

Module 2

Langage objet, métalangage et démonstration

Ce module sépare le langage que l'on étudie de celui dans lequel on l'étudie, puis donne un sens précis au mot « démonstration » en le distinguant de la dérivation, objet fini engendré par un système de règles. Il établit l'outil dont tous les modules suivants useront sans le redémontrer : la définition inductive et le principe d'induction qui l'accompagne.

$$\text{Der}(S) = \text{Ind}(S)$$

Ce qui s'engendre par le bas, ligne à ligne, et ce qui se découpe par le haut, comme plus petite partie close, sont le même ensemble. Tout le parcours démontre par induction en s'appuyant sur cette égalité.

Sommaire

Objectifs	3
Prérequis supposés acquis	4
Corps du cours	5
Le partage des niveaux	5
Alphabets, mots et expressions	6
Systèmes de règles et définitions inductives	8
Dérivabilité sous hypothèses	11
Un système jouet et une démonstration à son sujet	12
Démonstration et dérivation	14
Résumé des résultats	15
Glossaire du module	16
Pièges fréquents	17
Notations introduites	18
Checklist d'auto-vérification	19

Notations hors Charte. Les neuf notations suivantes sont nécessaires à ce module et absentes de la Charte ; elles sont proposées ici conformément à la Charte § 1.

Notation	Lecture / signification	Justification
$\mathcal{A}$	alphabet : ensemble non vide de symboles	la Charte § 6.7 emploie déjà $\mathcal{A}$ pour l'alphabet de ruban d'une machine de Turing ; il s'agit ici du même objet pris en général, sans conflit
$\mathbf{a}, \mathbf{b}$	symboles d'un alphabet, composés en caractères de machine à écrire	la Charte ne fixe aucune composition pour les symboles d'un alphabet arbitraire ; la fonte distingue à l'oeil le symbole mentionné du symbole employé, ce qui est l'objet même du module
uv	concaténation des mots u et v	la juxtaposition est l'usage universel et ne peut se confondre avec un produit, aucune structure multiplicative n'étant définie sur les mots dans le parcours
$\lg(w)$	longueur du mot w	la Charte § 6.2 réserve $ E $ au cardinal et la § 6.3 cite $ \varphi $ comme variante non retenue pour la hauteur ; $\lg$ évite les deux surcharges, et $h(\varphi)$ de la § 6.3 désigne une autre grandeur, la hauteur de l'arbre syntaxique
$\#_s(w)$	nombre d'occurrences du symbole s dans le mot w	aucun conflit : le signe $\#$ n'est cité par la Charte que comme variante non retenue $\#E$ du cardinal, et l'indice lève ici toute ambiguïté
$S = (U, \mathcal{R})$	système de règles : univers U , ensemble de règles $\mathcal{R}$	la Charte § 6.7 emploie déjà la fonte sans empattement pour un dispositif syntaxique, $\mathbf{M}$; $\mathcal{R}$ n'est retenue par la Charte pour aucun objet, la § 6.4 ne la citant que comme variante non retenue pour les symboles de relation
$\text{Ind}(S), \text{Der}(S)$	plus petite partie close pour $\mathcal{R}$; ensemble des éléments dérivables dans S	aucun conflit avec $\text{Cn}(T)$ de la Charte § 6.6, qui désigne un ensemble de conséquences sémantiques et non le clos d'un système de règles
$S[\Gamma]$	système S enrichi des éléments de Γ pris comme axiomes	même procédé d'enrichissement que $\mathcal{L}(C)$ à la Charte § 6.5 ; les crochets sont libres pour cet emploi, l'argument étant un ensemble d'éléments de l'univers et non une substitution
$\text{Cn}_S(\Gamma)$	ensemble des éléments dérivables de Γ dans S	la Charte § 6.6 réserve $\text{Cn}(T)$, sans indice, aux conséquences <i>sémantiques</i> $\{\sigma \mid T \models \sigma\}$; l'indice S marque ici la clôture par <i>dérivabilité</i> dans un système, et l'écriture sans indice reste réservée au sens de la Charte

Objectifs

À l'issue de ce module, le lecteur saura :

- distinguer, dans une phrase mathématique, ce qui relève du langage objet et ce qui relève du métalangage, et corriger les phrases qui confondent les deux niveaux ;

- décrire un dispositif syntaxique comme un système de règles sur un univers, et exhiber une dérivation dans un tel système ;
- démontrer que la définition d'un ensemble par le bas, au moyen de dérivations, et sa définition par le haut, comme plus petite partie close, coïncident ;
- justifier une preuve par induction sur un ensemble inductivement défini en invoquant ce théorème, et repérer les hypothèses sans lesquelles il tombe ;
- démontrer les propriétés structurelles de la dérivabilité — réflexivité, monotonie, finitude, transitivité — et reconnaître laquelle d'entre elles la sémantique ne fournit pas gratuitement ;
- démontrer qu'un objet n'est pas dérivable dans un système donné, en exhibant un invariant préservé par toutes les règles.

Prérequis supposés acquis

Les notions suivantes, introduites au module 1, sont mobilisées sans être redéfinies :

- l'appartenance, l'inclusion et la compréhension restreinte : définition 1.6 et notation 1.7 (module 1, « Ensembles, fonctions et cardinalité ») ;
- les opérations booléennes et l'intersection indexée, définition 1.8 (module 1), dont l'usage exige un ensemble d'indices non vide ;
- l'ensemble des parties, définition 1.10 (module 1) ;
- le couple, le produit cartésien, les n -uplets, l'ensemble E^* des suites finies et le mot vide ε : définition 1.12 (module 1) ;
- la notion de fonction totale, d'injection et de bijection : définitions 1.19 et 1.21 (module 1) ;
- la subpotence $\preceq$, notation 1.28 (module 1), et ses propriétés de préordre, proposition 1.29 (module 1) ;
- la finitude, la dénombrabilité et le caractère au plus dénombrable, définition 1.40 (module 1) ;
- la caractérisation $E \preceq \mathbb{N}$ du caractère au plus dénombrable, corollaire 1.42 (module 1), et le fait que E^* est au plus dénombrable dès que E l'est, proposition 1.47 (module 1).

Sont supposées acquises, en outre, les connaissances mathématiques générales suivantes, extérieures au parcours et non redémontrées. Les trois premières sont exactement celles déjà admises au module 1, rappelées ici sous la numérotation propre à ce module ; la quatrième est un emprunt nouveau, signalé comme tel.

1. Le raisonnement par récurrence sur $\mathbb{N}$, sous sa forme simple et sous sa forme forte, ainsi que le principe du bon ordre : toute partie non vide de $\mathbb{N}$ possède un plus petit élément, noté $\min$. Ce prérequis est identique au prérequis 1 du module 1.

2. La définition de suites par récurrence sur $\mathbb{N}$: étant donnés une valeur initiale et une loi de passage de l'étape n à l'étape $n + 1$, il existe une unique suite les vérifiant. Ce prérequis est identique au prérequis 2 du module 1 ; il sera démontré dans le cadre général du théorème de définition par induction structurale (module 3) et du théorème de récursion transfinie (module 16).
3. Les propriétés élémentaires des ensembles finis : toute partie d'un ensemble fini est finie ; la réunion de deux ensembles finis est finie ; le principe de choix fini, à savoir qu'un nombre fini de sélections successives dans des ensembles non vides se justifie par récurrence sur le nombre de sélections. Ce prérequis reprend le prérequis 4 du module 1 et l'étend à la réunion et au choix fini, deux points admis ici sans démonstration.
4. La divisibilité élémentaire dans $\mathbb{N}$, sous la seule forme suivante : pour tout $k \in \mathbb{N}$, si 3 divise $2k$, alors 3 divise k . Cet emprunt est nouveau ; il n'est utilisé que dans la preuve du théorème 2.36.

Aucune axiomatique n'est supposée : comme au module 1, le raisonnement se mène dans la théorie naïve des ensembles, dont le statut est précisément l'un des objets de ce module.

Corps du cours

Le partage des niveaux

Un texte de logique parle de langages, de formules, de dérivations. Il en parle dans un langage, qui n'est pas celui dont il parle. Tout le module tient dans cette phrase, et la difficulté est qu'elle est facile à admettre et difficile à respecter : les fautes de niveau ne produisent pas d'erreur visible, elles produisent des énoncés qui semblent avoir un sens et n'en ont pas.

Définition 2.1 (Langage objet, métalangage, métathéorie). Étant donné un travail mathématique portant sur un langage, on appelle **langage objet** le langage dont les expressions sont l'objet d'étude, et **métalangage** le langage dans lequel cette étude est conduite. On appelle **métathéorie** l'ensemble des énoncés démontrés dans le métalangage à propos du langage objet et des systèmes qui lui sont associés.

Dans tout le parcours, le métalangage est le français augmenté de la théorie naïve des ensembles du module 1, et les langages objets sont ceux que les modules 3, 6 et 16 construiront. Cette dissymétrie est délibérée : le langage objet est entièrement décrit, symbole par symbole, tandis que le métalangage est employé sans être décrit.

Notation 2.2 (Usage et mention). Une expression est **employée** lorsqu'elle sert à dire ce qu'elle signifie, et **mentionnée** lorsqu'elle est elle-même l'objet du propos. Dans tout le parcours, une expression du langage objet mentionnée est composée en mathématiques, éventuellement en caractères de machine à écrire pour les symboles d'un alphabet arbitraire ; un fragment de français mentionné est placé entre guillemets.

Exemple 2.3. Les deux phrases « Paris compte deux millions d'habitants » et « "Paris"

compte cinq lettres » ne portent pas sur le même objet : la première emploie le nom, la seconde le mentionne. De même, si l'on convient que le mot **ab** est formé des deux symboles **a** et **b**, la phrase « $\text{lg}(\mathbf{ab}) = 2$ » est une phrase du métalangage, dont le sujet est un objet syntaxique ; elle ne dit rien de ce que **a** et **b** pourraient signifier, et n'exige d'ailleurs pas qu'ils signifient quoi que ce soit.

Contre-exemple 2.4 (Deux confusions de niveaux). Les deux écritures suivantes sont fautives et resteront proscrites dans tout le parcours.

La première est $\mathcal{M} \models \varphi \rightarrow \mathcal{M} \models \psi$. Le signe $\rightarrow$ est un connecteur du langage objet : il ne relie que des formules de ce langage. Or $\mathcal{M} \models \varphi$ n'est pas une formule du langage objet, c'est une assertion du métalangage. L'écriture correcte est : si $\mathcal{M} \models \varphi$, alors $\mathcal{M} \models \psi$, ou, dans une chaîne alignée, $\mathcal{M} \models \varphi \implies \mathcal{M} \models \psi$ (Charte § 4.1).

La seconde est « l'énoncé $\Gamma \vdash \varphi$ est dérivable ». Le signe $\vdash$ appartient au métalangage : $\Gamma \vdash \varphi$ affirme l'existence d'une dérivation, et une telle affirmation ne se dérive pas, elle se démontre. L'écriture correcte est : on démontre que $\Gamma \vdash \varphi$ (Charte § 4.2).

Remarque 2.5. Le partage entre les deux niveaux n'est pas un partage entre deux langages fixés une fois pour toutes : il est relatif au travail en cours. La théorie des ensembles est ici le métalangage ; elle deviendra langage objet au module 16, où ZF est une théorie du premier ordre comme une autre. Symétriquement, l'arithmétique servira de métathéorie modeste avant d'être elle-même codée dans l'arithmétique (module 13), ce qui permettra à un énoncé du langage objet de porter sur les dérivations de sa propre théorie : c'est le mécanisme du premier théorème d'incomplétude de Gödel (module 14). L'effondrement complet des deux niveaux, lui, est impossible : c'est le contenu du théorème de Tarski (indéfinissabilité de la vérité) (module 14).

Exercice 2.6. Pour chacune des phrases suivantes, dire si elle appartient au langage objet ou au métalangage, et, dans le second cas, indiquer de quel objet elle parle : (i) $\forall x (x = x)$; (ii) la formule $\forall x (x = x)$ ne contient aucune variable libre ; (iii) $\varphi \wedge \psi$; (iv) Γ est un ensemble fini de formules ; (v) $\perp$.

Exercice 2.7. Corriger les trois phrases suivantes en respectant la Charte § 4.1, et dire dans chaque cas quel signe a été employé hors de son niveau : (i) « $\Gamma \vdash \varphi \wedge \Gamma \vdash \psi$ » ; (ii) « pour toute formule φ , $\forall \varphi (\varphi \vee \neg \varphi)$ » ; (iii) « la théorie T est cohérente $\rightarrow T$ admet un modèle ».

Alphabets, mots et expressions

Avant tout système, il faut des objets sur lesquels les règles opèrent. Ces objets sont des suites finies de symboles, et rien d'autre : c'est le degré zéro de la syntaxe, celui qui rend la notion de règle purement mécanique.

Définition 2.8 (Alphabet, symbole, mot). Un **alphabet** est un ensemble non vide $\mathcal{A}$, dont les éléments sont appelés **symboles**. Un **mot** sur $\mathcal{A}$ est un élément de $\mathcal{A}^*$, c'est-à-dire une suite finie de symboles au sens de la définition 1.12 (module 1, « Ensembles, fonctions et cardinalité ») ; le mot vide est noté ε . On convient que l'alphabet est choisi de sorte que les ensembles $\mathcal{A}^n$, pour $n \in \mathbb{N}$, soient deux à deux disjoints ; la **longueur** d'un mot w , notée $\text{lg}(w)$, est alors l'unique n tel que $w \in \mathcal{A}^n$.

Remarque 2.9. La convention de disjonction n'est pas une précaution rhétorique. Rien n'interdit *a priori* qu'un symbole soit lui-même un couple de symboles : l'alphabet

$\mathcal{A} := \{\mathbf{a}, (\mathbf{a}, \mathbf{a})\}$ contient un élément qui appartient aussi à $\mathcal{A}^2$, et pour cet alphabet la longueur ne serait pas définie sans ambiguïté. La convention est loisible : quitte à remplacer $\mathcal{A}$ par une copie disjointe, par exemple $\{(s, \emptyset) \mid s \in \mathcal{A}\}$, on peut toujours s'y ramener, et aucun résultat du parcours ne dépend du choix de la copie. Le module 1 avait déjà besoin de cette convention pour parler, dans la preuve de la proposition 1.47, de l'unique n tel que $w \in E^n$.

Notation 2.10 (Concaténation et occurrences). Pour $u, v \in \mathcal{A}^*$, la **concaténation** uv est définie par récurrence sur $\text{lg}(v)$ (prérequis 2) : $u\varepsilon := u$, et $u(v's) := (uv')s$ lorsque v s'écrit $v's$ avec $s \in \mathcal{A}$ et $v' \in \mathcal{A}^*$. Pour $s \in \mathcal{A}$ et $w \in \mathcal{A}^*$, le nombre d'occurrences de s dans w , noté $\#_s(w)$, est défini par la même récurrence : $\#_s(\varepsilon) := 0$, $\#_s(w't) := \#_s(w') + 1$ si t est s , et $\#_s(w't) := \#_s(w')$ sinon.

Proposition 2.11 (Le monoïde des mots). Pour tous mots u, v, w sur $\mathcal{A}$ et tout symbole s :

1. $(uv)w = u(vw)$, et $\varepsilon u = u\varepsilon = u$;
2. $\text{lg}(uv) = \text{lg}(u) + \text{lg}(v)$;
3. $\#_s(uv) = \#_s(u) + \#_s(v)$.

Preuve. Par récurrence sur $\text{lg}(w)$ pour le point 1, sur $\text{lg}(v)$ pour les points 2 et 3.

Point 1, associativité. Cas de base : si $\text{lg}(w) = 0$, alors w est ε , et $(uv)\varepsilon = uv = u(v\varepsilon)$ par la notation 2.10 appliquée deux fois. Hérédité : supposons l'égalité acquise pour tout mot de longueur n et soit w de longueur $n + 1$, écrit $w's$ avec $\text{lg}(w') = n$. Alors $(uv)(w's) = ((uv)w')s$ par la notation 2.10, puis $((uv)w')s = (u(vw'))s$ par l'hypothèse de récurrence, et enfin $(u(vw'))s = u((vw')s) = u(v(w's))$ par deux applications de la notation 2.10. Les deux membres coïncident.

Point 1, neutralité. L'égalité $u\varepsilon = u$ est la clause de base de la notation 2.10. L'égalité $\varepsilon u = u$ se démontre par récurrence sur $\text{lg}(u)$: elle est acquise pour u égal à ε , et si $\varepsilon u' = u'$, alors $\varepsilon(u's) = (\varepsilon u')s = u's$.

Point 2. Cas de base : $\text{lg}(u\varepsilon) = \text{lg}(u) = \text{lg}(u) + 0$. Hérédité : si $\text{lg}(uv') = \text{lg}(u) + \text{lg}(v')$, alors uv , pour v égal à $v's$, vaut $(uv')s$, dont la longueur est $\text{lg}(uv') + 1$, c'est-à-dire $\text{lg}(u) + \text{lg}(v') + 1 = \text{lg}(u) + \text{lg}(v)$.

Point 3. Cas de base : $\#_s(u\varepsilon) = \#_s(u) = \#_s(u) + \#_s(\varepsilon)$. Hérédité : soit v égal à $v't$. Si t est s , alors $\#_s(uv) = \#_s((uv')s) = \#_s(uv') + 1$, qui vaut $\#_s(u) + \#_s(v') + 1 = \#_s(u) + \#_s(v)$ par l'hypothèse de récurrence et par la notation 2.10. Si t n'est pas s , alors $\#_s(uv) = \#_s(uv') = \#_s(u) + \#_s(v') = \#_s(u) + \#_s(v)$, pour les mêmes raisons. Les deux cas sont exhaustifs. ■

Définition 2.12 (Facteur, préfixe, suffixe). Un mot x est un **facteur** du mot w lorsqu'il existe des mots u et v tels que $w = uxv$; c'est un **préfixe** lorsque u peut être pris égal à ε , et un **suffixe** lorsque v peut l'être.

Proposition 2.13 (Dénombrabilité des mots et des suites de mots). Si $\mathcal{A}$ est au plus dénombrable, alors $\mathcal{A}^*$ est au plus dénombrable, et il en va de même de $(\mathcal{A}^*)^*$, ensemble des suites finies de mots. Plus généralement, toute partie d'un ensemble au plus dénombrable est au plus dénombrable.

Preuve. Construction directe, par application de résultats du module 1.

Les deux premières assertions. La proposition 1.47 (module 1) affirme que E^* est au plus dénombrable dès que E l'est. Appliquée à $E := \mathcal{A}$, elle donne la première assertion ; appliquée ensuite à $E := \mathcal{A}^*$, qui vient d'être reconnu au plus dénombrable, elle donne la seconde.

L'assertion générale. Soient F au plus dénombrable et $D \subseteq F$. Par le corollaire 1.42 (module 1), $F \preccurlyeq \mathbb{N}$. Par la proposition 1.29 (iii) (module 1), $D \subseteq F$ donne $D \preccurlyeq F$, puis la transitivité, proposition 1.29 (ii) (module 1), donne $D \preccurlyeq \mathbb{N}$. Le corollaire 1.42, dans son sens réciproque, conclut que D est au plus dénombrable. ■

Remarque 2.14. Une syntaxe, dans tout le parcours, sera une partie de $\mathcal{A}^*$: les formules propositionnelles au module 3, les termes et formules du premier ordre au module 6. La proposition 2.13 fixe donc d'emblée la taille de ces ensembles : dès que l'alphabet est au plus dénombrable, il n'y a qu'au plus dénombrablement de formules, quoi qu'on fasse. C'est cette borne, et non un choix de rédaction, qui rend disponibles les énumérations sur lesquelles reposeront le lemme de Lindenbaum et le théorème de Löwenheim–Skolem descendant (module 9).

Exercice 2.15. Démontrer, par récurrence sur $\lg(v)$, que la concaténation est simplifiable à gauche : si $uv = uw$, alors $v = w$. En déduire qu'un mot admet une unique écriture comme concaténation d'un préfixe de longueur k et d'un suffixe, pour chaque $k \leq \lg(w)$.

Exercice 2.16. Soit $\mathcal{A}$ un alphabet fini à k symboles, $k \geq 1$. Démontrer par récurrence que $\mathcal{A}^n$ a exactement k^n éléments, puis que $\mathcal{A}^*$ est dénombrable au sens de la définition 1.40 (module 1). Pourquoi l'hypothèse $k \geq 1$ est-elle nécessaire à la seconde assertion, et que devient $\mathcal{A}^*$ lorsque $\mathcal{A}$ est vide, si l'on renonce à la clause de non-vacuité de la définition 2.8 ?

Systèmes de règles et définitions inductives

Tous les objets syntaxiques du parcours — formules, dérivations, théories closes par déduction — sont engendrés de la même façon : on part de quelques objets donnés et l'on applique un nombre fini de fois des règles à un nombre fini de prémisses. Il vaut la peine de traiter cette situation une fois pour toutes, en général, plutôt que de la refaire à chaque module.

Définition 2.17 (Système de règles). Soit U un ensemble, appelé **univers**. Une **règle** sur U est un couple (P, c) où P est une partie finie de U , appelée ensemble des **prémisses** de la règle, et $c \in U$, appelé sa **conclusion**. Un **système de règles** est un couple $S = (U, \mathcal{R})$ où $\mathcal{R}$ est un ensemble de règles sur U . Une règle dont l'ensemble de prémisses est vide est appelée **axiome** du système.

Exemple 2.18. Prenons $U := \mathbb{N}$ et $\mathcal{R} := \{(\emptyset, 0)\} \cup \{(\{n\}, n+2) \mid n \in \mathbb{N}\}$. Le système a un axiome, 0, et une infinité de règles à une prémisses. On attend de lui qu'il engendre les entiers pairs ; c'est ce que l'exercice 2.27 demande d'établir, une fois donnés les deux outils qui suivent.

Définition 2.19 (Partie close, ensemble inductivement défini). Soit $S = (U, \mathcal{R})$ un système de règles. Une partie $X \subseteq U$ est **close** pour $\mathcal{R}$ lorsque, pour toute règle $(P, c) \in \mathcal{R}$, l'inclusion $P \subseteq X$ entraîne $c \in X$. On pose

$$\text{Ind}(S) := \bigcap_{X \in \mathcal{C}} X, \quad \text{où } \mathcal{C} := \{X \in \mathcal{P}(U) \mid X \text{ est close pour } \mathcal{R}\}.$$

La famille $\mathcal{C}$ est un ensemble par compréhension restreinte à $\mathcal{P}(U)$ (notation 1.7 et définition 1.10, module 1) ; elle est non vide, car U lui-même est clos, ce qui légitime l'intersection indexée au sens de la définition 1.8 (module 1). Par construction, $\text{Ind}(\mathbf{S})$ est contenu dans toute partie close ; qu'il soit lui-même clos n'a rien d'immédiat et résultera du théorème 2.21.

Définition 2.20 (Dérivation, élément dérivable). Soit $\mathbf{S} = (U, \mathcal{R})$ un système de règles. Une **dérivation** dans $\mathbf{S}$ est une suite finie non vide $(x_1, \dots, x_n)$ d'éléments de U telle que, pour tout i compris entre 1 et n , il existe une règle $(P, x_i) \in \mathcal{R}$ vérifiant $P \subseteq \{x_1, \dots, x_{i-1}\}$. Un élément $x \in U$ est **dérivable** dans $\mathbf{S}$ lorsqu'il existe une dérivation dont il est le dernier terme ; on note $\text{Der}(\mathbf{S})$ l'ensemble des éléments dérivables.

Pour $i = 1$, l'ensemble $\{x_1, \dots, x_{i-1}\}$ est vide : la première ligne d'une dérivation est donc nécessairement un axiome. Une dérivation est un objet fini, et la vérification qu'une suite donnée en est une ne porte que sur des faits finis, ligne par ligne : c'est là tout l'intérêt de la notion, et l'on y reviendra à la remarque 2.42.

Théorème 2.21 (Adéquation des deux définitions). Soit $\mathbf{S} = (U, \mathcal{R})$ un système de règles. Alors $\text{Der}(\mathbf{S}) = \text{Ind}(\mathbf{S})$, et cet ensemble est la plus petite partie de U close pour $\mathcal{R}$: il est clos, et il est contenu dans toute partie close.

Preuve. *Par double inclusion : l'inclusion directe par récurrence forte sur le rang d'une ligne de dérivation, l'inclusion réciproque par minimalité, au moyen d'une assertion auxiliaire.*

Inclusion $\text{Der}(\mathbf{S}) \subseteq X$ pour toute partie close X . Soit X close pour $\mathcal{R}$ et soit $(x_1, \dots, x_n)$ une dérivation. Démontrons par récurrence forte sur i (prérequis 1) que $x_i \in X$ pour tout i compris entre 1 et n . Soit i tel que $x_j \in X$ pour tout $j < i$. Par la définition 2.20, il existe une règle $(P, x_i) \in \mathcal{R}$ avec $P \subseteq \{x_1, \dots, x_{i-1}\}$; par l'hypothèse de récurrence, $\{x_1, \dots, x_{i-1}\} \subseteq X$, donc $P \subseteq X$, et la clôture de X donne $x_i \in X$. En particulier $x_n \in X$. Tout élément dérivable étant le dernier terme d'une dérivation, $\text{Der}(\mathbf{S}) \subseteq X$. Comme X était une partie close quelconque, la définition 2.19 donne $\text{Der}(\mathbf{S}) \subseteq \text{Ind}(\mathbf{S})$.

Assertion auxiliaire. Si $(x_1, \dots, x_n)$ et $(y_1, \dots, y_m)$ sont deux dérivations dans $\mathbf{S}$, alors la suite $(x_1, \dots, x_n, y_1, \dots, y_m)$ en est une.

Preuve de l'assertion auxiliaire. *Vérification directe, ligne par ligne.* Notons $(z_1, \dots, z_{n+m})$ la suite concaténée. Pour $i \leq n$, on a $z_i = x_i$ et $\{z_1, \dots, z_{i-1}\} = \{x_1, \dots, x_{i-1}\}$, de sorte que la règle qui justifie x_i dans la première dérivation justifie z_i dans la suite concaténée. Pour $i = n+j$ avec $1 \leq j \leq m$, on a $z_i = y_j$, et la règle (P, y_j) qui justifie y_j dans la seconde dérivation vérifie $P \subseteq \{y_1, \dots, y_{j-1}\} \subseteq \{z_1, \dots, z_{i-1}\}$; elle justifie donc z_i . Toutes les lignes étant justifiées, la suite concaténée est une dérivation. $\square$

Clôture de $\text{Der}(\mathbf{S})$. Soit $(P, c) \in \mathcal{R}$ avec $P \subseteq \text{Der}(\mathbf{S})$. L'ensemble P est fini par la définition 2.17 ; écrivons $P = \{p_1, \dots, p_k\}$ avec $k \in \mathbb{N}$. Si $k = 0$, la suite à un terme (c) est une dérivation, puisque la règle $(\emptyset, c)$ justifie sa première ligne, et $c \in \text{Der}(\mathbf{S})$. Si $k \geq 1$, chaque p_j est le dernier terme d'une dérivation d_j ; on en fixe une pour chaque j , ce qui est un choix fini (prérequis 3) et ne fait donc pas appel à l'axiome du choix. Par l'assertion auxiliaire et une récurrence sur k , la suite d obtenue en concaténant $d_1, \dots, d_k$ dans cet ordre est une dérivation, et chaque p_j figure parmi ses termes. La suite d suivie de c est alors une dérivation : ses $\text{lg}(d)$ premières lignes sont justifiées comme dans d , et la dernière l'est par la règle (P, c) , dont les prémisses figurent toutes parmi les termes de d . Donc $c \in \text{Der}(\mathbf{S})$, et $\text{Der}(\mathbf{S})$ est close.

Conclusion. L'ensemble $\text{Der}(\mathbf{S})$ est une partie close de U ; il figure donc parmi les $X \in \mathcal{C}$ dont $\text{Ind}(\mathbf{S})$ est l'intersection, d'où $\text{Ind}(\mathbf{S}) \subseteq \text{Der}(\mathbf{S})$. Avec l'inclusion établie en premier lieu, les deux ensembles sont égaux. Cet ensemble est clos et contenu dans toute partie close : c'est bien la plus petite partie close pour $\mathcal{R}$. ■

Corollaire 2.22 (Principe d'induction). Soient $\mathbf{S} = (U, \mathcal{R})$ un système de règles et Q une propriété des éléments de U . Si, pour toute règle $(P, c) \in \mathcal{R}$, l'hypothèse « tout élément de P vérifie Q » entraîne « c vérifie Q », alors tout élément dérivable dans $\mathbf{S}$ vérifie Q .

Preuve. *Construction directe, par application du théorème 2.21.* Posons $X_Q := \{u \in U \mid Q(u)\}$, qui est une partie de U par compréhension restreinte (notation 1.7, module 1). L'hypothèse dit exactement que X_Q est close pour $\mathcal{R}$ au sens de la définition 2.19. Par le théorème 2.21, $\text{Der}(\mathbf{S})$ est contenu dans toute partie close, donc dans X_Q : tout élément dérivable vérifie Q . ■

Remarque 2.23. Le corollaire 2.22 est le seul principe d'induction dont le parcours aura besoin en syntaxe : l'induction structurelle sur les formules (module 3), l'induction sur la hauteur, l'induction sur les dérivations (modules 5 et 8) en sont des cas particuliers, obtenus en choisissant convenablement l'univers et les règles. La Charte § 4.3 en fixe la rédaction en trois temps ; le présent corollaire en fixe la justification. Une seule famille d'inductions échappera à ce cadre, l'induction transfinie (module 16), parce que ses règles y ont des ensembles infinis de prémisses — et l'exercice 2.26 montre que ce n'est pas un détail.

Proposition 2.24 (Dénombrabilité des dérivations). Si l'univers U est au plus dénombrable, alors l'ensemble des dérivations de $\mathbf{S} = (U, \mathcal{R})$ est au plus dénombrable, et $\text{Der}(\mathbf{S})$ l'est aussi.

Preuve. *Construction directe, par application de la proposition 2.13.* Notons D l'ensemble des dérivations de $\mathbf{S}$. Par la définition 2.20, une dérivation est une suite finie d'éléments de U , donc $D \subseteq U^*$. Par la proposition 2.13 appliquée à l'alphabet U , l'ensemble U^* est au plus dénombrable, et sa partie D l'est aussi par la dernière assertion de cette même proposition. Enfin $\text{Der}(\mathbf{S}) \subseteq U$ est au plus dénombrable pour la même raison. ■

Le second point de la proposition 2.24 est trivial ; le premier ne l'est pas, et c'est lui qui servira. Il dit qu'un système de règles sur un univers au plus dénombrable ne dispose que d'au plus dénombrablement de dérivations, quel que soit le nombre de ses règles. Aucune énumération de dérivations ne pourra donc jamais atteindre un ensemble non dénombrable d'objets : c'est la première apparition, encore muette, de l'écart entre ce qu'un système démontre et ce qu'il vise, écart que le théorème de Löwenheim–Skolem descendant (module 9) et le paradoxe de Skolem (module 9) rendront spectaculaire.

Exercice 2.25. Redémontrer, sans utiliser le théorème 2.21, que $\text{Ind}(\mathbf{S})$ est close pour $\mathcal{R}$, en établissant d'abord que toute intersection d'une famille non vide de parties closes est close. Comparer la longueur des deux arguments.

Exercice 2.26. On étend la définition 2.17 en autorisant des règles (P, c) dont l'ensemble de prémisses P est quelconque, la définition 2.19 étant inchangée et la définition 2.20 conservant des dérivations finies. Soit $U := \mathbb{N} \cup \{\mathbb{N}\}$ et $\mathcal{R} := \{(\emptyset, 0)\} \cup \{(\{n\}, n+1) \mid n \in \mathbb{N}\} \cup \{(\mathbb{N}, \mathbb{N})\}$. Démontrer que $\mathbb{N} \in \text{Ind}(\mathbf{S})$ mais que $\mathbb{N} \notin \text{Der}(\mathbf{S})$, et identifier précisément l'endroit de la preuve du théorème 2.21 où la finitude des prémisses a été employée.

Exercice 2.27. Pour le système de l'exemple 2.18, démontrer que $\text{Ind}(\mathbf{S})$ est exactement l'ensemble des entiers pairs, par double inclusion : l'inclusion directe au moyen du corollaire 2.22, l'inclusion réciproque en exhibant, pour chaque entier pair, une dérivation, et en invoquant le théorème 2.21.

Dérivabilité sous hypothèses

Un système de règles engendre un ensemble d'objets à partir de ses seuls axiomes. La pratique demande davantage : on veut dériver à partir d'hypothèses supplémentaires, provisoirement adoptées. Le procédé est uniforme, et les propriétés qui en résultent sont exactement celles que tous les systèmes de déduction du parcours exhiberont.

Définition 2.28 (Système enrichi, dérivabilité relative). Soient $\mathbf{S} = (U, \mathcal{R})$ un système de règles et $\Gamma \subseteq U$. Le **système enrichi** $\mathbf{S}[\Gamma]$ est le système $(U, \mathcal{R} \cup \{(\emptyset, g) \mid g \in \Gamma\})$, obtenu en adjoignant à $\mathcal{R}$ un axiome par élément de Γ . On écrit $\Gamma \vdash_{\mathbf{S}} x$ lorsque $x \in \text{Der}(\mathbf{S}[\Gamma])$, et l'on dit alors que x est **dérivable de** Γ dans $\mathbf{S}$. L'écriture $\emptyset \vdash_{\mathbf{S}} x$ équivaut à $x \in \text{Der}(\mathbf{S})$.

Théorème 2.29 (Propriétés structurelles de la dérivabilité). Soient $\mathbf{S} = (U, \mathcal{R})$ un système de règles, Γ, Δ des parties de U et $x \in U$.

1. *Réflexivité.* Si $x \in \Gamma$, alors $\Gamma \vdash_{\mathbf{S}} x$.
2. *Monotonie.* Si $\Gamma \subseteq \Delta$ et $\Gamma \vdash_{\mathbf{S}} x$, alors $\Delta \vdash_{\mathbf{S}} x$.
3. *Finitude.* Si $\Gamma \vdash_{\mathbf{S}} x$, il existe une partie finie $\Gamma_0 \subseteq \Gamma$ telle que $\Gamma_0 \vdash_{\mathbf{S}} x$.
4. *Transitivité.* Si $\Gamma \vdash_{\mathbf{S}} y$ pour tout $y \in \Delta$, et si $\Delta \vdash_{\mathbf{S}} x$, alors $\Gamma \vdash_{\mathbf{S}} x$.

Preuve. *Construction directe pour les points 1 et 2, analyse d'une dérivation ligne par ligne pour le point 3, application du principe d'induction pour le point 4.*

Point 1. Si $x \in \Gamma$, le couple $(\emptyset, x)$ est une règle de $\mathbf{S}[\Gamma]$ par la définition 2.28. La suite à un terme (x) est donc une dérivation dans $\mathbf{S}[\Gamma]$, et $\Gamma \vdash_{\mathbf{S}} x$.

Point 2. De $\Gamma \subseteq \Delta$ on tire que tout axiome de $\mathbf{S}[\Gamma]$ est un axiome de $\mathbf{S}[\Delta]$, donc que l'ensemble des règles de $\mathbf{S}[\Gamma]$ est inclus dans celui de $\mathbf{S}[\Delta]$. Or, si un système a plus de règles qu'un autre sur le même univers, toute dérivation du second est une dérivation du premier : la condition de la définition 2.20 exige l'existence d'une règle justifiant chaque ligne, et une règle du système le plus pauvre est aussi une règle du plus riche. Une dérivation de x dans $\mathbf{S}[\Gamma]$ est donc une dérivation de x dans $\mathbf{S}[\Delta]$.

Point 3. Soit $(x_1, \dots, x_n)$ une dérivation de x dans $\mathbf{S}[\Gamma]$, de sorte que $x_n = x$. Posons $\Gamma_0 := \Gamma \cap \{x_1, \dots, x_n\}$. C'est une partie de Γ , et elle est finie comme partie d'un ensemble fini (prérequis 3). Vérifions que la même suite est une dérivation dans $\mathbf{S}[\Gamma_0]$. Soit i compris entre 1 et n : il existe, par hypothèse, une règle (P, x_i) de $\mathbf{S}[\Gamma]$ avec $P \subseteq \{x_1, \dots, x_{i-1}\}$. Ou bien cette règle appartient à $\mathcal{R}$, et elle est aussi une règle de $\mathbf{S}[\Gamma_0]$. Ou bien elle est de la forme $(\emptyset, x_i)$ avec $x_i \in \Gamma$; alors x_i appartient à Γ et figure parmi les termes de la suite, donc $x_i \in \Gamma_0$, et $(\emptyset, x_i)$ est un axiome de $\mathbf{S}[\Gamma_0]$. Dans les deux cas, la ligne i est justifiée dans $\mathbf{S}[\Gamma_0]$. Les deux cas étant exhaustifs, la suite est une dérivation dans $\mathbf{S}[\Gamma_0]$ et $\Gamma_0 \vdash_{\mathbf{S}} x$. On notera qu'aucun choix n'est fait ici : Γ_0 est défini par compréhension et non par sélection.

Point 4. Posons $C := \{z \in U \mid \Gamma \vdash_{\mathbf{S}} z\}$, partie de U par compréhension restreinte

(notation 1.7, module 1). Démontrons que C est close pour l'ensemble des règles de $S[\Delta]$. Soit (P, c) une telle règle, avec $P \subseteq C$. Deux cas se présentent, exhaustifs par la définition 2.28. Ou bien (P, c) est de la forme $(\emptyset, d)$ avec $d \in \Delta$: alors $\Gamma \vdash_S d$ par l'hypothèse du point 4, donc $c = d \in C$. Ou bien $(P, c) \in \mathcal{R}$: c'est alors aussi une règle de $S[\Gamma]$, et comme $P \subseteq C = \text{Der}(S[\Gamma])$, la clôture de $\text{Der}(S[\Gamma])$ établie au théorème 2.21 donne $c \in \text{Der}(S[\Gamma])$, c'est-à-dire $c \in C$. Ainsi C est close pour les règles de $S[\Delta]$. Le théorème 2.21, appliqué au système $S[\Delta]$, donne $\text{Der}(S[\Delta]) \subseteq C$. Or $\Delta \vdash_S x$ signifie $x \in \text{Der}(S[\Delta])$, donc $x \in C$, c'est-à-dire $\Gamma \vdash_S x$. ■

Proposition 2.30 (Finitude des règles employées). Soient $S = (U, \mathcal{R})$ un système de règles et $x \in \text{Der}(S)$. Il existe alors une partie finie $\mathcal{R}_0 \subseteq \mathcal{R}$ telle que $x \in \text{Der}(U, \mathcal{R}_0)$.

Preuve. *Construction directe, à partir d'une dérivation de x .* Soit $(x_1, \dots, x_n)$ une dérivation de x dans S . Pour chaque i compris entre 1 et n , l'ensemble des règles de $\mathcal{R}$ justifiant la ligne i est non vide par la définition 2.20 ; on y prélève une règle r_i . Les indices étant en nombre fini, il s'agit d'un choix fini (prérequis 3), légitime sans l'axiome du choix, dont le module 17 étudiera les formes. Posons $\mathcal{R}_0 := \{r_1, \dots, r_n\}$, partie finie de $\mathcal{R}$. La même suite $(x_1, \dots, x_n)$ est une dérivation dans $(U, \mathcal{R}_0)$, puisque chaque ligne i y est justifiée par r_i , laquelle appartient à $\mathcal{R}_0$. Donc $x \in \text{Der}(U, \mathcal{R}_0)$. ■

Remarque 2.31. Les quatre points du théorème 2.29 sont les conditions dites de Tarski pour une relation de conséquence finitaire, et ils sont acquis ici *pour tout système de règles*, sans rien savoir des règles elles-mêmes. Il faut mesurer ce que cela signifie pour la suite : la correction et la complétude d'un système de déduction ne consisteront jamais à vérifier ces quatre propriétés du côté syntaxique, où elles sont automatiques, mais à confronter la relation $\vdash$ à la relation sémantique $\models$, qui, elle, ne les possède pas toutes gratuitement. La réflexivité, la monotonie et la transitivité de $\models$ se lisent directement sur sa définition ; la finitude, en revanche, n'a aucune raison d'être vraie d'une relation définie par « tout modèle de Γ satisfait φ », où Γ peut être infini. Que la conséquence sémantique soit malgré tout finitaire est un théorème, et un théorème difficile : c'est le théorème de compacité propositionnelle (module 4) et le théorème de compacité (module 9).

Exercice 2.32. Pour $\Gamma \subseteq U$, posons $\text{Cn}_S(\Gamma) := \{x \in U \mid \Gamma \vdash_S x\}$. Dédurre du théorème 2.29 que l'opérateur Cn_S est extensif ($\Gamma \subseteq \text{Cn}_S(\Gamma)$), croissant et idempotent, et vérifier que l'idempotence est exactement le point 4.

Exercice 2.33. Reprendre le système de l'exercice 2.26, avec sa règle à prémisses infinies, et démontrer que le point 3 du théorème 2.29 y devient faux si l'on définit la dérivabilité par la définition 2.19 plutôt que par la définition 2.20. Conclure sur ce que la finitude des prémisses garantit : ce n'est pas que les systèmes engendrent peu d'objets, mais que chaque objet engendré ne dépend que d'un fragment fini de données.

Un système jouet et une démonstration à son sujet

Les définitions qui précèdent restent vides tant qu'on n'a pas vu, sur un cas complet, ce qu'est une dérivation et ce qu'est une démonstration portant sur les dérivations. Le système suivant n'a aucune signification ; c'est délibéré. Ses règles sont des manipulations de symboles, et la question qu'on lui pose — un certain mot est-il dérivable ? — se tranche par un raisonnement qui ne se mène pas dans le système.

Définition 2.34 (Le système D). Soit $\mathcal{A} := \{a, b\}$. Le système $D := (\mathcal{A}^*, \mathcal{R}_D)$ a pour

univers l'ensemble des mots sur $\mathcal{A}$ et pour ensemble de règles

$$\mathcal{R}_D := \{(\emptyset, \mathbf{ab})\} \cup \{(\{\mathbf{aw}\}, \mathbf{aww}) \mid w \in \mathcal{A}^*\} \\ \cup \{(\{\mathbf{ubbbv}\}, \mathbf{uav}) \mid u, v \in \mathcal{A}^*\} \cup \{(\{\mathbf{uaav}\}, \mathbf{uv}) \mid u, v \in \mathcal{A}^*\}.$$

On désigne ces quatre familles par Ax. (l'unique axiome), R1 (duplication du suffixe après un **a** initial), R2 (remplacement d'un facteur **bbb** par **a**) et R3 (effacement d'un facteur **aa**).

Les trois dernières familles sont infinies : chacune de R1, R2, R3 n'est pas une règle mais un **schéma de règles**, une règle étant obtenue par le choix des mots u, v, w . Il en ira de même du schéma de séparation de ZF (module 16) et du schéma de récurrence de PA (module 13) : un système à ensemble infini de règles reste parfaitement légitime au sens de la définition 2.17, seule la finitude de chaque ensemble de prémisses étant requise.

Exemple 2.35. Voici deux dérivations dans D, présentées au format de la Charte § 5.1. La première ne dépend d'aucune hypothèse ; la colonne des dépendances y est donc constamment $\emptyset$.

Dép.	n	Mot	Justification
$\emptyset$	1	ab	Ax.
$\emptyset$	2	abb	R1 1, avec w égal à b
$\emptyset$	3	abbbb	R1 2, avec w égal à bb
$\emptyset$	4	aab	R2 3, avec u égal à a et v égal à b
$\emptyset$	5	b	R3 4, avec u égal à ε et v égal à b

La seconde dérive ε de l'hypothèse **abbbb**, au sens de la définition 2.28 ; la ligne 1 est un axiome du système enrichi $D[\{\mathbf{abbbb}\}]$, et son numéro reste porté par la colonne des dépendances jusqu'à la conclusion, aucune règle de D ne déchargeant d'hypothèse.

Dép.	n	Mot	Justification
1	1	abbbb	Hyp.
1	2	aa	R2 1, avec u égal à a et v égal à ε
1	3	ε	R3 2, avec u et v égaux à ε

Ainsi $\{\mathbf{abbbb}\} \vdash_D \varepsilon$. Le théorème 2.36 montrera que $\emptyset \vdash_D \varepsilon$ est faux : la conclusion tient à l'hypothèse, et non aux seules règles.

Théorème 2.36 (Invariant du système D). Pour tout mot w dérivable dans D, l'entier $\#_b(w)$ n'est pas divisible par 3.

Preuve. Par le principe d'induction du corollaire 2.22, avec un cas par famille de règles. Prenons pour propriété $Q(w)$: « 3 ne divise pas $\#_b(w)$ ». Il suffit, par le corollaire 2.22, de vérifier que Q se transmet des prémisses à la conclusion pour chacune des quatre familles de règles de la définition 2.34. Tous les calculs d'occurrences utilisent le point 3 de la proposition 2.11.

Axiome. On a $\#_b(\mathbf{ab}) = \#_b(\mathbf{a}) + \#_b(\mathbf{b}) = 0 + 1 = 1$, et 3 ne divise pas 1. La règle $(\emptyset, \mathbf{ab})$ n'ayant aucune prémisses, l'hypothèse du corollaire 2.22 est vide et la vérification est complète.

R1. Soit $w \in \mathcal{A}^*$ et supposons $Q(\mathbf{aw})$, c'est-à-dire que 3 ne divise pas $\#_b(\mathbf{aw}) = \#_b(\mathbf{a}) + \#_b(w) = \#_b(w)$. Posons $k := \#_b(w)$. La conclusion de la règle est $\mathbf{aww}$, dont le

nombre d'occurrences de $\mathbf{b}$ vaut $\#_{\mathbf{b}}(\mathbf{a}) + \#_{\mathbf{b}}(w) + \#_{\mathbf{b}}(w) = 2k$. Si 3 divisait $2k$, alors 3 diviserait k (prérequis 4), ce qui contredit l'hypothèse. Donc 3 ne divise pas $2k$, et $Q(\mathbf{a}ww)$ est acquis.

R2. Soient $u, v \in \mathcal{A}^*$ et supposons $Q(ubbbv)$. Posons $k := \#_{\mathbf{b}}(u) + \#_{\mathbf{b}}(v)$. Alors $\#_{\mathbf{b}}(ubbbv) = k + 3$, et la conclusion uav vérifie $\#_{\mathbf{b}}(uav) = k$, puisque $\#_{\mathbf{b}}(\mathbf{a}) = 0$. Si 3 divisait k , il diviserait $k + 3$, ce qui contredit l'hypothèse. Donc 3 ne divise pas k , et $Q(uav)$ est acquis.

R3. Soient $u, v \in \mathcal{A}^*$ et supposons $Q(uaav)$. Comme $\#_{\mathbf{b}}(\mathbf{a}\mathbf{a}) = 0$, on a $\#_{\mathbf{b}}(uaav) = \#_{\mathbf{b}}(u) + \#_{\mathbf{b}}(v) = \#_{\mathbf{b}}(uv)$. La conclusion a donc le même nombre d'occurrences de $\mathbf{b}$ que la prémisse, et $Q(uv)$ est acquis.

Les quatre familles de règles épuisent $\mathcal{R}_D$. Le corollaire 2.22 conclut : tout mot dérivable dans D vérifie Q . ■

Corollaire 2.37. Aucun mot ne comportant aucune occurrence de $\mathbf{b}$ n'est dérivable dans D . En particulier, ni le mot $\mathbf{a}$, ni le mot vide ε ne sont dérivables dans D .

Preuve. *Par l'absurde, à partir du théorème 2.36.* Soit w un mot sans occurrence de $\mathbf{b}$, c'est-à-dire tel que $\#_{\mathbf{b}}(w) = 0$, et supposons w dérivable dans D . Le théorème 2.36 donne alors que 3 ne divise pas $\#_{\mathbf{b}}(w) = 0$; or 3 divise 0. La contradiction est obtenue sur la divisibilité de 0 par 3, et l'hypothèse absurde — la dérivabilité de w — est réfutée. Les mots $\mathbf{a}$ et ε vérifient $\#_{\mathbf{b}} = 0$ par la notation 2.10, d'où le cas particulier. ■

Remarque 2.38. Il faut voir où vit chacun des deux raisonnements de cette sous-section. L'exemple 2.35 se passe dans le système : c'est une suite de mots, chaque ligne étant obtenue de la précédente par une règle, et sa vérification ne demande que de comparer des suites de symboles. Le théorème 2.36 ne se passe pas dans le système : D n'a aucun moyen d'exprimer « 3 ne divise pas $\#_{\mathbf{b}}(w)$ », et aucune dérivation ne saurait avoir pour conclusion une non-dérivabilité, puisque toute dérivation ne fait qu'ajouter des objets à la liste de ce qui est dérivable. Un énoncé négatif portant sur un système ne s'obtient jamais en dérivant davantage : il s'obtient en démontrant, dans la métathéorie, qu'une propriété est préservée par toutes les règles. C'est le schéma de toutes les preuves de correction (modules 5 et 8), et de toutes les preuves d'indépendance et d'incomplétude, où l'invariant est simplement plus difficile à trouver. Le tour de force des modules 13 à 15 consistera précisément à faire dire à un langage objet suffisamment riche une part de ce qui, ici, ne se dit que dans le métalangage.

Exercice 2.39. On ajoute à D le schéma de règles $R4$: de w , déduire $w\mathbf{b}$. Exhiber, au format de la Charte § 5.1, une dérivation du mot $\mathbf{a}$ dans le système ainsi obtenu, et identifier le cas de la preuve du théorème 2.36 qui cesse d'être valide. Que devient l'invariant ?

Exercice 2.40. On retire à D le schéma $R3$. Démontrer, au moyen du corollaire 2.22, que tout mot dérivable dans le système restant admet $\mathbf{a}$ pour préfixe, et en déduire que le mot $\mathbf{b}$ n'y est pas dérivable, alors qu'il l'est dans D d'après l'exemple 2.35. Commenter : retirer une règle à un système n'en diminue pas seulement les dérivations, cela peut rendre démontrables de nouveaux énoncés à son sujet.

Démonstration et dérivation

Il reste à nommer précisément ce que fait ce texte lui-même, et à mesurer ce que la formalisation déplace.

Définition 2.41 (Démonstration). Une **démonstration** est un raisonnement mené dans le métalangage, rédigé en français en phrases complètes, dont la conclusion est un énoncé portant sur les objets étudiés. Elle s'oppose à la dérivation de la définition 2.20, qui est un objet syntaxique fini, construit selon les règles d'un système fixé, et dont la conclusion est un élément de l'univers de ce système. On démontre qu'un objet est dérivable ; on construit ou l'on exhibe une dérivation.

Cette définition ne fait que fixer un vocabulaire, conformément à la Charte § 4.2 et § 7 : elle ne définit pas la démonstration comme un objet mathématique, et ne le peut pas ici. Une démonstration n'a pas de forme prescrite ; elle est reconnue correcte par un lecteur compétent, non vérifiée par un automate. Toute la logique mathématique tient dans le refus de se satisfaire de cette situation, sans pour autant pouvoir en sortir.

Remarque 2.42. Ce que la formalisation apporte est précis, et il est plus étroit qu'on ne le dit parfois. Elle ne fonde pas le raisonnement : pour vérifier qu'une suite de lignes est une dérivation, il faut déjà raisonner, et si l'on exigeait une dérivation de cette vérification, on ouvrirait une régression sans fin. Elle transforme en revanche une question de jugement en une question de calcul : la relation « la suite d est une dérivation de x dans S » ne porte, par la définition 2.20, que sur un nombre fini de lignes et un nombre fini de règles (proposition 2.30), là où la relation « x est dérivable dans S » comporte une quantification existentielle sur toutes les dérivations, c'est-à-dire sur un ensemble infini. Cet écart entre une propriété vérifiable pas à pas et une propriété seulement semi-décidable est la source de tout ce que les modules 11 et 12 établiront, jusqu'à l'indécidabilité du problème de l'arrêt (module 12) ; et c'est parce que la première est mécanique qu'elle pourra être codée dans l'arithmétique par le prédicat $\text{Dem}_T(y, x)$ de la Charte § 6.8, au module 13.

Remarque 2.43. Le programme du parcours peut maintenant s'énoncer sans métaphore. Un langage objet sera défini comme une partie de $\mathcal{A}^*$ engendrée par un système de règles (modules 3 et 6). Une sémantique lui attachera une relation $\models$, définie dans le métalangage (modules 4 et 7). Un système de déduction lui attachera une relation $\vdash$, définie comme au présent module (modules 5 et 8). Deux énoncés relieront alors ces deux relations : la correction, $\Gamma \vdash \varphi \implies \Gamma \models \varphi$, qui se démontrera par le principe d'induction du corollaire 2.22 appliqué au système de déduction ; et la complétude, $\Gamma \models \varphi \implies \Gamma \vdash \varphi$, qui exigera une construction de modèle et fait l'objet du théorème de complétude de Gödel (module 9). Les deux énoncés sont des énoncés de la métathéorie, et aucun des deux ne se dérive dans le système dont il parle.

Exercice 2.44. Reformuler chacune des trois phrases suivantes en distinguant explicitement ce qui relève du système et ce qui relève de la métathéorie, puis dire laquelle des deux relations $\vdash$ et $\models$ y est en jeu : (i) « ce théorème est vrai puisqu'on l'a démontré » ; (ii) « la cohérence de T signifie qu'on ne peut pas déduire de contradiction de T » ; (iii) « le théorème d'incomplétude dit qu'il existe des énoncés vrais et non démontrables ».

Exercice 2.45. Soit S un système de règles sur un univers U au plus dénombrable. Démontrer que l'ensemble des parties $\Gamma \subseteq U$ telles que $\Gamma \vdash_S x$ pour un x fixé n'est en général pas au plus dénombrable, alors que l'ensemble des parties finies de U l'est (exercice 1.51, module 1). Expliquer pourquoi le point 3 du théorème 2.29 rend cette différence sans conséquence pour l'étude de $\vdash_S$.

Résumé des résultats

Numéro	Nom	Énoncé abrégé	Dépendances
2.11	Le monoïde des mots	la concaténation est associative, de neutre ε ; longueur et nombre d'occurrences sont additifs	définition 2.8, notation 2.10, prérequis 2
2.13	Dénombrabilité des mots et des suites de mots	$\mathcal{A}$ au plus dénombrable entraîne $\mathcal{A}^*$ et $(\mathcal{A}^*)^*$ au plus dénombrables ; toute partie d'un ensemble au plus dénombrable l'est aussi	proposition 1.47, corollaire 1.42, proposition 1.29
2.21	Adéquation des deux définitions	$\text{Der}(\mathcal{S}) = \text{Ind}(\mathcal{S})$, plus petite partie close pour $\mathcal{R}$	définitions 2.17, 2.19, 2.20, prérequis 1, 3
2.22	Principe d'induction	une propriété transmise par toutes les règles vaut pour tout élément dérivable	théorème 2.21, notation 1.7
2.24	Dénombrabilité des dérivations	univers au plus dénombrable entraîne ensemble des dérivations au plus dénombrable	proposition 2.13, définition 2.20
2.29	Propriétés structurelles de la dérivabilité	$\vdash_{\mathcal{S}}$ est réflexive, monotone, finitaire et transitive	définition 2.28, théorème 2.21, prérequis 3
2.30	Finitude des règles employées	tout élément dérivable l'est au moyen d'un ensemble fini de règles	définition 2.20, prérequis 3
2.36	Invariant du système $\mathcal{D}$	tout mot dérivable dans $\mathcal{D}$ a un nombre d'occurrences de $\mathbf{b}$ non divisible par 3	corollaire 2.22, proposition 2.11, définition 2.34, prérequis 4
2.37	Non-dérivabilité des mots sans $\mathbf{b}$	ni $\mathbf{a}$ ni ε ne sont dérivables dans $\mathcal{D}$	théorème 2.36

Glossaire du module

Terme	Définition en une phrase	Numéro de la définition formelle
langage objet	langage dont les expressions sont l'objet de l'étude	2.1
métalangage	langage dans lequel l'étude est conduite	2.1
métathéorie	ensemble des énoncés démontrés dans le métalangage à propos du langage objet	2.1
employée, mentionnée	expression qui sert à dire ce qu'elle signifie ; expression qui est elle-même l'objet du propos	2.2
alphabet, symbole	ensemble non vide dont les éléments servent à former les mots ; élément d'un alphabet	2.8
mot	suite finie de symboles	2.8
longueur	unique entier n tel que le mot appartienne à $\mathcal{A}^n$	2.8
concaténation	mot obtenu en écrivant le second à la suite du premier	2.10
facteur, préfixe, suffixe	sous-mot contigu ; sous-mot contigu initial ; sous-mot contigu final	2.12
univers	ensemble sur lequel opèrent les règles d'un système	2.17

Terme	Définition en une phrase	Numéro de la définition formelle
règle, prémisses, conclusion	couple formé d'un ensemble fini d'éléments et d'un élément ; ses deux composantes	2.17
système de règles	univers muni d'un ensemble de règles	2.17
axiome	règle sans prémisses	2.17
close	partie stable par toutes les règles	2.19
dérivation	suite finie d'éléments dont chacun est conclusion d'une règle à prémisses antérieures	2.20
dérivable	dernier terme d'une dérivation	2.20
système enrichi	système augmenté d'un axiome par élément d'un ensemble d'hypothèses	2.28
dérivable de Γ	dérivable dans le système enrichi par Γ	2.28
schéma de règles	famille infinie de règles décrite par des paramètres	2.34
démonstration	raisonnement du métalangage concluant un énoncé sur les objets étudiés	2.41

Pièges fréquents

Employer un connecteur du langage objet comme articulation du raisonnement. C'est la faute décrite au contre-exemple 2.4, et elle est d'autant plus tenace qu'elle ne produit jamais d'erreur de résultat : les phrases fautives sont en général celles qu'on aurait écrites correctement en français. Le critère est mécanique : $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, $\forall$, $\exists$, $\perp$, $\top$, $=$ ne peuvent apparaître qu'à l'intérieur d'une formule mentionnée ; dès qu'un de ces signes relie deux assertions de la rédaction, la phrase est mal formée.

Confondre « non dérivable » et « faux ». La non-dérivabilité est une propriété d'un objet relativement à un système, établie dans la métathéorie, généralement par un invariant (théorème 2.36) ; la fausseté est une propriété relative à une structure (Charte § 7). Rien, à ce stade, ne relie les deux, et le programme des modules 5, 8 et 9 consiste précisément à établir ce lien pour des systèmes déterminés. Croire le lien acquis d'avance rend inintelligibles les théorèmes d'incomplétude, dont tout le contenu est que le lien se rompt (module 14).

Attendre d'une dérivation qu'elle établisse une impossibilité. Une dérivation ne fait qu'accroître la liste des objets dérivables ; aucune ne peut avoir pour conclusion « tel objet n'est pas dérivable ». C'est pourquoi les résultats négatifs du parcours sont tous des théorèmes de la métathéorie, et pourquoi la remarque 2.38 mérite d'être relue avant chaque preuve d'indépendance.

Confondre une règle et un schéma de règles. R1, R2 et R3 de la définition 2.34, comme le schéma de séparation ou le schéma de récurrence, désignent chacun une infinité de règles. Un système à ensemble infini de règles reste licite ; ce qui ne l'est pas, c'est une règle à ensemble infini de prémisses, et l'exercice 2.26 montre que la confusion entre les deux fait s'effondrer le théorème 2.21.

Croire le métalangage plus sûr que le langage objet. Le métalangage de ce parcours est le français et la théorie naïve des ensembles, dont le module 1 a montré qu'elle est contradictoire sous sa forme non restreinte (théorème 1.2, module 1). Il n'est ni plus

formel, ni mieux fondé que les systèmes qu'il étudie : il est seulement celui dans lequel on se tient. La remarque 2.5 rappelle que les rôles peuvent s'échanger, et le second théorème d'incomplétude de Gödel (module 15) dira ce qu'il en coûte de vouloir refermer la boucle.

Lire $\text{Ind}(\mathcal{S})$ comme « l'ensemble des objets vrais ». Un système de règles engendre ce que ses règles engendrent, ni plus ni moins ; la définition 2.19 le construit sans qu'aucune notion de vérité intervienne. Le seul énoncé qui traverse la définition est celui du corollaire 2.22, et il ne dit rien de plus que ceci : ce qui est préservé par les règles vaut pour tout ce qu'elles engendrent.

Écrire « démontrable dans T » pour « dérivable dans T ». La Charte § 7 réserve « démontrer » au métalangage et « dériver » au système formel, avec la seule exception lexicale du prédicat de prouvabilité (module 15). La définition 2.41 fixe cet usage ; l'observation rend indiscernables les deux énoncés qui, au module 14, doivent absolument le rester : « $\mathfrak{N} \models \sigma$ » et « $T \vdash \sigma$ ».

Prendre l'ordre des lignes d'une dérivation pour une donnée essentielle. La définition 2.20 n'impose qu'une condition d'antériorité des prémisses ; un même élément admet en général une infinité de dérivations, différant par leur ordre, par des lignes inutiles ou par les règles employées. Ce n'est pas une imprécision : la preuve du théorème 2.21 exploite cette latitude en concaténant des dérivations, et le module 19 étudiera précisément les formes normales que l'on peut imposer aux dérivations sans changer ce qu'elles concluent.

Notations introduites

Les notations suivantes sont introduites ou fixées dans ce module. Celles qui *ne figurent pas dans la Charte* sont signalées par une mention explicite dans la dernière colonne, conformément à la Charte § 1 ; elles sont reprises dans l'encadré de tête.

Notation	Lecture / signification	Variantes rencontrées dans la littérature
$\mathcal{A}$	alphabet : ensemble non vide de symboles	$\Sigma, A, V, \mathcal{V}$ — <i>hors Charte</i> (encadré de tête)
$\mathbf{a}, \mathbf{b}$	symboles d'un alphabet, composés en caractères de machine à écrire	a, b en italique, $\mathbf{a}, \underline{a}$ — <i>hors Charte</i> (encadré de tête)
uv	concaténation des mots u et v	$u \cdot v, u \frown v, u * v$ — <i>hors Charte</i> (encadré de tête)
$\text{lg}(w)$	longueur du mot w	$ w , \ell(w), \text{len}(w), \text{long}(w)$ — <i>hors Charte</i> (encadré de tête)
$\#_s(w)$	nombre d'occurrences du symbole s dans le mot w	$ w _s, \text{occ}_s(w), N_s(w)$ — <i>hors Charte</i> (encadré de tête)
$\mathcal{S} = (U, \mathcal{R})$	système de règles : univers et ensemble de règles	$(A, \Phi), (X, R)$, système de production, système inductif — <i>hors Charte</i> (encadré de tête)
(P, c)	règle de prémisses P et de conclusion c	$P \triangleright c, \frac{P}{c}, P \Rightarrow c$
$\text{Ind}(\mathcal{S})$	plus petite partie close pour $\mathcal{R}$	$I(\mathcal{R}), \text{Cl}(\mathcal{R}), \mu X.\mathcal{R}(X), \text{lfp}$ — <i>hors Charte</i> (encadré de tête)
$\text{Der}(\mathcal{S})$	ensemble des éléments dérivables dans $\mathcal{S}$	$\text{Thm}(\mathcal{S}), \mathcal{T}(\mathcal{S}), \text{Gen}(\mathcal{R})$ — <i>hors Charte</i> (encadré de tête)

Notation	Lecture / signification	Variantes rencontrées dans la littérature
$S[\Gamma]$	système enrichi des éléments de Γ pris comme axiomes	$S + \Gamma, S \cup \Gamma, S_\Gamma$ — <i>hors Charte</i> (encadré de tête)
$\Gamma \vdash_S x$	x est dérivable de Γ dans le système S	$\Gamma \vdash_{\mathcal{R}} x, \Gamma \Rightarrow_S x$
$Cn_S(\Gamma)$	ensemble des éléments dérivables de Γ dans S	$\bar{\Gamma}, \Gamma^+, Ded_S(\Gamma)$ — <i>hors Charte</i> (encadré de tête)

Checklist d'auto-vérification

- ✓ **Unicité des notations** — chaque concept est noté d'une seule façon dans tout le module, conformément à la § 6 ; aucune notation concurrente n'a été introduite en cours de route.
- ✓ **Notations hors Charte** — toute notation absente de la Charte est signalée dans l'encadré de tête et reprise dans la section « Notations introduites ».
- ✓ **Séparation objet / méta** — $\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \forall, \exists, \perp, \top, =$ n'apparaissent qu'à l'intérieur de formules du langage objet, c'est-à-dire, dans ce module, uniquement au contre-exemple 2.4 et aux exercices 2.6 et 2.7, où ils sont mentionnés ; $\implies, \iff, :=$ et les quantifications en français n'apparaissent que dans le métalangage ; aucune phrase de preuve n'utilise un connecteur objet comme articulation logique.
- ✓ **Démonstration vs dérivation** — le vocabulaire distingue partout démonstration (métathéorie) et dérivation (système formel) ; c'est l'objet même de la définition 2.41.
- ✓ **Format des environnements** — en-têtes en gras conformes au modèle ****Théorème 9.4 (Complétude)****, aucun environnement hors de la liste admise.
- ✓ **LaTeX systématique** — aucun symbole mathématique en Unicode brut ; aucun | littéral dans une cellule de tableau ; aucune formule

...

 dans un tableau.
- ✓ **Numérotation** — compteur unique, continu et croissant sur tout le module, de 2.1 à 2.45, préfixé par le numéro du module.
- ✓ **Renvois** — tous les renvois sont numérotés et au format de la § 2.4 ; les renvois externes mentionnent le module, le premier d'entre eux rappelant le titre abrégé ; aucun renvoi vague.
- ✓ **Preuves complètes** — toutes les hypothèses utilisées sont nommées, tous les cas d'induction sont traités, la méthode est annoncée en italique, la preuve se clôt par ■ ; la preuve emboîtée du théorème 2.21 se clôt par □ ; toute étape déléguée renvoie à un exercice numéroté existant.
- ✓ **Dérivations formelles** — format linéaire à quatre colonnes de la § 5.1, dépendances explicites, à l'exemple 2.35. (La colonne « Formule » y est intitulée « Mot », l'univers

du système D étant un ensemble de mots et non de formules ; aucune décharge ni condition de variable propre n'est à signaler, le système D ne comportant ni règle de décharge ni variable.)

- ✓ **Résultats nommés** — la § 8 n'assigne aucun résultat canonique au module 2 ; aucun nom canonique n'est donc employé, et les résultats des autres modules cités le sont sous leur nom canonique exact.
- ✓ **Glossaire** — les termes ambigus de la § 7 sont employés dans le sens retenu ; la section « Glossaire du module » couvre tous les termes nouveaux introduits en gras.
- ✓ **Gabarit** — les sept sections de la § 3 sont présentes, dans l'ordre, avec leurs titres exacts.