z of E that is the disjoint union of F and a set Y with cardinal $\mathfrak{b}$ (since $\mathfrak{c} \leq \mathfrak{b}$ implies $\mathfrak{c} + \mathfrak{b} < \mathfrak{a}$). The complement of $F \times F$ in $Z \times Z$ has cardinal $3\mathfrak{b}^2$ hence $\mathfrak{b}$. We can thus extend our function as a bijection from Z into $Z \times Z$. This contradicts minimality, and $\mathfrak{b} = \mathfrak{a}$. Thus we have shown (Theorem 2 [2, p. 186]): for every infinite cardinal $\mathfrak{a}$, we have $\mathfrak{a} = \mathfrak{a}^2$.

```
Definition set_for_equipotent_inf2_inf E psi:=
  Zo (set_of_sub_functions E (product E E))  (fun z  =>
    injective (inv_corr_value z) &
    range (P z) = product (P (Q z)) (P (Q z)) &
    sub (P psi) (P z)).

Lemma inductive_set_for_equipotent_inf2_inf: forall E psi,
  inc psi (set_for_equipotent_inf2_inf E psi) ->
  inductive_set (induced_order (opposite_order(extension_order E (product E E)))
  (set_for_equipotent_inf2_inf E psi)).  (* 106 *)

Lemma equipotent_inf2_inf1: forall E, infinite_set E ->
  exists psi, inc psi (set_of_sub_functions E (product E E)) &
    injective (inv_corr_value psi) &
    infinite_set (P (Q psi)) &
```

```
    range (P psi) = product (P (Q psi)) (P (Q psi)).
Lemma equipotent_inf2_inf2: forall E psi x,
  infinite_set (P (Q psi)) -> inc x (set_for_equipotent_inf2_inf E psi) ->
  inc psi (set_for_equipotent_inf2_inf E psi) ->
  is_infinite_c (cardinal (P (Q x))).

Theorem equipotent_inf2_inf: forall a, is_infinite_c a ->
  card_pow a (card_two) = a. (* 169 *)
```

By induction, $\mathfrak{a}^n = \mathfrak{a}$ if $\mathfrak{a}$ is an infinite cardinal and $n \geq 1$ is an integer. As a consequence, if $(\mathfrak{a}_i)_{i\in\mathrm{I}}$ is a finite family of non-zero cardinals, if the largest one is an infinite cardinal $\mathfrak{a}$, then the product is $\mathfrak{a}$. If $\mathfrak{a}_i \leq \mathfrak{a}$ then $\sum \mathfrak{a}_i \leq \mathfrak{a}$ and we have equality if one of the cardinals is $\mathfrak{a}$. The cardinals can be zero, and the index set can be infinite, provided that $\mathrm{Card}(\mathrm{I}) \leq a$. Finally, if $\mathfrak{a}$ and $\mathfrak{b}$ are two non-zero cardinals, one of them being infinite, then the sum and the product is the greatest of them.

Note. Bourbaki writes "$\sup(\mathfrak{a}, \mathfrak{b})$" instead of "the greatest of them"; our function *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 $\mathfrak{a}$ is infinite or $\mathfrak{b}$ is infinite, then $\mathfrak{a}+\mathfrak{b} = \sup(\mathfrak{a}, \mathfrak{b})$ is uneasy, since this means that $\mathfrak{a}+\mathfrak{b}$ is at least $\mathfrak{a}$, at least $\mathfrak{b}$, and at most any $\mathfrak{c}$ that is at least $\mathfrak{a}$ and at least $\mathfrak{b}$. It is much easier to say: if $\mathfrak{a}$ is infinite and $\mathfrak{b} \leq \mathfrak{a}$ then $\mathfrak{a}+\mathfrak{b} = \mathfrak{a}$, and use commutativity of addition when needed. Note that $\mathfrak{b}$ infinite implies $\mathfrak{a}$ infinite, and $\mathfrak{b}$ can be zero (since $\mathfrak{a}$ is infinite, it is clearly non-zero). In the case of a product, we need the condition $\mathfrak{b} \neq 0$.

```
Lemma power_of_infinite: forall a n, is_infinite_c a -> inc n Bnat ->
  n <> card_zero -> card_pow a n = a.
Lemma finite_family_product: forall a f, fgraph f ->
  is_finite_set (domain f) -> is_infinite_c a ->
  (forall i, inc i (domain f) -> cardinal_le (V i f) a) ->
  (forall i, inc i (domain f) -> V i f <> card_zero) ->
  (exists j,  inc j (domain f) & (V j f) = a) ->
  cardinal_prod f = a.
Lemma product2_infinite: forall a b, cardinal_le b a ->
  is_infinite_c a -> b <> card_zero -> card_mult a b = a.
Lemma notbig_family_sum: 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) ->
  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.
```

6.4 Countable sets

A countable set is one that is equipotent to a subset of **N**. Proposition 2 [2, p. 188] says that an infinite countable set is equipotent to **N**. We rewrite this as: a countable set is finite or equipotent to **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 $(X_\iota)_{\iota\in I}$ where X_ι 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 infinite and $\overset{-1}{f}\langle\{x\}\rangle$ 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 ->
  is_finite_set E \/ equipotent E Bnat.
Lemma countable_finite_or_N_c: 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_countable_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 $\mathfrak{F}_n$ as the set of all subsets with n elements of E and claims $\mathrm{Card}(\mathfrak{F}_n) \leq \mathrm{Card}(E)$. Thus, the cardinal of the union of these sets is at most $\sum_{n\in\mathbf{N}} \mathrm{Card}(E) = \mathrm{Card}(E)$. Thus $\mathrm{Card}(\mathfrak{F}) \leq \mathrm{Card}(E)$; equality holds because the set of singletons is equipotent to E and is a subset of $\mathfrak{F}$.

The Bourbaki claim is: for every $X \in \mathfrak{F}_n$ there is a bijection from $[1, n]$ onto X, so that the cardinal of $\mathfrak{F}_n$ is at most the cardinal of the set of functions from $[1, n]$ into X which is $\mathrm{Card}(E^n) = \mathrm{Card}(E)$. Our proof is as follows.

For every $X \in \mathfrak{F}_n$ 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 $f^{-1}\langle\{x\}\rangle$ 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 $f^{-1}\langle\{x\}\rangle$. 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 $a \leq \mathrm{Card}(E)$; otherwise $d = \mathrm{Card}(E)$. Hence $ac = b \leq \mathrm{Card}(E)$. If a is finite, we have $a \leq \mathrm{Card}(E)$; but if a is infinite, we have $a = ac$ (since c is non-zero finite). This implies $a \leq \mathrm{Card}(E)$.

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 **N**. Since E^I and I are equipotent and since the set of finite subsets of **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 $\mathfrak{P}(\mathbf{N})$. In this case, its cardinal is $2^{\aleph_0}$, and the set is not countable.

6.5 Stationary sequences

A sequence $(x_n)_{n\in\mathbf{N}}$ 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 **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:=
  fgraph f & domain f = Bnat & sub (range f) (substrate r) &
  forall n m, inc n Bnat  -> inc m Bnat -> cardinal_le n m ->
    gle r (V n f) (V m f).

Definition decreasing_sequence f r:=
  fgraph f & domain f = Bnat & sub (range f) (substrate r) &
  forall n m, inc n Bnat  -> inc m Bnat -> cardinal_le n m ->
    gle r  (V m f) (V n f).
```

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 func-

tion 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 *increasing_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. It 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 $\prod \mathrm{T}_x$ is non-empty, hence there is a function $f : \mathrm{A} \to \mathrm{A}$ 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, order r ->
  is_function f -> source f = Bnat -> sub (target f) (substrate r) ->
  (forall n, inc n Bnat -> gle r (W n f) (W (succ n) f)) ->
  increasing_sequence (graph f) r.
Lemma decreasing_prop: forall f r, order r ->
  is_function f -> source f = Bnat -> sub (target f) (substrate r) ->
  (forall n, inc n Bnat -> gge r (W n f) (W (succ n) f)) ->
  decreasing_sequence (graph f) r.
Theorem  increasing_stationary: forall r, order r ->
  (forall X, sub X (substrate r) -> nonempty X ->
     exists a,  maximal_element (induced_order r X) a) =
  (forall f, increasing_sequence f r -> stationary_sequence f). (* 43 *)
Theorem  decreasing_stationary: forall r, total_order r ->
  (worder r) =
  (forall f, decreasing_sequence f r -> stationary_sequence f). (* 38 *)
Theorem  finite_increasing_stationary: forall r, order r ->
  is_finite_set (substrate r) ->
  (forall f, increasing_sequence f r -> 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 $a \in \mathrm{E}$, if $\forall x, x > a \implies x \in \mathrm{F}$ then $a \in \mathrm{F}$; then $\mathrm{F} = \mathrm{E}$.

```
Theorem noetherian_induction: forall r F,  order r ->
  (forall X, sub X (substrate r) -> nonempty X ->
    exists a,  maximal_element (induced_order r X) a) ->
  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 7

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

$$
\begin{aligned}
(*) \qquad & \tau_{\mathrm{Z}}((\exists u)(\exists \mathrm{U})(u = (\mathrm{U}, \{\emptyset\}, \mathrm{Z}) \text{ and } \mathrm{U} \subset \{\emptyset\} \times \mathrm{Z} \\
& \text{and } (\forall x)((x \in \{\emptyset\}) \implies (\exists y)((x, y) \in \mathrm{U})) \\
& \text{and } (\forall x)(\forall y)(\forall y')(((x, y) \in \mathrm{U} \text{ and } (x, y') \in \mathrm{U}) \implies (y = y')) \\
& \text{and } (\forall y)((y \in \mathrm{Z}) \implies (\exists x)((x, y) \in \mathrm{U})))).
\end{aligned}
$$

Une estimation grossière montre que le terme ainsi *désigné* est un assemblage de plusieurs dizaines de milliers de signes (chacun de ces signes étant l'un des signes τ, $\square$, $\vee$, $\neg$, $=$, $\in$, $\supset$).

English translation is ([2, p. 158]): The mathematical *term denoted* (Chapter 1, § 1, no. 1) by the symbol "1" is of course not to be confused with the *word* "one" in ordinary language. The term denoted by "1" is equal, by virtue of the definition above, to the term denoted by the symbol (*). As a rough estimate, the term so *denoted* is an assembly of several tens of thousands of signs (each of which is one of τ, $\square$, $\vee$, $\neg$, $=$, $\in$, $\supset$).

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 $\mathrm{Card}(\{\emptyset\}) = \tau_{\mathrm{Z}}(\mathrm{Eq}(\{\emptyset\}, \mathrm{Z}))$.

If 1 is a big object, then how big is 2? or the set N of integers, or the set R of real numbers? If $\mathrm{P}(\mathrm{X}, n)$ is: $\mathrm{X} = (x, y, z)$ 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 $(\forall n)(n \in \mathrm{N} \implies (\exists \mathrm{X})(\mathrm{X} \in \mathrm{R}^3 \text{ and } \mathrm{P}(\mathrm{X}, n)))$? 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

$$
(**)\qquad
\begin{aligned}
\tau_Z((\exists u)(\exists U)(\quad & u = (U,Y,Z)\\
& \text{and } U \subset Y \times Z\\
& \text{and } (\forall x)((x \in Y) \implies (\exists y)((x,y) \in U))\\
& \text{and } (\forall x)(\forall y)(\forall y')(((x,y) \in U \text{ and } (x,y') \in U) \implies (y = y'))\\
& \text{and } (\forall y)((y \in Z) \implies (\exists x)((x,y) \in U))\\
& \text{and } (\forall x)(\forall x')(\forall y)(((x,y) \in U \text{ and } (x',y) \in U) \implies (x = x')))).
\end{aligned}
$$

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 P1 and P2 and P3 and P4 and P5 and P6. Properties P1 and P2 say that u is a correspondence with source Y, target Z and graph U, properties P3 and P4 say that u is a function, property P5 that u is injective, and P6 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 $\tau_Z(\mathrm{Eq}(Y,Z))$, as it should be. Note that P6 is missing in (*). In fact, if $(x,y) \in U$, then $x \in Y$, hence $x = \emptyset$, so that P6 is a consequence of other relations. Hence, the term designed by (*) is *equal* but not *identical* to 1. In what follows, we shall discuss the size of (**).

The case of Coq. The expression W has the form

```
exists u : Bset,
   exists U : Bset,
     u = J (J U emptyset) Z &
     (forall x : Bset, inc x U -> inc x (record Y (fun _ : Bset => Z))) &
     (forall x : Bset, inc x Y -> exists y : Bset, inc (J x y) U) &
     (forall x y y' : Bset, inc (J x y) U -> inc (J x y') U -> y = y') &
     (forall y : Bset, inc y Z -> exists x : Bset, inc (J x y) U) &
     (forall x x' y : Bset, inc (J x y) U -> inc (J x' y) U -> x = x')
```

Expanding everything but J gives:

```
exists u : Bset,
  exists U : Bset,
    u = J (J U emptyset) Z &
    (forall x : Bset,
     (exists a : U, Ro a = x) ->
     exists  a : record (IM (fun _ : one_point => emptyset))
             (fun _ : Bset => Z), Ro a = x) &
    (forall x : Bset,
     (exists a : IM (fun _ : one_point => emptyset), Ro a = x) ->
     exists y : Bset, exists a : U, Ro a = J x y) &
    (forall x y y' : Bset,
     (exists a : U, Ro a = J x y) -> (exists a : U, Ro a = J x y') -> y = y') &
    (forall y : Bset,(exists a : Z, Ro a = y) ->
     exists x : Bset, exists a : U, Ro a = J x y) &
    (forall x x' y : Bset, (exists a : U, Ro a = J x y) ->
     (exists a : U, Ro a = J x' y) -> x = x')
```

Because of our implementation of τ in Coq, the full expansion of 1 is three times as big as this quantity. This gives a total of 500 tokens (we count *forall*, *exists*, *Bset*, etc, as a single token). In [3], 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:

```
(exists a : U,
  Ro a = IM (fun t : two_points =>
        match t with
        | two_points_a => IM (fun _ : one_point => x')
        | two_points_b =>
           IM (fun t0 : two_points =>
              match t0 with
              | two_points_a => emptyset
              | two_points_b => IM (fun _ : one_point => y)
               end)
        end)) -> x = x')
```

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 $u = (\mathrm{U}, \mathrm{Y}, \mathrm{Z})$ and $\mathrm{U} \subset \mathrm{Y} \times \mathrm{Z}$), 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 $\mathrm{U} \subset \mathrm{Y} \times \mathrm{Z}$. 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:

$$\tau\neg\neg\neg\in\tau\neg\neg\in\square\square\square$$

It is easy to count them: there are 12 signs. The definition of the empty set is $\tau_x((\forall y)(y \not\in x))$. If P is a formula we denote by L[P] its length; assume that P depends on z and has α signs and β other signs. Remember that $(\exists z)\mathrm{P}(z)$ is $(\tau_z \mathrm{P}|z)\mathrm{P}$, this is the formula obtained by replacing all z by $\tau_z \mathrm{P}$. Thus we have

$$\mathrm{L}[(\exists z)\mathrm{P}(z))] = (\alpha+1)(\alpha+\beta).$$

Since $(\forall z)\mathrm{P}(z)$ is $\neg(\exists z)(\neg(\mathrm{P}z))$, we get

$$\mathrm{L}[(\forall z)\mathrm{P}(z)] = 1 + (\alpha+1)(\alpha+\beta+1).$$

In the case of $(\forall y)(y \not\in x)$, we have $\alpha = 1$ and $\beta = 4$, the length is 11, hence $\mathrm{L}[\emptyset] = 12$. The following formulas are obvious:

$$\mathrm{L}[\mathrm{A} \text{ or } \mathrm{B}] = 1 + \mathrm{L}[\mathrm{A}] + \mathrm{L}[\mathrm{B}]$$

$$\mathrm{L}[\mathrm{A} \text{ and } \mathrm{B}] = 4 + \mathrm{L}[\mathrm{A}] + \mathrm{L}[\mathrm{B}]$$

$$\mathrm{L}[\mathrm{A} \implies \mathrm{B}] = 2 + \mathrm{L}[\mathrm{A}] + \mathrm{L}[\mathrm{B}]$$

$$\mathrm{L}[\mathrm{A} \iff \mathrm{B}] = 8 + 2\mathrm{L}[\mathrm{A}] + 2\mathrm{L}[\mathrm{B}]$$

The set of all x such that $\mathrm{P}(z)$ is $\tau_y((\forall z)(z \in y) \iff \mathrm{P})$ hence

$$\mathrm{L}[\{z, \mathrm{P}(z)\}] = 4\alpha^2 + 36\alpha + 47 + (4\alpha+6)\beta.$$

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

$$\mathrm{L}[\{x, y\}] = 177 + 14x + 14y.$$

Since $\{\emptyset\} = \{\emptyset, \emptyset\}$ we get

$$\mathrm{L}[\{\emptyset\}] = 513.$$

Assume that W has length $\alpha + \beta\mathrm{U} + \gamma\mathrm{Z} + u$. The size of $(\exists\mathrm{U})\mathrm{W}$ is

$$(\beta + 1)(\alpha + \beta + \gamma\mathrm{Z} + u);$$

the size of $(\exists u)(\exists\mathrm{U})\mathrm{W}$ is

$$(\beta + 1)(\beta + 2)(\alpha + \beta + \gamma\mathrm{Z} + 1);$$

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 $u = (\mathrm{U}, \mathrm{Y}, \mathrm{Z})$, assuming that the triple is the pair of pairs $((\mathrm{U}, \mathrm{Y}), \mathrm{Z})$. Since the pair (x, y) is $\{\{x\}, \{x, y\}\}$ we have

$$\mathrm{L}[(x, y)] = 5133 + 588x + 196y.$$

$$\mathrm{L}[((x, y), z)] = 3023337 + 345744x + 115248y + 196z$$

$$\mathrm{L}[u = (\mathrm{U}, \mathrm{Y}, \mathrm{Z})] = 62\,145\,562 + 345\,744\mathrm{U} + 196\mathrm{Z} + u$$

Let α be the constant that appears here, and β 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

$$\mathrm{L}'[u = (\mathrm{U}, \mathrm{Y}, \mathrm{Z})] = u + \mathrm{U} + \mathrm{Z} + 516.$$

Size of a graph. We try to find the size of expression P2, namely $\mathrm{U} \subset \mathrm{Y} \times \mathrm{Z}$. If B is $\mathrm{Y} \times \mathrm{Z}$, this expression is $(\forall z)(z \in \mathrm{A} \implies z \in \mathrm{B})$, its size is $22 + 3\mathrm{A} + 3\mathrm{B}$. The size of "$z = (x, y)$ and $x \in \mathrm{Y}$ and $y \in \mathrm{Z}$" is $z + 2x + 2y + \mathrm{Y} + \mathrm{Z} + 12$. If this is P, then $\mathrm{Y} \times \mathrm{Z}$ is the set of all z so that there exists x such that there exists y such that P. Quantifying $\exists y$ gives $42 + 6x + 3\mathrm{Y} + 3\mathrm{Z} + 3z$, quantifying $\exists x$ gives $336 + 21(\mathrm{Y} + \mathrm{Z} + z)$. Taking the set of all z gives $32807 + 1890(\mathrm{Y} + \mathrm{Z})$.

$$\mathrm{L}'[\mathrm{U} \subset \mathrm{Y} \times \mathrm{Z}] = 98443 + 3\mathrm{U} + 5670(\mathrm{Y} + \mathrm{Z});$$

$$\mathrm{L}'[\mathrm{P2}] = 3\,007\,153 + 3\mathrm{U} + 5670\mathrm{Z}.$$

For the French version, the length of P is

$$589x + 5144 + 197y + z + \mathrm{Y} + \mathrm{Z}.$$

Quantifying over y gives

$$1057518 + 198\mathrm{Y} + 198\mathrm{Z} + 116622x + 198z.$$

Quantifying over x gives

$$136931729220 + 23091354(\mathrm{Y} + \mathrm{Z} + z).$$

Taking the set of all z gives

$$\mathrm{L}[\mathrm{Y} \times \mathrm{Z}] = 12649889797944532895 + 2132842656761388(\mathrm{Y} + \mathrm{Z});$$

$$\mathrm{L}[\mathrm{U} \subset \mathrm{Y} \times \mathrm{Z}] = 37949669393833598707 + 3\mathrm{U} + 6398527970284164(\mathrm{Y} + \mathrm{Z});$$

$$\mathrm{L}[\mathrm{P2}] = 41232114242589374839 + 3\mathrm{U} + 6398527970284164\mathrm{Z}.$$

This number is so big that it is impossible to put in a computer the full expansion of $\mathrm{U} \subset \{\emptyset\} \times \mathrm{Z}$.

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 $(x, y) \in \mathrm{U}$, the size is

$$5134 + 588x196y + \mathrm{U}; \text{ or } 2 + x + y + \mathrm{U}.$$

The size is $(\exists y)((x, y) \in \mathrm{U})$ is

$$1050010 + 197\mathrm{U} + 115836x \text{ or } 6 + 2\mathrm{U} + 2x.$$

The size of $x \in \mathrm{Y} \implies (\exists y)((x, y) \in \mathrm{U})$ is

$$1050013 + 197\mathrm{U} + 115837x + \mathrm{Y} \text{ or } 9 + 2\mathrm{U} + 3x + \mathrm{Y}.$$

The size of $(\forall x)(x \in \mathrm{Y} \implies (\exists y)((x, y) \in \mathrm{U}))$ is

$$135049848139 + 22820086\mathrm{U} + 115838\mathrm{Y} \text{ or } 53 + 8\mathrm{U} + 4\mathrm{Y}.$$

The size of P3 is

$$135109273033 + 22820086\mathrm{U} \text{ or } 2105 + 8\mathrm{U}.$$

The size of $(x, y) \in \mathrm{U}$ and $(x, y') \in \mathrm{U}$ is

$$10272 + 1176x + 196y + 196y' + 2\mathrm{U} \text{ or } 8 + 2x + y + y' + 2\mathrm{U};$$

The size of $(x, y) \in \mathrm{U}$ and $(x, y') \in \mathrm{U} \implies y = y'$ is

$$10275 + 1176x + 197y + 197y' + 2\mathrm{U} \text{ or } 11 + 2x + 2y + 2y' + 2\mathrm{U};$$

The size of $(\forall y')((x, y) \in \mathrm{U}$ and $(x, y') \in \mathrm{U} \implies y = y')$ is

$$2073655 + 396\mathrm{U} + 34848x + 39006y \text{ or } 43 + 6\mathrm{U} + 6x + 6y.$$

The size of $(\forall y)(\forall y')((x, y) \in \mathrm{U}$ and $(x, y') \in \mathrm{U} \implies y = y')$ is

$$82408606635 + 15446772\mathrm{U} + 9082701936x \text{ or } 351 + 42\mathrm{U} + 42x.$$

Finally the size of P4 is

$$830988285585569103965 + 140298425964797364\mathrm{U} \text{ or } 16943 + 1806\mathrm{U}.$$

The size of $(\exists x)((x,y) \in \mathrm{U})$ is

$$3370258 + 589\mathrm{U} + 115444y \text{ or } 6 + 2\mathrm{U} + 2y.$$

The size of $y \in \mathrm{Z} \implies (\exists x)((x,y) \in \mathrm{U})$ is

$$3370261 + 589\mathrm{U} + 115445y + \mathrm{Z} \text{ or } 9 + 2\mathrm{U} + 3y + \mathrm{Z}.$$

Hence the size of P5 is

$$402410930323 + 67997694\mathrm{U} + 115446\mathrm{Z} \text{ or } 53 + 8\mathrm{U} + 4\mathrm{Z}.$$

The size of $(x,y) \in \mathrm{U}$ and $(x',y) \in \mathrm{U} \implies x = x'$ is

$$10275 + 589x + 589x' + 392y + 2\mathrm{U} \text{ or } 11 + 2x + 2x' + 2y + 2\mathrm{U}.$$

The size of $(\forall y)((x,y) \in \mathrm{U}$ and $(x',y) \in \mathrm{U} \implies x = x')$ is

$$4192525 + 786\mathrm{U} + 231477(x + x') \text{ or } 43 + 6\mathrm{U} + 6x + 6x'.$$

The size of $(\forall x')(\forall y)((x,y) \in \mathrm{U}$ and $(x',y) \in \mathrm{U} \implies x = x')$ is

$$1024059366435 + 181941708\mathrm{U} + 53581833006x \text{ or } 351 + 42\mathrm{U} + 42x.$$

Hence the size of P6 is

$$57741990789964425582095 + 9748770215064355956\mathrm{U} \text{ or } 16943 + 1806\mathrm{U}.$$

The size of the expressions P3 to P6 is hence

$$58572979076087514889416 + 9889068641119971100\mathrm{U} + 115446\mathrm{Z} \text{ or } 36044 + 3628\mathrm{U} + 4\mathrm{Z}.$$

This gives, for the French version $\alpha = 58614211190330166409837$ $\beta = 9889068641120316847$ $\gamma = 6398527970399806$, 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

$$4\,150\,763\,939\,024\,663.$$

Moreover, the 1970 decision to remove the axiom of the ordered pair had a dramatic effect on the size of one, that increases to

$$5733067044017980337582376403672241161543539419681476659296689.$$

Chapter 8

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 (970), 7 (128), 8 (29), 9 (145), 10 (17), 11 (*)

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.

```
finition 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).  red in g.
assert (forall z, inc z g =(z = J TPa TPa \/ z = J TPb TPb \/ z = J TPa TPb)).
  ir. app iff_eq. ir. ufi g H. nin (union2_or H). nin (doubleton_or H0). 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 (Ha: related g TPa TPa). red. rw H. left. tv.
  assert (Hb: related g TPb TPb). red. rw H. right. left. tv.
  assert (Hc: related g TPa TPb). red. rw H. right. right. tv.
assert (substrate g = two_points). set_extens. rwi (inc_substrate1 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).
  wr (pr2_injective H2). rww (pr1_injective H3).
  nin H3; rww (pr2_injective H3).
  red. split. am. ir. red in H2. red in H3. rwi H H2. rwi H H3. nin H2.
```

```
  rw (pr1_injective H2). rw (pr2_injective H2).  tv.
  nin H2. rw (pr1_injective H2). rw (pr2_injective H2).  tv.
  nin H3. rw (pr1_injective H3). rw (pr2_injective H3).  tv.
  nin H3. rw (pr1_injective H3). rw (pr2_injective H3).  tv.
  wri H3 H2. ap (pr1_injective H2).
```

If X is a subset of E, it contains only α or β. 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 α. 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.

```
  red. ee. am. ir. apply by_cases with (inc TPa x). ir.
  apply by_cases with (inc TPb x). ir. assert (x = two_points).
  rwi H1 H3. ap extensionality. am. red. ir. rwi two_points_pr H7.
  nin H7; rww H7. exists TPa. red. aw. split. am. ir. aw.
  rwi H7 H8.  rwi two_points_pr H8. nin  H8; rww H8.
  ir. assert (x = singleton TPa). set_extens. cp (H3 _ H7). rwi H1 H8.
  rwi two_points_pr H8. nin H8. rw H8. fprops. elim H6. wrr H8.
  rww (singleton_eq H7). exists TPa.
  red. aw. split. am. ir. aw. rwi H7 H8. rww (singleton_eq H8).
  ir. nin H4. rwi H1 H3. cp (H3 _ H4). rwi two_points_pr H6. nin H6. elim H5.
  wrr H6. rwi H6 H4.
  assert (x = singleton TPb). set_extens.
  cp (H3 _ H7). rwi two_points_pr H8. nin H8. elim H5. wrr H8. rw H8. fprops.
  rww (singleton_eq H7).  exists TPb.
  red. aw. split. am. ir. aw. rwi H7 H8. rww (singleton_eq H8). rww H1.
Qed.
```

Let $\mathfrak{F}$ be a set of subsets of A, ordered by inclusion, and such that for every totally ordered subset $\mathfrak{G}$ of $\mathfrak{F}$ the union of the sets of $\mathfrak{G}$ belongs to $\mathfrak{F}$. Then $\mathfrak{F}$ is inductive with respect to the relation $\subset$.

```
Lemma inductive_example1: forall A F, sub A (powerset F) ->
  (forall S, (forall x y, inc x S -> inc y S -> sub x y \/ sub y x) ->
    inc (union S) A) ->
  inductive_set (inclusion_suborder A).
Proof. ir. red. ir.  exists (union X). red.
  assert (inc (union X) A). app H0. ir. red in H2.
  ee. awi H5. cp (H5 _ _ H3 H4). awi H6. nin H6.  ee. left. am. red in H6.
  awi H6. ee; right. am. am. am. am. am. fprops. am.  split. aw. ir. aw.
  awi H1. ee.  app H1. am. app union_sub.
Qed.
```

The set $\Phi(E,F)$ of mappings of subsets of E into subsets of F is inductive, with respect to the order "v extends u" between u and v (i.e., the opposite of the extension ordering), because there is a common prolongation 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).
  rwi set_of_sub_functions_pr1 H5. rwi set_of_sub_functions_pr1 H6. ee.
  cp (H2 _ _ H3 H4). ufi gge H13. red. rw Hc. rw Hc. ee.
  app intersection2sub_first. app intersection2sub_second.
  awi H13. ufi extends_in H13. nin H13. ee. ir. app W_extends. rw Hc.
  app (intersection2_first H16). am. ee. ir. sy. app W_extends. rw Hc.
  app (intersection2_second H16). am. am. am. am. am. am. am. am. am.
  cp (prolongation_covering _ _ Ha Hb Hc Hd). nin H3. clear H4. nin H3. ee.
  assert (inc (corr_value x) (set_of_sub_functions a b)).
  rw set_of_sub_functions_pr. exists x. ee. am. rw H4. red. ir.
  nin (unionf_exists H7). nin H8. cp (H0 _ H8).  wri Hc H9.
  rwi set_of_sub_functions_pr1 H10. ee. app H11. am. am. tv.
  exists (corr_value x). red. ee. aw. ir. aw. red. ee. app H0. am.
  cp (H0 _ H8). rwi set_of_sub_functions_pr1 H9. ee. rww inv_corr_value_pr.
  red. rw H11. rw H5. ee. am. am. cp (H6 _ H8). red in H13. ee. red. ir.
  cp (in_graph_W H9 H16). rwi H17 H16.  cp (inc_pr1graph_source H9 H16).
  rwi Hc H18. wri (H15 _ H18) H17. rw H17. app defined_lem. app H13. am.
  fprops.  app extension_is_order. app opposite_is_order.
Qed.
```

8.1 Section 1

1. *Let* E *be an ordered set in which there exists at least one pair of distinct comparable elements. Show that if* R⦃x, y⦄ *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.*

```
Lemma Exercise1_1: forall r, let E:= substrate r in
  let s := fun x y => (inc x E & inc y E & glt r x y) in
    order r ->  (exists x, exists y, x <> y & related r x y)
    -> (transitive_r s &  antisymmetric_r s & ~(reflexive_rr s)).
Proof. ir. split. red. uf s. uf glt. ir. ee. am. am. red in H; ee.
  nin H10. app (H12 _ _ _ H7 H4). red. ir. wri H9 H4.
  rwi (order_antisymmetry H H7 H4) H8. elim H8. tv.
  split. red.  uf s. uf glt. ir. ee. app (order_antisymmetry H H7 H4).
  red. ir. red in H1.  nin H0. nin H0.  nin H0.
  assert (s x x0). uf s.  split. ap (inc_arg1_substrate H2).
  split. ap (inc_arg2_substrate H2). red. intuition.
  cp (H1 _ _ H3). nin H4. ufi s H4. ufi glt H4. intuition.
Qed.
```

---

2. *(a) Let* E *be a preordered set and let* S⦃x, y⦄ *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 $\leq_{\mathrm{E}}$ the given preorder, and by $x \leq_{\mathrm{E}} y$ the associated preorder relation; in the same way, $\leq_{\mathrm{Q}}$ is the quotient preorder and $x \leq_{\mathrm{Q}} y$ its associated relation. In other words, $x \leq_{\mathrm{Q}} y$ is the relation $\mathrm{R}\{\!\{x, y\}\!\}$ defined in the text and $\leq_{\mathrm{Q}}$ 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 $x \leq_{\mathrm{Q}} y$ 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. 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 $\leq_{\mathrm{Q}}$ is a preorder on E/S, associated to the relation $x \leq_{\mathrm{Q}} y$.

```
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. rw 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.
```

(b) Let ϕ 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 ϕ 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.
  rwi quotient_order_pr H9.  red in H5. ee.  red in H14. simpl in H14.
  red in H9. ee. cp H12. simpl in H12. wri H12 H14.
  cp (inc_rep_itself H  H9). nin (H16 _ H18). nin H19.
  assert (inc (rep x) (substrate r)). app (inc_arg1_substrate H20).
  assert (inc x0 (substrate r)). app (inc_arg2_substrate H20).
  cp (H14 _ _ H21 H22 H20).  rwi H17 H21; rwi H17 H22.
  rwii W_compose H23. rwii W_compose H23. awi H23; try am.
  assert (class s (rep x) = x). app class_rep. rwii H24 H23.
  assert (y = class s x0). assert (class s (rep y) = y). app class_rep.
  wr H25. cp (related_rep_in_class H H15 H19). rwi related_rw H26. ee. am.
  am. rww H25.

Qed.
```

The converse is true if ϕ 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.
  rw source_canon_proj. wr H1. uf increasing_map. rw substrate_quotient_order.
  rw target_canon_proj. assert (Ha: is_graph s). nin H; am.
  ap iff_eq. ir. ee; try am. app function_canon_proj. tv.
  tv. ir. rw quotient_order_pr. rww W_canon_proj. rww W_canon_proj.
  uf quotient_order_r. ee. app inc_class_quotient. app inc_class_quotient.
  ir. red in H3. ee. rwi inc_class H7.
  nin (H10 _ _ _ H6 H7).  exists x1. rw inc_class. am. am. am.
  ir. ee. red. ee.  am. am. 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 H11.
  ufi quotient_order_r H13.
  ee. wri inc_class H10.  nin (H15 _ H10). nin H16.
  exists x0. split. wr inc_class.  am. am. am. am. am. am. am. am. am. am. am.
Qed.
```

(c) Let E_1 *and* E_2 *be two preordered sets. Show that if* S_1 *is the equivalence relation* $\mathrm{pr}_1 z = \mathrm{pr}_1 z'$ *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* ϕ_1 *is the canonical mapping of* $E_1 \times E_2$ *onto* $(E_1 \times E_2)/S_1$*, and if* $\mathrm{pr}_1 = f_1 \circ \phi_1$ *is the canonical decomposition of* 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 $\mathrm{pr}_1 z = \mathrm{pr}_1 z'$.

```
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.
  rww 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. wrr 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 x' y,  gle r x y -> related s x x' -> 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)).
  app preorder_product2_order.  set_extens. uf coarse.
  assert (is_pair x). red in H0. ee. app H0. app product_inc.
  app inc_pr1_substrate. app inc_pr2_substrate. ufi coarse H4.
  rwi inc_product H4. ee. nin H1.
  set (x1:= J y (Q x)). set (x2:= J y (P x)).
  assert (inc x1 (product (substrate r1) (substrate r2))). uf x1. fprops.
  assert (inc x2 (product (substrate r1) (substrate r2))). uf x2. fprops.
  assert (gle (product2_order r1 r2) x1 x1). wrr preorder_reflexivity.
  rww substrate_preorder_product2_order.
  set (s:=first_proj_equivalence (substrate r1) (substrate r2)).
  assert (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 x_1 and x_2 exchanged.

```
Lemma exercise1_2c3: forall r1 r2,
  let compatibility r s :=
   (forall x y y',  gle r x y -> related s y 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 $\mathrm{pr}_1 = f_1 \circ \phi_1$ implies that f_1 is an isomorphism; we first introduce the definition of a pre-order isomorphism. If E_2 is empty, then pr_1 is in general not surjective, thus f_1 is not surjective; this explains why we add the condition $\mathrm{E}_2 \neq \emptyset$. If $f_1(x) = f_1(y)$, where x and y are the classes of x' and y', then $\mathrm{pr}_1 x' = \mathrm{pr}_1 y'$, hence $x' \equiv y'$ and $x = y$, so that f_1 is injective. With the same notations, $f_1(x) \leq f_1(y)$ if and only if $\mathrm{pr}_1 x' \leq \mathrm{pr}_1 y'$.

```
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.
  rww substrate_preorder_product2_order.
  assert(Hb:substrate s =  product E1 E2). uf s.
  rww 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.
  tv.
  assert (Hd:preorder r).  uf r. app preorder_product2_order.
  assert (source (canon_proj s)= product E1 E2). tv.
  red. ee. app quotient_is_preorder. rww 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.
  rw 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))).
  rww H7. wr Hb. app inc_rep_substrate. wri (W_compose H6 H15) H10.
  assert (inc (rep y) (source (canon_proj s))). rww H7. wr Hb.
  app inc_rep_substrate. wri (W_compose H6 H16) H10. rwi H5 H10.
  rwii W_first_proj H10. rwii W_first_proj H10. fprops. wrr H7. fprops. wrr H7.
  app surjective_pr6. rw H1. ir.  nin H4. exists (W (J y y0) (canon_proj s)).
  assert (inc (J y y0) (source (canon_proj s))). rw H7. fprops.
  ee. assert (source f = target (canon_proj s)). tv.
  rw H10. app inc_W_target. app function_canon_proj. wr (W_compose H6 H9).
  rw H5. rw W_first_proj. aw. fprops. fprops. sy; rww substrate_quotient_order.
  rww 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 (u = W x f). tv. wri H11 H14. assert (v = W y f). tv. wri H13 H15.
  assert (inc (rep x) (source (canon_proj s))).
  rww H7. wr Hb. app inc_rep_substrate. wri (W_compose H6 H16) H14.
  assert (inc (rep y) (source (canon_proj s))). rww H7. wr Hb.
  app inc_rep_substrate. wri (W_compose H6 H17) H15. rwi H5 H14. rwi H5 H15.
  rwi W_first_proj H14.  rwi W_first_proj H15.  rw H14; rw H15.
  rw 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. rwi product2_order_pr H23. ufi product2_order_r H23. ee.
  cp (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).
  wri H27 H29. ufi s H29. rwi first_proj_equivalence_related H29. ee. wrr H31.
  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. rww 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). rw inc_class. uf s.
  rw first_proj_equivalence_related. ee. wr H7. am. am. sy. aw. nin Hc; am.
  uf r. rw  product2_order_pr. red. ee. am. am. aw. rw H15.
  assert (inc (rep x) x). app (inc_rep_itself Hc H10).
  cp (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).
  wri H23 H25. ufi s H25. rwi first_proj_equivalence_related H25. ee. rww H27.
  aw. red in H3. ee. red in H22. ee. app H24. awi H21; ee; am. fprops. wrr H7.
  fprops. wrr H7.
```

```
Qed.
```

(d) With the hypothesis of (a), suppose that E *is an* ordered *set and that the following condition is satisfied:*

(C') The relations $x \leq y \leq z$ *and* $x \equiv z \pmod{\mathrm{S}}$ *in* E *imply* $x \equiv y \pmod{\mathrm{S}}$.

Show that $\mathrm{R}\{\!\{x, y\}\!\}$ *is then an* order *relation between* X *and* Y *in* E/S.

```
Definition quotient_order_axiom r s:=
  forall x y z, gle r x y -> gle r y z -> related s x z -> related s x y.

Lemma Exercise1_2d: forall r s,
  is_equivalence s -> order r -> substrate s = substrate r ->
  quotient_order_axiom r s ->
  order (quotient_order r s).
Proof. ir. assert (preorder r). red in H0. red. intuition.
  cp (quotient_is_preorder H H3 H1). red in H4. ee. red. ee. am. am. am.
  red. ee.  am. ir. rwi quotient_order_pr H7. rwi quotient_order_pr H8.
  red in H7. red in H8. ee. set_extens. nin (H12 _ H13). ee.
  nin (H10 _ H14). ee. assert (related s x0 x2). rw in_class_related.
  exists x. ee. wrr inc_quotient. am. am. am. red in H2.
  cp (H2 _ _ _ H15 H17 H18). cp (is_class_pr H H14 H11). rw H20.
  rw inc_class. app symmetricity. nin H; am.
  nin (H10 _ H13). ee. nin (H12 _ H14). ee. assert (related s x0 x2).
  rw in_class_related. exists y. ee. wrr inc_quotient. am. am. am. red in H2.
  cp (H2 _ _ _ H15 H17 H18). cp (is_class_pr H H14 H7). rw H20.
  rw inc_class. app symmetricity. nin H; 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 $\mathrm{X} \leq \mathrm{Y}$, 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* $\mathrm{S}\{\!\{x, y\}\!\}$ *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* $y' \in \mathrm{E}$ *such that* $x' \leq y'$ *and* $f(y) = f(y')$. *Let* $f = g \circ \phi$ *be the canonical decomposition of* f. *Then* g *is an isomorphism of* E/S *onto* $f(\mathrm{E})$ *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, increasing_fun f r r' ->
  quotient_order_axiom r (eq_rel_associated f).
Proof. ir. red. ir. red in H. ee. cp (inc_arg1_substrate H1).  rwi H5 H8.
  rw related_ea. rwi related_ea H2.  ee. am. am.  cp (H7 _ _ H2 H8 H0).
  cp (H7 _ _ H8 H9 H1). simpl in H11. simpl in H12. wri H10 H12.
  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 x'). rw related_ea.  ee.
  wr H2. app (inc_arg1_substrate H6). am. am. am. nin (H11 _ _ _ H6 H12).
  rwi related_ea H13. ee. exists x0. intuition. am. ir. ee.
  red in H0; red; ee;am. app equivalence_graph_ea. rww substrate_graph_ea.
  sy; am. ir. rwi 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 $g(\mathrm{X}) = f(x)$. The equivalence relation is defined by $a \in \mathrm{X}$ 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). rwii class_rep H9.
  assert (W (W (rep x) (canon_proj s)) g = W x g). rww H9. wri W_compose H10.
  wri H1 H10. am. 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.
  rwi related_ea H9. am. am. ir. wr (class_rep Ha H7). rw inc_class.
  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 equivalence classes, then $f(x) \leq f(y)$ implies $\mathrm{X} \leq \mathrm{Y}$. 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)). rww Hb. rww H4.
  assert (inc x (class s x)). app inc_itself_class.
  assert (inc (class s x) (quotient s)). app inc_class_quotient.
```

```
  rwi (Hf _ x H14) H13. cp (He _ H14). ee. wri H18 H10. rwi H16 H10.
  assert(inc y (substrate s)). rww Hb. rww H4.
  assert (inc y (class s y)). app inc_itself_class.
  assert (inc (class s y) (quotient s)). app inc_class_quotient.
  rwi (Hf _ y H21) H20. cp (He _ H21). ee. wri H25 H10. rwi H23 H10.
  red in H7. ee. wri H30 H10.  rwi quotient_order_pr H10. red in H10. ee.
  nin (H32 _ H11). exists x0. nin  H33. rwi (Hf _ x0 H21) H33. ee. am. am.
  assert (inc y (class s y)). app inc_itself_class. rwi (Hf _ y H21) H37.
  ee. wrr H39. red in H7. ee. wr H28. rww substrate_quotient_order.
  red in H7. ee. wr H28. rww substrate_quotient_order.
```

It is now easy to show that if g is a morphism, then the two conditions are true.

```
  ee. red. ir.
  assert (inc x (source f)). wr H4. app (inc_arg1_substrate H9).
  assert (inc y (source f)). wr H4. app (inc_arg2_substrate H9).
  cp (H6 _ _ H12 H13 H9). simpl in H14. rwi H11 H14.
  assert (inc x' (class s x')). app inc_itself_class. rww Hb. rww H4.
  nin (H8 _ _ _ H10 H13 H14  H15). exists x0. am.
  red. ir. assert (inc x (class s x)). app inc_itself_class. rww Hb. rww H4.
  cp (H8 _ _ _ H9 H10 H11 H12).  nin H13. exists x. exists x0. ee. tv. am. am.
```

We now show the converse.

```
  red. ir. assert (order (quotient_order r s)). app Exercise1_2d.
  ufi CC H7; ufi DD H7. nin H7.
  assert(substrate (quotient_order r s) = source g).  red in H0. ee. rw H11.
  rww substrate_quotient_order.
  assert (is_function g). red in H0; ee; am.
  assert (forall x y, inc x (source g) -> inc y (source g) ->
    gle (quotient_order r s) x y = gle r' (W x g) (W y g)). ir.
  wri H10 H12. wri H10 H13. rwii substrate_quotient_order H12.
  rwii substrate_quotient_order H13. nin (He _ H12). nin (He _ H13).
  wr H15. wr H17. ap iff_eq. ir. rwi quotient_order_pr H18. red in H18. ee.
  nin (H20 _ (inc_rep_itself Ha H18)). nin H21. rwi (Hf y x0 H13) H21. ee.
  rw H24. app H6. ir.  rw quotient_order_pr. red. ee. am. am.
  cp (H9 _ _ H14 H16 H18). nin H19; nin H19. ee. ir.
  rwi (Hf x x2 H12) H22. nin H22. nin H23. rwi H19 H24.
  nin (H7 _ _ _ H21 H23 H24). exists x3. ee. rw Hf. ee. am. am. rww H20.
  am. am. ee. am. am.  red. ee. am. ir.
  assert (gle r' (W x g) (W y g)). rw H15. wr order_reflexivity. rw H5.
  rw H1. rw target_compose. app inc_W_target. am.
  assert (gle r' (W y g) (W x g)). rw H15. rwi H15 H16. am.
  wri H12 H16. wri H12 H17. app (order_antisymmetry  H8 H16 H17). am. am. am.
  am. am. rw H5. rw H1. rw target_compose. tv. am.
Qed.
```

---

3. *Let* I *be an ordered set and let* $(\mathrm{E}_\iota)_{\iota\in\mathrm{I}}$ *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* $(\mathrm{E}_\iota)_{\iota\in\mathrm{I}}$*; for each* $x \in \mathrm{F}$*, let* $\lambda(x)$ *be the index* ι *such that* $x \in \mathrm{E}_\iota$*; and let* G *be the graph consisting of all the pairs* $(x, y) \in \mathrm{F}\times\mathrm{F}$ *such that either* $\lambda(x) < \lambda(y)$ *or else* $\lambda(x) = \lambda(y)$ *and* $x \leq y$ *in* $\mathrm{E}_{\lambda(x)}$*. 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* $(E_\iota)_{\iota\in I}$ *(relative to the ordering on* I*) and is denoted* $\sum_{\iota\in I} E_\iota$. *Show that the equivalence relation corresponding to the partition* $(E_\iota)_{\iota\in I}$ *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 2.7, 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_ι), r is an ordering on the index set, g is a family of orderings on E_ι. We shall denote the ordinal sum by F and its support (the disjoint union) by sF or $\bar{F}$. The quantity *lam* will be the function λ, i.e., the surjective function on $\bar{F}$ defined by $\lambda(x) = \mathrm{pr}_2 x$. Finally S the equivalence associated to λ. Assumption H2 says that the sets E_ι are non-empty.

```
Section Exercise1_3a.
Variables r f g: Bset.
Definition E13_lam := second_proj (disjoint_union f).
Definition E13_S:= eq_rel_associated (second_proj (disjoint_union f)).
Definition E13_F:= ordinal_sum r f g.
Definition E13_sF:= disjoint_union f.
Definition E13_H1:= ordinal_sum_axioms r f g.
Definition E13_H2:= is_graph f &
  (forall 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.
  rw source_second_proj. rw target_second_proj.
  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. rw target_second_proj.
  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 (singleton_eq 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.
  rw source_second_proj. rww substrate_ordinal_sum. rw H2. app Exercise1_3a3.
  red. uf E13_lam. rw source_second_proj. ir. cp Exercise1_3a1.
  rww W_second_proj. rww W_second_proj. ufi E13_F H10. awi H10. ee. nin H13.
  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 $(E_\iota)_{\iota\in I}$ of F". The set $\bar{F}$ is the union of f', the graph of $\iota \mapsto E_\iota \times \{\iota\}$, where f is the graph of $\iota \mapsto E_\iota$. Consider now a function f'' whose graph is f'. This function defines a partition. By abuse of notations, F is identified with $\bar{F}$, $E_\iota \times \{\iota\}$ with E_ι 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 $\mathrm{pr}_2 x = \mathrm{pr}_2 y$. 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 (singleton_eq H7);   rw (singleton_eq 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.
  awi H5; awi H4. ee. rwi (singleton_eq H9) H3. rwi (singleton_eq 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_ea. rw source_second_proj.
  app iff_eq. ir. nin H1; nin H2. rwii W_second_proj H3.
  rwii 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 $E_\iota \times \{\iota\}$. If ϕ is the canonical projection of $\bar{F}$ on $\bar{F}/S$, there exists a function g defined by $\lambda = g \circ \phi$ (canonical decomposition) because of the surjectivity of λ, it is unique. It is the function induced by λ by passing on the quotient. We

can restate it as: an element X of the quotient is of the form $\iota \mapsto E_\iota \times \{\iota\}$, and $g(X) = \iota$. 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. rww inc_quotient. rww is_class_rw.
  assert (substrate E13_S = disjoint_union f). uf E13_S. rw substrate_graph_ea.
  rw source_second_proj. 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.
  rwi (H4 y x H2) H9. ufi E13_S H9. rwi Exercise1_3a6 H9. ee.
  cp (du_index_pr H10). ee. app product_inc. rww H11. rw H11. fprops.
  rw (H4 _ x H2). uf E13_S. awi H9. ee. cp (singleton_eq H11). rw Exercise1_3a6.
  ee. am. uf E13_sF. uf disjoint_union. rw unionb_rw. exists (Q y).
  uf disjoint_union_fam. split. bw. bw. aw. ee. am. am. fprops. sy; am.
  ir. nin H2. nin H2. assert (sub a (disjoint_union f)). red. ir.
  uf disjoint_union.  rw unionb_rw. exists x. ee. uf disjoint_union_fam. bw.
  uf disjoint_union_fam. bw. wrr H3.
  ee. nin H. ee. cp (H5 _ H2). nin H6. exists (J y x). rw H3. fprops. rww H1.
  ir. uf E13_S. rw Exercise1_3a6. ap iff_eq. ir. ee. app H4. app H4.
  rwi H3 H5. awi H5. rwi H3 H6. awi H6. ee. rw (singleton_eq H10).
  rw (singleton_eq H8). tv. ir. ee.  rw H3. cp (du_index_pr H7).
  rwi H3 H5. awi H5.  nin H5. nin H10. rwi (singleton_eq H11) H8.
  aw. ee. am. rww H8. rw H8. fprops.
Qed.

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.
  rw source_foqc. tv.
Qed.

Lemma Exercise1_3a11:
  E13_lam =  compose (fun_on_quotient E13_S E13_lam) (canon_proj E13_S).
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.
  assert (Q (rep x) = W (rep x) E13_lam). uf E13_lam. rww W_second_proj.
  ap Exercise1_3a1. ufi E13_lam H3. rwi source_second_proj H3. rw H3.
  app inc_rep_substrate. rww W_foqc. wr H4.
```

```
  rwi (Exercise1_3a8 x H) H0. nin H0. nin H0. exists x0. ee. am. am.
  assert (inc (rep x) x). app nonempty_rep. nin H. ee. nin (H6 _ H0).
  exists (J y x0). rw H5. aw. ee.  fprops. am. fprops. set (t:=rep x) in *.
  rwi H5 H6. awi H6. ee.  ap (singleton_eq H8).
Qed.

Lemma Exercise1_3a13: E13_H2 ->  bijective (fun_on_quotient E13_S E13_lam).
Proof. ir.  cp  Exercise1_3a9. red. split. red.  split. am. rw source_foqc.
  ir. nin (Exercise1_3a12 H H1).  nin (Exercise1_3a12 H H2). ee.
  rw H8; rw H6; wr H9; rw H3;rw H7. tv.
  app surjective_pr6. rw source_foqc. rw target_foqc.  wrr Exercise1_3a3.
  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.
  cp Exercise1_3a7. cp (inc_rep_itself H6 H2).  set (t:= rep a) in H7.
  cp H7. ufi a H7. awi H7. rwi H4 H8. awi H8. ee. wr (singleton_eq H12).
  wr (singleton_eq H10). tv.
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.
  elim H12.  am. nin H7. red in H9. ee.  elim H12. rww H7. nin H9. am. am. am.
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.
  rww source_second_proj. rw H3. uf E13_F. split. ir. awi H4.  ee.
  assert (W x E13_lam = Q x). uf E13_lam. rww W_second_proj.
  assert (W x' E13_lam = Q x'). uf E13_lam. rww W_second_proj.
  assert (W y E13_lam = Q y). uf E13_lam. rww W_second_proj.
  nin H8. exists y.  ee. am.  aw. ee. am. am. left. wr H10. wr H6. rww H9. tv.
  exists x'. ee. am.  wr order_reflexivity. rww substrate_ordinal_sum. am.
  wr H6. rw H11. rw H9. sy. am. 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.
  rww substrate_ordinal_sum. am. exists y. ee. tv. tv. aw. ee. am. am. left.
  assert (W x E13_lam = Q x). uf E13_lam. rww W_second_proj.
  assert (W y E13_lam = Q y). uf E13_lam. rww 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* $(J_\lambda)_{\lambda\in L}$ *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 $y \le x$, we deduce $x \in E_2$. Obviously, for all $z \in E_2$ we have $z \le x$. 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.
  aw. 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.
  aw. 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_ω *is right directed for each* ω *of* I.

(d) An ordinal sum $\sum_{\iota\in I} E_\iota$ *is totally ordered if and only if* I *and each* E_ι *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* (λ,μ) *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_α *such that the set* $\{x,y\}$ *is bounded above (resp. bounded below) in* E_α*, the set* $\{x,y\}$ *has a least upper bound (resp. greatest lower bound) in* E_α*.*
>
> *(III) For each* $\alpha \in I$ *such that* E_α *contains a set of two elements which has no upper bound (resp. no lower bound) in* E_α*, the set of indices* $\lambda \in I$ *such that* $\lambda > \alpha$ *(resp.* $\lambda < \alpha$*) has a least element (resp. a greatest element)* β*, and* E_β *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 ω de E, E_ω soit filtrant à droite." This can be translated as:

An ordinal sum $\sum_{\iota\in I} E_\iota$ is right directed if and only if I is right directed and E_ω is right directed for each maximal element ω 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 $i \le k$ and $j \le k$. 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). awi H22. am.
  cp (related_ordinal_sum_order_id H H18). awi 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). awi H19.
  cp (du_index_pr H16). ee. rwi H2 H11. cp (H11 _ H20 H19).
  awi H17; awi 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 $x \in \mathrm{E}_a$, $y \in \mathrm{E}_b$ and $z = \sup(x, y)$. We have $z \in \mathrm{E}_c$, 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 $t \in \mathrm{E}_d$ we have $x < t$ and $y < t$ hence $z \leq t$ hence $c \leq d$.

```
Lemma ordinal_sum_pr1: forall r f g,
  ordinal_sum_axioms1 r f g ->
  forall i, inc i (domain f) -> exists y, inc y (V i f) &
    inc (J y i) (substrate (ordinal_sum r f g)).
Proof. ir. red in H. ee. nin (H1 _ H0). exists y. ee. am.
  cp (inc_disjoint_union H0 H2). aw.
Qed.


Lemma ordinal_sum_lattice1: forall r f g,
  ordinal_sum_axioms1 r f g ->
  lattice (ordinal_sum r f g) -> (lattice r).
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.
   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.
  apply by_cases with (gle r x y). exists y. app sup_comparable. ir.
  apply by_cases with (gle r y x). exists x. rw doubleton_sym.
  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.
  cp (related_ordinal_sum_order_id H3 H16). awi H25. am.
  ufi F H1. cp (related_ordinal_sum_order_id H3 H17). awi H25. am.
  ir. cp (inc_arg2_substrate H25). rwi H4 H27. nin (Ha _ H27). nin H28.
  assert (gle F (J x0 x) (J x2 t)). uf F. aw. ee. wrr Hb. wrr Hb. left.
  red. ee. am.  red. ir. wri H30 H26. elim H20. am.
  assert (gle F (J x1 y) (J x2 t)). uf F. aw. ee. wrr Hb. wrr Hb. left.
  red. ee. am.  red. ir. wri H31 H25. elim H19. am. cp (H18 _ H30 H31).
  ufi F H32. cp (related_ordinal_sum_order_id H3 H32). awi H33. am.
  cp (lattice_inf_pr H0 H15 H14).  fold F in H16. ee. red.
  apply by_cases with (gle r x y). exists x. app inf_comparable. ir.
  apply by_cases with (gle r y x). exists y. rw doubleton_sym.
  app inf_comparable. ir.
  set (z:= (inf 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 greatest_lower_bound_doubleton. ufi F H16.
  cp (related_ordinal_sum_order_id H3 H16). awi H25. am.
  ufi F H1. cp (related_ordinal_sum_order_id H3 H17). awi H25. am.
  ir. cp (inc_arg1_substrate H25). rwi H4 H27. nin (Ha _ H27). nin H28.
  assert (gle F (J x2 t) (J x0 x)). uf F. aw. ee. wrr Hb. wrr Hb. left.
  red. ee. am.  red. ir. rwi H30 H26. elim H19. am.
  assert (gle F (J x2 t) (J x1 y)). uf F. aw. ee. wrr Hb. wrr Hb. left.
  red. ee. am.  red. ir. rwi H31 H25. elim H20. am. cp (H18 _ H30 H31).
  ufi F H32. cp (related_ordinal_sum_order_id H3 H32). awi H33. am.
Qed.
```

With the same notations as before, assume that a and b cannot be compared, let $x \in \mathrm{A}_a$ $y \in \mathrm{E}_b$ and $z \in \mathrm{E}_c = \sup(x, y)$. Then $c = \sup(a, b)$. Every z' in E_c is an upper bound of x and y. Hence $\sup(x, y)$ is the smallest element of E_c.

```
Lemma ordinal_sum_lattice2: forall r f g,
  ordinal_sum_axioms1 r f g ->
  lattice (ordinal_sum r f g) ->
  (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))).
Proof. ir. cp (ordinal_sum_lattice1 H H0).  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.
  apply by_cases with (gle r i j).  ir. left. am. ir.
  apply by_cases with (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:= inf F (J x i) (J x0 j)) in H20. set (a:= inf r i j).
  set (B:= sup F (J x i) (J x0 j)) in H19. set (b:= sup r i j). ee.
  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).
  ufi F H21. cp (related_ordinal_sum_order_id H6 H21). awi H31. awi H32.
  app H27. cp (inc_arg1_substrate H25). rwi 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. rwi H35 H26. elim H13. am.
  assert (gle F (J x1 a) (J x0 j)). uf F. aw. ee. wrr Hb. wrr Hb. left.
  red. ee. am. red. ir. rwi H36 H25. elim H14. am.
  cp (H22 _  H35 H36).  uf F.  cp (related_ordinal_sum_order_id H6 H37).
  awi 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). rwi 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. aw. 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).
  awi H38. ap (order_antisymmetry H H38 H31).
  cp (inc_arg2_substrate H23). rwi Hb H31. cp (du_index_pr H31). ee.
  wri (H12 _ H32) H33. rwi Hd H33.
  cp (inc_arg1_substrate H21). rwi Hb H35. cp (du_index_pr H35). ee.
  wri (H12 _ H36) H37. rwi Hc H36. exists (P B). exists (P A). ee.
  red. ee. am. ir. rwii 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. aw. 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.
```

```
  elim H46. am.  ee. wrr H45. am. wrr Hd.
  red. ee. wrr Hc. ir. rwii H12 H39.
  assert (inc (J x1 a) (disjoint_union f)). app inc_disjoint_union.
  assert (gle F (J x1 a) (J x i) ). uf F. aw. ee. am. wrr Hb. left.
  red. ee. am. red. ir. rwi H41 H26. elim H13. am.
  assert (gle F (J x1 a) (J x0 j)). uf F. aw. ee. am. wrr Hb. left.
  red. ee. am. red. ir. rwi H42 H25. elim H14. am.
  cp (H22 _  H41 H42). ufi F H43. awi H43. ee.  nin H45. red in H45. ee.
  elim H46. sy. am. ee. am. am.
Qed.
```

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 $z \in \mathrm{E}_a$, 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. aw.
  cp (inc_arg1_substrate H2). cp (inc_arg2_substrate H2).
  cp (inc_arg1_substrate H3).
  assert (inc (J x i) (substrate F)). uf F. aw. app inc_disjoint_union. wrr H12.
  assert (inc (J y i) (substrate F)). uf F. aw. app inc_disjoint_union. wrr H12.
  assert (inc (J t i) (substrate F)). uf F. aw. 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. aw. ee.  wrr Hb. wrr Hb. right. ee. tv.
  am. assert (gle F (J x i) (J t i)). uf F. aw. 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 (related_ordinal_sum_order_id H6 H24). awi H26.
  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. aw. app inc_disjoint_union.
  wrr H12. cp (inc_arg2_substrate H28). am.
  assert (gle F (J y i) (J t0 i)). uf F. aw. ee.  wrr Hb. wrr Hb. right. ee. tv.
  am. assert (gle F (J x i) (J t0 i)). uf F. aw. 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. aw.
```

```
  cp (inc_arg2_substrate H2). cp (inc_arg1_substrate H2).
  cp (inc_arg2_substrate H3).
  assert (inc (J x i) (substrate F)). uf F. aw. app inc_disjoint_union. wrr H12.
  assert (inc (J y i) (substrate F)). uf F. aw. app inc_disjoint_union. wrr H12.
  assert (inc (J t i) (substrate F)). uf F. aw. app inc_disjoint_union. wrr H12.
  cp (lattice_inf_pr H0 H17 H16). ee.
  assert (gle F (J t i) (J y i)). uf F. aw. ee.  wrr Hb. wrr Hb. right. ee. tv.
  am. assert (gle F (J t i) (J x i)). uf F. aw. ee.  wrr Hb. wrr Hb. right.
  ee. tv. am. cp (H21 _ H22 H23). set (z:= inf F (J y i) (J x i)) in *.
  cp (related_ordinal_sum_order_id H6 H19). awi H25.
  cp (related_ordinal_sum_order_id H6 H24). awi H26.
  cp (order_antisymmetry H H25 H26).
  exists (P z). ap greatest_lower_bound_doubleton. app H11.
  ufi F H20. awi H20. ee. nin H29. red in H29. nin H29. elim  H30. am. wr H27.
  ee;am. am. ufi F H19. awi H19. ee. nin H29. red in H29. nin H29. elim  H30.
  am. wr H27.  ee;am. am. ir.
  assert (inc (J t0 i) (substrate F)). uf F. aw. app inc_disjoint_union.
  wrr H12. cp (inc_arg1_substrate H28). am.
  assert (gle F (J t0 i) (J y i)). uf F. aw. ee.  wrr Hb. wrr Hb. right. ee. tv.
  am. assert (gle F (J t0 i) (J x i)). uf F. aw. 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. wrr H27. am.
Qed.
```

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 $]a, \rightarrow[$.

```
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) ->
  (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.
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 x 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).
  exists (Q Z). ee. am. red. ee.  aw. Ztac.  ir. awi H26. Ztac.
  clear H26. aw. nin (Ha _ H27). ee.
  assert (gle 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 (related_ordinal_sum_order_id H7 H32). awi H33. am.
  Ztac. Ztac. am. am. exists (P Z). red. ee. rww H13.
  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. awi 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. aw.
  assert (inc (J x 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_inf_pr H0 H14 H15). ee. set (Z:=inf 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 H16).  ee. am.
  assert (glt r (Q Z) i). nin H22. am.  nin H20. am. ee.
  cp (du_index_pr H16). ee. rwi 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).
  exists (Q Z). ee. am. red. ee.  aw. Ztac.  ir. awi H26. Ztac.
  clear H26. aw. nin (Ha _ H27). ee.
  assert (gle F (J x1 x0) (J x i)). uf F. aw. ee. wrr Hb. am. left. am.
  assert (gle F (J x1 x0) (J y i)). uf F. aw. ee. wrr Hb. am. left. am.
  cp (H18 _ H30 H31). cp (related_ordinal_sum_order_id H7 H32). awi H33. am.
  Ztac. Ztac. am. am. exists (P Z). red. ee. rww H13.
  cp (du_index_pr H17). ee. am.  ir.  rwi H13 H26.
  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. aw. ee. am. am. left. am.
  assert (gle F (J x0 (Q Z)) (J y i)). uf F. aw. ee. am. am. left. am.
  cp (H18 _ H28 H29). ufi F H30. awi H30. ee.  nin H32. red in H32. ee.
  elim  H33. tv. ee. am. 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) &
    (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))) &
    (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_infimum (V i g) (doubleton x y)) &
```

```
  (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 k i)))
        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). rww 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 (du_index_pr H15). cp (du_index_pr H16). ee. wri H3 H17. wri H3 H18.
  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 H26).
  ufi F H26. cp (related_ordinal_sum_order_id H2 H27). cp (H25 _ H28 H29). am.
  rwi 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. rww H27. right. ee. am. app H33. rww H27.
  am. 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. wrr H27. ir.
ufi F H31; ufi F H38; awi H31; awi 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. rww H8. left. apply by_cases with (glt r (Q x) (Q t)). ir.
assert (inc (Q t) (Zo (domain f) (fun k  => glt r (Q x) k))). Ztac.
wr H3. app (inc_lt2_substrate H44). cp (H35 _ H45). awi H46.
red. ee. am. am. cp (inc_arg1_substrate H46). awi H47. am. am. am. am.
ir.  nin H42. elim H44. am. nin H40. elim H44. rww H27. ee.
cp (du_index_pr  H41).  ee. wri H42 H48. elim (H29 _ H48). ee. am. rww H27.
am. am. am. am. am. am. am.
cp (H10 _ _ H17 H18). nin (equal_or_not (Q y) a).
assert (gle F x y). uf F. aw.  ee. am. am. left. red. ee. rww H29. am.
exists y. app sup_comparable. nin (equal_or_not (Q x) a).
assert (gle F y x). uf F.  aw.  ee. am. am. left. red. ee. rww H30. intuition.
exists x. rw doubleton_sym. app sup_comparable.
nin H28. assert (gle r  (Q y) (Q y)). wr order_reflexivity. rww H3. am.
cp (order_antisymmetry H H24  (H25 _ H28 H31)). elim H29; am.
nin H28. assert (gle r  (Q x) (Q x)). wr order_reflexivity. rww H3. am.
cp (order_antisymmetry H H23 (H25 _ H31 H28)). elim H30. am.
nin H28; nin H28; nin H28. fold a in H28. red in H28. ee.
assert (inc (J x0 a) (disjoint_union f)). app inc_disjoint_union. wr H3.
app (inc_arg2_substrate H23). wrr H8. wr H3.  app (inc_arg2_substrate H23).
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. awi H34. ufi F H35. awi 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.
```

Let's show the existence of an infimum.

```
ee. red.  rwi Hb H15. rwi Hb H16.
cp (du_index_pr H15). cp (du_index_pr H16). ee. wri H3 H17. wri H3 H18.
cp (lattice_inf_pr H9  H17 H18). ee. set (a:= inf r (Q x) (Q y)) in *.
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).
ufi F H26. cp (related_ordinal_sum_order_id H2 H27). cp (H25 _ H28 H29). am.
rwi 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) t(P x) &gle (V (Q x) g) t (P y))).
nin H28. nin H28.  cp (H12 _ _ _ _ H17 H28 H29).
wri H8  H21;wri H8  H19. cp (inf_pr (H7 _ H17) H21 H19 H30).
ee.  set (z:= inf (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_arg1_substrate  H31). am. exists (J z (Q x)).
ap greatest_lower_bound_doubleton. am. uf F. aw. ee.  wrr Hb.  am. right.
ee. tv. am. uf F. aw. ee.  wrr Hb. am. right. ee.  am. am. ir.
ufi F H35; ufi F H36; awi H35; awi H36. ee. uf F. aw. ee. am.  wrr Hb.
nin H40.  left. am. nin H38. left. rww H27. right. ee. am. rw H40. app H33.
rww H27. wr H38. am. wr H40. am. am. am. am. am. am. am.
assert (forall t, inc t (V (Q x) f) -> ~ (gle (V (Q x) g) t (P x) &
  gle (V (Q x) g) t (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) (disjoint_union f)). app inc_disjoint_union. wrr H8.
assert(Hc:sub (Zo (domain f) (fun k => glt r k (Q x))) (substrate r)).
```

```
  rw H3. app Z_sub.  red in H31. ee. awi H35. awi H31. Ztac.  clear H31.
  exists  (J x1 x0). ap greatest_lower_bound_doubleton. am. uf F. aw. ee. am.
  am. left. am. uf F. aw. ee. am. am. left. wrr H27. ir.
  ufi F H31; ufi F H38; awi H31; awi H38. ee. uf F. aw. ee. am. am.
  nin (equal_or_not x0 (Q t)). right. ee. sy;am. wr H43. app H33.
  cp (du_index_pr H38).  ee. rw H43. rww H8. left.
  apply by_cases with (glt r (Q t) (Q x)). ir.
  assert (inc (Q t) (Zo (domain f) (fun k  => glt r k (Q x)))). Ztac.
  wr H3. app (inc_lt1_substrate H44). cp (H35 _ H45). awi H46.
  red. ee. am. intuition. am. cp (inc_arg2_substrate H46). awi H47. am. am.
  am. ir.  nin H42. elim H44. am. nin H40. elim H44. rww H27. ee.
  cp (du_index_pr  H31). ee. rwi H42 H48. elim (H29 _ H48). ee. wrr H42.
  wrr H42.  am. am. am. am. am. am. am.
  cp (H10 _ _ H17 H18). nin (equal_or_not (Q y) a).
  assert (gle F y x). uf F. aw.  ee. am. am. left. red. ee. rww H29. intuition.
  exists y.  rw doubleton_sym. app inf_comparable.  nin (equal_or_not (Q x) a).
  assert (gle F x y). uf F.  aw.  ee. am. am. left. red. ee. rww H30. am.
  exists x.  app inf_comparable.
  nin H28. assert (gle r  (Q x) (Q x)). wr order_reflexivity. rww H3. am.
  cp (order_antisymmetry H H23  (H25 _ H31 H28)). elim H30; sy;am.
  nin H28. assert (gle r  (Q y) (Q y)). wr order_reflexivity. rww H3. am.
  cp (order_antisymmetry H H24 (H25 _ H28 H31)). elim H29. sy;am.
  nin H28; nin H28; nin H28. fold a in H31. red in H31. ee.
  assert (inc (J x1 a) (disjoint_union f)). app inc_disjoint_union. wr H3.
  app (inc_arg1_substrate H23). wrr H8. wr H3.  app (inc_arg1_substrate H23).
  exists (J x1 a).  ap greatest_lower_bound_doubleton. am. uf F. aw. ee. am. am.
  left. red. ee. am. intuition. uf F. aw. ee. am. am. left. red. ee. am.
  intuition.  ir.  cp (H26 _ H34 H35).
  ufi F H34. awi H34. ufi F H35. awi H35. uf F. aw. ee. am. am.
  nin (equal_or_not a (Q t)). right. ee. sy;am. wr H41. app H32. rw H8. rw H41.
  cp (du_index_pr H35). ee; am.  wr H3. app (inc_arg1_substrate H23).
  left.  red. ee. am. intuition. am. am.
Qed.
```

---

4. * *Let* E *be an ordered set, and let* $(\mathrm{E}_\iota)_{\iota\in\mathrm{I}}$ *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 $\iota \neq \kappa$ *and if* $x \in \mathrm{E}_\iota$ *and* $y \in \mathrm{E}_\kappa$*, then* x*,* y *are comparable; and that if, for example,* $x \leq y$*,* $y' \in \mathrm{E}_\kappa$*, and if* $y' \neq y$*, then also* $x \leq y'$ *(use the fact that there exists no partition of* E_κ *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_ι) *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 $\mathrm{E} = \mathrm{F} \times \mathrm{G}$ *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_ι are the equivalence classes of S.

```
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. ir. uf not_comp_rel. app iff_eq. 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.
  ir. red. uf Exercice1.Sgraph. uf graph_on. ee. Ztac. fprops. red.
  aw. exists (Exercice1.chain_pair x y). ee. simpl. intuition. simpl. tv.
  simpl.  tv.
Qed.
```

We restate "$\iota \neq \kappa$ and if $x \in \mathrm{E}_\iota$ and $y \in \mathrm{E}_\kappa$, 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 $\mathrm{R}\{\!\{x, y\}\!\}$ implies $\mathrm{S}\{\!\{x, y\}\!\}$.

```
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. wrr 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 $a \in \mathrm{A}$ and $b \in \mathrm{B}$. 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 $a' \in \mathrm{A}$ and $b' \in \mathrm{B}$ 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 $b' \in \mathrm{A}$, the result follows by induction, otherwise $b' \in \mathrm{B}$ 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, inc u a -> inc v b -> gle r u v \/ gle r v u) ->
    a = emptyset \/ b = emptyset \/ nonempty (intersection2 a b).
Proof. ir. nin (emptyset_dichot a). left. am. right. nin (emptyset_dichot b).
  left. am. right. nin H3. nin H4. cp (ncr_properties H). ee.
  assert (Ha:is_class (ncr_equiv r) (union2 a b)). rw H1.
  app is_class_class. rww H6.
  assert (related (ncr_equiv r) y0 y1). rw in_class_related.
  exists (union2 a b). ee. am. app union2_first. app union2_second. am.
  red in H9. ufi ncr_equiv H9. ufi Exercice1.Sgraph H9. ufi graph_on H9. Ztac.
  awi H11. red in H11. nin H11. ee.
  assert (inc (Exercice1.chain_head x) a). rw H12. am. clear H12.
  assert (inc (Exercice1.chain_tail x) b). rw H13. am. clear H13.

  assert (exists u, exists v, inc u a & inc v b & (not_comp_rel r) u v).
  nin x. simpl in H11. simpl in H12. simpl in H14. exists b0. exists b1.
  intuition. simpl in H11. simpl in H14. simpl in H12. ee.
  apply by_cases with (inc (Exercice1.chain_head x) a). ir. app IHx.
  ir. set (v:= (Exercice1.chain_head x)) in *.
  cp (H8 _ _ H11). rwi is_class_rw Ha. ee. wri H19 H16. assert (inc v b).
  nin (union2_or H16). elim H15. ee. am. am. exists b0. exists v.
  intuition. app union2_first. am. nin H13. nin H13. ee. red in H16.
  ee. nin H18. exists x0. app intersection2_inc. rww H18. elim H18. app H2.
Qed.
```

Let C be a class for S, $x \in E - C$, 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', order r ->
  inc x (substrate r) -> related (ncr_equiv r) y y' -> gle r x y ->
  related (ncr_equiv r) x y \/ gle r x y'.
Proof. ir.  cp (ncr_properties H). ee. set (C:= class (ncr_equiv r) y).
  set (A:=Zo C (fun z => gle r x z)). set (B:=Zo C (fun z => gle r z x)).
  assert (forall u v, inc u A -> inc v B -> gle r u v \/ gle r v u).
  ir. ufi A H7. Ztac.  clear H7. ufi B H8. Ztac. right.
  app (order_transitivity H H11 H10).
  nin (p_or_not_p (related (ncr_equiv r) x y)). left. am. right.
  assert(inc y (substrate r)). app (inc_arg2_substrate H2).
  assert (union2 A B = class (ncr_equiv r) y). set_extens. nin (union2_or H10).
  ufi A H11. Ztac. am. ufi B H11. Ztac. am.
  assert (inc x0 (substrate r)). wr H4. app (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. am. exists x0. ee. rww related_class_eq.
  app reflexivity_e. rww 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.
  app reflexivity_e.  rww H4. red in H3; ee; am.  elim (emptyset_pr H12).
  nin H11. assert (inc y' C). uf C. rw inc_class. am. red in H3; ee; am.
  ufi C H12. wri H10 H12. nin (union2_or H12). ufi A H13. Ztac. am.
  rwi H11 H13. elim (emptyset_pr H13). nin H11.
  cp (intersection2_first H11). ufi A H12. Ztac. clear H12.
  cp (intersection2_second H11). ufi B H12. Ztac. elim H8.
  rw (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 $\mathrm{R}(x', y')$. 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. wrr related_class_eq.
  assert (related (ncr_equiv r) x' x).  app symmetricity.
  nin (Exercice1_4a3 H H9 H14 H12). elim H2.
  wrr related_class_eq. app transitivity.  exists x'. ee. am.
  app symmetricity.  app transitivity.  exists y'. ee. am. am.
  wri (order_antisymmetry H H13 H15) H1. elim H2. wrr related_class_eq.
  app symmetricity.  elim H2. wrr related_class_eq.
  app transitivity.  exists x'. ee. am. app transitivity. exists y'. ee.
  rww related_class_eq.  app reflexivity_e. rww H5. app symmetricity.
  app reflexivity_e. rww 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 $x \in \mathrm{X}$ and $y \in \mathrm{Y}$, the compatibility condition says $\mathrm{X} \leq \mathrm{Y}$ 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. rww H1.
  app (inc_arg1_substrate H5).
  assert (class (ncr_equiv r) x <> class (ncr_equiv r) y). red. ir.
  elim H7. app symmetricity. rww related_class_eq. sy; am.
  cp (Exercice1_4b1 H H6 H8 H9 H4). cp (order_antisymmetry H H5 H10).
  rww 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. rwi (inc_quotient x H0) H5.  rwi (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 y) <> class (ncr_equiv r) (rep x)).
  intuition. 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 $\mathrm{E} = \mathrm{F} \times \mathrm{G}$. Let's determine the set of components. We have $x \leq y$ if and only if $\mathrm{pr}_1 x \leq \mathrm{pr}_1 y$ and $\mathrm{pr}_2 x \leq \mathrm{pr}_2 y$. We exclude the case where the sets are empty. If G is a singleton, then $\mathrm{pr}_2 x \leq \mathrm{pr}_2 y$ 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 $y \in \mathrm{C}$. In fact, if $a < b$, then $\mathrm{R}\{(a, c'), (b, b')\}$ and $\mathrm{R}\{(a, c'), (c, b')\}$, so that (b, b') and (c, b') are in the same class. On the other hand, if $a' < b'$, then $\mathrm{R}\{(c, a'), (b, b')\}$ and $\mathrm{R}\{(c, a'), (b, c')\}$, so that (b, b') and (b, 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 $\{b, c, d\} \times \{b', c'\}$, minus the greatest and least elements are in the same class. By symmetry, if $d' \in \mathrm{F}$, 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 $x \in \mathrm{E}$ and $y \in \mathrm{E}$ 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* $\mathfrak{I}$ *be the set of free subsets of* E. *Show that, on* $\mathfrak{I}$, *the relation "given any* $x \in \mathrm{X}$, *there exists* $y \in \mathrm{Y}$ *such that* $x \leq y$*" is an order relation between* X *and* Y, *written* $\mathrm{X} \leq \mathrm{Y}$. *The mapping* $x \to \{x\}$ *is an isomorphism of* E *onto a subset of the ordered set* $\mathfrak{I}$. *If* $\mathrm{X} \subset \mathrm{Y}$ *where* $\mathrm{X} \in \mathfrak{I}$ *and* $\mathrm{Y} \in \mathfrak{I}$, *show that* $\mathrm{X} \leq \mathrm{Y}$. *The ordered set* $\mathfrak{I}$ *is totally ordered if and only if* E *is totally ordered, and then* $\mathfrak{I}$ *is canonically isomorphic to* E.

We restate the definition as: if $x \in \mathrm{X}$ and $y \in \mathrm{X}$ 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:=
  Zo (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 follow from the fact that if $x \in X, y \in Y, x \leq y$ and $x' \in X, y \leq x'$ w have $x \leq x'$ by transitivity, then $x = x'$ 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.
  cp (order_transitivity H H8 H10).  ufi set_of_free_subsets H4.  Ztac.
  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. wrr order_reflexivity.
  ufi set_of_free_subsets H0. Ztac. rwi powerset_inc_rw H4. app H4. am. am.
  ir. exists x0. split. am. wrr order_reflexivity.
  ufi set_of_free_subsets H1. Ztac. rwi powerset_inc_rw H4. app H4.
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.
  awi 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 $\mathfrak{I} - \{\emptyset\}$.

```
Lemma Exercise1_5b: forall r x, order r ->
  inc x (substrate r) -> inc (singleton x) (set_of_free_subsets r).
Proof. ir. uf set_of_free_subsets. Ztac. app powerset_inc. red. ir.
  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. rw af_source. rw af_target. 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 $X \subset Y$ then $X \leq Y$ (this is trivial). If E is totally ordered so is $\mathfrak{I}$. In fact, the empty set is the least element of $\mathfrak{I}$; two non-empty sets are singletons, and singletons are compared according to there elements. The converse is trivial. Bourbaki says that $\mathfrak{I}$ is canonically isomorphic to E in this case. This is obviously wrong: as noted above $x \mapsto \{x\}$ is an isomorphism between E and $\mathfrak{I} - \{\emptyset\}$.

```
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. 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. rww 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 H3; Ztac. clear H3. rwi powerset_inc_rw H9.
  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.
```

```
  assert (y = singleton y1). set_extens. red in H6. rw (H6 _ _ H8 H15). fprops.
  rw (singleton_eq H15). am.  rw H14; rw H15.
  nin (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* $\mathscr{A}(\mathrm{E},\mathrm{F})$ *be the subset of the product ordered set* F^{E} *consisting of the* increasing *mappings of* E *into* F.

We change the definition of $\mathscr{A}(\mathrm{E},\mathrm{F})$: it will be a subset of $\mathscr{F}(\mathrm{E};\mathrm{F})$, 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.
  rwi 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.
  nin (set_of_functions_inc H7). ee. ufi sof_value H6.
  wr H15. wr H11. rw inv_corr_value_pr. rw inv_corr_value_pr. awi H6.
  wri H11 H6. wri H15 H6. ufi corr_value H6. awi H6.
  wr (corr_propc x).  wr (corr_propc x0).  rw H9; rw H10; rw H13; rw H14; am.
  am. am.  am. am. am. am.
  ir. ee. uf increasing_mappings_order. aw.
  ufi set_of_increasing_mappings H1. Ztac. clear H1.
  ufi set_of_increasing_mappings H2. Ztac. clear H2.
  uf function_order. red. uf graph_on. Ztac. aw. ee. fprops. am. am.
  cp (sof_value_pr H4). cp (sof_value_pr H1). ee.  wri H13 H3. wri H10 H3.
  rwi 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* $\mathscr{A}(\mathrm{E},\mathrm{F}\times\mathrm{G})$ *is isomorphic to the product ordered set* $\mathscr{A}(\mathrm{E},\mathrm{F})\times\mathscr{A}(\mathrm{E},\mathrm{G})$.

Given a function $f:\mathrm{E}\to\mathrm{F}\times\mathrm{G}$, we can consider the two projections $f_1:\mathrm{E}\to\mathrm{F}$ and $f_2:\mathrm{E}\to\mathrm{G}$. We first show that $f\mapsto(f_1,f_2)$ is a bijection $\mathscr{F}(\mathrm{E};\mathrm{F}\times\mathrm{G})$ onto $\mathscr{F}(\mathrm{E};\mathrm{F})\times\mathscr{F}(\mathrm{E};\mathrm{G})$.

```
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). rwi H1 H3. awi 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). rwi H1 H4. awi 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.
  ir. nin (set_of_functions_inc H1). nin (set_of_functions_inc H2).  ee.
  wr H11; wr H8; wri H11 H3; wri H8 H3; repeat rwi inv_corr_value_pr H3.
  cp (pair_extensionality_first H3).  cp (pair_extensionality_second H3).
  rewrite  correspondence_extensionality1 in H12, H13 |- *.
  app funct_extensionality. rww H6. rww  H7. rw H9. ir.
  cp (Exercice1_6a H4 H9 H10). cp (Exercice1_6a H5 H6 H7). ee.
  app pair_extensionality. assert (inc (W x1 x) (product b c)).  wr H10.
  app inc_W_target. rww 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.
  wr H26. wr H21. rww H13. am. am.
 (* surjectivity *)  app surjective_af_function. ir. awi H1. ee.
  nin (set_of_functions_inc H2). nin (set_of_functions_inc H3).  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. aw. ee. fprops. wr H10. app inc_W_target.  rww 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 H13 H14 H15). 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.
  rw H21. uf f. aw. wrr H9. wrr H9.  aw. wr H8.
  rewrite correspondence_extensionality1. app funct_extensionality. ir.
  rw H22. uf f. aw. wrr H6. wrr H6.
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 $f \mapsto (f_1, f_2)$ induces a bijection $\mathscr{A}(\mathrm{E}, \mathrm{F} \times \mathrm{G})$ onto $\mathscr{A}(\mathrm{E}, \mathrm{F}) \times \mathscr{A}(\mathrm{E}, \mathrm{G})$. 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'').
```

```
Proof. ir. red in H2. nin H2; nin H3; nin H4; nin H5; nin H6.
  symmetry in H5; symmetry in H6. bwi H6.
  cp (Exercice1_6a H2 H5 H6). ee. red. ee.  am. am. am. tv. tv.  red. simpl.
  ir. rw H12. rw H12. red in H7. ee. rwi H5 H7. cp (H7 _ _ H14 H15 H16).
  rwi product2_order_pr H17. red in H17. ee. am. am. am.
  red. ee. am. am. am. tv. tv.  red. simpl.
  ir. rw H13. rw H13. red in H7. ee. rwi H5 H7. cp (H7 _ _ H14 H15 H16).
  rwi product2_order_pr H17. red in H17. ee. am. 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'')).
  cp (Exercice1_6b  (a:=substrate r) (b:=substrate r') (c:=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.
  rwi 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.
  rw 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 (secnd_projection x1 (substrate r) (substrate r'')).
  ee.  am. tv. tv. am. tv. am. am. am. am. am. app order_product2_order.
  ufi set_of_increasing_mappings H4.  Ztac. bwi H7. am. am. am. fprops.
Qed.

Lemma Exercice1_6f: forall  r r' r'', order r -> order r' -> order r'' ->
  bijective (two_projections_increasing r r' r'').
Proof. ir.  cp (Exercice1_6e H H0 H1).
  cp (Exercice1_6c (substrate r) (substrate r') (substrate r'')). nin H3.
  assert (is_function (two_projections_increasing r r' r'')).
  uf two_projections_increasing. app function_restriction2.
  red. split. uf two_projections_increasing. app injective_restriction2.
  uf two_projections_increasing. app surjective_pr6. rw source_restriction2.
  rw target_restriction2. ir.
  assert (inc y (target  (two_projections (substrate r) (substrate r')
    (substrate r'')))). simpl. awi H6. ee. ufi set_of_increasing_mappings H7.
  ufi set_of_increasing_mappings H8. aw. fprops.  ee. am. clear H8. Ztac. am.
  Ztac. am. nin (surjective_pr2 H4 H7). nin H8.
  assert (inc x (set_of_increasing_mappings r (product2_order r' r''))).
```

```
  ufi two_projections H9. rwii W_af_function H9.
  ufi two_projections H8. rwi af_source H8.
  rw set_of_increasing_mappings_pr. nin (set_of_functions_inc H8). ee.
  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:= secnd_projection x0 (substrate r) (substrate r'')) in *.
  rw product2_order_pr. red. split. wr H12. app inc_W_target. split.
  wr H12. app inc_W_target. rwi H11 H20; rwi H11 H21. wr H18. wr H19.
  wr H18. wr H19. rwi H9 H6. awi H6. ee.
  rwi set_of_increasing_mappings_pr  H23. nin H23. ee.
  rwi correspondence_extensionality1 H28. wr H28. red in H27. ee. app H33.
  wrr H31. wrr H31. am. am.
  rwi set_of_increasing_mappings_pr  H24. nin H24. ee.
  rwi correspondence_extensionality1 H28. wr H28. red in H27. ee. app H33.
  wrr H31. wrr H31. am. am. am. am. am. am. am. am. app order_product2_order.
  app Exercice1_6b. exists x. ee. am. rww 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. rww imo_substrate.  rww imo_substrate.
  app imo_order. app imo_order. uf 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). rww W_restriction2. rww W_restriction2. clear H6.
  assert (Ha:= H3). assert (Hb:= H4).
  rwii set_of_increasing_mappings_pr H3. rwii set_of_increasing_mappings_pr 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. rww W_af_function. rww 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.
  rw 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. am.
  assert (inc (corr_value (secnd_projection x0 (substrate r) (substrate r'')))
   (set_of_increasing_mappings r r'')).  rw set_of_increasing_mappings_pr.
  exists (secnd_projection x0 (substrate r) (substrate r'')). ee. am.
  tv. tv. am. tv. am. 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.
  tv. tv. am. tv. am. am.
  assert (inc (corr_value (secnd_projection x1 (substrate r) (substrate r'')))
   (set_of_increasing_mappings r r'')).  rw set_of_increasing_mappings_pr.
  exists (secnd_projection x1 (substrate r) (substrate r'')). ee. am.
  tv. tv. am. tv. am. am.
  ee.  fprops. am. am. fprops. am. am. am. am. red. ee. am. am. tv. tv. tv.
  tv. ir. rw H24. rw H19. red in H35. ee.  cp (H42 _ H36).
  rwi product2_order_pr H43. red in H43.  ee; am. am. am. am. am. red. ee.
  am. am. tv. tv. tv. tv.  ir. rw H25. rw H20. red in H35. ee.  cp (H42 _ H36).
  rwi product2_order_pr H43. red in H43.  ee; am. am. am.
  (* converse *) ir. ee. rww H13. rww H9. red. ee. am. am. am. am. am. am.
  ir. red in H34. ee. cp (H47 _ H41). rwi H25 H48. rwi H20 H48.
  red in H36. ee. cp (H54 _ H41). rwi H24 H55. rwi H19 H55.
  rw product2_order_pr. red. ee. wr H11. app inc_W_target. rww H10.
  wr H7. app inc_W_target. rww H6. am. am. am. am. am. am. am. am. am. am.
  am. am. am. am. am. am. ufi set_of_increasing_mappings Hb. Ztac.
  bwi H26. am. am. am. ufi set_of_increasing_mappings Ha. Ztac.
  bwi H26. am. am. am. am. am. am. am.
Qed.
```

(b) Show that if E, F, G *are three ordered sets, then the ordered set* $\mathscr{A}(\mathrm{E}\times\mathrm{F},\mathrm{G})$ *is isomorphic to the ordered set* $\mathscr{A}(\mathrm{E},\mathscr{A}(\mathrm{F},\mathrm{G}))$.

Let's show that $\mathrm{S}=\mathscr{A}(\mathrm{E}\times\mathrm{F},\mathrm{G})$ is isomorphic to the ordered set $\mathrm{T}=\mathscr{A}(\mathrm{E},\mathscr{A}(\mathrm{F},\mathrm{G}))$. We shall assume E and F non-empty. For otherwise, the product $\mathrm{E}\times\mathrm{F}$ is empty, case where there is a single element in S. If F is empty, $\mathscr{A}(\mathrm{F},\mathrm{G})$ has a single element (the empty function) and $\mathscr{A}(\mathrm{E},\mathscr{A}(\mathrm{F},\mathrm{G}))$ has a single element (that maps everything to the empty function). Assume E empty. Then $\mathscr{A}(\mathrm{E},\mathscr{A}(\mathrm{F},\mathrm{G}))$ 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 $f : r\times r' \to r''$ if a function with source $\mathrm{E}\times\mathrm{F}$ 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 $\mathrm{E}\times\mathrm{F}$, 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 $x\in\mathrm{E}$. 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 -> order r' ->
  nonempty (substrate r) -> nonempty (substrate r') ->
  increasing_fun f (product2_order r r') r'' ->
 ( (domain (source f)) = substrate r & (range (source f)) = substrate r').
Proof. ir. red in H3. ee. wr H6. bw. rw domain_product. tv. am.
  wr H6. bw. rw range_product. tv. am.
Qed.

Lemma Exercice1_6i: forall f x r r' r'',  order r -> order r' ->
  nonempty (substrate r) -> nonempty (substrate r') ->
  increasing_fun f (product2_order r r') r'' ->
  inc x (substrate r) -> 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.
  wri H5 H4. cp (function_spf H12 H4). red. ee. am. am. am. rw source_spf.
  sy; am. rw target_spf. am. red. rw source_spf. ir. rww W_spf. rww W_spf.
```

```
  assert (inc (J x x0) (source f)). wr H9. bw. aw. ee. fprops. wrr H5. wrr H6.
   assert (inc (J x y) (source f)). wr H9. bw. aw. ee. fprops. wrr H5. wrr H6.
  app H11. rw product2_order_pr. red. bwi H9. rw H9. ee. am. am. aw.
  wrr order_reflexivity. wrr H5. aw. am. am.
Qed.


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'')).
Proof. ir.  nin (Exercice1_6h H H0 H1 H2 H3). red in H3. ee.
  assert (partial_fun_axioms f). red. split. am. wr H8. bw.
  exists (substrate r). exists (substrate r'). tv.
  cp (function_spfa H11). red. ee. am.  rw source_spfa. rw H4. fprops.
  rw target_spfa. rw H5. uf set_of_increasing_mappings. wr H9. app Z_sub.
  red. ir. ufi image_by_fun H13. awi H13. nin H13. ee. red in H14.
  cp (W_pr H12 H14). rwi W_spfa H15. rw H15. rw set_of_increasing_mappings_pr.
  exists (second_partial_fun f x0). ee. app function_spf. rww H4.
  rw source_spf. rww H5. rw target_spf. sy; am.
  app (Exercice1_6i (r:=r) (f:=f) (x:=x0)). red; intuition. tv. am. am. am.
  rww H4. fprops.
Qed.
```

We consider now $\Phi =$*second_partial_map* (this is the bijection from $\mathscr{F}(\mathrm{E}\times\mathrm{F};\mathrm{G})$ onto $\mathscr{F}(\mathrm{E},\mathscr{F}(\mathrm{F};\mathrm{G}))$. For each $a\in\mathrm{E}$, $\Phi(f)(a)$ is in $\mathscr{F}(\mathrm{F};\mathrm{G})$; if f is increasing this is in $\mathscr{A}(\mathrm{F},\mathrm{G})$. Thus we can restrict $\Phi(f)$ as a function $\overline{\Phi(f)}$ from E into $\mathscr{A}(\mathrm{F},\mathrm{G})$. The mapping $f\mapsto\overline{\Phi(f)}$ 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 $a\le a'$ and $b\le b'$ implies $f_a(b)\le f_a(b')\le f_{a'}(b')$ so that f is increasing. Conversely, if f is increasing, then f_a is increasing since if $b\le b'$ then $f_a(b)\le f_a(b')$, using $a\le a$; and $a\mapsto f_a$ is increasing since if $a\le a'$ then $f_a(b)\le f_{a'}(b)$, using $b\le b$. 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_propc. am. am. rw H9. clear H9. clear f.
  cp (Exercice1_6j H H0 H2 H3 H7).
```

```
  nin (Exercice1_6h H H0 H2 H3 H7).
  assert (Ha: partial_fun_axioms x). red. split. am.
  rw 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.
  rw set_of_increasing_mappings_pr. exists g. ee. am. uf g.
  rww source_restriction2. uf g. rw target_restriction2. rww imo_substrate.
  red. ee. am. am. app imo_order. uf g. rww source_restriction2.
  rw imo_substrate.  uf g. rww target_restriction2. am. am. red. uf g.
  rw source_restriction2. ir. rw W_restriction2. rw W_restriction2.
  rw W_spfa. rw W_spfa. rw imo_pr. rw inv_corr_value_pr. rw inv_corr_value_pr.
  uf function_order_r.
  cp (Exercice1_6i H H0 H2 H3 H7 H13). cp (Exercice1_6i H H0 H2 H3 H7 H14).
  cp H16. red in H16. cp H17. red in H17. ee.
  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. am.  am. am. sy; am. sy; am. sy; am.
  sy; am. ir. rw W_spf. rw 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. aw. ee. fprops. am. am. aw. ee. fprops.
  am. am.  aw. aw. wrr order_reflexivity. am. rww H10. rww H11. am.
  rww H10. rww H11. am. am. am.  rww H10. am.  rww H10. am. am. am. am. tv.
  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. rw af_source. rw af_target. ee.
  app af_function. app Exercice1_6k. tv. tv. red. split.
  (* injectivity *) app injective_af_function.  app Exercice1_6k. ir.
  rwi correspondence_extensionality1 H6.
  rwi set_of_increasing_mappings_pr H4. nin H4. ee. wri H10 H6. wr H10.
  rwi set_of_increasing_mappings_pr H5. nin H5. ee. wri H14 H6. wr H14.
  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. aw. app corr_propc. am. am. fold f1 in H6. rwi 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. aw. app corr_propc. am. am. fold f1 in H6. rwi 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.
rw source_spfa. rw source_spfa. rw H7; rw H11; tv.
rw target_spfa. rw target_spfa. rw H8; rw H12;rw H7; rw H11; tv.
rw source_spfa. 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.
app funct_extensionality.  rww H11. rww H12. rw H7. ir. bwi H6. awi H6. ee.
assert (inc (P x1) (domain (source x))). rww H15. cp (W_spfa Ha H22).
assert (inc (P x1) (domain (source x0))). rww H16. cp (W_spfa Hb H24).
rwi H19 H23. rwi H25 H23. rwi correspondence_extensionality1 H23. clear H25.
assert (x1 = J (P x1) (Q x1)).  sy.  app pair_recov. rw H25.
assert (inc (Q x1) (range (source x))). rww H18. wr (W_spf Ha H22 H26).
assert (inc (Q x1) (range (source x0))). rww H17.  wr (W_spf 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.
rwi set_of_increasing_mappings_pr H4. nin H4. ee.
assert (substrate (product2_order r r') =
  product (substrate r) (substrate r')). bw.
assert (transf_axioms (fun z => W (Q z) (sof_value (substrate r')
  (substrate r'') (W (P z) x)))
  (product (substrate r)(substrate r')) (substrate r'')).
red. ir. set (f1:= sof_value (substrate r')(substrate r'') (W (P c) x)).
awi H10. ee. wri H5 H11. cp (inc_W_target H4 H11). rwi H6 H13.
rwi imo_substrate H13.  rwi set_of_increasing_mappings_pr H13. nin H13.
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)))
  (product (substrate r)(substrate r')) (substrate r'')).
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)).
awi H12; awi H13; ee. wri H5 H17. wri H5 H15.  cp (inc_W_target H4 H17).
cp (inc_W_target H4 H15). rwi H6 H19. rwi H6 H20.
rwi imo_substrate H19.  rwi set_of_increasing_mappings_pr H19. nin H19.
rwi imo_substrate H20.  rwi 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.
red in H7. ee. red in H35. rwi product2_order_pr H14. red in H14. ee.
cp (H35 _ _ H17 H15 H37). rwi imo_pr H39. ee. wri H28 H41; wri H24 H41.
rwi inv_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.
```

```
  app H53. rw H45. am.  rww H45.
  app (order_transitivity H1 H48 H49). am. am. am. am. am. am. am. am. am. am.
  assert (partial_fun_axioms g). red. split. am. simpl.
  exists (substrate r). exists (substrate r'). tv.
  exists (corr_value g). split. rw set_of_increasing_mappings_pr. exists g.
  ee. am. sy;  tv. tv. am. tv. app order_product2_order. am.
  assert (sof_value (product (substrate r) (substrate r'))
    (substrate r'') (corr_value g) = g). uf corr_value. aw.
  uf sof_value. aw. rw H14.
  wr H8. rw correspondence_extensionality1. app funct_extensionality.
  app function_restriction2. app Exercice1_6j. rw target_restriction2.
  rwi imo_substrate H6. am. am. am. ir. rw W_restriction2.
  assert (Ha: inc x0 (domain (source g))).  simpl. rww domain_product. wrr H5.
  rw W_spfa. cp (inc_W_target H4 H15). rwi H6 H16. rwi imo_substrate H16.
  rwi set_of_increasing_mappings_pr H16. nin H16. ee. wr H20.
  rw correspondence_extensionality1. app funct_extensionality.
  app function_spf. simpl. rw range_product. am.
  am. ir. rw W_spf. uf g. rw W_af_function. aw.
  assert (sof_value (substrate r') (substrate r'') (W x0 x) = x1).
  wr H20. uf corr_value. wr H17. wr H18. uf sof_value.  aw. nin x1. tv.
  rww H22. am. wr H17. wr H5. fprops. am. am. simpl. rww range_product.
  wrr H17. am. am. am. am. am.  am. app Exercice1_6j. wrr H5. am.
  app imo_order.
Qed.


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 H1 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.
  rww imo_pr. rww imo_pr. wr 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 |-*.
  rww W_af_function. rww W_af_function.  rwii  W_af_function H10.
  rwii  W_af_function H11. clear H15.
  rwii set_of_increasing_mappings_pr H8. rwii set_of_increasing_mappings_pr H9.
  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. aw. 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. aw.  wr H16. bwi H15.
  wr H15. nin x1. tv. am. am. rw H23; rwi H23 H11; clear H23.
  rw inv_corr_value_pr. rw inv_corr_value_pr. rw imo_substrate.
  red. rw source_restriction2. rw target_restriction2. rw source_restriction2.
  rw target_restriction2.
```

```
cp (Exercice1_6j H H0 H2 H3 H21). cp (Exercice1_6j H H0 H2 H3 H17).
ee. app function_restriction2. app function_restriction2.  tv. tv. tv. tv.
ir.  rww W_restriction2.  rww W_restriction2.
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).
ee. app function_spf. rww source_spf. rww target_spf.
app (Exercice1_6i H H0  H2 H3 H21 H25). tv.
rw set_of_increasing_mappings_pr. ee. exists (second_partial_fun x1 i).
ee. app function_spf. rww source_spf. rww target_spf.
app (Exercice1_6i H H0  H2 H3 H17 H25). tv. am. am.
red.  ee. app function_spf. app function_spf. rww source_spf. rww target_spf.
rww source_spf. rww target_spf. ir. rw W_spf. rw W_spf.
nin H14. ee. wri H22 H36; wri H18 H36. rwi inv_corr_value_pr H36.
rwi inv_corr_value_pr H36. app H36. bw.  fprops. am.  am. rww H29. am. am.
rww H28. am. 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 *.
ee. 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. rwii W_af_function H22.
ufi second_partial_map2 H23. rwii W_af_function H23.
rwi 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.
rw inv_corr_value_pr. red. ee. am. 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. aw. 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. aw. nin x1. tv.
am. am.  rwi H33 H23. clear H33.
bwi H32. awi 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 = J (P i) (Q i)). sy; app pair_recov. rw H39. cp (H20 _ H33).
rwi 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).
rwii W_restriction2 H40.  rwii W_restriction2 H40. clear H21; clear H22.
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). rwii W_spf H46. rwii W_spf H46. am. am. am. am. am. am.
  am. am. am. am. am. am. am. am. am. am. app imo_order.
Qed.
```

(c) If $\mathrm{E} \neq \emptyset$*, then* $\mathscr{A}(\mathrm{E},\mathrm{F})$ *is a lattice if and only if* F *is a lattice.*

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 -> order r'-> nonempty (substrate r) ->
  lattice r' = lattice (increasing_mappings_order r r').
Proof. ir. app iff_eq. clear H1. ir. uf lattice. split. app imo_order.
  rw 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').
  set (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 $\mathscr{A}(\mathrm{E},\mathrm{F})$.

```
  assert (Ha:increasing_fun f1 r r'). red.  ee; try am. tv. tv. red. uf f1.
  simpl. ir.  aw. set (a:= W x2 x0). set (b:= W x2 x1).
  assert (inc a E'). wr H13. uf a. app inc_W_target. rww H12.
  assert (inc b E'). wr H9. uf b. app inc_W_target. rww H8.
  set (a':= W y0 x0). set (b':= W y0 x1).
  assert (inc a' E'). wr H13. uf a'. app inc_W_target. rww H12.
  assert (inc b' E'). wr H9. uf b'. app inc_W_target. rww H8.
  cp (lattice_sup_pr H1 H19 H20). cp (lattice_sup_pr H1 H21 H22). ee.
  ap H28. assert (gle r' a a').  uf a; uf a'. red in H14. ee. app H33.
  rww H12. rww H12. app (order_transitivity H0 H29 H24).
  assert (gle r' b b').  uf b; uf b'. red in H10. ee. app H33.
  rww H8. rww H8. app (order_transitivity H0 H29 H25).
  assert (Hb:increasing_fun f2 r r'). red.  ee; try am. tv. tv. red. uf f2.
  simpl. ir.  aw. set (a:= W x2 x0). set (b:= W x2 x1).
  assert (inc a E'). wr H13. uf a. app inc_W_target. rww H12.
  assert (inc b E'). wr H9. uf b. app inc_W_target. rww H8.
  set (a':= W y0 x0). set (b':= W y0 x1).
  assert (inc a' E'). wr H13. uf a'. app inc_W_target. rww H12.
  assert (inc b' E'). wr H9. uf b'. app inc_W_target. rww H8.
  cp (lattice_inf_pr H1 H19 H20). cp (lattice_inf_pr H1 H21 H22). ee.
  ap H26. assert (gle r' a a').  uf a; uf a'. red in H14. ee. app H33.
  rww H12. rww H12. app (order_transitivity H0 H23 H29).
  assert (gle r' b b').  uf b; uf b'. red in H10. ee. app H33.
```

```
rww H8. rww H8. app (order_transitivity H0 H27 H29).
assert (inc (corr_value f1) (set_of_increasing_mappings r r')).
rw set_of_increasing_mappings_pr. exists f1. ee. am. tv.
tv. am. tv. am. am.
assert (inc (corr_value f2) (set_of_increasing_mappings r r')).
rw set_of_increasing_mappings_pr. exists f2. ee. am. tv.
tv. am. tv. am. am.
```

The mapping $x \mapsto \sup(f(x), g(x))$ is the supremum.

```
ee. exists (corr_value f1). rw least_upper_bound_pr. split. red. split.
rww imo_substrate. ir. nin (doubleton_or H18); rw H19; rw imo_pr. ee.  am.
am. red. ee. wr H17. aw. aw. wr H17. aw.
wr H17. aw. aw. aw. wr H17. ir. aw. uf f1. aw.
assert (inc (W i x0)  E'). wr H15. app inc_W_target. rww H14.
assert (inc (W i x1) E'). wr H11. app inc_W_target. rww H10.
cp (lattice_sup_pr H1 H21 H22).  nin H23. am. am. am.
ee. am. am. red. ee. wr H13. aw. aw. wr H13.
aw. wr H13. aw. aw. aw. wr H13. ir. aw. uf f1. aw.
assert (inc (W i x0)  E'). wr H15. app inc_W_target. rww H14.
assert (inc (W i x1) E'). wr H11. app inc_W_target. rww H10.
cp (lattice_sup_pr H1 H21 H22). ee. am. am. am.
ir. red in H18. nin H18. assert (inc x (doubleton x y)). fprops.
cp (H19 _ H20).  assert (inc y (doubleton x y)). fprops.  cp (H19 _ H22).
rw imo_pr.  rwi imo_pr H21; rwi imo_pr H23. ee.  am. am. aw. red. ee. am.
red in H25; ee; am. tv. tv. red in H25; ee; am. red in H25; ee; am. ir.
red in H27; red in H25; ee. cp (H40 _ H28). cp (H34 _ H28). uf f1. aw.
wri H17 H41; wri H13 H42. awi H41. awi H42.
assert (inc (W i x0) E'). wr H15. app inc_W_target. rww H14.
assert (inc (W i x1) E'). wr H11. app inc_W_target. rww H10.
cp (lattice_sup_pr H1 H43 H44).  ee. app H47. am. am. am. am. am. am. am.
am. am. am. app imo_order. rw imo_substrate. red. ir.
nin (doubleton_or H18); rw H19; am. am. am.
```

The mapping $x \mapsto \inf(f(x), g(x))$ is the infimum.

```
exists (corr_value f2). rw greatest_lower_bound_pr. split. red. split.
rww imo_substrate. ir. nin (doubleton_or H18); rw H19; rw imo_pr. ee.  am.
am. red. ee. aw. wr H17. aw. aw.  aw. wr H17. aw.
wr H17. aw. ir. aw. uf f2. aw.
assert (inc (W i x0)  E'). wr H15. app inc_W_target. rww H14.
assert (inc (W i x1) E'). wr H11. app inc_W_target. rww H10.
cp (lattice_inf_pr H1 H21 H22). wr H17. ee. aw. am. am. ee. am. am.
red. ee.  aw.  wr H13. aw. aw. aw. wr H13. aw. wr H13. aw. ir. aw.
wr H13. uf f2. aw.
assert (inc (W i x0)  E'). wr H15. app inc_W_target. rww H14.
assert (inc (W i x1) E'). wr H11. app inc_W_target. rww H10.
cp (lattice_inf_pr H1 H21 H22). ee. am. am. am.
ir. red in H18. nin H18. assert (inc x (doubleton x y)). fprops.
cp (H19 _ H20).  assert (inc y (doubleton x y)). fprops.  cp (H19 _ H22).
rw imo_pr.  rwi imo_pr H21; rwi imo_pr H23. ee.  am. am. aw. red. ee.
red in H25; ee; am. am. red in H25; ee; am. red in H25; ee; am.  tv. tv. ir.
red in H27; red in H25; ee. cp (H40 _ H28). cp (H34 _ H28). uf f2. aw.
wri H17 H41; wri H13 H42. awi H41. awi H42.
assert (inc (W i x0) E'). wr H15. app inc_W_target. rww H14.
```

```
assert (inc (W i x1) E'). wr H11. app inc_W_target. rww H10.
cp (lattice_inf_pr H1 H43 H44).  ee. app H47. am. am. am. am. am. am. am.
am. am. am. app imo_order. rw imo_substrate. red. ir.
nin (doubleton_or H18); rw H19; am. am. am. am.  am. am. am. am. am.
```

Conversely. Given two values a and b in F, we can consider the two constant functions $x \mapsto a$ and $x \mapsto b$. They are increasing.

```
ir. red. split. am.
set (E:=substrate r) in *;  set (E':=substrate r') in *. nin H1. ir.
set (f1:= constant_function E E' x H3).
set (f2:= constant_function E E' y0 H4).
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.
assert (inc (corr_value f1) (substrate (increasing_mappings_order r r'))).
rw imo_substrate. am. am. am.
assert (inc (corr_value f2) (substrate (increasing_mappings_order r r'))).
rw imo_substrate. am. am. am.
```

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 $c \leq c'$.

```
split. cp (lattice_sup_pr  H2 H7 H8).
set (f3:=  (sup (increasing_mappings_order r r') (corr_value f1)
           (corr_value f2))) in *.
ee. assert (inc f3 (substrate (increasing_mappings_order r r'))).
app (inc_arg2_substrate H9). rwi imo_substrate H12.
rwi set_of_increasing_mappings_pr H12. nin H12. ee.
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.
rwi imo_pr H9. nin H9. nin H20. awi H21. red in H21. ee. cp (H27 _ H1).
wri H16 H28. awi H28. ufi f1 H28. rwi W_constant H28. am. am. am. am.
rwi imo_pr H10. nin H10. nin H20. awi H21. red in H21. ee. cp (H27 _ H1).
wri H16 H28. awi H28. ufi f2 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')).
rw set_of_increasing_mappings_pr. exists f4. ee.  uf f4.
app function_constant_fun. tv. tv. red. ee.  uf f4.
app function_constant_fun. am. am. tv. tv. red. simpl. ir. uf f4.
rw W_constant. rw W_constant. wrr order_reflexivity. am. am. tv. am. am.
assert (gle (increasing_mappings_order r r')(corr_value f1) (corr_value f4)).
red. rw imo_pr. split. am. split. am. aw. red. ee. uf f1.
app function_constant_fun. uf f4. app function_constant_fun.  tv. tv. tv.
tv. uf f1. uf f4. ir. rw W_constant. rw W_constant. app H19. fprops. am. am.
am. am.
assert (gle (increasing_mappings_order r r')(corr_value f2) (corr_value f4)).
```

```
  red. rw imo_pr. split. am. split. am. aw. red. ee. uf f2.
  app function_constant_fun. uf f4. app function_constant_fun.  tv. tv. tv.
  tv. uf f2. uf f4. ir. rw W_constant. rw W_constant. app H19. fprops. am. 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 (substrate (increasing_mappings_order r r'))).
  app (inc_arg1_substrate H9). rwi imo_substrate H12.
  rwi set_of_increasing_mappings_pr H12. nin H12. ee.
  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.
  rwi imo_pr H9. nin H9. nin H20. awi H21. red in H21. ee. cp (H27 _ H1).
  wri H16 H28. awi H28. ufi f1 H28. rwi W_constant H28. am. am. am. am.
  rwi imo_pr H10. nin H10. nin H20. awi H21. red in H21. ee. cp (H27 _ H1).
  wri H16 H28. awi H28. ufi f2 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')).
  rw set_of_increasing_mappings_pr. exists f4. ee.  uf f4.
  app function_constant_fun. tv. tv. red. ee.  uf f4.
  app function_constant_fun. am. am. tv. tv. red. simpl. ir. uf f4.
  rw W_constant. rw W_constant. wrr order_reflexivity. am. am. tv. am. am.
  assert (gle (increasing_mappings_order r r')(corr_value f4) (corr_value f1)).
  red. rw imo_pr. split. am. split. am. aw. red. ee. uf f4.
  app function_constant_fun. uf f1. app function_constant_fun.  tv. tv. tv.
  tv. uf f1. uf f4. ir. rw W_constant. rw W_constant. app H19. fprops. am. am.
  am. am.
  assert (gle (increasing_mappings_order r r')(corr_value f4) (corr_value f2)).
  red. rw imo_pr. split. am. split. am. aw. red. ee. uf f4.
  app function_constant_fun. uf f2. app function_constant_fun.  tv. tv. tv.
  tv. uf f2. uf f4. ir. rw W_constant. rw W_constant. app H19. fprops. am. 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.
```

(d) Suppose that E *and* F *are both non-empty. Then* $\mathscr{A}$(E, F) *is totally ordered if and only if one of the following conditions is satisfied:*
*(*α*)* F *consists in a single element;*
*(*β*)* E *consists in a single element and* F *is totally ordered;*
*(*γ*)* E *and* F *are both totally ordered and* F *has two elements.*

We first show that if $\mathscr{A}$(E, F) is totally ordered and E non-empty, then F is totally ordered, using constant functions as above.

```
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.
  awi 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.
  awi 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. am.
Qed.
```

If F is a singleton, then $\mathscr{A}(E,F)$ has a single element, hence is totally ordered. If E is a singleton, all functions are constant and $\mathscr{A}(E,F)$ 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. rww 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 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. rww H8.  assert (inc (W i x1)  (substrate r')). wr H5.
  app inc_W_target. rww 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. 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. rww 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. rww H11.
  rw H1. fprops.
  assert (inc b (substrate r')). wr H8. uf b. app inc_W_target. rww 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.
  nin H2.  nin (H19 _ _ H15 H16). left. ee. am. am.  red. ee. wr H14. aw.
  wr H10. aw. wr H14. aw. wr H14. aw. wr H10. aw. wr H10. aw.
  wr H14; wr H10. ir.  aw.  rw H17. rw H18. am. am. am.
  right.  ee. am. am.  red. ee. wr H10. aw. wr H14. aw. wr H10. aw. wr H10.
  aw. wr H14. aw. wr H14. aw. wr H14; wr H10. ir. aw. rw H17. rw H18. am. am.
  am.  am. am. am. am. am. am. am. am.
```

```
Qed.
```

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 H3. nin H3.
  red. ee. app imo_order. rww imo_substrate. ir. cp H5; cp H6.
  rwi set_of_increasing_mappings_pr H5. nin H5.
  rwi set_of_increasing_mappings_pr H6. nin H6. ee.
  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.
  apply by_cases with (exists u, inc u (substrate r)& glt r' (W u x4) (W u x5)).
  ir. nin H18. ee. left. rw imo_pr. ee. am. am. red. ee. wr H16. aw. wr H12.
  aw. wr H16.  aw. wr H16. aw. wr H12. aw. wr H12. aw. ir. wr H16. wr H12.
  aw. assert (inc (W i x4) (substrate r')). wr H14. app inc_W_target.
  rww H13. assert (inc (W i x5) (substrate r')). wr H10. app inc_W_target.
  rww H9. nin H2.  rwi H3 H21. rwi H3 H22. nin (doubleton_or H21).
  rw H24. nin (doubleton_or H22); rw H25.  wrr  order_reflexivity.
  rw H3. fprops. nin H4. am. rw H24. nin (doubleton_or H22); rw H25.
  cp (H17 _ H18 H19). nin H1.  assert (inc x6 (source x5)).  rww H9.
  assert (inc i (source x5)).  rww 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. wr H12. aw. wr H12. aw. wr H16. aw. wr H16. aw. ir. wr H16. wr H12.
  aw. assert (inc (W i x4) (substrate r')). wr H14. app inc_W_target.
  rww H13. assert (inc (W i x5) (substrate r')). wr H10. app inc_W_target.
  rww H9. nin H2. nin (H22 _ _ H20 H21).
  nin (equal_or_not (W i x5) (W i x4)).  rw H24. wrr order_reflexivity.
  elim H18. exists i. split. am. red. split. am. intuition. am. am. am. am.
  am. am. am.
Qed.
```

Converse. Assume $\mathscr{A}(\mathrm{E},\mathrm{F})$ 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: forall r r', order r -> order r'->
  nonempty(substrate r) -> nonempty (substrate r') ->
  total_order (increasing_mappings_order r r') ->
  (is_singleton (substrate r') \/
   (is_singleton (substrate r) & total_order r') \/
   (total_order r' & total_order r
     & exists u , exists v, substrate r' = doubleton u v)).
Proof. ir. cp (Exercice1_6o H H0 H1 H3). nin H2.
  apply by_cases with (substrate r' = singleton y). ir. left.
  exists y. tv. ir. right. nin H1.
  apply by_cases with (substrate r = singleton y0). ir. left. split.
  exists y0. tv. am. ir. right. split. am.
  assert (exists y1, inc y1 (substrate r') & y1 <> y). app exists_proof. red.
  ir. elim H5.  set_extens. nin (equal_or_not x y). rw H9. fprops.
  elim (H7 x). intuition. rw (singleton_eq H8). am. nin H7.
  assert (exists u,  exists v, inc u (substrate r') & inc v (substrate r')
    & glt r' u v). ee.  nin H4. nin (H9 _ _ H2 H7). exists y; exists x. ee.
  am. am.  red. ee. am. intuition. exists x; exists y. ee. am. am. red. ee.
  am. am. clear H2.  clear H5. clear H7. nin H8. nin H2.
  assert (exists y1, inc y1 (substrate r) & y1 <> y0). app exists_proof. red.
  ir. elim H6.  set_extens. nin (equal_or_not x2 y0). rw H8. fprops.
  elim (H5 x2). intuition. rw (singleton_eq H7). am. 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 $\mathscr{A}(\mathrm{E},\mathrm{F})$ 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 (f1:= fun u=> Yo (gle r u x0) b b').
  assert (transf_axioms f1 (substrate r) (substrate r')).
  red. ir. uf f1. apply by_cases with  (gle r c x0). ir.
  rww Y_if_rw. ir. rww Y_if_not_rw.
  assert (inc (corr_value (BL f1 (substrate r) (substrate r')))
    (set_of_increasing_mappings r r')). rw 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.  rww W_af_function. rww W_af_function. uf f1.
  apply by_cases with  (gle r x1 x0). ir. rww Y_if_rw.
  apply by_cases with  (gle r y1 x0). ir. rww Y_if_rw.
  wrr order_reflexivity. ir. rww Y_if_not_rw. nin H9. am. ir.
  rww Y_if_not_rw. apply by_cases with  (gle r y1 x0). ir.
  rww Y_if_rw. elim H16. app (order_transitivity H H15 H17). ir.
  rww Y_if_not_rw.  wrr order_reflexivity.  tv. am. am.
  set (f2:= fun u=> Yo (gle r u y0) b b').
  assert (transf_axioms f2 (substrate r) (substrate r')).
  red. ir. uf f2. apply by_cases with  (gle r c y0). ir.
  rww Y_if_rw. ir. rww Y_if_not_rw.
  assert (inc (corr_value (BL f2 (substrate r) (substrate r')))
```

```
  (set_of_increasing_mappings r r')). rw set_of_increasing_mappings_pr.
exists  (BL f2 (substrate r) (substrate r')). ee. app af_function. tv. tv.
red. ee.  app af_function. am. am. tv. tv. red. ir. simpl in H15.
simpl in H15.  rww W_af_function. rww W_af_function. uf f2.
apply by_cases with  (gle r x1 y0). ir. rww Y_if_rw.
apply by_cases with  (gle r y1 y0). ir. rww Y_if_rw.
wrr order_reflexivity. ir. rww Y_if_not_rw. nin H9. am. ir.
rww Y_if_not_rw. apply by_cases with  (gle r y1 y0). ir.
rww Y_if_rw. elim H18. app (order_transitivity H H17 H19). ir.
rww Y_if_not_rw.  wrr order_reflexivity.  tv. am. am.
nin H3. rwi imo_substrate H16. nin (H16 _ _ H13 H15).
rwi imo_pr H17. ee. red in H19. ee. awi H25. ufi f1 H25; ufi f2 H25.
cp (H25 _ H11). awi H26. apply by_cases with (gle r y0 x0). ir.
right. red. am. ir. rwi Y_if_not_rw H26.  rwi Y_if_rw H26. nin H9. elim H28.
app (order_antisymmetry H0 H9 H26). wr order_reflexivity. am. am. am. am.
am. am. am. am. am.
red in H17. rwi imo_pr H17. ee. red in H19. ee. awi H25.
ufi f1 H25; ufi f2 H25. cp (H25 _ H10). awi H26.
apply by_cases with (gle r x0 y0). ir. left. am. ir. rwi Y_if_not_rw H26.
rwi Y_if_rw H26. nin H9. elim H28.
app (order_antisymmetry H0 H9 H26). wr order_reflexivity. am. am. am. am.
am. am. am. am. am. am. am.
```

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 $x_0 < x_1 < x_2$.

```
split. am. apply by_cases with (substrate r'= doubleton b b'). ir.
exists b. exists b'. rw H8. tv. ir.
assert (exists b'', inc b'' (substrate r') & b'' <> b & b'' <> b').
app exists_proof. red. ir. elim H8. set_extens. nin (equal_or_not x0 b).
rw H11. fprops. nin (equal_or_not x0 b'). rw H12. fprops. elim (H9 x0).
intuition. ee. nin (doubleton_or H10); rw H14; am.
assert (exists u, exists v, exists w,
  inc u (substrate r') & inc v (substrate r') & inc w (substrate r') &
  glt r' u v & glt r' v w).  nin H9. ee. red in H4. ee. nin (H15 _ _ H9 H2).
exists x0; exists b; exists b'. ee. am. am. am. red. split. am. am. am.
nin (H15 _ _ H9 H13). exists b; exists x0; exists b'. ee. am. am. am.
red. red in H16. ee. am. intuition. red. ee. am. am.
exists  b; exists b'; exists x0. ee. am. am. am. am. red. ee.  red in H17.
am. intuition. clear  H2. clear H9. clear H8. nin H10. nin H2. nin H2. ee.
```

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 $x2$ otherwise. The same arguments as above show that they are increasing. Since $\mathscr{A}(\mathrm{E}, \mathrm{F})$ is totally ordered, we may compare them. We have $f(v) < g(v)$ 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')). uf f.
rw set_of_increasing_mappings_pr.
exists (constant_function (substrate r) (substrate r') x1 H8). simpl. ee.
app function_constant_fun. tv. tv.  red. ee.  app function_constant_fun.
am. am. tv. tv. red.  simpl. ir. rw W_constant. rw W_constant.
wrr order_reflexivity. am. am. tv. am. am.
cp (total_order_lattice H7). cp (lattice_sup_pr H14 H1 H5).
```

```
  cp (lattice_inf_pr H14 H1 H5). set (u:=inf r a a').
  assert (inc u (substrate r)).  nin H16. app (inc_arg1_substrate H16).
  set (v:=sup r a a').
  assert (inc v (substrate r)). nin H15. app (inc_arg2_substrate H15).
  assert (glt r u v). red. ee. ap (order_transitivity H H16 H15). red. ir.
  ufi u H23; ufi v H23. rwi H23 H16. rwi H23 H19.
  cp (order_transitivity H H15 H19). cp (order_transitivity H H21 H16).
  elim H12.  app (order_antisymmetry H H25 H24).
  set (g:= fun x=> Yo (gle r x u) x0 x2).
  assert (transf_axioms g (substrate r) (substrate r')).
  red. ir. uf g. apply by_cases with  (gle r c u). ir.
  rww Y_if_rw. ir. rww Y_if_not_rw.
  assert (inc (corr_value (BL g (substrate r) (substrate r')))
    (set_of_increasing_mappings r r')). rw set_of_increasing_mappings_pr.
  exists  (BL g (substrate r) (substrate r')). ee. app af_function. tv. tv.
  red. ee.  app af_function. am. am. tv. tv. red. ir. simpl in H25.
  simpl in H26.  rww W_af_function. rww W_af_function. uf g.
  apply by_cases with  (gle r x3 u). ir. rww Y_if_rw.
  apply by_cases with  (gle r y0 u). ir. rww Y_if_rw.
  wrr order_reflexivity. ir. rww Y_if_not_rw. nin H10. nin H11.
  app (order_transitivity H0 H10 H11). ir.
  rww Y_if_not_rw. apply by_cases with  (gle r y0 u). ir.
  rww Y_if_rw.  elim H28. app (order_transitivity H H27 H29). ir.
  rww Y_if_not_rw.  wrr order_reflexivity.  tv. am. am.
  nin H3. rwi imo_substrate H22. nin (H22 _ _ H13 H21).
  rwi imo_pr H23. ee. red in H25. ee. awi H35. ufi f H35. awi H35.
  cp (H35 _ H17). awi H36. rwi W_constant H36. ufi g H36. rwi Y_if_rw H36.
  nin H10. elim H37. app (order_antisymmetry H0 H10 H36). wrr order_reflexivity.
  am. am. am. am. am. red in H23. rwi imo_pr H23. ee. red in H25. ee. awi H35.
  ufi f H35. awi H35. cp (H35 _ H18). awi H36. rwi W_constant H36. ufi g H36.
  rwi Y_if_not_rw H36. nin H11. elim H37. app (order_antisymmetry H0 H11 H36).
  red.  ir. nin H19. elim H38. app (order_antisymmetry H H19 H37).
  am. am. am. am. am. am. am.
Qed.
```

---

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:= fun x y => (gle r x y \/ 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 : Bset,
    comp_rel r x y -> (inc x (substrate r) & inc y (substrate r))). ir. nin H0.
  split.  app (inc_arg1_substrate H0). app (inc_arg2_substrate H0).
  split. app (inc_arg2_substrate H0). app (inc_arg1_substrate H0).
  assert (reflexive_r (comp_rel r) (substrate r)).
  red. ir. app iff_eq.  uf comp_rel. ir. ee.  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. rw inc_class.
  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. app (transitivity H2 (u:=x)(w:= x0)).
  exists x1. split; 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. rw inc_class.
  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. app (transitivity H2 (u:=x)(w:= x0)).
  exists x1. split; 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 H0. ee. red in H9. red in H14. wri H12  H14. wri H12 H9.
```

```
  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).
  cp (H14 _ _ H4 H3 H1). red in H16.
  ap (order_antisymmetry H11 H16 H15).
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' f, increasing_fun f r r' ->
  decreasing_fun f r r' ->
  (exists x, inc x (substrate r) & cr_component r x = substrate r)
  -> (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, comp_rel r x y ->  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.
  wri H8  H14. wri (H6 _ H1) H14. rwi inc_class H14.
  assert (related (cr_equiv r) u x). apply symmetricity. am. am.
  ufi cr_equiv H15. ufi Exercice1.Sgraph H15. ufi graph_on H15. red in H15.
  Ztac. nin H17. awi H17. ee.
  assert (forall x1, Exercice1.chained_r (comp_rel r) x1 ->
    Exercice1.chain_tail x1 = x  ->
    W (Exercice1.chain_head x1) f = W x f). ir. nin x2. simpl. simpl in H21.
  simpl in H20. wr H21. app H9. simpl. simpl in H20. ee. cp (IHx2 H22 H21).
  simpl in H20. rww (H9 _ _ H20). wr (H20 _ H17 H19). rww H18.  nin H3; ee; am.
  rw (H14 _ H11). rw (H14 _ H12). tv.
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', order r -> order r' ->
  (exists u, exists v, inc u (substrate r') & inc v (substrate r')  & u <>v)
  -> (exists x, inc x (substrate r) & cr_component r x <> substrate r)
  -> exists f, increasing_fun f r r' &  decreasing_fun f r r' &
    ~(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. apply by_cases with (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.
  assert (~ is_constant_function g). red. ir. red in H13. ee.
  assert (inc x1 (source g)). uf g. am. elim H3.  app extensionality.
  wr H9. wr H8. app sub_class_substrate. am. red. ir.
  assert (inc x2 (source g)). uf g. am. cp (H14 _ _ H15 H17).
  ufi g H18. awi H18. ufi f H18. rwi Y_if_rw H18.
  apply by_cases with (inc x2 (cr_component r x1)). tv. ir.
```

```
  rwi Y_if_not_rw H18. elim H5. am. am. wrr H9. rw inc_class.
  app reflexivity_e. rww H8.  nin H6; am. am. am. am. am.
```

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.

```
  assert (forall a b, inc a (substrate r) -> inc b (substrate r) ->
    gle r a b -> (inc a (cr_component r x1) = inc b (cr_component r x1))).
  ir. wrr H9. rww inc_class. rww inc_class. assert (comp_rel r a b). red. left.
  am. cp (H10 _ _ H17). app iff_eq. ir.
  app (transitivity H6 (u:=x1)(w:= b)). exists a. split;am. ir.
  app (transitivity H6 (u:=x1)(w:= a)). exists b. split. am.
  app symmetricity. nin H6; am. nin H6; am.
  assert (forall a b, inc a (substrate r) -> inc b (substrate r) ->
    gle r a b ->  W a g = W b g). ir. uf g. aw. uf f.
  apply by_cases with (inc a (cr_component r x1)). ir. rww Y_if_rw. rww Y_if_rw.
  wrr (H14 _ _ H15 H16 H17). ir.  rww Y_if_not_rw. rww Y_if_not_rw.
  wrr (H14 _ _ H15 H16 H17).
  exists g. ee. red. ee. am. am. am. tv. tv. red. ir. ufi g H16; ufi g H17.
  rww (H15 _ _ H16 H17 H18). wrr order_reflexivity.
  change (inc (W y g) (target g)). app inc_W_target.
  red. ee. am. am. am. tv. tv. red. ir. ufi g H16; ufi g H17.
  rww (H15 _ _ H16 H17 H18). tv. red. wrr order_reflexivity.
  change (inc (W y g) (target g)). app inc_W_target. am.
Qed.
```

---

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.
  clear H1. uf B. Ztac.  red in H. ee. rw H6. app inc_W_target. wrr H5.
  rww 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. wrr 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.
  red. ir. ufi image_by_fun H8.  awi H8. nin H8. nin H8. red in H9.
  rw (W_pr H H9). app H1. fprops.
  assert (is_function h). uf h. app function_restriction2.
  assert (injective h). red. split. am. uf h. simpl.
  intros x y Hx Hy. rww W_restriction2. rww W_restriction2. ir.
  ufi A Hx; ufi A Hy. Ztac. wr H7. clear Hy. Ztac. wr H5. sy; am.
```

```
  assert (surjective h). app surjective_pr6. uf h. simpl.
  ir. exists (W y g). split. app H2.
  rww W_restriction2.  ufi B H6. sy. Ztac. am.  app H2. exists h.
  red in H. ee. assert (sub A (substrate r)). uf A. app Z_sub.
  assert (sub B (substrate r')). uf B. app Z_sub.
  red. ee. fprops. fprops. red; split;am. aw. aw. uf h. simpl. ir.
  rww W_restriction2. rww W_restriction2. app iff_eq. ir. awi H16. aw. app H11.
  wr H9. app H12. wr H9. app H12. app H1. app H1. am. am. ir.
  cp (H1 _ H14). cp (H1 _ H15). awi H16. aw.
  ufi A H14. Ztac. clear H14.  ufi A H15. Ztac.
  wr H20. wr H21. red in H0; ee. app H26. wr H24; app H13.  wr H24; app H13.
  am. am.
Qed.
```

---

9. ** If* E *is a lattice, prove that*

$$\sup_j(\inf_i x_{ij}) \leq \inf_i(\sup_j x_{ij})$$

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. rww 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.
  ee.  cp (H11 _ H10). apply order_transitivity with x. am. am. am. rww H10.
  ir. red in H10. app H9. ee. app H5. red. ee. am. ir. app H11. fprops. ee.
  app H11. fprops.
Qed.
```

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 $i \in E$.

```
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 $\inf_i x_{ij} \leq x_{ij} \leq \sup_j x_{ij}$; 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 : Bset => 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 frange_inc_rw H12.
  nin H12. ee. bwi H12. bwi H13. rw H13. app Hb. am. gprops.
  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 : Bset => 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 frange_inc_rw H12.
  nin H12. ee. bwi H12. bwi H13. rw H13. app Hb. am. gprops.
  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. rw H15. app H14. uf fb. bw.
  am. gprops. bw. bw. red. ir. rwi frange_inc_rw H8. nin H8. bwi H8.  ee.
  rw H9. app lattice_finite_sup5. gprops.  bw.  bw.
  red. ir.  rwi frange_inc_rw H10.  nin H10. nin H10. bwi H10. bwi H11.
  rww H11. app Hb. am. gprops. ee;am. gprops. am. gprops.  bw. bw.
  red. ir.  rwi frange_inc_rw H7.  nin H7. nin H7. bwi H7. bwi H8. rw H8.
  app  lattice_finite_inf5. gprops. bw. bw. red. ir.
  rwi frange_inc_rw H9. nin H9. nin H9. bwi H9. bwi H10. rw H10. app Hb.
  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 $\mathbf{N} \times \mathbf{N}$ into the orders set $\mathbf{N}$ such that the relation*

$$f(\inf(x,y)) = \inf(f(x), f(y))$$

*is false for at least one pair $(x,y) \in \mathbf{N} \times \mathbf{N}$.**

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,
  lattice r ->  lattice r' -> is_function f -> substrate r = source f ->
  substrate r' = target f ->
  (increasing_fun f r r') =
  (forall x y, inc x (substrate r) -> inc y (substrate r) ->
    gle r' (W (inf r x y) f) (inf r' (W x f) (W y f))).
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).
  wri H10 H15; wri H10 H16. cp (lattice_inf_pr H0 H15 H16). ee. app H19.
  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.

(b) A product of ordered sets is a complete lattice if only if each of the factors is a complete lattice.

(c) An ordinal sun (Exercise 3) $\sum_{\iota\in I} E_\iota$ 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_σ has a least element.
(III) For each $\iota \in I$ every subset of E_ι which has an upper bound in E_ι has a least upper bound in E_ι.
(IV) For each $\iota \in I$ such that E_ι has no greatest element, the set of all $\kappa > \iota$ has a least element α and E_α has a lest element.

(d) The ordered set $\mathscr{A}(E, F)$ 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.

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 supremum, 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.
  nin H3. am. ir. app H4. red.  split.  app H1. ir. ufi Z H6. Ztac.
  nin H8.  app H9. ir. nin H3. app H6. uf Z. Ztac.  nin H5. am.
Qed.
```

The second claim is easy. Let X be a subset of $\prod E_i$ and $X_i = \mathrm{pr}_i X$. 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. Con-

versely, 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 $X_i = pr_i X$. 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. wr target_pri. 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 H7; 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.
  nin (H7 _ H8). awi H9. Ztac. wrr H4. app H3. app Z_sub. am.
  exists v. rw least_upper_bound_pr. split. red. split. am.
  ir. rww 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_lem.
  fprops. app H3. app H6. ir. nin H9.  rww related_product_order. ee.
  wrr Ha. wrr Ha. ir. cp (H7 _ H11). rwi least_upper_bound_pr H12. nin H12.
  app H13. red. split. rw H4. rwi Ha H9. rwi productb_pr H9. ee.  app H15.
  rww H14. am. am. ir. ufi Xi H14. awi H14. ufi image_by_fun H14. awi H14.
  nin  H14. ee. cp (H10 _ H14). rwi related_product_order H16. ee.
  assert (y = V i x). awi H15. red in H15. wr (W_pri (f:=f)). app W_pr.
  app function_pri. am. am. am. rw H19. app H18. am.
  assert (is_function (pr_i f i)). app function_pri. fprops. app H3. app H6.
  app order_product_order.  am.
Qed.

Lemma exercise1_11d: forall f g, axioms_product_order f g ->
  complete_lattice (product_order f g) ->
  (forall i, inc i (domain f) -> 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.
  rwi 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.
  app productb_monotone1. uf Y. gprops. uf Y. bw. ir. uf Y. ufi Y H10. bwi H10.
  bw. nin (equal_or_not i0 i). rw Y_if_rw. wrr H6. rww H11. am.
  rw Y_if_not_rw. red. ir. rw (singleton_eq H12). app H9. rww H8. am.
  nin H0. cp (H11 _ H10).  nin H12. nin H12.
  rwi least_upper_bound_pr H12. ee. red in H12. ee. awi H12.
  assert (W x0 (pr_i f i) = V i x0). rww W_pri.
  ee. exists (W x0 (pr_i f i)). rw least_upper_bound_pr. split. red. ee.
  rww H6. rw H16. rwi productb_pr  H12.  ee.  app H18. rww H17. am.
  ir. assert (inc (L(domain f)(fun j=> (Yo (j = i) y (V j x)))) (productb Y)).
```

```
  rw 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. wrr H6.
  tv. rw Y_if_not_rw. app H9. rww H8. am. am.
  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.
  uf w. bw. rwi productb_pr H19. ee. rwi H21 H22. ufi Y H22. bwi H22.
  cp (H22 _ H20). bwi H23. nin (equal_or_not i0 i). rw Y_if_rw.
  rwi Y_if_rw H23. red in H17. ee. rw H24. app H25. wrr H24. am. am.
  rw Y_if_not_rw. rwi Y_if_not_rw H23. rw (singleton_eq H23).
  wr order_reflexivity. rww H6. app H9.  rww 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.
  am. app H5. am. am. am. am. am.
Qed.
```

12. Let Φ be a mapping of a set A into itself. Let $\mathfrak{F}$ be the subset of $\mathfrak{P}(A)$ consisting of all $X \subset A$ such that $f(X) \subset X$ for each $f \in \Phi$. Show that $\mathfrak{F}$ is a complete lattice with respect to the relation of inclusion.

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 $x \in E$, $f(x) \geq x$, (3) for each $x \in E$, $f(f(x)) = f(x)$. Let F be the set of elements of E which are invariant under f.

(a) Show that for each $x \in E$ the set F_x of elements $y \in F$ such that $x \leq y$ is not empty and has a least element, namely $f(x)$. Conversely, if G is a subset of E such that, for each $x \in E$, the set of all $y \in G$ such that $x \leq y$ 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 $f(\sup(x, y)) = f(\sup(f(x), y))$ for each pair of elements x, y of E.

14. 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 ρ and σ are decreasing mappings and that the mapping $X \to \sigma(\rho(X))$ and $Y \to \rho(\sigma(Y))$ are closures (Exercise 13) in $\mathfrak{P}(A)$ and $\mathfrak{P}(B)$ respectively (ordered by inclusion).

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 $\mathfrak{P}(E)$, the set $\tilde{E}$ of subsets X such that $X = \sigma(\rho(X))$ is a complete lattice, and that the mapping $i : x \to \sigma(\{x\})$ is an isomorphism (called *canonical*) of E onto an ordered subset E' of $\tilde{E}$ such that, if a family (x_ι) 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_ι. $\tilde{E}$ 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

$$\inf(z, \sup(x, \inf(y, z))).)$$

¶ 17. A lattice E which has a least element α 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.

(a) Show that the set E of vector subspaces of a vector space of dimension ≥ 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.

(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 ω. For each $x \in E$, let x^* be the complement of x with respect to ω. The the mapping $x \to x^*$ 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 $\mathfrak{P}(A)$ of all subsets A, ordered by inclusion, is a Boolean lattice.

(c) If E is a *complete* Boolean lattice (Exercise 11), show that for each family (x_λ) of elements of E and each $y \in E$ we have

$$\inf(y, \sup_\lambda(x_\lambda)) = \sup_\lambda(\inf(y, x_\lambda)).$$

(Reduce to the case $y = \alpha$, and use the fact that if $\inf(z, x_\lambda) = \alpha$ for every index λ, then $x^* \geq x_\lambda$ for every λ).

¶ 18. *Let A be a set with at least three elements, let $\mathscr{P}$ be the set of all partitions of A, ordered by the relation "ϖ is finer than ϖ'" between ϖ and ϖ' (no 1, Example 4). Show that $\mathscr{P}$ 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 $]x, y[$ is not empty. Show that the ordinal sum $\sum_{\iota \in I} E_\iota$ (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 $\iota \in I$ such that E_ι contains two distinct comparable elements.

(II) Each E_i which contains at least two distinct comparable elements is without gaps.

(III) If α, β are two elements of I such that $\alpha < \beta$ and if the interval $]\alpha, \beta[$ in I is empty, then either E_α has no maximal element or else E_β has no minimal element.

In particular, every ordinal sum $\sum_{\iota \in I} E_\iota$ of sets without gaps is itself without gaps, provided that no E_ι has a maximal element (or provided that no E_ι has a minimal element). If I is without gaps, and if each E_ι is either without gaps or contains no two distinct comparable elements, then $\sum_{\iota \in I} E_\iota$ 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 $]x', y'[$ is empty. *Give an example of a totally ordered set which satisfies this condition and is not scatted (consider Cantor's triadic set).*

(b) An ordinal sum $\sum_{\iota \in I} E_\iota$ (where neither I nor any E_ι is empty) is scattered if and only if I and each E_ι 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 $x \in \mathrm{U}$, U contains the interval $[x, \rightarrow[$. An open set U is said to be *regular* if there exists no open set $\mathrm{V} \supset \mathrm{U}$, distinct from U such that U is cofinal in V. Show that every open set U is cofinal in exactly one regular open set $\bar{\mathrm{U}}$. The mapping $\mathrm{U} \rightarrow \bar{\mathrm{U}}$ is increasing. If U, V are two open sets such that $\mathrm{U} \cap \mathrm{V} = \emptyset$, then also $\bar{\mathrm{U}} \cap \bar{\mathrm{V}} = \emptyset$.

(b) Show that the set R(E) of regular open sets of E, ordered by inclusion, is a complete Boolean lattice (Exercise 17). For 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 $\mathrm{U} \rightarrow \mathrm{U} \cap \mathrm{F}$ is an isomorphism of R(E) onto R(F).

(d) If E_1, E_2 are two ordered sets, then every open set in $\mathrm{E}_1 \times \mathrm{E}_2$ is of the form $\mathrm{U}_1 \times \mathrm{U}_2$, where U_i is open in E_i $(i = 1, 2)$. The set $\mathrm{R}(\mathrm{E}_1 \times \mathrm{E}_2)$ is isomorphic to $\mathrm{R}(\mathrm{E}_1) \times \mathrm{R}(\mathrm{E}_2)$.

¶ 23. Let E be an ordered set and let $\mathrm{R}_0(\mathrm{E}) = \mathrm{R}(\mathrm{E}) - \emptyset$ (Exercise 22). For each $x \in \mathrm{E}$, 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 $\mathrm{R}_0(\mathrm{E})$. Endow $\mathrm{R}_0(\mathrm{E})$ with the order relation *opposite* to the relation of inclusion.

(a) Show that the mapping r is increasing and that $r(\mathrm{E})$ is cofinal in $\mathrm{R}_0(\mathrm{E})$.

(b) An ordered set E is said to be *antidirected* if the canonical mapping $r : \mathrm{E} \rightarrow \mathrm{R}_0(\mathrm{E})$ 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 $z \in \mathrm{E}$ 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, $\mathrm{R}_0(\mathrm{E})$ is antidirected and that the canonical mapping of $\mathrm{R}_0(\mathrm{E})$ into $\mathrm{R}_0(\mathrm{R}_0(\mathrm{E}))$ is bijective (use Exercise 22(a)).

24. * (a) An ordered set E is said to be *branched* (on the right) if for each $x \in \mathrm{E}$ 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 $\mathscr{R}$ 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 $\sum_{\xi \in \mathrm{E}} \mathrm{F}_\xi$ contains a cofinal subset isomorphic to E).*

8.2 Section 2

1. Show that, in the set of orderings on a set E, the minimal elements (with respect to the ordered relation "Γ is coarser than Γ'" between Γ and Γ') are the total orderings on E and that if Γ is any ordering on E, the graph of Γ is the intersection of the graphs of the total orderings on E which are coarser than Γ (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 $\mathfrak{B}$ 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 $\mathfrak{B}$ is an order relation between X and Y and that $\mathfrak{B}$ 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 $Y - X$ 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 $\mathfrak{S}$ 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 top M. For each $a \in E$, show that the intersection C_a of the sets of $\mathfrak{S}$ which contain a also belongs to $\mathfrak{S}$; 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 and have a least upper bound m in E such that $m \notin X$ or $f(m) > m$, and apply Lemma 3 of no. 3 to the set $\mathfrak{M}$.)

(b) Deduce from (a) that if E is inductive, then there exists $b \in E$ such that $f(b) = b$.

¶ 7. Let E be an ordered set and let F be the set of all closures (§ 1, Exercise 13) in E. Order F by putting $u \leq v$ whenever $u(x) \leq v(x)$ for all $x \in E$. Then F has a least element e, the identity mapping of E onto itself. For each $u \in F$, let $I(u)$ denote the set of elements of E which are invariant under u.

(a) Show that $u \leq v$ in F if and only if $I(v) \subset I(u)$.

(b) Show that if every pair of elements of E has a greatest lower bound in E, then every pair of elements of F has a greatest lower bound in F. If E is a complete lattice, then so is F (§ 1, Exercise 11).

(c) Show that if E is inductive (with respect to the relation $\leq$), then every pair u, v of elements of F have a least upper bound in F (Show that if $f(x) = v(u(x))$ and if $w(x)$ denotes the greatest element of the chain of x, relative to f (Exercise 6), then w is a closure in E and is the least upper bound of u and v.)

¶ 8. An ordered set E is said to be *ramified* (on the right) if, for each pair of elements x, y of E such that $x < y$, there exists $z > x$ such that y and z are not comparable. E is said to be *completely ramified* (on the right) if it is ramified and has no maximal elements. Every antidirected set (§ 1, Exercise 22) is ramified.

(a) Let E be an ordered set and let a be an element of E. Let $\mathfrak{R}_a$ denote the set of ramified subsets of E which have a as least element. Show that $\mathfrak{R}_a$, ordered by inclusion, has a maximal element.

(b) If E is branched (§ 1, Exercise 24), show that every maximal element of $\mathfrak{R}_a$ 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 $]\leftarrow, x]$ is totally ordered. Show that E has an antidirected cofinal subset (§ 1, Exercise 22) (use (b)).

9. An ordinal sum $\sum_{\iota\in I} E_\iota$ (§ 1, Exercise 3) is well-ordered if and only if I and each E_ι is well-ordered.

10. Let I be an ordered set and let $(E_\iota)_{\iota\in I}$ be a family of ordered sets, all equal to the same ordered set E. Show that the ordinal sum $\sum_{\iota\in I} E_\iota$ (§ 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.I.

¶ 11. *Let I be a well-ordered set and let $(E_\iota)_{\iota\in I}$ be a family of ordered sets, each of which contains at least two distinct comparable elements. Then the lexicographic product of the E_ι is well-ordered if and only if each of the E_ι is well-ordered and I is *finite* (if I is infinite, construct a strictly decreasing infinite sequence in the lexicographic product if the E_ι). *

¶ 12. Let I be a totally ordered set and let $(E_\iota)_{\iota\in I}$ be a family of ordered sets indexed by I. Let $R\{\!\{x,y\}\!\}$ denote the following relation on $E = \prod_{\iota\in I} E_\iota$: "the set of indices $\iota \in I$ such that $\mathrm{pr}_\iota x \neq \mathrm{pr}_\iota y$ is well-ordered, and if κ is the least element of this subset of I, we have $\mathrm{pr}_\kappa x < \mathrm{pr}_\kappa y$". Show that $R\{\!\{x,y\}\!\}$ is an order relation between x and y on E. If the E_ι 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_ι has at least two elements. Then E is totally ordered if and only if I is well-ordered and each E_ι is totally ordered (use Exercise 3); and E is then the lexicographic product of the E_ι.

13. (a) Let $\mathrm{Is}(\Gamma,\Gamma')$ be the relation "Γ is an ordering (on E) and Γ' is an ordering (on E'), and there exists an isomorphism of E, ordered by Γ, onto E', ordered by Γ'". Show that $\mathrm{Is}(\Gamma,\Gamma')$ is an equivalence relation on every set whose elements are orderings. The term $\tau_\Delta(\mathrm{Is}(\Gamma,\Delta))$ is an ordering called the *order-type* of Γ and denoted by $\mathrm{Ord}(\Gamma)$, or $\mathrm{Ord}(E)$ by abuse of notations. Two ordered sets are isomorphic if and only if their order-types are equal.

(b) Let $R\{\lambda,\mu\}$ be the relation: "λ is an order-type, and μ is an order-type and there exists an isomorphism of the set ordered by λ onto a subset of the set ordered by μ". Show that $R\{\lambda,\mu\}$ is a preorder relation between λ and μ. It will be denoted by $\lambda \prec \mu$.

(c) Let I be an ordered set and let $(\lambda_\iota)_{\iota\in I}$ 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 λ_ι ($\iota \in I$) is called the *ordinal sum* of the order-types λ_ι ($\iota \in I$) and is denoted by $\sum_{\iota\in I}\lambda_\iota$. If $(E_\iota)_{\iota\in I}$ is a family of ordered sets, the order type of $\sum_{\iota\in I}E_\iota$ is $\sum_{\iota\in I}\mathrm{Ord}(E_\iota)$. If I is the ordinal sum of a family $(J_\kappa)_{\kappa\in K}$, show that

$$\sum_{\kappa\in K}\Big(\sum_{\iota\in J_\kappa}\lambda_\iota\Big)=\sum_{\iota\in I}\lambda_\iota.$$

(d) Let I be a well-ordered set and $(\lambda_\iota)_{\iota\in I}$ be a family of order-types indexed by I. The order-type of the lexicographic product of the family of sets indexed by by the λ_ι ($\iota \in I$) is called the *ordinal product* of the order-types λ_ι ($\iota \in I$) and is denoted by $\mathop{\mathsf{P}}_{\iota\in I}\lambda_\iota$. If $(E_\iota)_{\iota\in I}$ is a family of ordered sets, the order type of the lexicographic product of the family $(E_\iota)_{\iota\in I}$ is $\mathop{\mathsf{P}}_{\iota\in I}\mathrm{Ord}(E_\iota)$. If I is the ordinal sum of a family of well-ordered sets $(J_\kappa)_{\kappa\in K}$ indexed by a well-ordered set K, show that

$$\mathop{\mathsf{P}}_{\kappa\in K}\Big(\mathop{\mathsf{P}}_{\iota\in J_\kappa}\lambda_\iota\Big)=\mathop{\mathsf{P}}_{\iota\in I}\lambda_\iota.$$

(e) We denote by $\lambda+\mu$ (resp. $\mu\lambda$) the ordinal sum (resp. ordinal product) of the family $(\xi_\iota)_{\iota\in J}$ where $J=\{\alpha,\beta\}$ 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 λ and if $(\mu_\iota)_{\iota\in I}$ is a family of order-types such that $\mu_\iota=\mu$ for each $\iota\in I$ then $\sum_{\iota\in I}\mu_\iota=\mu\lambda$. 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 $(\lambda_\iota)_{\iota\in I}$ and $(\mu_\iota)_{\iota\in I}$ be two families of order-types indexed by the same ordered set I. Show that if $\lambda_\iota\prec\mu_\iota$ for each $\iota\in I$, then $\sum_{\iota\in I}\lambda_\iota\prec\sum_{\iota\in I}\mu_\iota$ and (if I is well-ordered) $\mathop{\mathsf{P}}_{\iota\in I}\lambda_\iota\prec\mathop{\mathsf{P}}_{\iota\in I}\mu_\iota$. If J is a subset of I, show that $\sum_{\iota\in J}\lambda_\iota\prec\sum_{\iota\in I}\lambda_\iota$ and (if I is well-ordered and the λ_ι are non-empty) $\mathop{\mathsf{P}}_{\iota\in J}\lambda_\iota\prec\mathop{\mathsf{P}}_{\iota\in I}\lambda_\iota$.

(g) Let λ^* denote the order-type of the set ordered by the opposite of the ordering λ. Then we have

$$(\lambda^*)^*=\lambda \qquad\text{and}\qquad \Big(\sum_{\iota\in I}\lambda_\iota\Big)^*=\sum_{\iota\in I^*}\lambda_\iota^*$$

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 $(\lambda_\iota)_{\iota\in I}$ is a family of ordinals indexed by a well-ordered set I, then the ordinal sum $\sum_{\iota\in I}\lambda_\iota$ is an ordinal; *and that, if moreover, I is finite, then the ordinal product $\mathop{\mathsf{P}}_{\iota\in I}\lambda_\iota$ 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

$$\alpha + 0 = 0 + \alpha = \alpha \qquad \text{and} \qquad \alpha.1 = 1.\alpha = \alpha$$

for every ordinal α.

(b) Show that the relation "λ is an ordinal and μ is an ordinal and $\lambda \prec \mu$" is a *well-ordering* relation, denoted by $\lambda \leq \mu$ (Note that, if λ are μ are ordinals, the relation $\lambda \prec \mu$ is equivalent to "λ is equal to the order-type of a segment of μ" (no. 5, Theorem 3, Corollary 3): given a family $(\lambda_\iota)_{\iota \in I}$ of ordinals, consider a well-ordering in I and take the ordinal sum of the family of sets ordered by the λ_ι; finally use Proposition 2 of no 1.).

(c) Let α be an ordinal. Show that the relation "ξ is an ordinal and $\xi \leq \alpha$" is collectivizing in ξ, and that the set O_α of ordinals $< \alpha$ is a well-ordered set such that $\mathrm{Ord}(O_\alpha) = \alpha$. We shall often identify O_α with α.

(d) Show that for every family $(\xi_\iota)_{\iota \in I}$ there exists a unique ordinal α such that the relation "λ is an ordinal and $\xi_\iota \leq \lambda$ for all $\iota \in I$ is equivalent to $\alpha \leq \lambda$ By abuse of language, α is called the *least upper bound* of the family of ordinals $(\xi_\iota)_{\iota \in I}$, and we write $\alpha = \sup_{\iota \in I} \xi_\iota$ (it is the greatest element of the union of $\{\alpha\}$ and the set of the ξ_ι). The least upper bound of the set of ordinals $\xi < \alpha$ is either α or an ordinal β such that $\alpha = \beta + 1$. In the latter case β is said to be the predecessor of α.

15. (a) Let α and β 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 ξ 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 α, β, μ 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 α and β are such that $\alpha \leq \beta$ if and only if there exists and ordinal ξ such that $\beta = \alpha + \xi$. This ordinal is then unique and is such that $\xi \leq \beta$; it is written $(-\alpha) + \beta$.

(f) Let α, β, ζ be three ordinals such that $\zeta < \alpha\beta$. Show that there exists two ordinals ξ, η such that $\zeta = \alpha\eta + \xi$ and $\xi < \alpha$, $\eta < \beta$ (cf. No. 5, Theorem 3, Corollary 3). Moreover, ξ and η are uniquely determined by these conditions.

¶ 16. An ordinal $\rho > 0$ is said to be *indecomposable* if there exists no pair of ordinals ξ, η such that $\xi < \rho$, $\eta < \rho$ and $\xi + \eta = \rho$.

(a) An ordinal ρ is indecomposable if and only if $\xi + \rho = \rho$ for every ordinal ξ such that $\xi < \rho$.

(b) If $\rho > 1$ is an indecomposable ordinal and if α is any ordinal > 0, then $\alpha\rho$ is indecomposable, and conversely (use Exercise 15(f)).

(c) If ρ is indecomposable and if $0 < \alpha < \rho$, then $\rho = \alpha\xi$, where ξ is an indecomposable ordinal (use Exercise 15(f)).

(d) Let α be an ordinal > 0. Show that there exists a greatest indecomposable ordinal among the indecomposable ordinals $\leq \alpha$ (consider the decomposition $\alpha = \rho + \xi$, where ρ is indecomposable).

(e) If E is a set of indecomposable ordinals, deduced from (d) that the least upper bound of E (Exercise 14(d)) is an indecomposable ordinal.

¶ 17. Given an ordinal α_0, a term $f(\xi)$ is said to be an *ordinal functional symbol (with respect to* ξ*) defined for* $\xi \geq \alpha_0$ if the relation "ξ is an ordinal and $\xi \geq \alpha_0$" implies the relation "$f(\xi)$ is an ordinal"; $f(\xi)$ is said to be *normal* if the relation $\alpha_0 \leq \xi < \eta$ implies $f(\xi) < f(\eta)$ and if for each family $(\xi_\iota)_{\iota \in I}$ of ordinals $\geq \alpha_0$ we have $\sup\limits_{\iota \in I} f(\xi_\iota) = f(\sup\limits_{\iota \in I} \xi_\iota)$ (cf. Exercise 14(d)).

(a) Show that for each ordinal $\alpha > 0$, $\alpha + \xi$ and $\alpha\xi$ are ordinal functional symbols defined for $\xi \geq 0$ (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 "ξ and η are ordinals such that $g(\xi, \eta) > \xi$". 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 $\eta > 1$, $f(\xi, \eta) = \sup\limits_{0<\zeta<\eta} g(f(\xi, \zeta), \xi)$ (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 η (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 (α, β) of ordinals such that $\alpha > 0$, $\alpha \geq \alpha_0$ and $\beta \geq w(\alpha)$ there exists a unique ordinal ξ 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 $f(\xi, \eta) = \xi\eta$.

(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 $\alpha_0 \leq \xi \leq \xi'$, $\alpha_0 \leq \eta < \eta'$ imply $g(\xi, \eta) < g(\xi, \eta')$ and $g(\xi, \eta) \leq g(\xi', \eta)$, then the relations $\alpha_0 \leq \xi < \xi'$ and $\eta \geq 0$ imply $f(\xi, \eta + 1) \leq f(\xi', \eta + 1)$.

(e) Suppose that $w(\xi) = \xi$ and that the relations $\alpha_0 \leq \xi \leq \xi'$, $\alpha_0 \leq \eta < \eta'$ 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 η (defined for $\eta \geq \alpha_0$), and that, whenever $\xi \geq \alpha_0$, $\eta \geq \alpha_0$, and $\zeta \geq \alpha_0$, we have the associativity relation

$$g(g(\xi, \eta), \zeta) = g(\xi, g(\eta, \zeta)).$$

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).

¶ 18. In the definition procedure defined in Exercise 17 (b), take $\alpha_0 = 1+1$ (denoted by 2 by abuse of language),

$$w(\xi) = \xi, \qquad g(\xi,\eta) = \xi\eta.$$

Denote $f(\xi,\eta)$ by ξ^η and define α^0 to be 1 for all ordinals α. Also define 0^β to be 0 and 1^β to be 1 for all ordinals $\beta \geq 1$.

(a) Show that if $\alpha > 1$ and $\beta < \beta'$, we have $\alpha^\beta < \alpha^{\beta'}$, and that, for each ordinal $\alpha > 1$, α^ξ is a normal functional symbol with respect to ξ. Moreover, if $0 < \alpha \leq \alpha'$, we have $\alpha^\beta \leq \alpha'^\beta$.

(b) Show that $\alpha^\xi.\alpha^\eta = \alpha^{\xi+\eta}$ and $(\alpha^\xi)^\eta = \alpha^{\xi\eta}$.

(c) Show that if $\alpha \geq 2$ and $\beta \geq 1$, $\alpha^\beta \geq \alpha\beta$.

(d) For each pair of ordinals $\beta \geq 1$ and $\alpha \geq 2$, there exists three ordinals ξ, γ, δ such that $\beta = \alpha^\xi\gamma + \delta$ where $0 < \gamma\alpha$ and $\delta < \alpha^\xi$, and these ordinals are uniquely by these conditions.

19. * Let α and β be two ordinals and let E and F be two well-ordered sets such that $\mathrm{Ord}(E) = \alpha$ and $\mathrm{Ord}(F) = \beta$. 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 be a *finite* number of elements $y \in F$. 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 $\mathrm{Ord}(G) = \alpha^\beta$ (use the uniqueness property of Exercise17 (b)). *

¶ 20. A set X is said to be *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 $(Y_\iota)_{\iota\in I}$ is a family of transitive sets, then $\bigcup_{\iota\in I} Y_\iota$ and $\bigcap_{\iota\in I} Y_\iota$ are transitive.

(b) A set X is a *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 *decent* if the relation $x \in S$ implies $x \notin x$. 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 $\emptyset$ 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 $(X_\iota)_{\iota\in I}$ is a family of pseudo-ordinals then $\bigcap_{\iota\in I} X_\iota$ 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 α there exists a unique pseudo-ordinal E_α such that $\mathrm{Ord}(E_\alpha) = \alpha$ (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

$$\emptyset, \quad \{\emptyset\}, \quad \{\emptyset,\{\emptyset\}\}, \quad \{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\}$$

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 $Y \subset x$.

8.3 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* $E^F \neq F^E$. *Deduce that if* E *and* F *are the cardinals 2 and 4 (= 2 + 2), then at least one of the sets* E^F, F^E *is not a cardinal.*

Assume $E^F = F^E$. 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^F. The domain of this graph is F; from $E^F = F^E$ 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 *pow*(F, E) the cardinal of $\mathscr{F}(E;F)$, the set of functions from F into E. We have shown (lemma *power_2_4*) that $pow(2,4) = pow(4,2)$. Thus, if a is a cardinal equipotent to $\mathscr{F}(2;4)$ and b a cardinal equipotent to $\mathscr{F}(4;2)$, 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^E; it is F^E if F^E is a cardinal.

¶ 3. Let $(\mathfrak{a}_\iota)_{\iota\in I}$ and $(\mathfrak{b}_\iota)_{\iota\in I}$ be two families of cardinals such that $\mathfrak{b}_\iota \geq 2$ for each $\iota \in I$.

(a) Show that, if $\mathfrak{a}_\iota \leq \mathfrak{b}_\iota$ for each $\iota \in I$, then

$$\sum_{\iota\in I} \mathfrak{a}_\iota \leq \mathop{\mathsf{P}}_{\iota\in I} \mathfrak{b}_\iota.$$

(b) Show that, if $\mathfrak{a}_\iota < \mathfrak{b}_\iota$ for each $\iota \in I$, then

$$\sum_{\iota\in I} \mathfrak{a}_\iota < \mathop{\mathsf{P}}_{\iota\in I} \mathfrak{b}_\iota.$$

(Note that a product $\prod_{\iota\in I} E_\iota$ cannot be the union of a family $(A_\iota)_{\iota\in I}$ such that $\mathrm{Card}(A_\iota) < \mathrm{Card}(E_\iota)$ for all $\iota \in I$, by observing that $\mathrm{Card}(\mathrm{pr}_\iota(A_\iota)) < \mathrm{Card}(E_\iota)$.).

4. Let E be a set and let f be a mapping of $\mathfrak{P}(E) - \emptyset$ into E such that for each non-empty subset X of E we have $f(X) \in X$ ("Choice function").

(a) Let $\mathfrak{b}$ be cardinal and let A be the set of all $x \in E$ such that $\mathrm{Card}(\overset{-1}{f}(x)) \leq \mathfrak{b}$. Show that if $\mathfrak{a} = \mathrm{Card}(A)$, then $2^{\mathfrak{a}} \leq 1 + \mathfrak{a}\mathfrak{b}$ (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 $\overset{-1}{f}(x)$, $\mathrm{Card}(X) \leq \mathfrak{b}$. Show that $\mathrm{Card}(B) \leq \mathfrak{b}$.

5. Let $(\lambda_\iota)_{\iota\in I}$ be a family of order-types (§2, Exercise 13), indexed by an ordered set I. Show that

$$\mathrm{Card}\Big(\sum_{\iota\in I} \lambda_i\Big) = \sum_{\iota\in I} \mathrm{Card}(\lambda_i)$$

and that, if I is well-ordered,

$$\mathrm{Card}\Big(\mathop{\mathsf{P}}_{\iota\in I} \lambda_i\Big) = \mathop{\mathsf{P}}_{\iota\in I} \mathrm{Card}(\lambda_i)$$

6. Show that for every set E there exists $X \subset E$ such that $X \not\subset E$ (use Theorem 2 of no. 6).

8.4 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 $\mathfrak{P}(E)$ satisfying the following conditions: (i) $\emptyset \in \mathfrak{G}$; (ii) the relation $X \in \mathfrak{G}$ and $x \in E$ imply $X \cup \{x\} \in G$.

(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 § 5; no 1 Proposition 1, Corollary 1).

(c) Deduce from (a) and (b) that for every finite set E the set $\mathfrak{P}(E)$ is finite (consider the set of subsets X of E such that $\mathfrak{P}(X)$ is finite; cf § 5; no 1 Proposition 1, Corollary 4).

2. Show that a set E is finite if and only every non-empty subset of $\mathfrak{P}(E)$ 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 (§ 1, Exercise 5). Show that E can be partitioned into k totally ordered subsets (with respect to the induced ordering)[1]. 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 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 then sets F_i and use the fact that C_0 is strongly related to obtain a contradiction).

[1] This is called Dilworth's theorem in the French edition

¶ 6. (a) Let A be a set and let $(X_i)_{1\le i\le m}$, $(Y_j)_{m+1\le j\le m+n}$ be two finite families of subsets of A. Let h be the least integer such that, for each integer $r \le m-h$ and each subset $\{i_1,\dots,i_{r+h}\}$ of $r+h$ elements of $[1,m]$, there exists a subset $\{j_1,\dots,j_r\}$ of r elements of $[m+1,m+n]$ for which the union of the sets X_{i_α} $(1\le\alpha\le r+h)$ meets each of the sets Y_{j_β} $(1\le\beta\le r)$ (which implies that $m\le n+h$). Show that there exists a finite subset B of A with at most $n+h$ elements such that every X_i $(1\le i\le m)$ and every Y_j $(m+1\le j\le m+n)$ meets B. (Consider the order relation on the interval $[1,m+n]$ whose graph is the union of the diagonal and the set of pairs (i,j) such that $1\le i\le m$ and $m+1\le j\le m+n$ and $X_i\cap Y_j\neq\emptyset$, 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 $\mathfrak{P}(F)$. 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 $\mathrm{Card}\big(\bigcup_{x\in H} A(x)\big)\ge \mathrm{Card}(H)$ (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 $f(E)\supset G$ 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 $\ge \mathrm{Card}(L)$. (Let $(a_i)_{1\le i\le p}$ be the sequence of distinct elements of G, arranged in some order; let $(b_j)_{p+1\le j\le p+m}$ be the sequence of distinct elements of F, arranged in some order; and let $(c_k)_{p+m+1\le k\le P+M+n}$ 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

$$1\le i\le p \text{ and } p+1\le j\le p+m \text{ and } a_i=b_j,$$

$$\text{or } 1\le i\le p \text{ and } p+m+1\le j\le p+m+n \text{ and } a_i\in A(c_j),$$

$$\text{or } p+1\le i\le p+m \text{ and } p+m+1\le j\le p+m+n \text{ and } b_i\in A(c_j);$$

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 $\sup(e_1,\dots,e_k)$ where the e_i $(1\le i\le n)$ 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 $\le x$. Show that the mapping $x\to S(x)$ is an isomorphism of E onto a subset of $\mathfrak{P}(J)$, ordered by inclusion, and that $S(\inf(x,y))=S(x)\cap S(y)$.

¶ 8. (a) Let E be a distributive lattice (§ 1, Exercise 16). If a is irreducible in E (Exercise 7), show that the relation $a\le\sup(x,y)$ implies $a\le x$ or $a\le y$.

(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 $x\to S(x)$ of E onto a subset of $\mathfrak{P}(J)$ 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 $\mathscr{A}(J^*,I)$ of increasing mappings of J^* into $I=\{0,1\}$ (§ 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 $y_1,\dots,y_k$ be the distinct minimal elements of the interval $]x,\to[$ in E;

for each index i, let q_i be an element of P such that $q_i \notin \mathrm{S}(x)$ and $q \in \mathrm{S}(y_i)$. 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

$$v_i = \sup_{1 \le j \le k, j \ne i} (q_j) \qquad (1 \le i \le k).$$

Show that $v_i < u$ for $1 \le i \le k$. Let $x = \inf(v_1, \ldots, v_k)$ and let

$$y_i = \inf_{1 \le j \le k, j \ne i} (v_j)$$

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, $\sup_{\mathrm{E}}(x, y)$ and $\inf_{\mathrm{E}}(x, y)$ belong to A.

(a) Let $(\mathrm{C}_i)_{1 \le i \le n}$ be a finite family of totally ordered sets and let $\mathrm{E} = \prod_{i=1}^{n} \mathrm{C}_i$ 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

$$v_j = \inf_{1 \le j \le r, j \ne i} (a_j)$$

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 (§ 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 $(1 \le i \le n)$. With each $x \in \mathrm{F}$ associate the family $(x_i)_{1 \le i \le n}$ where x_i is the least upper bound in C_i of the sets of elements of P_i which are $\le x$.)

¶ 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 $\mathrm{F} = \prod_{i=1}^{n} \mathrm{F}_i$ is a product of n totally ordered sets, the 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 Γ on E is such that there exists another ordering Γ' on E with the property that any two distinct elements of E are comparable with respect to exactly one of the orderings Γ and Γ'.

(c) Let A be a finite set of n elements. Let E be the subset of $\mathfrak{P}(\mathrm{A})$ consisting of all subsets $\{x\}$ and $\mathrm{A} - \{x\}$ 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 $\mathfrak{R}$ be a subset of the set $\mathfrak{F}(\mathrm{A})$ of finite subsets of A. $\mathfrak{R}$ is set to be *mobile* if it satisfies the following condition:
(MO) If X, Y are two distinct elements of $\mathfrak{R}$ and if $z \in \mathrm{X} \cap \mathrm{Y}$, then there exists $\mathrm{Z} \subset \mathrm{X} \cap \mathrm{Y}$ belonging to $\mathfrak{R}$ such that $z \notin \mathrm{Z}$.
A subset P of A is then said to be *pure* if it contains no set belonging to $\mathfrak{R}$.

(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 $x \in \complement\mathrm{M}$ there exists a unique finite subset $\mathrm{E_M}(x)$ of M such that $\mathrm{E_M}(x) \cup \{x\} \in \mathfrak{R}$. Moreover, if $y \in \mathrm{E_M}(x)$, the set $(\mathrm{M} \cup \{x\}) - \{y\}$ is a maximal pure subset of A.

(c) Let M, N be two maximal pure subsets of A, such that $\mathrm{N} \cap \complement\mathrm{M}$ is finite. Show that $\mathrm{Card(M)} = \mathrm{Card(N)}$. (Proof by induction on the cardinal of $\mathrm{N} \cap \complement\mathrm{M}$, using (b).)

(d) Let M, N be two maximal pure subsets of A, and put $\mathrm{N}' = \mathrm{N} \cap \complement\mathrm{M}$, $\mathrm{M}' = \mathrm{M} \cap \complement\mathrm{N}$. Show that $\mathrm{M}' \subset \bigcap_{x \in \mathrm{N}'} \mathrm{E_M}(x)$. * Deduce that $\mathrm{Card(M)} = \mathrm{Card(N)}$ (by virtue of (c), we are reduced to the case where N' and M' are infinite; show then that $\mathrm{Card(M')} \leq \mathrm{Card(N')}$). *

8.5 Section 5

1. Prove the formula

$$\sum_{k=q+1}^{n-p+q+1} \binom{n-k}{p-q-1}\binom{k-1}{q} = \binom{n}{p},$$

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

$$\binom{n}{0}\binom{n}{p} + \binom{n}{1}\binom{n-1}{p-1} + \binom{n}{2}\binom{n-2}{p-2} + \cdots + \binom{n}{p}\binom{n-p}{0} = 2^p\binom{n}{p},$$

$$\binom{n}{0}\binom{n}{p} - \binom{n}{1}\binom{n-1}{p-1} + \binom{n}{2}\binom{n-2}{p-2} - \cdots + (-1)^p\binom{n}{p}\binom{n-p}{0} = 0.$$

(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.)

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

$$\sum_{i=1}^{h} u(x) \leq n$$

onto the set of strictly increasing mappings of $[1, h]$ into $[1, n+h]$.

5. * (a) Let E be a distributive lattice and let f be a mapping of E into a commutative semigroup 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

$$f(\sup(\mathrm{I}))+\sum_{2n\le \mathrm{Card(I)}}\Big(\sum_{\mathrm{H}\subset \mathrm{I},\mathrm{Card(H)}=2n} f(\inf(\mathrm{H}))\Big)=\sum_{2n+1\le \mathrm{Card(I)}}\Big(\sum_{\mathrm{H}\subset \mathrm{I},\mathrm{Card(H)}=2n+1} f(\inf(\mathrm{H}))\Big)$$

(By induction on Card(I)).) *

(b) In particular let A be a set, let $(\mathrm{B}_i)_{i\in \mathrm{I}}$ 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 $\mathrm{B_H}=\bigcap_{i\in \mathrm{H}}\mathrm{B}_i$. Show that

$$\mathrm{Card(B)}+\sum_{2n\le \mathrm{Card(I)}}\Big(\sum_{\mathrm{Card(H)}=2n}\mathrm{Card(B_H)}\Big)=\sum_{2n+1\le \mathrm{Card(I)}}\Big(\sum_{\mathrm{Card(H)}=2n+1}\mathrm{Card(B_H)}\Big).$$

6. Prove the formula

$$\binom{n+h}{h}=1+\binom{h}{1}\binom{n+h-1}{h}-\binom{h}{2}\binom{n+h-2}{h}+\ldots+(-1)^h\binom{h}{h}\binom{n}{h}.$$

(If F denotes the set of mappings u of $[1,h]$ into $[0,n]$ such that $\sum_{x=1}^{h}u(x)\le n$, consider for each subset H of $[1,h]$ the set of all $u\in \mathrm{F}$ such that $u(x)\ge 1$ for each $x\in \mathrm{H}$, and use Exercise 5.)

7. (a) Let $\mathrm{S}_{n,p}$ denote the number of mappings of $[1,n]$ *onto* $[1,p]$. Prove that

$$\mathrm{S}_{n,p}=p^n-\binom{p}{1}(p-1)^n+\binom{p}{2}(p-2)^n-+\ldots+(-1)^{p-1}\binom{p}{p-1}.$$

(Note that $p^n=\mathrm{S}_{n,p}=\binom{p}{1}\mathrm{S}_{n,p-1}+\binom{p}{2}\mathrm{S}_{n,p-2}+\ldots+\binom{p}{p-1}$ and use Exercise 3.)

(b) Prove that $\mathrm{S}_{n,p}=p(\mathrm{S}_{n-1,p}+\mathrm{S}_{n-1,p-1})$ (method of no. 8, Proposition 13).

(c) Prove that

$$\mathrm{S}_{n+1,n}=\frac{n}{2}(n+1)!\qquad\text{and}\qquad \mathrm{S}_{n+2,n}=\frac{n(3n+1)}{24}(n+2)!$$

(consider the elements r of $[1,n]$ whose inverse image consists of more than one element).

(d) If $\mathrm{P}_{n,p}$ is the number of partitions into p parts of a set of n elements, show that $\mathrm{S}_{n,p}=p!\mathrm{P}_{n,p}$.

8. Let p_n be the number of permutations of a set E with n elements such that $u(x)\ne x$ for all $x\in \mathrm{E}$. Show that

$$p_n=n!-\binom{n}{1}(n-1)!+\binom{n}{2}(n-2)!-\cdots+(-1)^n$$

* 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

$$(qn)!/(n!(q!)^n).$$

(b) Suppose that $\mathrm{E} = [1, qn]$. 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

$$\frac{(qn)!}{n!(q!)^n} - \frac{(qn-q+1)!}{1!(n-1)!(q!)^{n-1}} + \frac{(qn-2q+2)!}{2!(n-2)!(q!)^{n-2}} - \cdots + (-1)^n$$

(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

$$q_{n,k} = \binom{[\frac{n+k}{2}]}{k}.$$

¶ 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 $\mathrm{L}_0(\mathrm{S})$ 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

$$u_n = 2.6\ldots(4n-6) \qquad (n \geq 2)$$

(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 ith 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

$$v_{n+1} = v_1 v_n + v_2 v_{n-1} + \cdots + v_{n-1} v_2 + v_n v_1.$$

¶ 12. (a) let p and q be two integers ≥ 1, let $n = 2p+q$, let E be a set with n elements and let $\mathrm{N} = \binom{n}{p} = \binom{n}{p+q}$. Let $(\mathrm{X}_i)_{1\leq i\leq \mathrm{N}}$ (resp $(\mathrm{Y}_i)_{1\leq i\leq \mathrm{N}}$) 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 ϕ of $[1,n]$ onto itself such that $\mathrm{X}_{\phi(i)} \subset \mathrm{Y}_i$ for all i. (The method is analogous to that of Exercise 6 of § 4: observe that for each $r \leq \mathrm{N}$ the number of sets Y_j which contain at least one of X_1, …, X_r is $\geq r$).

(b) Let h, k be two integers ≥ 1, let n be an integer such that $2h+k<n$, let E be a set with n elements and let $(\mathrm{X}_i)_{1\leq i\leq r}$ be a sequence of distinct subsets of E, each having h elements. Show that there exists a sequence $(\mathrm{Y}_j)_{1\leq j\leq r+1}$ 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 $\mathscr{F}$ be the set of all subsets $\mathfrak{S}$ of $\mathfrak{P}(\mathrm{E})$ with the following property: if X and Y are two distinct elements of $\mathfrak{S}$ such that $\mathrm{X} \subset \mathrm{Y}$, then $\mathrm{Y} - \mathrm{X}$ has at most $2q$ elements.

(a) Let $\mathfrak{M} = (\mathrm{A}_i)_{1\le i\le p}$ be an element of $\mathscr{F}$ such that $p = \mathrm{Card}(\mathfrak{M})$ is as large as possible. Show that $m - q \le \mathrm{Card}(\mathrm{A}_i) \le m + q$ for $1 \le i \le p$ (Argue by contradiction. Suppose, for example, that there exists indices i such that $\mathrm{Card}(\mathrm{A}_i) < m - q$ and consider those of the A_i for which $\mathrm{Card}(\mathrm{A}_i)$ has the least possible value $m-q-s$ (where $s \ge 1$). Let $\mathrm{A}_1, \ldots, \mathrm{A}_r$, say, these sets. Let $\mathfrak{G}$ be the set of subsets of E each of which is the union of some A_i $(1 \le i \le r)$ and a subset of $2q+1$ elements contained in $\mathrm{E}-\mathrm{A}_i$. Show that $\mathfrak{G}$ contains at least $r+1$ elements (cf. Exercise 12), and that if $\mathrm{B}_1, \ldots, \mathrm{B}_{r+1}$ are $r+1$ distinct elements of $\mathfrak{G}$, the set whose elements are B_j $(1 \le j \le r+1$ and A_i $(r+1 \le i \le p)$ belongs to $\mathscr{F}$, contrary to the hypothesis.)

(b) Deduce from (a) that the number of elements p of each $\mathfrak{S} \in \mathscr{F}$ satisfies the inequality

$$p \le \sum_{k=0}^{2q} \binom{2m}{m-q+k}.$$

(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 $(a_j)_{1\le j\le n}$ be the sequence of elements of E arranged in some order, and let $(\mathrm{A}_i)_{1\le i\le m}$ be a sequence of subsets of E.

(a) For each index j, let k_j be the number of indices i such that $a_j \in \mathrm{A}_i$, and let $\mathrm{S}_i = \mathrm{Card}(\mathrm{A}_i)$. 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 $a_j \notin \mathrm{A}_i$, then $\mathrm{S}_i \le k_j$.

(c) With the hypotheses of (b), show that $m \ge n$ (Let k_n be the least of the numbers k_j. Show that we may suppose that, whenever $i \le k_n$, $j \le k_n$, and $i \ne j$, we have $a_j \notin \mathrm{A}_i$ and $a_n \notin \mathrm{A}_j$ for all $j \ge k_n$.)

(d) With the hypotheses of (b), show that $m = n$ if and only if one of the following two alternatives is true: (i) $\mathrm{A}_1 = \{a_1, a_2, \ldots, a_{n-1}\}$, $\mathrm{A}_i = \{a_{i-1}, a_n\}$ 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 $\mathfrak{L}$ and $\mathfrak{C}$ be two disjoint non-empty subsets of $\mathfrak{P}(\mathrm{E})$, and let λ, h, k, l be four integers ≥ 1 with the following properties: (i) for each $\mathrm{A} \in \mathfrak{L}$ and each $\mathrm{B} \in \mathfrak{C}$, $\mathrm{Card}(\mathrm{A} \cap \mathrm{B}) \ge \lambda$; (ii) for each $\mathrm{A} \in \mathfrak{L}$, $\mathrm{card}(\mathrm{A}) \ge h$; (iii) for each $\mathrm{B} \in \mathfrak{C}$, $\mathrm{card}(\mathrm{B}) \le k$; (iv) for each $x \in \mathrm{E}$ the number of elements of $\mathfrak{L} \cup \mathfrak{C}$ which contain x is exactly l. Show that $\mathrm{Card}(\mathrm{E}) \le hk/\lambda$. (Let $(a_i)_{1\le i\le n}$ 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 $\mathfrak{L}$ to which a_i belongs. Show that, if $\mathrm{Card}(\mathfrak{L}) = s$ and $\mathrm{Card}(\mathfrak{C}) = t$, then we have

$$\sum_{i=1}^{n} r_i \le sh, \qquad \sum_{i=1}^{n} (l - r_i) \le tk, \qquad \sum_{i=1}^{n} r_i(l - r_i) \ge \lambda st.)$$

For $\mathrm{Card}(\mathrm{E})$ to be equal to hk/λ it is necessary and sufficient that for each $\mathrm{A} \in \mathfrak{L}$ and each $\mathrm{B} \in \mathfrak{C}$ we have $\mathrm{card}(\mathrm{A}) = h$, $\mathrm{card}(\mathrm{B}) = k$, $\mathrm{Card}(\mathrm{A} \cap \mathrm{B}) = \lambda$ and that there exists an $r \le l$ such that for each $x \in \mathrm{E}$ the number of elements of $\mathfrak{L}$ to which x belongs is equal to r.

16. Let E be a finite set with n elements, let $\mathfrak{D}$ be a non-empty subset of $\mathfrak{P}(\mathrm{E})$, and let λ, k, l be three integers ≥ 1 with the following properties: (i) if A and B are distinct elements of $\mathfrak{D}$, then $\mathrm{Card}(\mathrm{A} \cap \mathrm{B}) = \lambda$; (ii) for each $\mathrm{A} \in \mathfrak{D}$, $\mathrm{card}(\mathrm{A}) \leq k$; (iii) for each $x \in \mathrm{E}$ the number of elements of $\mathfrak{D}$ 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 $\mathrm{Card}(\mathfrak{D}) = n$. (Given $a \in \mathrm{E}$, let $\mathfrak{L}$ be the set of all $\mathrm{A} - \{a\}$ where $\mathrm{A} \in \mathfrak{D}$ and $a \in \mathrm{A}$, and let $\mathfrak{C}$ be the set of all $\mathrm{A} \in \mathfrak{D}$ such that $a \notin \mathrm{A}$. Apply the results of Exercise 15 to $\mathfrak{L}$ and $\mathfrak{C}$.

¶ 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 $m_i(h,k)$ with the following properties: for each finite set E with at least $m_i(h,k)$ elements, and each partition $(\mathfrak{X}, \mathfrak{Y})$ of the set $\mathfrak{F}_i(\mathrm{E})$ of subsets of i elements of E, it is impossible that every subset of h elements of E contains a subset $\mathrm{X} \in \mathfrak{X}$ and that every subset of k elements of E contains a subset $\mathrm{Y} \in \mathfrak{Y}$; in other words, if every subset of h elements of E contains some $\mathrm{X} \in \mathfrak{X}$ there exists a subset A of k elements of E such that every subset of i elements of A belongs to $\mathfrak{X}$ (Proof by induction. Show that we may take $m_1(h,k) = h + k - 1$, $m_i(i,k) = k$ and $m_i(h,i) = h$ and finally $m_i(h,k) = m_{i-1}(m_i(h-1,k), m_i(h,k-1)) + 1$. If E is a set with $m_i(h,k)$ elements if $a \in \mathrm{E}$ and $\mathrm{E}' = \mathrm{E} - \{a\}$, show that if the proposition were false, then every subset of $m_i(h-1,k)$ elements of E' would contain a subset X' of $i-1$ elements such that $\mathrm{X}' \cup \{a\} \in \mathfrak{X}$, and that every subset of $m_i(h,k-1)$ elements of E' would contain a subset Y' of $i-1$ elements such that $\mathrm{Y}' \cup \{a\} \in \mathfrak{Y}$.

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 ≥ 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 $(x_i)_{i \in \mathrm{I}}$ of elements of a totally ordered set E, there exists either a subset H of h elements of I such that the sequence $(x_i)_{i \in \mathrm{H}}$ is increasing, or else a subset K of k elements of I such that the sequence $(x_i)_{i \in \mathrm{H}}$ is decreasing. (Use (a) applied to $\mathrm{I} \times \mathrm{E}$.)

8.6 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* $\mathrm{S} \neq \mathrm{E}$ *and* $f(\mathrm{S}) \subset \mathrm{S}$.

Assume E non-empty, and let $f : \mathrm{E} \to \mathrm{E}$. Fix $x \in \mathrm{E}$, and define by induction $g(n+1) = f(g(n))$, with $g(0) = x$. Let G be the range (or target) of g and $\mathrm{S} = f(\mathrm{G})$. Then G and S are non-empty and stable by f. If $x \notin \mathrm{S}$, then $\mathrm{S} \neq \mathrm{E}$. 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 $\mathrm{S} \neq \mathrm{E}$.

```
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.
```

```
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 : Bset => W n f) y).
set (g:=induction_defined (fun n : Bset => 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 H11. nin H11. ee. wri H9 H11. ufi image_of_fun H11. awi H11. nin H11. ee.
red in H13. cp (W_pr H6 H13). red in H12.  cp (W_pr H0 H12). rwi H14 H15.
rwi H5 H11. rw H15. wr H8. app inc_W_target. rw H5. fprops. am. fprops.
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.
ufi image_by_fun H3. awi H3. nin H3. nin H3. red in H13.
ufi F H3. wri H9 H3.  ufi image_of_fun H3. awi H3. nin H3. ee. red in H14.
cp (W_pr H6 H14). cp (W_pr H0 H13). rwi H15 H16. wri H8 H16. wri H7 H16.
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. rww zero_unit_sum2. 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. rww 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.
rww zero_unit_sum1. fprops. ir. rw card_mult_commutative.
rw mult_via_plus. rw card_plus_associative. wr H18. rww card_mult_commutative.
fprops. fprops.
assert (forall z, inc z E -> exists m, cardinal_lt m k & z = W m g). ir.
wri H12 H20. ufi G H20. ufi image_by_fun H20. awi H20. nin H20. nin H20.
red in H21. rw (W_pr H0 H21). ufi F H20. wri H9 H20. ufi image_of_fun H20.
awi H20. nin H20. nin H20. red in H22. rw (W_pr H6 H22). wr H8.
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.
cp (division_exists H23 H24 H25). nin H26. nin H26. ee. red in H28. ee.
rw H28. rw card_plus_commutative. exists x4.  split. am.
rww card_mult_commutative. wr H19. tv. am. am. wrr 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.
assert (inc x2 Bnat). red in H23. ee. rw inc_Bnat. rwi inc_Bnat H22.
app (le_int_is_int H22 H23). uf image_by_fun. aw.
exists x2. ee. rw interval_co_0a_pr2.  split; am. am.
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. wrr H5.
fprops. fprops. uf image_by_fun. red. ir. awi H12. nin H12. nin H12.
```

```
ufi G H12. ufi image_by_fun H12. awi H12. nin H12. nin H12.
uf G. uf image_by_fun. aw. exists x0. split.  app H11. uf image_by_fun.
aw. exists x1. split; am. fprops. am. fprops. fprops. fprops.
```

Converse. We assume that for every function $f : \mathrm{E} \to \mathrm{E}$ there is a non-trivial subset of E invariant by f. This implies E non-empty. Assume E finite. There is a bijection $\mathrm{T} : [0, n[\to \mathrm{E}$, 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 $g(\mathrm{S}) \subset \mathrm{S}$. Since this set is not empty, it contains an element $\mathrm{T}(i)$. By induction it contains all $\mathrm{T}(i+j \pmod{n})$, thus all elements of E.

```
ir. red. split. fprops. red. ir. set (n:= cardinal E).
assert (inc n Bnat). rww inc_Bnat.
assert (equipotent E (interval_co_0a n)). wr cardinal_equipotent.
rw cardinal_interval_co_0a1. tv. am. red in H2. nin H2. ee.
set  (y:=inverse_fun x).
assert (nonempty E). set (f:=identity_fun E).
assert (is_function f). uf f.  app function_identity. assert (source f = E).
uf f. tv. assert (target f = E). uf f. tv. nin (H _ H5 H6 H7). ee.
nin H9. exists y0. app H8. assert (n <> card_zero). red. ee. ir. ufi n H6.
rwi zero_is_emptyset H6. rwi cardinal_emptyset H6. rwi H6 H5. nin H5.
elim (emptyset_pr H5). set (f:= fun i=> card_rem (succ i) n).
assert (Ha: forall i, inc i Bnat -> inc (card_rem i n) (interval_co_0a n)).
ir. rw interval_co_0a_pr2. cp (Bnat_division H7 H1 H6).
ee. am. red in H10; ee; am. am.
assert (Hb:sub  (interval_co_0a n)  Bnat). uf interval_co_0a.
uf interval_co. rw substrate_Bnat_order. app Z_sub.
assert (forall i, inc i (interval_co_0a n) -> inc (f i) (interval_co_0a n)).
ir. uf f. app Ha. cp (Hb _ H7). fprops.
cp (inverse_bij_is_bij_alt H2). cp (bij_is_function H2).
cp (bij_is_function H8).
set (g:= fun u => W (f  (W u x)) y).
assert (transf_axioms g E E). red.  ir. uf g. uf y.
assert (E = target (inverse_fun x)). rw target_inverse. sy; am. rw H12.
app inc_W_target. rw source_inverse. rw H4. app H7. wr H4. app inc_W_target.
rww 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. wrr 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). wrr H22.
assert (forall j, inc j Bnat -> inc (W (card_rem (card_plus i j)n) y) x0).
app cardinal_c_induction_v. rw  zero_unit_sum1.
assert (card_rem i n = i). cp (Bnat_division H19 H1 H6). ee.
assert (division_prop i n  card_zero i). red. split. rw zero_prod_absorbing.
rw  zero_unit_sum2. tv. fprops.   assert (inc i (target x)).
uf i. app inc_W_target. rww H3. app H15. rwi H4 H24.
rwi 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:= card_rem (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 = 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. wri 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 H23 H22. red in H8. ee. fold y in H24.
  cp (surjective_pr2 H24 H22). nin H25. ee. rw H26. ufi y H25.
  rwi source_inverse H25. rwi H4 H25.
  assert (inc i (target x)). uf i. app inc_W_target. rww H3. app H15.
  rwi H4 H27.  rwi interval_co_0a_pr2 H27. ee.  red in H28.
  set (j:= card_sub n i). ee. cp (card_sub_pr H1 H27 H28). fold j in H30.
  assert (inc j Bnat). uf j. fprops.
  set (k:= card_plus j x2).  assert (inc k Bnat). uf k. fprops.
  cp (H21 _ H32). assert (card_rem (card_plus i k) n = x2).
  assert (division_prop (card_plus i k) n card_one x2). red.
  rw one_unit_prod1. split. uf k. rw card_plus_associative. rww H30.
  rwi interval_co_0a_pr2 H25. ee; am. am. fprops.
  assert (inc (card_plus i k) Bnat). fprops.
  cp (Bnat_division H35 H1 H6). ee.
  cp (division_unique H35 H1 (inc1_Bnat) (Hb _ H25) H37 H36 H6 H34 H38).
  ee. sy; am.  rwi H34 H33. am. am.
Qed.
```

---

2. *Show that, if* $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ *and* $\mathfrak{d}$ *are four cardinals such that* $\mathfrak{a} < \mathfrak{c}$ *and* $\mathfrak{b} < \mathfrak{d}$ *then* $\mathfrak{a} + \mathfrak{b} < \mathfrak{c} + \mathfrak{d}$ *and* $\mathfrak{a}\mathfrak{b} < \mathfrak{c}\mathfrak{d}$. *(cf. Exercise 21 (c)).*

We first assume $\mathfrak{c} \leq \mathfrak{d}$. If $\mathfrak{d}$ is finite, all quantities are finite and the result is obvious.

```
Lemma exercice6_2: forall a b c d, cardinal_lt a c ->
  cardinal_lt b d ->
  (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 -> cardinal_lt a c ->
  cardinal_lt b d ->
  (cardinal_lt (card_plus a b) (card_plus c d) &
    cardinal_lt (card_mult a b) (card_mult c d))).
```

```
ir.  assert (Ha:c <> card_zero). red. ir. rwi H2 H0.
app (zero_smallest1 H0).
apply by_cases with (is_finite_c d). ir.
cp (le_int_is_int H2 H).
assert (is_finite_c a). nin H0. app (le_int_is_int H3 H0).
assert (is_finite_c b). nin H1. app (le_int_is_int H2 H1).
split. app finite_sum2_lt. rww inc_Bnat. rww inc_Bnat. rww inc_Bnat.
rww inc_Bnat.  nin H0. am. app finite_prod2_lt. rww inc_Bnat. rww inc_Bnat.
rww inc_Bnat. rww inc_Bnat. nin H0. am.
```

We have now $\mathfrak{c} + \mathfrak{d} = \mathfrak{c}\mathfrak{d} = \mathfrak{d}$. Such a formula holds if one of $\mathfrak{a}$ or $\mathfrak{b}$ is infinite (the result is trivial is none is infinite). Note that if one of the cardinals is zero, so is the product, thus is $< \mathfrak{d}$.

```
ir. assert (is_infinite_c d). red. ee.  nin H.  nin H3. am. am.
rw (card_mult_commutative c d). rww (product2_infinite H H3 Ha).
rw (card_plus_commutative c d). rw (sum2_infinite H H3).
apply by_cases with (is_finite_c a). ir.
apply by_cases with (is_finite_c b). ir.
wri inc_Bnat H4; wri inc_Bnat H5.
assert (is_finite_c (card_plus a b)). fprops. wr inc_Bnat. fprops.
assert (is_finite_c (card_mult a b)). fprops. wr inc_Bnat. fprops.
split. app finite_lt_infinite. app finite_lt_infinite.
ir. assert (is_infinite_c b). red. ee. red in H1. ee.  red in H1; ee; am. am.
cp  (finite_le_infinite H4 H6).
split. rw card_plus_commutative. rw (sum2_infinite H7 H6). am.
nin (equal_or_not a card_zero). rw H8.
rw card_mult_commutative. rw zero_prod_absorbing.  app finite_lt_infinite.
wr inc_Bnat. fprops. rw card_mult_commutative.
rww (product2_infinite H7 H6 H8). ir. assert (is_infinite_c a). red. ee.
red in H0. ee.  red in H0; ee; am. am.
apply by_cases with (is_finite_c b). ir.
cp  (finite_le_infinite H6 H5). split. rw (sum2_infinite H7 H5).
app (cardinal_lt_le_trans H0 H).
nin (equal_or_not b card_zero). rw H8. rw zero_prod_absorbing.
app finite_lt_infinite. wr inc_Bnat. fprops.
rww (product2_infinite H7 H5 H8).  app (cardinal_lt_le_trans H0 H).
```

Here all cardinals are infinite. In particular, they are non-zero. We have $\mathfrak{a} + \mathfrak{b} = \mathfrak{a}\mathfrak{b} = \mathfrak{a}'$ where $\mathfrak{a}' < \mathfrak{d}$ is the greatest of the two cardinals.

```
ir. assert (is_infinite_c b). red. ee. red in H1. ee. red in H1; ee; am. am.
 assert (cardinal_le a b \/ cardinal_le b a).
 nin H0. nin H0.nin H1; nin H1. nin (cardinal_le_total_order1 H0 H1).
 left. rw H12. fprops. nin H12.  nin H12. left. am. nin H12. right. am.
 nin H8.  split. rw card_plus_commutative. rw (sum2_infinite H8 H7). am.
 nin (equal_or_not a card_zero). rw H9.
 rw card_mult_commutative. rw zero_prod_absorbing.  app finite_lt_infinite.
 wr inc_Bnat. fprops. rw card_mult_commutative.
 rww (product2_infinite H8 H7 H9). rw (sum2_infinite H8 H5).  split.
 app (cardinal_lt_le_trans H0 H). nin (equal_or_not b card_zero). rw H9.
 rw zero_prod_absorbing.  app finite_lt_infinite. wr inc_Bnat. fprops.
 rww (product2_infinite H8 H5 H9).  app (cardinal_lt_le_trans H0 H).
```

The result is now clear. If $\mathfrak{c} \geq \mathfrak{d}$, we use commutativity.

```
  ir. assert (cardinal_le c d \/ cardinal_le d c).
  red in H0. red in H1. ee. red in H0; red in H1; ee.
  nin (cardinal_le_total_order1 H6 H4).
  left. rw H8. fprops. nin H8.  nin H8. left. am. nin H8. right. am.
  nin H2. app H.
  rw (card_plus_commutative c d). rw (card_mult_commutative c d).
  rw (card_plus_commutative a b). rw (card_mult_commutative a b). app H.
Qed.
```

---

3. *If* E *is an infinite set, the subsets of* E *which are equipotent to* E *is equipotent to* $\mathfrak{P}(E)$ *(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 $E_1 \cup E_2 \to E$. Xe 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 ->
  equipotent (powerset E) (Zo (powerset E) (fun z => equipotent z E)).
Proof. ir. set (Qo:= Zo (powerset E) (fun z : Bset => 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 (equipotent E2 n). eqtrans E.  eqsym. uf E2. fprops. uf n. fprops.
  assert (disjoint E1 E2). uf E1; uf E2. app disjoint_union2_pr. fprops.
  cp (card_plus_pr1 H5 H3 H4). rwi H2 H6. ufi n H6. awi H6. nin H6. ee.
  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.
  ufi image_by_fun H10. awi H10. nin H10. ee. red in H12. wr H8.
  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.
  rwi powerset_inc_rw H11.  uf Qo. Ztac. app powerset_inc. app H9.
  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.

```
  set_extens. 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.
  awi H18. nin H18. ee. red in H19. cp (W_pr H15 H19). unfold y in H20.
  assert (inc x1 (source x)). rw H7. nin (union2_or H18).  app union2_first.
  uf E1. awi H21. ee. aw. ee.  am. rwi powerset_inc_rw H13.  app H13. am.
  app union2_second. nin H6. nin H6. cp (H23 _ _ H17 H21 H20).
  nin (union2_or H18).  awi H25.  ee. wri H24 H26. awi H26. am. ufi E2 H25.
  awi H25. ee. wri H24 H27. awi H27. cp (singleton_eq 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. aw. ee.
  fprops. rwi powerset_inc_rw H13. app H13. fprops.
  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.
  awi H18. nin H18. ee. red in H19. cp (W_pr H15 H19). unfold y in H20.
  assert (inc x1 (source x)). rw H7. nin (union2_or H18).  app union2_first.
  uf E1. awi H21. ee. aw. ee.  am. rwi powerset_inc_rw H12.  app H12. am.
  app union2_second. nin H6. nin H6. cp (H23 _ _ H17 H21 H20).
  nin (union2_or H18).  awi H25.  ee. wri H24 H26. awi H26. am. ufi E2 H25.
  awi H25. ee. wri H24 H27. awi H27. cp (singleton_eq H27).
  elim two_points_distinct. am. fprops.
  assert (cardinal_le (cardinal (powerset E)) (cardinal Qo)). red. ee.
  fprops. fprops. wr cardinal_le2. rw cardinal_le1. exists F. ee. am. uf F.
  tv. uf F. tv. wr cardinal_equipotent.
  app cardinal_antisymmetry1.
Qed.
```

---

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 ϖ be a partition, and $\tilde{\varpi}$ be the union of all $A \times A$ with $A \in \varpi$. We know that $\tilde{\varpi} \supset \tilde{\varpi}'$ is an order (see chapter one), so that the function $\varpi \mapsto \tilde{\varpi}$ is injective. Let Q be the set of partitions; this shows $\mathrm{Card}(Q) \leq \mathrm{Card}(\mathfrak{P}(E \times E))$, hence $\mathrm{Card}(Q) \leq \mathrm{Card}(\mathfrak{P}(E)$.

```
Lemma Exercise6_4: forall E, infinite_set E ->
  equipotent (set_of_partition_set E)(powerset E).
Proof. ir.  set (q:=set_of_partition_set E).
  set (f:= BL (fun y=> partition_relation_set y E) q (powerset (coarse E))).
  assert (injective f). uf f. app injective_af_function. red. ir.
  app powerset_inc. app sub_partition_relation_set_coarse. ufi q H0.
  ufi set_of_partition_set H0. Ztac. am. uf q. uf set_of_partition_set. ir.
  Ztac. clear H1. Ztac. sy.
  app (partition_relation_set_order_antisymmetric H4 H5).
```

```
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_equipotent.  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 $\mathrm{I} \mapsto \{\mathrm{I}, \mathrm{E}-\mathrm{I}\}$. This mapping is not injective for $\mathrm{I} \subset \mathrm{E}$, but it is injective for $\mathrm{I} \subset \mathrm{F}$, where F is strict subset of E. Since there is at least one element y in E, we may consider $\mathrm{F} = \mathrm{E} - singletony$.

```
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.
nin (doubleton_inj H7). nin H8. am. nin H8.
assert (inc y F).  app H5. rw H8. rw inc_complement. split. am. red. ir.
cp (H6 _ H10). ufi F H11. rwi inc_complement H11. ee. elim H12. fprops.
ufi F H10. rwi inc_complement H10. ee. elim H11. fprops.
```

If I is a non-empty subset of F then $\mathrm{I} \mapsto \{\mathrm{I}, \mathrm{E}-\mathrm{I}\}$ 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.
nin (union_exists H9). nin H10. nin (doubleton_or H11). app H8. wrr H12.
rwi H12 H10. rwi inc_complement H10. nin H10; am.
apply by_cases with (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). rww H10. rw H10.
exists y. rw inc_complement. split. am. red. ir. cp (H6 _ H11).
ufi F H12. rwi inc_complement H12. ee. elim H13. fprops.
ir.  nin (doubleton_or H9); nin (doubleton_or H10); rw H11; rw H12.
left. tv. right. app disjoint_complement.  right.
app disjoint_symmetric. app disjoint_complement. left. tv.
```

All that remains to do is to show that $\mathrm{Card}(\mathfrak{P}(\mathrm{E}-\{y\})-\{\emptyset\}) = \mathrm{Card}(\mathfrak{P}(\mathrm{E}))$.

```
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.
app injective_af_function. red. ir. ufi T H7. rwi inc_complement H7. ee.
app H6.  app powerset_sub. nin (emptyset_dichot c).  elim H8. rw H9. fprops.
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.
```

```
  rw card_powerset. ir.
  assert (card_pow card_two F = card_pow card_two (cardinal F)).
  app card_pow_pr. fprops.  fprops. rwi H10 H9.
  assert (is_cardinal (cardinal F)). fprops. cp (cantor  H11). nin H12.
  cp (le_int_is_int H9 H12). wri H8 H14. nin H. ee. elim H15. am.
  cp (cardinal_comp_singl_inf emptyset H9). fold T in H10. wri H10 H7.
  assert (cardinal (powerset F) = cardinal (powerset E)).
  rw card_powerset. rw card_powerset.  app card_pow_pr. fprops.
  symmetry in H8. awi H8. am. rwi H11 H7. cp (cardinal_antisymmetry1 H2 H7).
  awi H12. am.
Qed.
```

5. If E is an infinite set, the set of all permutations of E is equipotent to $\mathfrak{P}(E)$. (Use Proposition 3 of No. 4 to shat 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 $\mathrm{Card}(E) \leq \mathrm{Card}(F)$. 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 $\mathfrak{P}(F)$.

7. Let E, F be two infinite sets such that $\mathrm{Card}(E) < \mathrm{Card}(F)$. 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 $\mathfrak{P}(E)$ (Use Exercise 5).

9. Let E be a non-empty well-ordered set in which every element x other then the least element of E has a predecessor (the greatest element of $]\leftarrow, x[$). Show that E is isomorphic to either $\mathbf{N}$ or an interval $[0, n$ of $\mathbf{N}$ (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 ω or ω_0 denote the ordinal $\mathrm{Ord}(\mathbf{N})$ (§ 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 by n (by abuse of language) the ordinal $\mathrm{Ord}([0, n[)$.

(a) Show that for each cardinal $\mathfrak{a}$ the relation "ξ is an ordinal and $\mathrm{Card}(\xi) < \mathfrak{a}$ is collectivizing (use Zermelo's theorem). Let $W(\mathfrak{a})$ denote the set of all ordinals ξ such that $\mathrm{Card}(\xi) < \mathfrak{a}$.

(b) For each ordinal $\alpha > 0$ define a function f_α 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 ξ such that $0 < \xi \leq \alpha$, $f_\alpha(\xi)$ is the least upper bound (§ 2, Exercise 14 (d)) of the set of ordinals ζ such that $\mathrm{Card}(\zeta) \leq \mathrm{Card}(f_\alpha(\eta))$ for at least one ordinal $\eta < \xi$. Show that if $0 \leq \eta < \xi \leq \alpha$, then $\mathrm{Card}(f_\alpha(\eta)) < \mathrm{Card}(f_\alpha(\xi))$ and that, if $\xi \leq \alpha \leq \beta$, then $f_\alpha(\xi) = f_\beta(\xi)$. Put $\omega_\alpha = f_\alpha(\alpha)$; ω_α is said to be the *initial ordinal of index* α. Put $\aleph_\alpha = \mathrm{Card}(\omega_\alpha)$; $\aleph_\alpha$ is said to be the *aleph of index* α. In particular, $\aleph_0 = \mathrm{Card}(\mathbf{N})$.

(c) Show that for each infinite cardinal $\mathfrak{a}$, the least upper bound λ of the set of ordinals $W(\alpha)$ is an initial ordinal ω_α, and that $\mathfrak{a} = \aleph_\alpha$ (consider the least ordinal μ such that $\omega_\mu \geq \lambda$); in other words ω_α is the least ordinal ξ such that $\mathrm{Card}(\xi) = \aleph_\alpha$. For each ordinal α the mapping $\xi \mapsto \aleph_\xi$, defined on $O'(\alpha)$, is an isomorphism of the well-ordered set $O'(\alpha)$ onto the well-ordered set of cardinals $\leq \aleph_\alpha$; in particular $\aleph_{\alpha+1}$ is the least cardinal $> \aleph_\alpha$. Show that if α has no predecessor, then for every strictly increasing mapping $\xi \mapsto \sigma_\xi$ of an ordinal β into α such that $\alpha = \sup_{\xi<\beta} \sigma_\xi$, we have

$$\sum_{\xi<\beta} \aleph_{\sigma_\xi} = \aleph_\alpha.$$

(d) Deduce from (c) that ω_ξ is a normal ordinal functional symbol (§ 2, Exercise 17).

¶ 11. (a) Show that the ordinal ω_α is the least ordinal > 0 which has no predecessor, that ω 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 ω^β (use Exercise 18 (d) of § 2).

¶ 12. (a) Show that for each ordinal α and each ordinal $\gamma > 1$, there exists two finite sequences of ordinals (λ_i) and (μ_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 (λ_i), (μ_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 σ runs through the set of permutations of the interval $[1, n]$. Show that

$$f(n) = \sup_{1\leq k\leq n-1} (k.2^{k-1} + 1) f(n-k). \tag{1}$$

(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 α_i for which $\phi(\alpha_i)$ 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 $f(n) = 81 f(n-5)$.

(c) Show that the $n!$ ordinals $(\omega + \sigma(1))(\omega + \sigma(2)) \ldots (\omega + \sigma(n))$ where σ 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 η (argue by contradiction). Deduce that there exists α such that $w(\xi) \geq \xi$ for all $\xi \geq \alpha$ (take α 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 β there exist at most a finite number of ordinals η for which the equation $f(\xi, \eta) = \beta$ has at least one solution (Note that if ξ_1 is the least solution of $f(\xi, \eta_1) = \beta$ and if ξ_2 is the least solution of $f(\xi, \eta_2) = \beta$ then the relation $\eta_1 < \eta_2$ 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 ξ 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 γ is the least upper bound of A, show that γ 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 that the least upper bound of the sequence (α_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 β has no predecessor, then α^β is an indecomposable ordinal (cf § 2, Exercise16 (a)); if α is finite and if $\beta = \omega\gamma$, then $\alpha^\beta = \omega^\gamma$; if α is infinite and if π is the greatest indecomposable ordinal $\leq \alpha$, then $\alpha^\beta = \pi^\beta$ (use Exercise 11).

(b) An ordinal δ is critical with respect to the functional symbol $f(\xi, \eta) = \xi\eta$ if and only if, for each α such that $1 < \alpha \leq \delta$, the equation $\delta = \alpha^\xi$ has a solution; the unique solution ξ 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 π, α^π is a critical ordinal with respect to $\xi\eta$ (use Exercise 13 (c)). Deduced that δ is a critical ordinal with respect to $\xi\eta$ if and only if δ is of the form ω^{ω^μ} (cf. Exercise 11 (b)).

(c) For an ordinal ϵ to be critical with respect to the functional symbol $f(\xi, \eta) = \xi^\eta$, i.e. such that $\gamma^\epsilon = \epsilon$ for each γ satisfying $2 \leq \gamma \leq \epsilon$, it is sufficient that $2^\epsilon = \epsilon$. Show that the least critical ordinal ϵ_0 with respect to ξ^η is countable (cf. Exercise 13 (d)).

¶ 15. Let γ be an ordinal > 1, and for each ordinal α let $L(\alpha)$ denote the set of exponents λ_i in the expression for α 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 α is a critical ordinal with respect to ξ^η (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 β 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 ξ^η (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 Ord(M) of the well-ordered cofinal subsets M of E is said the *final character* of E.

(a) An ordinal ξ is said to be *regular* if it is equal to its final character, and *singular* otherwise. Show that every infinite regular ordinal is an an initial ordinal ω_α (Exercise 10). Conversely, every initial ordinal ω_α, whose index α is either 0 or has a predecessor, is a regular ordinal. An initial ordinal ω_α whose index α has no predecessor is singular if $0 < \alpha < \omega_\alpha$; in particular, ω_ω is the least infinite singular initial ordinal.

(b) An initial ordinal ω_α is said to be *inaccessible* if it is regular and its index α has no predecessor. Show that if $\alpha = 0$, then $\omega_\alpha = \alpha$; in other words, α is a critical ordinal with respect to the normal functional symbol ω_η (Exercise 10 (d) and 13 (c)). Let κ be the least critical ordinal with respect to this functional symbol. Show that ω_κ is singular, with final character ω (cf Exercise 13(d)). In other words, there exists no inaccessible ordinal ω_α such that $0 < \alpha \leq \kappa$ (At present, it is not known whether or not there exist inaccessible ordinals other than ω).

(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 $\omega_{\bar\alpha}$ is the final character of ω_α, then $\bar\alpha \leq \alpha$; and ω_α is regular if and only if $\alpha = \bar\alpha$.

(d) Let ω_α be a regular ordinal and let I be a well-ordered set such that $\mathrm{Ord}(I) < \omega_\alpha$. Show that, for each family $(\xi_\iota)_{\iota\in I}$ of ordinals such that $\xi_\iota < \omega_\alpha$ for all $\iota \in I$, we have $\sum_{\iota\in I} \xi_\iota < \omega_\alpha$.

17. A cardinal $\aleph_\alpha$ is said to be *regular* (resp. *singular*) if the initial ordinal ω_α is regular (resp. singular). For $\aleph_\alpha$ to be regular if is necessary and sufficient that for every family $(\mathfrak{a}_\iota)_{\iota\in I}$ of cardinals such that $\mathrm{Card}(I) < \aleph_\alpha$ and $\mathfrak{a}_\iota < \aleph_\alpha$ for all $\iota \in I$, we have

$$\sum_{\iota\in I} \mathfrak{a}_\iota < \aleph_\alpha.$$

$\aleph_\omega$ is the least singular cardinal.

¶ 18. (a) For each ordinal α and each cardinal $\mathfrak{m} \neq 0$ we have $\aleph_{\alpha+1}^{\mathfrak{m}} = \aleph_\alpha^{\mathfrak{m}} \cdot \aleph_{\alpha+1}$ (reduce to the case where $\mathfrak{m} < \aleph_{\alpha+1}$ and consider the mappings of the cardinal $\mathfrak{m}$ into the ordinal $\omega_{\alpha+1}$).

(b) Deduce from (a) that, for each ordinal γ such that $\mathrm{Card}(\gamma) \leq \mathfrak{m}$ we have $\aleph_{\alpha+\gamma}^{\mathfrak{m}} = \aleph_\alpha^{\mathfrak{m}} \cdot \aleph_{\alpha+\gamma}^{\mathrm{Card}(\gamma)}$ (by transfinite induction on γ).

(c) Deduce from (b) that, for each ordinal α such that $\mathrm{Card}(\alpha) \leq \mathfrak{m}$, we have $\aleph_\alpha^{\mathfrak{m}} = 2^{\mathfrak{m}} \cdot \aleph_\alpha^{\mathrm{Card}(\alpha)}$.

¶ 19. (a) Let α and β be two ordinals such that α has no predecessor, and let $\xi \to \sigma_\xi$ be a strictly increasing mapping of the ordinal ω_β into the ordinal α such that $\sup_{\xi<\omega_\beta} \sigma_\xi = \alpha$. Show that

$$\aleph_\alpha^{\aleph_\beta} = \prod_{\xi<\omega_\beta} \aleph_{\sigma_\xi}.$$

(With each mapping f of the ordinal ω_β into the ordinal ω_α associate an injective mapping $\bar f$ of ω_β into the set of all ω_{σ_ξ} $(\xi < \omega_\beta)$ such that $f(\zeta) \leq \bar f(\zeta)$ for all $\zeta < \omega_\beta$. Calculate the cardinal of the set of mappings f associated with then same $\bar f$ and observe that

$$\mathfrak{m} = \prod_{\xi<\omega_\beta} \aleph_{\sigma_\xi} \geq 2^{\mathrm{card}(\omega_\beta)}$$

and $\mathfrak{m} \geq \aleph_\alpha$ (cf. § 3, Exercise 3).)

(b) Let $\bar{\alpha}$ be the ordinal such that $\omega_{\bar{\alpha}}$ is the final character of ω_α. Show that that $\aleph_\alpha^{\aleph_{\bar{\alpha}}} > \aleph_\alpha$ and that if there exists $\mathfrak{n}$ such that $\aleph_\alpha = \mathfrak{n}^{\alpha_\gamma}$ then $\gamma < \bar{\alpha}$ (use (a) and Exercise 3 of § 3).

(c) Show that if $\lambda < \bar{\alpha}$ then

$$\aleph_\alpha^{\aleph_\beta} = \sum_{\xi<\alpha} \aleph_\alpha^{\aleph_\lambda}$$

(argue as in Exercise 18 (a)).

¶ 20. (a) For a cardinal $\mathfrak{a}$ to be regular (Exercise 17) it is necessary that for every cardinal $\mathfrak{b} \neq 0$ we should have

$$\mathfrak{a}^{\mathfrak{b}} = \mathfrak{a}. \sum_{\mathfrak{m}<\mathfrak{a}} \mathfrak{m}^{\mathfrak{b}}.$$

(Use Exercise 19 and consider separately the cases (i) $\mathfrak{b}$ is finite, (ii) $\aleph_0 \leq \mathfrak{b} < \mathfrak{a}$, (iii) $\mathfrak{b} \geq \mathfrak{a}$; also use Exercise 3 of § 3.) The generalized continuum hypothesis implies that the above condition is also sufficient.

(b) Show that if a cardinal $\mathfrak{a}$ is such that $\mathfrak{a}^{\mathfrak{m}} = \mathfrak{a}$ for every cardinal $\mathfrak{m}$ such that $0 < \mathfrak{m} < \mathfrak{a}$, then $\mathfrak{a}$ is regular (use Exercise 3 of § 3).

(c) Show that the proposition "for every regular cardinal $\mathfrak{a}$ and every cardinal $\mathfrak{m}$ such that $0 < \mathfrak{m} < \mathfrak{a}$, we have $\mathfrak{a} = \mathfrak{a}^{\mathfrak{m}}$ is equivalent to the generalized continuum hypothesis (use (a)).

¶ 21. An infinite cardinal $\mathfrak{a}$ is said to be *dominant* if for each pair of cardinals $\mathfrak{m} < \mathfrak{a}$, $\mathfrak{n} < \mathfrak{a}$ we have $\mathfrak{m}^{\mathfrak{n}} < \mathfrak{a}$.

(a) For $\mathfrak{a}$ to be dominant it is sufficient that $2^{\mathfrak{m}} < \mathfrak{a}$ for every cardinal $\mathfrak{m} < \mathfrak{a}$.

(b) Define inductively a sequence $(\mathfrak{a}_n)$ of cardinals as follows: $\mathfrak{a}_0 = \aleph_0$, $\mathfrak{a}_{n+1} = 2^{\mathfrak{a}_n}$ Show that the sum $\mathfrak{b}$ of the sequence $\mathfrak{a}_n$ is a dominant cardinal. $\aleph_0$ and $\mathfrak{b}$ are the two smallest dominant cardinals.

(c) Show that $\mathfrak{b}^{\aleph_0} = \aleph_0^{\mathfrak{b}} = 2^{\mathfrak{b}}$ (Note that $2^{\mathfrak{b}} \leq \mathfrak{b}^{\aleph_0}$). Deduce that $\mathfrak{b}^{\aleph_0} = (2^{\mathfrak{b}})^{\mathfrak{b}}$, although $\mathfrak{b} < 2^{\mathfrak{b}}$ and $\aleph_0 < \mathfrak{b}$.

¶ 22. A cardinal $\aleph_\alpha$ is said to be *inaccessible* if the ordinal ω_α is inaccessible (Exercise 16 (b)). We have then $\omega_\alpha = \alpha$ if $\omega_\alpha \neq \omega_0$. A cardinal $\mathfrak{a}$ 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 $\mathfrak{a} \geq 3$ to be strongly inaccessible it is necessary and sufficient that, for each family $(\mathfrak{a}_\iota)_{\iota\in I}$ of cardinals such that

$$\mathrm{Card}(I) < \mathfrak{a} \text{ and } \mathfrak{a}_\iota < \mathfrak{a}$$

for all $\iota \in I$, we should have $\prod_{\iota\in I} \mathfrak{a}_\iota < \mathfrak{a}$.

(c) For an infinite cardinal $\mathfrak{a}$ 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) $\mathfrak{a}^{\mathfrak{b}} = \mathfrak{a}$ for every cardinal $\mathfrak{b}$ such that $0 < \mathfrak{b} < \mathfrak{a}$; (ii) $\mathfrak{a}^{\mathfrak{b}} = \mathfrak{a}.2^{\mathfrak{b}}$ for every cardinal $\mathfrak{b} > 0$ (Use Exercises 20 and 21).

¶ 23. Let α be an ordinal > 0. A mapping f of the ordinal α 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 $\mu_0 \leq \xi < \alpha$ implies $\lambda_0 \leq f(\xi) < \alpha$. (this condition may be written as $\lim_{\xi\to\alpha,\xi<\alpha} f(\xi) = \alpha$)

(a) Let ϕ be a strictly increasing mapping of an ordinal β into α such that

$$\phi(\sup_{\zeta<\gamma}\zeta) = \sup_{\zeta<\gamma}\phi(\zeta) \text{ for all } \gamma < \beta,$$

and such that

$$\sup_{\zeta<\beta}\phi(\zeta) = \alpha.$$

(if we extend ϕ be defining $\phi(\beta) = \alpha$, the conditions above signify that ϕ is continuous) Then there exists a divergent mapping f of α into itself, such that $f(\xi) < \xi$ for all ξ satisfying $0 < \xi < \alpha$, if and only if there exists a divergent mapping of β into itself of the same type.

(b) Deduce from (a) that there exists a divergent mapping of ω_α into itself, such that $f(\xi) < \xi$ for all ξ satisfying $0 < \xi < \alpha$ if and only if the final character of ω_α is ω_0. (If ω_α is a regular ordinal $> \omega_0$, defined inductively a strictly increasing sequence (η_n) as follows: $\eta_1 = 1$, and η_{n+1} is the least ordinal ζ such that $f(\xi) > \eta_n$ for all $\xi \geq \zeta$.)

(c) Let $\omega_{\bar\alpha}$ be the final character of ω_α (Exercise 16). Show that, if $\bar\alpha > 0$ and if f is a mapping of ω_α into itself such that $f(\xi) < \zeta$ for all ξ such that $0 < \xi < \omega_\alpha$, then there exists an ordinal λ_0 such that the set of solutions to the equation $f(\xi) = \lambda_0$ has a cardinal $\geq \aleph_{\bar\alpha}$.

¶ 24. Let $\mathfrak{F}$ be a set of subsets of a set E such that for every $A \in \mathfrak{F}$ we have $\mathrm{Card}(A) = \mathrm{Card}(\mathfrak{F}) = \mathfrak{a} \geq \aleph_0$. Show that E has a subset P such that $\mathrm{Card}(P) = \mathfrak{a}$ and such that no set of $\mathfrak{F}$ is contained in P (If $\mathfrak{a} = \aleph_\alpha$, define by transfinite induction two injective mappings $\xi \to f(\xi)$, $\xi \to g(\xi)$ of ω_α 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 $\mathrm{Card}(\mathfrak{G}) < \alpha$, the complement in E of the union of the sets $A \in \mathfrak{G}$ has cardinal $\geq \mathfrak{a}$. Show that E then has a subset P such that $\mathrm{Card}(P) = \mathfrak{a}$ and such that, for each $A \in \mathfrak{G}$, $\mathrm{card}(P \cap A) < \mathfrak{a}$ (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 $\mathfrak{c}$ such that $\mathfrak{c}$ is *strictly greater* than the cardinals $\mathrm{Card}(X \cap Y)$ for each pair of distinct sets $X, Y \in \mathfrak{F}$. If $\mathrm{Card}(E) = \mathfrak{a}$ and $\mathrm{Card}(\mathfrak{F}) = \mathfrak{b}$, show that $\mathfrak{b} \leq \mathfrak{a}^{\mathfrak{c}}$ (note that a subset of E of cardinal $\mathfrak{c}$ is contained in at most one set of $\mathfrak{F}$).

(b) Let ω_α be an initial ordinal and let F be set such that $2 \leq \mathfrak{p} = \mathrm{Card}(F) < \aleph_\alpha$. Let E be the set of mappings of segments of ω_α, other then ω_α itself, into F. The we have $\mathrm{Card}(E) \leq \mathfrak{p}^{\aleph_\alpha}$. For each mapping f of ω_α into F, let K_f be the subset of E consisting of the restrictions of f to the segments of ω_α (other than ω_α itself). Show that the set $\mathfrak{F}$ of subsets of K_f is a covering of E such that $\mathrm{Card}(\mathfrak{F}) = \mathfrak{p}^{\aleph_\alpha}$ and that its degree of disjointness is equal to ω_α.

(c) Let E be an infinite set of cardinal $\mathfrak{a}$ and let $\mathfrak{c}$, $\mathfrak{p}$ be two cardinal > 1 such that $\mathfrak{p} < \mathfrak{c}$, $\mathfrak{p}^{\mathfrak{m}} < \mathfrak{a}$ for all $\mathfrak{m} < \mathfrak{c}$ and $\mathfrak{a} = \sum_{\mathfrak{m}<\mathfrak{c}} \mathfrak{p}^{\mathfrak{m}}$. Deduce from (b) that there exists a covering $\mathfrak{F}$ of E consisting of sets of cardinal $\mathfrak{c}$, with degree of disjunction equal to $\mathfrak{c}$ and such that $\mathrm{Card}(\mathfrak{F}) = \mathfrak{p}^{\mathfrak{c}}$. In particular, if E is countably infinite, there exists a covering $\mathfrak{F}$ of E by infinite sets such that $\mathrm{card}(\mathfrak{F}) = 2^{\aleph_0}$ 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

$$\mathrm{card}(A) = \mathrm{card}(\mathfrak{F}) = \mathrm{card}(E) = \mathfrak{a} \geq \aleph_0.$$

Show that there exists a partition $(B_\iota)_{\iota\in I}$ of E such that

$$\mathrm{card}(I) = \mathrm{card}(B_\iota) = \mathfrak{a}$$

for all $\iota \in I$ and such that $A \cap B_\iota \neq \emptyset$ for all $A \in \mathfrak{F}$ and all $\iota \in I$. (With the notation of Exercise 24 (a), consider first a surjective mapping f of ω_α 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 $\mathfrak{a}$. Then, by transfinite induction, define a bijection g of ω_α 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 $\mathrm{card}(E_\lambda) > n$ is equipotent to L. Show that there exists a subset F of the product $E = \prod_{\lambda\in L} E_\lambda$, such that $\mathrm{Card}(F) = 2^{\mathrm{Card}(L)}$, 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 $(L_j)_{j\in\mathbf{N}}$ of L such that $\mathrm{Card}(L_j) = \mathrm{Card}(L)$ for all j, and such that $\mathrm{Card}(E_\lambda) \geq 2^j$ 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 $(\mathfrak{X}_i)_{1\leq i\leq m}$ 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 $\mathfrak{X}_i$. (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 $\mathfrak{X}_{j(a)}$. 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 $f(x) = T\{\!\{f^{(x)}\}\!\}$, where $f^{(x)}$ denotes the mapping of $]\leftarrow, x[$ onto $]\leftarrow, f(x)[$ 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 $\sup(e_1, e_2, \ldots, e_n)$ where

$e_1, \dots, e_n$ 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.

¶ 31. Let A be an infinite set and let E be the set of all infinite subsets of A, ordered by inclusion. Show that E is completely ramified (§ 2, Exercise 8) but not antidirected (§ 1, Exercise 23) and that E has an antidirected cofinal subset F. (Consider first the set $\mathfrak{D}(A)$ of countable infinite subsets of A (which is cofinal in E) and let $Z = R_0(\mathfrak{D}(A))$ (§ 1, Exercise 23). Write Z in the form $(z_\lambda)_{\lambda \in L}$, where L is a well-ordered set, and take F to be a set of countable subsets X_n^λ, where λ runs through a suitable subset of L, $n \in \mathbf{N}$, $X_m^\lambda \supset X_n^\lambda$ whenever $m \leq n$, $X_n^\lambda - X_{n+1}^\lambda$ is infinite for all $n \geq 0$ and $\cup_{n \in \mathbf{N}} X_n^\lambda = \emptyset$; the X_n^λ, are to be defined by transfinite induction in such a way that the images of the sets X_n^λ, under the canonical mapping $r : \mathfrak{D}(A) \to Z$ (§ 1, Exercise 23) are mutually disjoint and form a cofinal subset of Z.)

¶ 32. * Let (M_n), (P_n) be two sequences of mutually disjoint finite sets (not all empty), indexed by the set $\mathbf{Z}$ of rational integers. Let $\alpha_n = \mathrm{Card}(M_n)$, $\beta_n = \mathrm{card}(P_n)$. Suppose that there exists an integer $k > 0$ such that for each $n \in \mathbf{Z}$ and each integer $l \geq 1$ 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 ϕ of M onto P such that

$$\phi(M_n) \subset \bigcup_{i=n-k-1}^{n+k+1} P_i \text{ and } \overset{-1}{\phi}(P_n) \subset \bigcup_{i=n-k-1}^{n+k+1} M_i$$

for each $n \in \mathbf{Z}$ (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 $(M_n)_{n \in \mathbf{Z}}$ (resp. $(P_n)_{n \in \mathbf{Z}}$). 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 $\cup_{j=n_0-k}^{n_0+k} P_j$ and show that one of these isomorphisms satisfies the required conditions. Let δ 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 $n \in \mathbf{Z}$ and all $l \geq 1$. If $n \in \mathbf{Z}$ 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 ϕ to be such that the least element of P_{n-k} is the image under ϕ of the least element of M_n. *

¶ 33. Soient $\mathfrak{a}$, $\mathfrak{b}$ deux cardinaux tels aue $\mathfrak{a} \geq 2$, $\mathfrak{b} \geq 1$, l'un au moins des deux étant infini. Soient E un ensemble, $\mathfrak{F}$ une partie de $\mathfrak{P}(E)$, telle que $\mathrm{card}(\mathfrak{F}) > \mathfrak{a}^{\mathfrak{b}}$ et $\mathrm{card}(X) \leq \mathfrak{b}$ pour tout $X \in \mathfrak{F}$. On se propose de montrer qu'il exists une partie $\mathfrak{G} \subset \mathfrak{F}$ telle que $\mathrm{card}(\mathfrak{G}) > \mathfrak{a}^{\mathfrak{b}}$ et que deux quelconques des ensembles appartenant à $\mathfrak{G}$ aient *le même intersection.* On pourra procéder de la façon suivante.

a) soit $\mathfrak{c}$ le plus petit des cardinaux $> \mathfrak{a}^{\mathfrak{b}}$ et soit Ω le plus petit ordinal de cardinal $\mathfrak{c}$. On considère une application injective $\nu \mapsto X(\nu)$ de Ω dans $\mathfrak{F}$ et on pose $M = \cup_{\nu \in \Omega} X(\nu)$; on peut supposer que $\mathrm{card}(M) = \mathfrak{c}$, et il y a donc une bijection $\nu \mapsto x_\nu$ de Ω sur M, ordonnat M.

b) Pour tout $\nu \in \Omega$ soit ρ_ν l'ordinal type d'ordre du sous-ensemble $X(\nu)$ de M (on a $\mathrm{Card}(\rho_\nu) \geq \mathfrak{b}$) et soit $\mu \mapsto y_\mu^{(\nu)}$ l'unique application bijective croissante de ρ_ν sur $X(\nu)$. On note M_μ l'ensemble des $y_\mu^{(\nu)}$ lorsque ν parcourt Ω. Montrer qu'il existe au moins un ordinal μ tel que $\mathrm{Card}(M_\mu) = \mathfrak{c}$. On désigne par α le *plus petit* de ces ordinaux; la réunion de M_γ pour $\gamma < \alpha$ a un cardinal $\leq \mathfrak{a}^{\mathfrak{b}} < \mathfrak{c}$.

c) Montrer qu'il existe un partie $N_0 \subset \Omega$ telle que $\mathrm{Card}(N_0) = c$ et que l'application $\nu \mapsto y_\alpha^{(\nu)}$ de N_0 dans M soit injective. Montrer, par récurrence ur β, qu'il existe une partie $N_\beta \subset N_0$ de cardinal $\mathfrak{c}$ telle que l'élément $y_\lambda^{(\nu)} = z_\lambda$ soit indépendant de ν pour $\nu \in N_\beta$ et pour tout $\lambda \leq \beta$. Montrer que l'intersection N des N_β pout $\beta < \alpha$ a pour cardinal $\mathfrak{c}$ (considérer son complémentaire). Soit Q l'ensemble des z_λ pour $\lambda < \alpha$.

d) Pour tout $\nu \in N$, on définit par récurrence un ordinal λ_ν par la condition suivante : c'est le plus petit ordinal dans N tel que $y_\alpha^{(\lambda_\nu)}$ 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 9

Theorems, Notations, Definitions

List of all theorems of Bourbaki, with ther 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 ...» , [10].

Proposition 2 (*decreasing_composition*) says that $u(v(x)) \geq x$ and $v(u(x)) \geq x$ and decreasing imply $u \circ v \circ u = u$ and $v \circ u \circ v = v$, [20].

Proposition 3 (*adjoin_greatest*) says that we can add a greatest element to an ordered set, [23].

Proposition 4 (*compare_inf_sup1* and *compare_inf_sup2*) characterizes the supremum and infimum of a subset, [28].

Proposition 5 (*sup_increasing* and *inf_decreasing*) says that $\sup_A$ and $\inf_A$ are increasing functions of the set A, [29].

Proposition 6 (*sup_increasing2* and *inf_decreasing2*) says that $\sup f$ and $\inf f$ are increasing functions of the function f, [29].

Proposition 7 (*sup_distributive1* and *inf_distributive2*) asserts associativity of sup, [29].

Proposition 8 (*sup_in_product* and *inf_in_product*) characterizes supremum and infimum in a product, [31].

Proposition 9 (*sup_induced2* and 3 variants) characterizes supremum of a subset of a subset, [31].

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», [32].

Proposition 11 (*total_order_monotone_injective* and *total_order_increasing_morphism*) characterizes increasing functions and morphism on totally ordered sets, [34].

Proposition 12 (*sup_in_total_order* and *inf_in_total_order*) characterizes supremum and infimum in a totally ordered set, [34].

Proposition 13 (*intersection_interval*) says that in a lattice, the intersection of two intervals is an interval, [36].

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 $]\leftarrow, a[$, where $a \in$ E, [41].

Proposition 2 (*isomorphism_set_of_segments_iso* and *set_of_segments_worder*) studies $x \mapsto]\leftarrow, x[$ [42].

Proposition 3 (*worder_merge*) studies the supremum of compatible well-orderings, [43].

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, [45].

Criterion C60 (*transfinite_definition* and *transfinite_definition_stable*) (Definition of a mapping by transfinite induction), [45].

Lemma 3 (*Zermelo_aux*) is a helper for Theorem 1.

Theorem 1 (*Zermelo*) says that «every set E can be well-ordered», [48].

Proposition 4 (*Zorn_aux*) is a generalization of Zorn's lemma [49].

Theorem 2 (*Zorn_lemma*) says «every inductive ordered set has a maximal element», [49].

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, [50].

Lemma 4 (*increasing_function_segments*), [50].

Corollary 1 (*unique_isomorphism_onto_segment*), [51].

Corollary 2 (*bij_pair_isomorphism_onto_segment*), [51].

Corollary 3 (*isomorphic_subset_segment*) [51].

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, [62].

Corollary 1 (*cardinal_le_total_order*).

Corollary 2 (*cardinal_antisymmetry2*).

Proposition 2 (*cardinal_supremum*) says that a family of cardinals has a supremum, [63].

Proposition 3 (*surjective_cardinal_le*) says «if there exists a surjection f of X onto Y, then Card(Y) $\leq$ Card(X), [63].

Proposition 4 (*cardinal_prod_pr* and *cardinal_sum_pr*) says that the cardinal sum or cardinal product of the family Card(E_ι) is the cardinal of the sum or the product of the sets E_ι; [63].

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, [64].

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, [66].

Corollary 1 (*zero_unit_sumr*, *zero_unit_suml*, *one_unit_prodr*, *one_unit_prodl*).

Corollary 2 (*sum_of_ones* and *sum_of_same*).

Proposition 7 (*zero_cardinal_product*) says that a cardinal product is non-zero if and only if each factor is non-zero, [67].

Proposition 8 (*succ_injective*) asserts injectivity of the successor function, [67].

Proposition 9 (*cardinal_pow_pr1*) says that a^b remains unchanged if letters are replaced by equipotent sets, [68].

Proposition 10 *cardinal_pow_pr3* says that a^b is a product where all factors are the same [68].

Corollary 1 (*power_of_sum*).

Corollary 2 (*power_of_prod*).

Corollary 3 (*power_of_prod2*).

Proposition 11 (*power_x_0* and variants), states $\mathfrak{a}^0 = 1$, $\mathfrak{a}^1 = \mathfrak{a}$, $1^{\mathfrak{a}} = 1$, and $0^{\mathfrak{a}} = 0$, [69].

Proposition 12 (*cardinal_powerset*) says $\mathrm{Card}(\mathfrak{P}(X)) = 2^X$, [69].

Proposition 13 (*cardinal_le_when_complement*) states that «$\mathfrak{a} \geq \mathfrak{b}$ if and only if there exists a cardinal $\mathfrak{c}$ such that $\mathfrak{a} = \mathfrak{b} + \mathfrak{c}$», [69].

Proposition 14 (*sum_increasing* and *product_increasing*) says the sum and product are increasing functions, [70].

Corollary 1 (*sum_increasing1*, *product_increasing1*).

Corollary 2 (*power_increasing1*).

Theorem 2 (*cantor*) says $X < 2^X$, [70].

Corollary (*cantor_bis*).

Theorems of Chapter 4

Proposition 1 (*is_finite_succ*) says that «a cardinal a is finite if and only if $a+1$ is finite», [72].

Proposition 2 (*le_int_is_int*, *exists_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 $a < n$, [73].

Corollary 1 (*sub_finite_set*).

Corollary 2 (*strict_sub_smaller*).

Corollary 3 (*finite_image*).

Corollary 4 (*bijective_if_same_finite_c_inj*, *bijective_if_same_finite_c_surj*).

Criterion C61 (*cardinal_c_induction* and variants) (principle of induction), [76]

Proposition 3 (*finite_subset_directed_bounded*, *finite_subset_lattice_inf*, *finite_subset_lattice_sup*, *finite_subset_torder_greatest*, *finite_subset_torder_least*) gives some properties of a finite subset of an ordered set [78].

Corollary 1 (*finite_set_torder_greatest*, *finite_set_torder_worder*)

Corollary 2 (*finite_set_maximal*).

Theorem 1 (*maximal_inclusion*) says that every nonempty set which is of finite character has a maximal element, [107].

Theorems of Chapter 5

Proposition 1 (*finite_sum_finite* and *finite_product_finite*) says that a finite sum or product of integers is an integer, [88].

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 $b = c + a$; [90].

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, [91].

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) $[0, b] \to [a, a + b]$, [97].

Proposition 5 (*cardinal_interval*) gives the cardinal of $[a, b]$, [97].

Proposition 6 (*finite_ordered_interval*) asserts that every finite totally ordered set is isomorphic to a unique interval $[1, n]$, [98].

Proposition 7 (*char_fun_union* and others) states properties of the characteristic function of a set, [106].

Theorem 1 (*division_unique*, *division_exists*) asserts existence and uniqueness of Euclidean division, [107].

Proposition 8 is expansion to base b [110].

Proposition 9 (*shepherd_principle*) says that if f is a function from a set with cardinal $\mathfrak{a}$ onto a set with cardinal $\mathfrak{b}$, and if all set $f^{-1}\langle\{x\}\rangle$ have the same cardinal $\mathfrak{c}$, then $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, [113].

Proposition 10 (*number_of_injections_prop*) gives the number of injections from a finite set into another one, [114].

Corollary (*number_of_permutations*).

Proposition 11 (*number_of_partitions*) gives the number of partitions with p_i elements, [115].

Corollary 1 (*binomial7*).

Corollary 2 (*cardinal_set_of_increasing_functions*).

Proposition 12 (*sum_of_binomial*) $\sum_p \binom{n}{p} = 2^n$ [119].

Proposition 13 is the binomial formula (is a definition in Coq) [119].

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 $1 \leq i < j \leq n$, [123].

Corollary (*sum_of_i*).

Proposition 15 counts the number of monomials, [124].

Theorems of Chapter 6

Theorem 1 «The relation 'x is an integer' is collectivizing » (see *inc_Bnat*), [75].

Criterion C62 (restatement on C61, not shown in Coq).

Criterion C63 (*integer_induction*), [130].

Lemma 1 (*infinite_greater_countable*) «Every infinite set, E contains a set equipotent to **N**».

Lemma 2 (*equipotent_N2_N*) «The set $\mathbf{N} \times \mathbf{N}$ is equipotent to $\mathbf{N}$».

Theorem 2 (*equipotent_inf2_inf*) «for every infinite cardinal $\mathfrak{a}$, we have $\mathfrak{a} = \mathfrak{a}^2$» [133]

Corollary 1 (*power_of_infinite*).

Corollary 2 (*finite_family_product*).

Corollary 3 (*notbig_family_sum1*).

Corollary 4 (*sum2_infinite*, *product2_infinite*).

Proposition 1 (*countable_subset*, *countable_product countable_union*) states properties of countable sets [135].

Proposition 2 (*countable_finite_or_N*) «Every countable infinite set E is equipotent to $\mathbf{N}$», [135].

Proposition 3 (*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 $\mathbf{N}$, [135].

Proposition 4 (*countable_inv_image*) says that if f is a function from E onto F, such that F is infinite and $f^{-1}\langle\{x\}\rangle$ is countable for any $x \in$ F, then F is equipotent to E, [135].

Proposition 5 (*infinite_finite_subsets*) says that the set of finite subsets of an infinite set E is equipotent to E, [135].

Proposition 6 (*increasing_stationary*) characterizes stationary sequences, [136].

Corollary 1 (*decreasing_stationary*).

Corollary 2 (*finite_increasing_stationary*).

Proposition 7 (*noetherian_induction*) (Principle of Noetherian induction), [137].

Symbols

$x \wedge y$ is often replaced by "and". The Coq equivalent is `/\`.

$x \vee y$ is often replaced by "or". The Coq equivalent is `\/`.

$\neg x$ is often replaced by "not". The Coq equivalent is `~`.

$(a|b)c$ is a Bourbaki notation, meaning the relation obtained by replacing b by a in c.

$\mathrm{R}\{\!\{x\}\!\}$ 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 $(x|y)\mathrm{R}$.

$\tau_x(\mathrm{R})$ is a Bourbaki notation, it is the generic element satisfying $\mathrm{R}\{\!\{x\}\!\}$.

$x \implies y$ is represented in Coq by `x -> y`.

$x \to y$ 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.

$f\langle x\rangle$ is the value of f on the set x, see *fun_image*, *image_by_graph*, *image_by_fun*.

$\overset{-1}{f}\langle x\rangle$, see *inverse_image*.

$(\forall x)\mathrm{P}$ and *forall x, p* are similar constructions.

$(\exists x)\mathrm{P}$ and *exists x, p* are similar constructions.

$(\exists! x)\mathrm{P}$ means sometimes *exists_unique*.

$x \in y$, $x \ni y$ (is element of): see *inc* and *elt*.

$x \subset y$ (is subset of): see *sub*.

$\emptyset$ (empty set): see *emptyset*.

$\{x, \mathrm{R}\}$ (set of x such that R): see *Zo*.

$\{x\}$, $\{x, y\}$: see *singleton* or *doubleton*.

$a - b$, $a \setminus b$, $\complement a$: see *complement*.

(x, y) (ordered pair): see *J*.

$\bigcup \mathrm{X}$, $\bigcup_{\iota \in \mathrm{I}} \mathrm{X}_\iota$, see *union*.

$a \cup b$, $a \cap b$, see *union2, intersection2*.

$\mathrm{A} \times \mathrm{B}$, $u \times v$, $\mathrm{R} \times \mathrm{R}'$, see *product, ext_to_prod, prod_of_relation*.

$f \circ g$, see *fcompose, gcompose, compose_graph, compose, composeC*.

Δ_{A}, see *diagonal*.

$\overset{-1}{\mathrm{G}}$ see *inverse_graph* , *inverse_fun* or *inverseC*.

$x \mapsto y$ or $x \to y$ is the function that maps x to y, for instance $x \mapsto \sin x$ (source and target are implicit).

$\boldsymbol{x} \to \boldsymbol{T}$ ($\boldsymbol{x} \in \boldsymbol{A}, \boldsymbol{T} \in \boldsymbol{C}$), is the function with source A, target C that maps x to T.

$(f_x)_{x \in \mathrm{A}}$ is a shorthand for $x \to f(x)$ ($x \in \mathrm{A}$); see above, the piece $\boldsymbol{T} \in \boldsymbol{C}$ is implicit.

$\hat{f}$, see *extension_to_parts*.

F^{E}, set of graphs of functions from E to F, see *set_of_gfunctions*.

$\mathscr{F}(\mathrm{E};\mathrm{F})$, set of functions from E to F, see see *set_of_functions*.

$\Phi(\mathrm{E},\mathrm{F})$, set of functions from a subset of E to F, see *set_of_sub_functions*.

f_x, f_y sometimes denotes the mappings $y \mapsto f((x, y))$ or $x \mapsto f((x, y))$, implemented as *first_partial_fun, second_partial_fun*.

$\tilde{f}$, sometimes denotes the mappings $x \mapsto f_x$ or $y \mapsto f_y$. Implemented as *first_partial_function, second_partial_function*.

$f \mapsto \tilde{f}$, implemented as *first_partial_map, second_partial_map*, is a bijection from $\mathscr{F}(\mathrm{B} \times \mathrm{C};\mathrm{A})$ into $\mathscr{F}(\mathrm{B};\mathscr{F}(\mathrm{C};\mathrm{A})$ or $\mathscr{F}(\mathrm{C};\mathscr{F}(\mathrm{B};\mathrm{A}))$.

$\prod_{\iota \in \mathrm{I}} \mathrm{X}_\iota$, product of a family of sets, see *productt*.

$(x_\iota)_{\iota \in \mathrm{I}}$ denotes an element of a product indexed by I.

$x \overset{r}{\sim} y$ is sometimes used instead of $r(x, y)$, especially when r is the graph of an equivalence relation.

$g_{\mathrm{E}}(\sim)$, the graph of $\sim$ on E, see *graph_on*.

$\sim_f$ may denote *eq_rel_associated f*.

$\bar{x}$, may denote the equivalence class of x, see *class*.

$\hat{x}$ may denote a representative of the equivalence class x.

$\mathrm{E}/\sim$, E/R (quotient set of E) see *quotient*.

R/S (quotient of two equivalence relations) see *quotient_of_relations*.

X_f sometimes means $f^{-1}\langle f\langle \mathrm{X}\rangle\rangle$, see *inverse_direct_value*.

R_{A} see *induced_relation*.

$x \succ_r y$, $y \prec_r x$, notations used when x and y are related by a preorder relation,[5].

$x \leq_r y$, $y \geq_r x$, notations used when x and y are related by an order relation.

$x \leq y$, $y \geq x$, $x < y$, $x > y$: notations used when x and y are related by an order relation, see *gle, gge, glt, ggt*.

$f \mapsto \mathrm{G}_f$ see *graph_of_function*.

$\varpi \mapsto \tilde{\varpi}$ see *graph_of_partition*.

$\sup(x, y)$, $\sup_{\mathrm{E}} \mathrm{X}$, $\sup \mathrm{X}$, $\sup_{x \in \mathrm{A}} f(x)$ see *supremum, sup, sup_graph*.

$\inf(x, y)$, $\inf_{\mathrm{E}} \mathrm{X}$, $\inf \mathrm{X}$, $\inf_{x \in \mathrm{A}} f(x)$ see *infimum, inf, sup_graph*.

$[a,b]$, $[a,b[$, $]a,b]$, $]a,b[$, $[a,\rightarrow[$, $]a,\rightarrow[$, $]\leftarrow,b]$, $]\leftarrow,b]$, $]\leftarrow,\rightarrow[$, see interval.

$\mathfrak{r} \leq_{\mathrm{Card}} \mathfrak{n}$, order on cardinals, see *cardinal_le*.

$g^{(x)}$ is the restriction of g to $]\leftarrow,x[$ see *restriction_to_segment*

$\mathrm{Card}(x)$ is the cardinal of x, see *cardinal*.

0, 1, 2, 3, 4: see *card_zero* or *card_three*.

$\sum_{\iota\in I} \mathfrak{a}_\iota$, $\mathop{\mathsf{P}}_{\iota\in I} \mathfrak{a}_\iota$: cardinal sum or cardinal product of a family of cardinals, see *cardinal_sum* and *cardinal_prod*.

$\mathfrak{a}+\mathfrak{b}$, $\mathfrak{a}.\mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$, is the cardinal sum or cardinal product of two cardinals, see *card_plus card_mult*

$\mathrm{E}_1+\mathrm{E}_2$ denotes also the ordinal sum, see *ordinal_sum*.

$\mathrm{X}_{xy}(a,b)$ is the family $x \mapsto a$ and $y \mapsto b$, see page 59.

$\mathrm{X}(a,b)$ is $\mathrm{X}_{\alpha,\beta}(a,b)$, for some fixed α and β.

$a_x \cup b_y$ is the disjoint union of $\mathrm{X}_{xy}(a,b)$, i.e., $a\times\{x\}\cup b\times\{y\}$.

$\mathfrak{a}^{\mathfrak{b}}$ is the cardinal power of two cardinals, see *card_pow*.

a^b is the power of two integers, see *pow*.

$\mathbb{N}$, $\mathbf{N}$, set of integers, see *Bnat*.

$a-b$ is the difference in $\mathbf{N}$, see *card_sub*: can also means *minus*, the difference in $\mathbb{N}$.

$[a,b]$ is an interval on $\mathbf{N}$, [95]

$\sum_{i=a}^{b} t_i$ is $\sum_{i\in[a,b]} t_i$.

a::b is *cons a b*, it is the list obtained by putting the element a in front of the list b.

ϕ_{A} is the characteristic function on E.

a/b is the quotient of a and b.

$n!$ is the factorial of n.

$\binom{n}{p}$, see binom.

Letters

$\mathscr{B}$ see *Bo*.

$\mathscr{C}_{\mathrm{C}}(a,b)$, $\mathscr{C}_{\mathrm{T}}(p,q)$, $\mathscr{C}(p)$: see *by_cases a b*, *chooseT* and *choose*.

$\mathrm{C}_{xy}a$ stands for *constant_function x y a*, it is the constant function from x to y with value a.

$\mathrm{C}_{\mathrm{R}}x$ may denote the equivalence class of x for R, see *class*.

$\mathrm{Coll}_{\boldsymbol{x}}\boldsymbol{R}$ says that R is collectivizing in x.

$\mathscr{E}$, see *Bset*.

$\mathscr{E}_x(\mathrm{R})$ appears in the English version where $\{x,\mathrm{R}\}$ is used in the French version; see *Zo*.

I_{A}, see *identity*.

I_{xy} see *inclusionC*, *canonical_injection*.

$\mathscr{I}(\mathrm{E},\mathrm{T},f)$ says that f is defined by transfinite induction, see *transfinite_def*.

$\mathscr{L}_{\mathrm{X}}f$, $\mathscr{L}f$, $\mathscr{L}_{\mathrm{A};\mathrm{B}}f$ (creating functions): see *L*, *acreate*, *BL*.

$\mathscr{M}f$, $\mathscr{M}_{\mathrm{A};\mathrm{B}}f$ (inverse of $\mathscr{L}$) see *bcreate1* and *bcreate*.

$\mathbb{N}$, $\mathbf{N}$, set of integers, see *Bnat*.

$\mathscr{N}$, is the bijection from $\mathbb{N}$ onto $\mathbf{N}$, see *nat_to_B*.

$\mathfrak{P}(x)$, see *powerset*.

$\mathrm{pr}_1 z$, $\mathrm{pr}_2 z$, $\mathrm{pr}_\iota f$, $\mathrm{pr}_\jmath f$ (projections), see P, Q, *pr_i*, *pr_j*.

$\mathscr{R} x$ see *Ro*.

$\mathrm{R}_{ab} f$ (restriction) see restriction2.

$\mathscr{V}(x, f)$, $\mathscr{V}_f x$ (value of a function): see *V*.

$\mathscr{W}_f x$ (value of a function): see *W*.

$\mathscr{X}(f, y)$, see *Xo*.

$\mathscr{Y}(\mathrm{P}, x, y)$ see *Yo*.

$\mathscr{Z}(x, \mathrm{P})$ see *Zo*.

¶ is not defined. We use it as a paragraph separator.

Words

acreate f, $\mathscr{L} f$, is the correspondence associated to the Coq function f.

agrees_on x ff', *agreeC x ff'* is the property that for all $a \in x$, $f(a)$ and $f'(a)$ are defined and equal.

antisymmetric_r r says that the relation r is antisymmetric, [5].

axioms_product_order f g is the condition under which *product_order f g* is an order, [16].

back_to_nat f n returns the value of f (defined on a subset of **N**) as is if f were defined on $\mathbb{N}$, [101].

bcreate f A B, $\mathscr{M}_{\mathrm{A};\mathrm{B}} f$, is a kind of inverse of $\mathscr{L}$.

bcreate1 f, $\mathscr{M} f$, is a kind of inverse of $\mathscr{L}$.

bijective f, *bijectiveC f*, means that f is a bijection.

binom n p, $\binom{n}{p}$, is the binomial coefficient, [118].

BL f a b, $\mathscr{L}_{\mathrm{A};\mathrm{B}} f$, *fun_function f a b*, is function from A to B whose graph is $\mathscr{L}_{\mathrm{A}} f$.

Bnat or **N** is the set of all integers, [75].

Bnat_divides b a says that $a = bq$ for some q, [107].

Bnat_order, *Bnat_le x y*, *Bnat_lt x y* is the ordering on **N**, and the relations $x \leq y$ or $x < y$ on **N**, [75].

Bset or $\mathscr{E}$ is the type of sets.

Bo, $\mathscr{B}$, is an inverse of $\mathscr{R}$.

bounded_above r X, *bounded_below r X*, *bounded_both r X*, mean that X is bounded for r (from above, below or both), [24].

by_cases a b, $\mathscr{C}_{\mathrm{C}}(a, b)$, defines an object by applying a if P is true, and b if P is false.

canonical_injection x y, I_{xy}, is the inclusion map on $x \subset y$.

canon_proj r, is the mapping $x \mapsto \bar{x}$ from E onto E/R, where E/R is the quotient set of r.

card_mult a b, $\mathfrak{a}.\mathfrak{b}$ or $\mathfrak{a}\mathfrak{b}$, is the cardinal product of a family of two elements, [64].

card_plus a b, $\mathfrak{a} + \mathfrak{b}$, is the cardinal sum of a family of two elements, [64].

card_quo a b and *card_rem a b* are the quotient and remainder in the division of a by b [107].

card_pow a b, $\mathfrak{a}^{\mathfrak{b}}$, is the cardinal is the set of functions (or graphs of functions) from y into x. [68].

card_sub a b, $a - b$ is the difference of the two cardinals. [93].

card_three, *card_four*, or 3 and 4, are the cardinals $2 + 1$ and $3 + 1$, [72]

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 [60].

cardinal x, $\mathrm{Card}(x)$ is some set equipotent to x, [60].

cardinal_le x y, $x \leq_{\mathrm{Card}} y$, says that x and y are two cardinals such that x is equipotent to a subset of y, [61].

cardinal_lt x y is $x \leq_{\mathrm{Card}} y$ and $x \neq y$.

cardinal_prod x, $\mathop{\mathsf{P}}_{\iota \in \mathrm{I}} \mathfrak{a}_\iota$, is the cardinal of the product of the family of sets, [63].

cardinal_nat x maps every set equipotent to the n-th ordinal to the natural number n, [84].

cardinal_sum x, $\sum_{\iota \in \mathrm{I}} \mathfrak{a}_\iota$, is the cardinal of the disjoint of the family of sets, [63].

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 $\{0,1\}$, [106].

choose p, $\mathscr{C}(p)$, 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, $\mathscr{C}_{\mathbb{N}}(p)$, is some integer i such that $p(i)$ is true, zero if no i satisfies p, [83].

chooseT p q, $\mathscr{C}_{\mathrm{T}}(p,q)$, is our basic axiom of choice.

coarse x is $x \times x$.

coarser x is the order associated to *coarser_c*, [9].

coarser_c f g, *coarser_covering I f J g*, two definitions that say for all $j \in \mathrm{J}$ there is $i \in \mathrm{I}$ 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, [15].

cofinal_set r A says that x in the substrate of r there is an $y \in \mathrm{A}$ such that $x \leq_r y$, [23].

coinitial_set r A says that x in the substrate of r there is an $y \in \mathrm{A}$ such that $x \geq_r y$, [23].

common_prolongation_order_axiom g are the conditions on g for which an order can be put on the union, [43].

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, [43].

common_worder_axiom g are the conditions on g for which an well-ordering can be put on the union of the family [44].

compatible_with_equiv_p p r means that $p(x)$ and $x \overset{r}{\sim} y$ implies $p(y)$.

compatible_with_equiv f r means that $x \overset{r}{\sim} y$ is equivalent to $f(x) = f(y)$.

compatible_with_equivs f r r' means that $x \overset{r}{\sim} y$ is equivalent to $f(x) \overset{r'}{\sim} f(y)$.

complement a b, $a - b$, $a \setminus b$, $\complement b$, 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 $f : \mathrm{A} \times \mathrm{B} \to \mathrm{B}$ is a function, v an object of type B. If L is a list of type A C(L) is defined by $\mathrm{C}(a :: b) = f(a, \mathrm{C}(b))$ and $\mathrm{C}(nil) = v$,[102].

correspondenceC is a data type with three slots, source, target and graph.

corr_value f associates to a correspondence f its triple $(\mathrm{G}, \mathrm{A}, \mathrm{B})$.

covering f x, covering_f I f x, covering_s f x, 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 $r\langle x\rangle$.

decent_set x says that no element y of x satisfies $y \in y$, [80].

decreasing_map f s r r', decreasing_fun f r r' is a function such that $x \leq_r y$ implies $f(x) \geq_{r'} f(y)$, [18].

decreasing_sequence f r says that f is a decreasing function with source **N** and target r, [136].

diagonal A, Δ_{A}, is the set of all (x, x) such that $x \in \mathrm{A}$.

diagonal_application A is the diagonal mapping $x \mapsto (x, x)$ of A into Δ_{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 $\mathrm{pr}_1\langle f\rangle$.

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 $\mathrm{Q}(x, y)$, whenever x comes before y, [101].

EEE is a shorthand for the type *Bset* → *Bset* → *Bset*.

EEP is a shorthand for the type *Bset* → *Bset* → *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, [61].

equivalence_associated f is the equivalence relation $f(x) = f(y)$.

equivalence_associated_o r is the equivalence relation $x \prec_r y$ and $y \prec_r x$, [11]

equivalence_r r, equivalence_re r x, says that the relation r is an equivalence relation (in x).

equivalence_corr r says that the correspondence r is associated ton 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 $\sum f_i b^i$ [111].

extends g f, extendsC g f says $g(x) = f(x)$ whenever $f(x)$ is defined.

extends_in E F is the relation *extends* in $\Phi(\mathrm{E}, \mathrm{F})$, [8].

extension_order E F is the order associated to *extends_in E F*, [8].

ext_map_prod I X Y g is the function $(x_\iota)_{\iota\in\mathrm{I}} \mapsto (g_\iota(x_\iota))_{\iota\in\mathrm{I}}$ from $\prod_{\mathrm{I}} \mathrm{X}_\iota$ into $\prod_{\mathrm{I}} \mathrm{Y}_\iota$.

ext_to_prod u v is the function $(x, y) \mapsto (u(x), v(y))$, sometimes denoted $u \times v$.

extension_to_parts f, denotes the function $x \mapsto f\langle x\rangle$, from $\mathfrak{P}(\mathrm{A})$ into $\mathfrak{P}(\mathrm{B})$.

factorial n, $n!$, is the factorial function, [113].

fct_to_list A f n is the list of type A containing $f(i)$ for $i < n$, [99]

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*, [104].

finer_equivalence s r, comparison of equivalences, $x \overset{s}{\sim} y$ implies $x \overset{r}{\sim} y$.

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, [88].

first_proj g is the function $x \mapsto \mathrm{pr}_1 x$ $(x \in g)$.

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 $\mathscr{F}(\mathrm{E};\mathrm{F})$ by $\forall x, f(x) \prec_{\mathrm{G}} g(x)$, [16].

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 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 $(\prod \mathrm{X}_\iota)^{\mathrm{E}}$ and $\prod \mathrm{X}_\iota^{\mathrm{E}}$.

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 $y \leq x$, [12]

ggt r x y, $x > y$, says that $x \geq y$ and $x \neq y$, [12]

gle r x y, $x \leq y$, says that x and y are related by r, [12]

glt r x y, $x < y$, says $x \leq y$ and $x \neq y$, [12]

graph f is a part of a correspondence.

graph_of_function X Y is the function $f \mapsto \mathrm{G}_f$ defined on $\Phi(\mathrm{E},\mathrm{F})$, where G_f is the graph of f, [14].

graph_of_partition, is the function $\varpi \mapsto \tilde{\varpi}$, see *partition_relation_set*, [15]

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 F^{E} by $\forall x, f(x) \prec_{\mathrm{G}} g(x)$, [16].

greatest_element r a is the property that a is the greatest (unique maximal) element of the substrate of the order r, [21].

greatest_lower_bound r X a is the property that a is the greatest element of the set of lower bounds of X, [25].

has_infimum r X says that X has a infimum, [25].

has_inf_graph r f says that the image of the graph f has an infimum, [28].

has_supremum r X says that X has an supremum, [25].

has_sup_graph r f says that the image of the graph f has a supremum, [28].

identity A, I_{A}, is is the graph of the identity function on the set A.

identity_fun A, I_{A}, is the identity function on the set A.

IM stands for the image of a function. Its axioms implement the Scheme of Selection and Union.

image_by_fun f A, $f\langle \mathrm{A}\rangle$, is $\{t, \exists x \in \mathrm{A}, t = f(x)\}$.

image_by_graph f x, $f\langle \mathrm{A}\rangle$, is $\{t, \exists x \in \mathrm{A}, (x, t) \in f\}$.

image_of_fun f, is the image of f.

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 $\mathfrak{P}(\mathrm{A})$ [7].

inclusion_suborder A, is the order induced by $\subset$ on A [7].

increasing_map f s r r', *increasing_fun f r r'* is a function such that $x \leq_r y$ implies $f(x) \leq_{r'} f(y)$, [18].

increasing_pre f r r' says that f is an increasing function for preorders r and r', [148].

increasing_sequence f r says that f is an increasing function with source **N** and target r, [136].

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 [7].

induction_defined s a is the function f defined by $f(0) = a$ and $f(n+1) = s(f(n))$, [131].

induction_defined1 E h a is the function f defined by $f(0) = a$ and $f(n+1) = h(n, f(n))$, [131].

induction_defined2 E h a p is the function f defined for $n < p$ by $f(0) = a$ and $f(n+1) = h(n, f(n))$, [131].

inductive_set r means that r is an order whose substrate is inductive, [49].

inf r x y, $\inf(x, y)$, is the greatest lower bound of pair $\{x, y\}$ (if it exists), [25].

infimum r X, $\inf_{\mathrm{E}} \mathrm{X}$, is the greatest lower bound of X (if it exists), [25].

infinite_set x means that x is a not a finite set, [75].

inf_graph r f, $\inf\limits_{x \in \mathrm{A}} f(x)$, is the greatest lower bound of the image of the graph f (if it exists), [28].

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, $\bigcap \mathrm{X}$, is the intersection of a set of sets.

intersectiont I f, *intersectionf x f*, *intersectiont g*, $\bigcap\limits_{\iota \in \mathrm{I}} \mathrm{X}_\iota$ is the set of elements a such that forall $\iota \in \mathrm{I}$ we have $a \in \mathrm{X}_\iota$.

intersection2 X Y, $\mathrm{X} \cap \mathrm{Y}$, 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*, *interval_co r a b*, *interval_cc r a b*, *interval_cu r a interval_uo r b*n, *interval_uc r b interval_uu r*; Intervals, [35].

interval_Bnat a b, *interval_co_0a c* is the interval $[a, b]$ or $[0, c[$ as a subset of **N**.[95]

interval_Bnato a b, *interval_Bnatco a* is the interval $[a, b]$ or $[0, c[$ as an ordered set.[96]

inverse_direct_value f X, X_f, is $f^{-1}\langle f\langle \mathrm{X}\rangle\rangle$.

inverse_graph G, $\overset{-1}{\mathrm{G}}$, inverse graph of the graph G.

inverse_fun f or *inverseC a b f H*, $\overset{-1}{f}$, inverse of the function f.

inverse_image x f, $\overset{-1}{f}\langle x\rangle$, 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.

inv_image_by_graph f x, *inv_image_by_fun r x*, $\overset{-1}{f}\langle x\rangle$, direct image of a set by the inverse function

inv_corr_value t associates to a $t = (\mathrm{G}, \mathrm{A}, \mathrm{B})$ its correspondence f.

inv_graph_canon G is the bijection $(x, y) \mapsto (y, x)$ from G to G^{-1}.

is_antisymmetric r says that the graph r is antisymmetric, [5].

is_bounded_interval r x, see interval.

is_cardinal x says that x is of the form $\mathrm{Card}(x)$, [61].

is_class r x says that x is an equivalence class for r.

is_closed_interval r x, see interval.

is_countable_set x says that x is equipotent to $\mathbf{N}$, [135].

is_correspondence f says that f is associated to a triple $(\mathrm{G}, \mathrm{A}, \mathrm{B})$.

is_equivalence r says that the graph r is an equivalence.

is_expansion f b k say that f is a functional graph, defined for $i < k$ and such that $f_i < b$, [111].

is_finite_c x, *is_finite_set y*: a cardinal x is finite if $x \neq x+1$, a set is finite if its cardinal is finite, [72].

is_function f says that f is a function in the sense of Bourbaki.

is_graph f says that f is a set of pairs.

is_graph_of g r is true if g is the graph of the relation r.

is_infinite_c x means that x is a cardinal that is not finite, [75].

is_inf_fun r f x, *is_inf_graph r f x*, says that x is the supremum of the image of the function of graph f for the order r, [27].

is_interval r x, see interval.

is_left_inverse r f means that r is a retraction or left-inverse of f, and $r \circ f$ is the identity.

is_left_unbounded_interval r x, see interval.

is_open_interval r x, see interval.

is_reflexive r says that the graph r is reflexive.

is_restriction f g says that f is the restriction of g to some set.

is_right_inverse s f means that s is a section or right-inverse of f, and $f \circ s$ is the identity.

is_right_unbounded_interval r x, see interval.

is_segment r s, says that s is the interval $]\leftarrow, x[$ or the whole substrate of a well ordered relation r, [40].

is_semi_open_interval r x, see interval.

is_singleton x means that x is a singleton.

is_sup_fun r f x, *is_sup_graph r f x*, says that x is the supremum of the image of the function or graph f for the order r, [27].

is_symmetric r says that the graph r is symmetric.

is_unbounded_interval r x, see interval.

is_transitive r says that the graph r is transitive.

J x y, or (x, y), is an ordered pair, formed of two items x and y.

nil is the empty list.

L X f, *fcreate X f*, $\mathscr{L}_{\mathrm{X}} f$ is the graph formed of all $(x, f(x))$ with $x \in \mathrm{X}$.

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, [33].

least_element r a ids the property that a is the least (unique minimal) element of the substrate of the order r, [21].

least_upper_bound r X a is the property that a is the least element of the set of upper bounds of X, [25].

left_directed r means that each doubleton is bounded below, [32].

left_inverseC, 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_ι is f_ι, 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, [52].

LHS is the left hand side of an equality.

list_range L is the smallest set containing all elements of the list, [102]

list_subset L E says that all elements of the list L belong to the set E, [102]

list_sum L, *list_prod L*, is the sum or product of the element of the list L [104].

list_to_fct L, *list_to_f L*, *list_to_fctB L*, *list_to_fB L E*, converts the list L into a mapping $\mathbb{N} \to \mathbb{N}$, or a function with source $[0, n[$ and target **N** or E.[99], [100].

lower_bound r X x says that for all $y \in$ X, we have $x \leq_r y$, [24].

Lvariant a b x y, *variant a x y*, *Lvariantc x y*, these are functions whose range is the doubleton $\{x, y\}$.

maximal_element r a says that $x \leq_r a$ implies $x = a$, [20].

merge_int n m is a bijection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, [133].

minimal_element r a says that $x \geq_r a$ implies $x = a$, [20].

monotone_fun f r r' is a, increasing or decreasing function, [18].

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 *nat* to the set of finite cardinals, [85].

natR n is maps a natural number onto a pseudo-ordinal, [82]

neq x y, $x \neq y$, is inequality.

Nquo a b and *Nrem a b* are the quotient and remainder in the division of a by b, [108].

number_of_injections b a is $a!/(a-b)!$, [114].

of_finite_character x says that x is of finite character, [79].

one_point is the basic singleton.

opposite_relation r is the relation $r(y, x)$ between x and y, [5].

opposite_order r is inverse graph of r, [5].

order r says that the graph r is an order, [6].

order_associated r is the order associated to a preorder by passing on the quotient of "$x \prec y$ and $y \prec x$", [11]

order_axioms r s is the condition on which r is an order on s [12].

order_c f says that the graph of the function r is an order, [6].

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', [13].

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', [13].

order_r r says that the relation r is an order, [5].

order_re r x says that the relation r is an order on x, [6].

order_with_greatest r a is the order obtained from r by adjoining a greatest element a, [23]

ordinal_sum r f g, $\sum_{\iota\in I} X_\iota$, 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. [53].

ordinal_sum2 r r', $E_1 + E_2$, is ordinal sum of two sets. [54].

P z, $\mathrm{pr}_1 z$ denotes x if z is the pair (x, y).

partial_fun1 f y, *partial_fun1 f x*, 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 int $\mathfrak{P}(X)$, (if Y is a partition of X then $Y \in \mathfrak{P}(\mathfrak{P}(X))$) [8].

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 $y = \omega$ of x, [9].

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, [116].

pow x y, x^y, is the power function on the type *nat*, [85].

powerset x, $\mathfrak{P}(x)$, is the set of subsets of x.

$\mathrm{pr}_1 z$, $\mathrm{pr}_2 z$ stand for *pr1 z* and *pr2 z*. These are also denoted by P and Q. If z is the pair (x, y), these functions return x and y respectively.

pr_i f i, *pr_it f i*, $\mathrm{pr}_i f$, denotes a component of an element of a product.

pr_j f J, $\mathrm{pr}_J f$, is the function $(x_\iota)_{\iota\in I} \mapsto (x_\iota)_{\iota\in J}$

prec x is the finite cardinal y whose successor is y. It exists if x is a non-zero finite cardinal, [73].

preorder r is a reflexive and transitive graph, [10].

preorder_r is a reflexive and transitive relation, [10].

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 $\prod F_\iota \times \prod F'_\iota$ and $\prod(F_\iota \times F'_\iota)$.

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 $b \in B$

productt I X, *product b g* or *productf I f*, $\prod_{\iota\in I} X_\iota$ is the product of a family of sets.

product1 x a is the product of the family defined on the singleton $\{a\}$ via value x.

product1_canon x a is the canonical application from x into *product1 x a*.

product2 x y is the product of the family defined on the doubleton $\{a, b\}$ via value x and y.

product2_canon x y is the canonical application from $x \times y$ into *product2 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 Γ_i (where f defines the family X_i and g defined the family Γ_i), [16].

pseudo_ordinal x says that x is a pseudo-ordinal, [80].

Q z, $\mathrm{pr}_2 z$ 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 preorder $\succ_R$, where E is the common substrate of R and S, [148].

range f is the set of y for which there is an x with $(x, y) \in f$, it is $\mathrm{pr}_2\langle f\rangle$.

reflexive_r r x says that the relation r is reflexive in x.

reflexive_rr r says that the relation r is reflexive, [5].

related r x y is a short-hand for $(x, y) \in r$.

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 s 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 $[0, a]$ and $[b, a+b]$, [97]

restricted_eq E is the relation "$x \in$ E and $y \in$ E and $x = y$".

restriction_function f x is like *restr*, but f and the restrictions are functions.

restriction2_axioms f x y is the condition: f is a function whose source contains x, whose target contains y, moreover $a \in x$ implies $f(a) \in y$.

restriction2 f x y, *restriction2C f x y*, restriction of f as a function $x \to y$.

restrictionC f H is the restriction to x of the function $f : a \to b$, where H proves $x \subset a$ implicitly.

restriction_product f j is the product of the restrictions of $\prod f$ to J.

restriction_to_image f is the restriction of the function f to its range.

restriction_to_segment r x g, $g^{(x)}$, is the restriction of g to the segment S_x defined by the order r, [45]

restriction_to_segment_axiom r x g is the property for *restriction_to_segment* to be well-behaved, [45]

retraction: see *is_left_inverse*.

RHS is the right hand side of an equality.

right_directed r means that each doubleton is bounded above, [32].

right_inverseC, right inverse of a Coq function.

Ro x or $\mathscr{R}x$ converts its argument x of type u to a set, which is an element of u.

saturated r x means: for every $y \in x$, the class of x for the relation r is a subset of x.

saturation_of r x is the saturation of x for r.

second_proj g is the function $x \mapsto \mathrm{pr}_2 x$ $(x \in g)$.

section: see *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 $]\leftarrow, x[$, [40].

set_for_equipotent_inf2_inf E psi is a set used when proving that E is qequipoptent to $E \times E$ when E is infinite, [133].

set_of_correspondences A B means the set of triples

set_of_cardinals_le x is the set of all cardinals $\leq x$, [63].

set_of_endomorphisms E, is the set of triples (G, E, E) associated to functions from E into E.

set_of_finite_subsets x is the set of finite subset sof x, [78].

set_of_functions E F, denoted $\mathscr{F}$(E; F), is the set of triples (G, E, F) associated to functions from E into F.

set_of_functions_sum_le E n, *set_of_functions_sum_eq E n* is the set of functions f : $E \to [0, n]$ such that the sum $\sum f(i)$ is $\leq n$ or $= n$, [125].

set_of_gfunctions E F, denoted F^E, is the set of graphs of functions from E to F

set_of_injections E F is the set of injective functions from E into F, [114].

set_of_majorants1 is used in an example.

set_of_partition p E is the set of all partitions X_i of E, where each X_i has p_i elements, [116].

set_of_partition_set X is the set of all partitions of X, [8].

set_of_permutations E F, is the set of injective functions from E onto itself, [114].

set_of_segments r, *set_of_segments_strict r*, is the set of all segments of an ordered set (with possible exclusion of the whole set), [42].

set_of_sub_functions E F, denoted Φ(E; F) is the set of triples (G, A, F) associated to functions from $A \subset E$ into F.

set_of_graphs E F, is the set of functional graphs from E to F, [14].

set_of_preorders E, is the set of preorders on E, [15].

singleton x, $\{x\}$, is a set with one element.

single_list_prop A L Q says that all elements of the list L of type A satisfy the predicate Q, [101].

sof_value x y z converts three elements into a correspondence,.

small_set x means that x hast at most one element.

smallest_partition x is the singleton $\{x\}$.

source f contains (resp. is equal to) the domain of the graph of a correspondence f (resp. function f).

stationary_sequence f says that the restriction of f to some interval $[n, \to[$ is constant, [136].

strict_decreasing_map f s r r', *strict_decreasing_fun f r r'* is a function such that $x <_r y$ implies $f(x) >_{r'} f(y)$, [18].

strict_increasing_map f s r r', *strict_increasing_fun f r r'* is a function such that $x <_r y$ implies $f(x) <_{r'} f(y)$, [18].

strict_monotone_fun f r r' is a strictly increasing or strictly decreasing function, [18].

strict_sub x y, $x \subsetneq y$, means $x \subset y$ and $x \neq y$.

sub x y, $x \subset y$, means that x is a subset of y.

substrate r is the union of the domain and range.

subsets_with_p_elements p E, is the set of subsets of E having p elements, [119].

succ x is $x + 1$, [72].

sup r x y, $\sup(x, y)$, is the least upper bound of the pair $\{x, y\}$ (if it exists), [25].

supremum r X, $\sup_{\mathrm{E}} \mathrm{X}$, is the least upper bound of X (if it exists), [25].

sup_graph r f, $\sup\limits_{x\in\mathrm{A}} f(x)$, is the least upper bound of the image of the graph f (if it exists), [28].

surjective f, *surjectiveC 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 a correspondence f.

transf_axioms f A B says that for all $x \in \mathrm{A}$ we have $f(x) \in \mathrm{B}$, case where $\mathscr{L}_{\mathrm{A};\mathrm{B}} f$ is a function.

transfinite_def r p f, $\mathscr{I}(\mathrm{E}, p, f)$, says that f is defined by transfinite induction on the set E, well-ordered by r, via the property p, [45].

transfinite_defined r p is the function defined by the property p by transfinite induction on the well-ordered set r, [45].

transitive_r r says that the relation r is transitive.

transitive_set x says that if $a \in b$ and $b \in x$ then $a \in x$, [80].

total_order r means that r is a total order, [33].

two_points is the basic doubleton.

union X, $\bigcup \mathrm{X}$, is the union of a set of sets.

uniont I f, *unionf x f*, *uniont g*, $\bigcup\limits_{\iota\in\mathrm{I}} \mathrm{X}_\iota$ is the set elements a with $a \in \mathrm{X}_\iota$ for some $\iota \in \mathrm{I}$.

union2 a b, $a \cup b$, is the union of two sets.

upper_bound r X x says that for all $y \in \mathrm{X}$, we have $y \leq_r x$, [24].

V x f, $\mathscr{V}(x, f)$ or $\mathscr{V}_f x$, is the value at the point x of the graph f.

variant, see *Lvariant*.

W x f, $\mathscr{W}_f x$, 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, [39]

worder_r r says that r is a relation, that induces a well-ordering on each set where it is reflexive, [60].

Xo f y, $\mathscr{X}(f, y)$, this is $f(x)$ if $y = \mathscr{R} x$.

Yo P x y, $\mathscr{Y}(\mathrm{P}, x, y)$, is a function that associates to z the value x is P is true, and y if P is false.

Zo x R, $\mathscr{Z}(x, \mathrm{R})$, $\mathscr{E}_x(\mathrm{R})$ or $\{x, \mathrm{R}\}$: it is the set of all x that satisfy R.

Bibliography

[1] Yves Bertod and Pierre Castéran. *Interactive Theorem Proving and Program Development.* Springer, 2004.

[2] N. Bourbaki. *Elements of Mathematics, Theory of Sets.* Springer, 1968.

[3] N. Bourbaki. *Éléments de mathématiques, Théorie des ensembles.* Diffusion CCLS, 1970.

[4] Coq Development Team. The Coq reference manual. http://coq.inria.fr.

[5] José Grimm. Implementation of Bourbaki's Elements of Mathematics in Coq: Part One, Theory of Sets. Research Report RR-6999, INRIA, 2009.

[6] Douglas Hofstadter. *Gödel, Escher, Bach: An Eternal Golden Braid.* Basic Books, 1979.

[7] Jean-Louis Krivine. *Théorie axiomatique des ensembles.* Presses Universitaires de France, 1972.

Contents

1 Order relations. Ordered sets **5**

1.1 Definition of an order relation 5

1.2 Preorder relations 10

1.3 Notation and terminology 12

1.4 Ordered subsets. Product of ordered sets 13

1.5 Increasing mappings 18

1.6 Maximal and minimal elements 20

1.7 Greatest element and least element 21

1.8 Upper and lower bounds 24

1.9 Least upper bound and greatest lower bound 25

1.10 Directed sets 32

1.11 Lattices 33

1.12 Totally ordered sets 33

1.13 Intervals 35

2 Well-ordered sets **39**

2.1 Segments of a well-ordered set 39

2.2 The principle of transfinite induction 44

2.3 Zermelo's theorem 47

2.4 Inductive sets 49

2.5 Isomorphisms of well-ordered sets 50

2.6 Lexicographic products 51

2.7 Ordinals 52

3 Equipotent Sets. Cardinals **57**

3.1 The cardinal of a set 58

3.2 Order relation between cardinals 60

3.3 Operations on cardinals 63

3.4 Properties of the cardinals 0 and 1 66

3.5 Exponentiation of cardinals . . . 68
3.6 Order relation and operations on cardinals . . . 69

4 Natural integers. Finite sets **71**
4.1 Definition of integers . . . 72
4.2 Inequalities between integers . . . 73
4.3 The set of natural integers . . . 74
4.4 The principle of induction . . . 76
4.5 Finite subsets of ordered sets . . . 78
4.6 Properties of finite character . . . 79
4.7 Finite cardinals and the type nat . . . 79
4.7.1 Pseudo-ordinals . . . 79
4.7.2 Pseudo-ordinals and the type nat . . . 81
4.7.3 Bijection between nat and the integers . . . 84

5 Properties of integers **87**
5.1 Operations on integers and finite sets . . . 87
5.2 Strict inequalities between integers . . . 89
5.3 Intervals in sets of integers . . . 95
5.4 Finite sequences . . . 98
5.4.1 Lists as functions . . . 99
5.4.2 Contracting lists . . . 103
5.5 Characteristic functions on sets . . . 106
5.6 Euclidean Division . . . 107
5.7 Expansion to base b . . . 110
5.8 Combinatorial analysis . . . 113
5.8.1 Iterated functions . . . 113
5.8.2 Factorial . . . 113
5.8.3 Number of injections . . . 114
5.8.4 Number of coverings . . . 115
5.8.5 The binomial coefficient . . . 118
5.8.6 Number of increasing functions . . . 121
5.8.7 Number of monomials . . . 124

6 Infinite sets **129**
6.1 The set of natural integers . . . 129
6.2 Definition of mappings by induction . . . 130
6.3 Properties of infinite cardinals . . . 132

6.4 Countable sets 135
6.5 Stationary sequences 136

7 The size of one **139**

8 Exercises **145**
8.1 Section 1 147
1. 147
2. 147
3. 155
4. 169
5. 173
6. 176
7. 195
8. 198
9. 199
10. 202
8.2 Section 2 209
8.3 Section 3 215
8.4 Section 4 216
8.5 Section 5 219
8.6 Section 6. 223
1. 223
2. 226
3. 228
4. 229

9 Theorems, Notations, Definitions **241**

Centre de recherche INRIA Sophia Antipolis – Méditerranée
2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Centre de recherche INRIA Bordeaux – Sud Ouest : Domaine Universitaire - 351, cours de la Libération - 33405 Talence Cedex
Centre de recherche INRIA Grenoble – Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier
Centre de recherche INRIA Lille – Nord Europe : Parc Scientifique de la Haute Borne - 40, avenue Halley - 59650 Villeneuve d'Ascq
Centre de recherche INRIA Nancy – Grand Est : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex
Centre de recherche INRIA Paris – Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex
Centre de recherche INRIA Rennes – Bretagne Atlantique : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex
Centre de recherche INRIA Saclay – Île-de-France : Parc Orsay Université - ZAC des Vignes : 4, rue Jacques Monod - 91893 Orsay Cedex

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399