UNIVERSITE LIBRE DE BRUXELLES

Faculté des Sciences

UNE THÉORIE INTUITIONNISTE DES ENSEMBLES

Mémoire présenté en vue de l'obtention
du grade de Licencié en Sciences mathématiques
(Grade légal)

Année académique 1965-1966

Pierre DELIGNE

UNIVERSITE LIBRE DE BRUXELLES

Faculté des Sciences

UNE THEORIE INTUITIONNISTE DES ENSEMBLES

Mémoire présenté en vue de l'obtention du grade de Licencié en Sciences Mathématiques.

(Grade légal)

Année Académique 1965-1966

Pierre DELIGNE

AXIOMATIQUE D'UNE THEORIE INTUITIONISTE DES ENSEMBLES.

INTRODUCTION.

L'intuitionisme est né en 1908 avec l'article scandaleux Brouwers (1) : "De onbetrouwbaarheid der logische principes". Son idée fondamentale est que les conjonctions logiques et les quantificateurs, tels qu'entendus classiquement, perdent tout sens dès qu'apparaissent des ensembles infinis.
Il faut les remplacer par des variantes, plus constructives, ayant parfois des propriétés divergentes du cas classique.

Pour un exposé très intuitif, on peut consulter Heyting (3) Brouwers précisera les fondements de sa théorie dans une série d'articles (2). Il utilise pour les ensembles (appelés "species") une théorie des types qui le met à l'abri du paradoxe de Russel, mais il ne rejette pas les définitions imprédicatives. C'est en analyse qu'il obtient son résultat le plus amusant, la continuité des fonctions de variable réelle.
(- cf Ch. III § 2 de ce travail).

Pour les intuitionistes, aucun formalisme ne peut traduire toute la mathématique. Le théorème de Gödel est une éclatante confirmation de ce point de vue.

Ils reconnaissent néanmoins l'utilité des formalismes et

Heyting (1) donne une axiomatique de la logique, Heyting (2) une de l'analyse, très lourde d'ailleurs d'après Kleene (2) qui en donne une autre, et une interprétation classique. Dans le livre fondamental Kleene (1) se trouve une axiomatique de l'arithmétique intuitioniste, et une interprétation classique.

Le but de ce travail est de fonder une théorie des ensembles intuitionistes dont découle, sur le modèle classique, toute la mathématique intuitioniste existante.
Les bases en sont essentiellement différentes de celles suggérées par Brouwers (2), en ce que les définitions imprédicatives sont rejetées, par un procédé qui me semble beaucoup plus souple qu'une théorie avec types et ordres à la Russel.

Le long § 3 du Chapitre II est consacré à une comparaison entre la théorie des ensembles et l'arithmétique.
On montre combien il faut affaiblir la première pour obtenir une théorie équivalente à la seconde : en l'absence d'axiome de l'ensemble des parties, toute la différence provient de la puissance relative des méthodes de définition par récurrence (transfinie). Il résulte de ce résultat (qui est valable classiquement aussi) que les raisonnements d'analyse "prédicative" peuvent se transcrire en arithmétique formelle.

Je ne suis pas intuitioniste, mais je crois que la théorie a un sens et un intérêt propre, d'autant plus grand que les interprétations classiques dont on dispose sont moins satisfaisantes. Telle est la raison pour laquelle ce sujet de mémoire me tenait à coeur, et je remercie Monsieur Papy d'avoir

bien voulu l'accepter. Je remercie aussi tous ceux grâce auxquels cette année 1965-1966 s'est déroulée pour moi dans les meilleures conditions.

CHAPITRE 1.

La partie élémentaire de la théorie. Idées directrices.

§ 1 Préliminaires.

Comme toute axiomatique qui se respecte, celle-ci se basera sur les mots composés avec certains signes, dits primitifs. Parmi ces signes, on distingue une infinité (potentielle) de "lettres". Précisons qu'un mot sera une suite de signes, certains, autres que les lettres, pouvant être joint par un trait courant au-dessus de la ligne. (ces traits sont appelés liens). On définit par récurrence les notions de "terme" et d' "assertion" : un mot est un terme (resp. une assertion) s'il est obtenu à partir de termes et/ou assertions par application de certaines règles de construction, dites règles formatives, la base de la récurrence étant que les lettres sont des termes. Ces règles formatives augmentent la longueur des mots : on dispose d'un procédé de décision pour savoir si un mot est un terme, ou est une assertion. Un mot étant donné, ou plus une règle formative permet de le construire à partir de termes et assertions, qui sont uniquement déterminé pour l'essentiel. Je donnerai bien sûr ces règles, mais sans aller jusqu'à préciser si j'utilise des parenthèses ou une notation fonctionnelle à la Łukasiewicz. Le lecteur arrangera telle variante à son goût ; je lui laisserai aussi le soin de ne pas énoncer et de ne pas vérifier les propriétés du type suivant : "si R est une assertion (resp. un terme), x une lettre et T un terme, alors $(T|x)R$,

obtenu en remplaçant x par T dans R est encore une assertion (resp. un terme)".

Parmi les lettres, certaines seront distinguées et appelées constantes, les autres étant appelées variables libres. Intuitivement, les constantes seront des objets particuliers sur lesquels ont fait des hypothèses exprimées par des axiomes. Quand une lettre x figure dans une assertion R, on pourra toujours regarder R comme exprimant une propriété susceptible d'être possédée par x : il n'y aura pas de "variable liée", leur emploi étant remplacé par celui des liens et d'un signe $\square$, comme dans Bourbaki (1).

On appellera axiome une assertion prise dans une liste qui sera donnée, ou obtenue à partir de termes et/ou assertions par un procédé de construction ("schéma d'axiome") appartenant à une liste qui sera donnée. Si A est un axiome, x une variable libre, T un terme, alors $(T|x)$ A sera encore un axiome. On dispose d'un procédé de décision pour savoir si une assertion donnée est un axiome. On définit par récurrence la notion de "théorème" : une assertion est un théorème si elle peut être obtenue à partir de théorèmes par application de certaines règles, dites règles de déduction, la base de la récurrence étant que les axiomes sont des théorèmes.

De ces règles on s'empressera d'en dériver d'autres, plus rapides. On introduira aussi des définitions, c'est-à-dire des notations abrégées et essentiellemat univoques pour désigner des termes et assertions.

§ 2 - La logique.

La théorie comprend des signes pour les opérateurs logiques ou, et, implique (noté $\Rightarrow$) et il est faux que (noté -).

Règle formative : si A et B sont des assertions, A ou B, A et B, $A \Rightarrow B$, -A sont encore des assertions.

Désignant par des majuscules des assertions, on pose la règle de déduction et lesschémas d'axiomes suivants :

Schémas d'axiomes pour la logique.

L_1 $\quad A \Rightarrow (B \Rightarrow A)$

L_2 $\quad (A \Rightarrow B) \Rightarrow ((A \Rightarrow (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$

L_3 $\quad A \Rightarrow (B \Rightarrow (A \text{ et } B)$

L_4 $\quad (A \text{ et } B) \Rightarrow A$ $\qquad$ L_5 $\quad (A \text{ et } B) \Rightarrow B$

L_6 $\quad A \Rightarrow A \text{ ou } B$ $\qquad$ L_7 $\quad B \Rightarrow A \text{ ou } B$

L_8 $\quad (A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow ((A \text{ ou } B) \Rightarrow C))$

L_9 $\quad (A \Rightarrow B) \Rightarrow ((A \Rightarrow -B) \Rightarrow -A)$

L_{10} $\quad -A \Rightarrow (A \Rightarrow B)$

Règle de déduction ("modus ponens"). Si A et $A \Rightarrow B$ sont des théorèms, B est un théorème.

Ce qui se note en raccourci :

$$\frac{A \qquad A \Rightarrow B}{B}$$

Ce système d'axiomes est recopié de Kleene (1) pg.82 (et pg. 101 pour L_{10}).

Ses conséquences sont bien connues et Gentzen a montré qu'il existait un procédé explicite pour savoir si une assertion donnée en était une. Voir Kleene (1) §§ 77, 78, 80. L'habitude semble montrer que ce sont exactement les énoncés logiquement tautologiques dans l'interprétation suivante, que le formalisme est censé représenter :

ou : on peut affirmer A ou B lorsqu'on sait pouvoir affirmer soit A, soit B (et qu'on a donc en particulier un procédé explicite pour désigner A, ou B, qui soit vrai).

et : comme classiquement, on peut affirmer A et B si on peut affirmer chacun d'eux.

$\Rightarrow$: on peut affirmer $A \Rightarrow B$ si on dispose d'un procédé explicite qui à partir d'une éventuelle démonstration de A (qui n'a pas à être formalisable dans un système donné) fournisse une démonstration de B.

non : $-A$ peut être affirmé si il est absurde que l'on démontre A ; si f est une assertion absurde, $-A \Leftrightarrow (A \Rightarrow f)$

Ainsi par exemple le principe du tiers enclus n'a pas à être un théorème, A ou $-A$ signifiant qu'on sait si A est vrai ou faux : par contre, $--(A \text{ ou } -A)$ est un théorème

logique ; il faut montrer $\neg(A \text{ ou } \neg A)$ absurde; s'il est absurde que l'on ait A ou $\neg A$, il est en effet en particulier absurde que l'on ait A, ce qui signifie la vérité de $\neg A$, d'où celle de A ou $\neg A$ et la contradiction en résulte : plus brièvement :

$\neg(A \text{ ou } B) \Rightarrow \neg A \text{ et } \neg B$ est clair, en particulier

$\neg(A \text{ ou } \neg A) \Rightarrow \neg A \text{ et } \neg\neg A$ et le 2e membre est absurde

d'où :

$\neg\neg(A \text{ ou } \neg A)$

J'utiliserai sans démonstration les conséquences des axiomes et règle introduits.

On obtiendrait une formalisation de la logique classique en remplaçant L_{10} par L_{10}^{cl} $\neg\neg A \Rightarrow A$, sans justification ici comme le montre l'exemple repris plus haut. La position intuitioniste vis-à-vis du sens classique des opérateurs logiques est que ce sens n'existe pas et n'est qu'un jeu de mots.

On a pu montrer qu'aucun des 4 opérateurs ou, et, $\Rightarrow$, $\neg$ ne pouvait être exprimé à l'aide des autres (Mc Kinsey (1)).

§ 3. Appartenance et quantificateurs.

Dans les exemples qui seront donnés, ? désignera une assertion que l'on suppose vraie, mais non démontrée. On ne saura donc pasintuitionistiquement si ? ou $\neg$?. ?(n) désignera une assertion similaire dépendant d'un paramètre entier n.

Que sera un sous-ensemble d'un ensemble donné E ? Classiquement, ces sous-ensembles peuvent être identifés aux propriété susceptibles d'être possédée par les éléments de E seuls. De même les ensembles intuitionistes doivent être vus comme des "propriétés", $x \in F$ signifiant que x possède la propriété F, et l'identité entre ensembles étant l'équivalence entre propriétés. Cependant :

1) ces "propriétés" n'ont pas le caractère mythique de leurs analogues classiques, où N a $2^{\aleph_0} > \aleph_0$ parties : quand on parle d'une propriété on sous-entend l'avoir définie (mais pas nécessairement dans le cadre d'un formalisme donné).

2) il n'y a pas de raison qu'une partie de $\{\emptyset\}$ par exemple soit nécessairement une des 2 qu'on croit : laquelle des 2 serait $\{x \mid x \in \{\emptyset\} \text{ et } ?\}$? En fait, on construira une suite X_n de parties de $\{\emptyset\}$ telle que $\vdash \neg\forall n (X_n = \emptyset \text{ ou } X_n = \{\emptyset\})$ ce qui ne signifie pas $\exists n \neg(X_n = \emptyset \text{ ou } X_n = \{\emptyset\})$, assertion que le lecteur montrera facilemat être fausse.

La "notion" de tous les ensembles n'est pas claire et distincte ; je dirais même plus : elle ne signifie rien. Le paradoxe de Russel montre que chaque fois qu'on se donne un ensemble on peut en nommer un autre qui n'y appartienne pas.

Ce qu'on peut faire est définir des ensembles par divers procédés qu'il serait difficile d'énumérer, et par exemple considérer l'ensemble réunion des ensembles qu'on peut définir dans un formalisme sensé donné : mais ce n'est pas là ce qu'on croit entendre par "tous les ensembles". Quand on parle d'une propriété vraie pour "tous les ensembles", on entend en fait

seulement par là une conséquence formelle d'axiomes tels qu'on n'aura envie d'appeler des objets de la nature qu'on trouverait sur son chemin "ensembles" que s'ils y satisfont.

En particulier, il n'aura pas de sens de dire :

"Il existe en ensemble (arbitraire) tel que ..." ou

"Pour tout ensemble, on a ..." ou

"L'ensemble de tous les ensembles tels que ..."

Par contre, si on se donne un ensemble E, on suppose savoir de quoi on parle, et on pourra se demander si

"Il existe un élément de E tel que ..." ou si

"Pour tout éléments de E, on a ..." et on pourra définir

"L'ensemble des éléments de E tels que ..."

Ces considérations me semblent tout aussi valables en mathématiques classiques.

Ceci étant admis, quelle marchandise douteuse recouvre le vocable "variable libre" ? Aucune en fait, je considère que les seules assertions de la théorie ayant un sens sont celles où ne figure aucune variable libre. On appellera "sensées" les assertions de ce type.

Je montrerai brièvement comment modifier les axiomes et règles de déduction pour éliminer les variables libres sans altérer la classe des théorèmes sensés. Elles ne jouent qu'un rôle abréviatif et simplificateur.

La signification intuitioniste des quantificateurs est différente de leur signification classique que, comme pour la logique, les intuitionistes ne comprennent pas.

$\exists x \in E\ R(x)$ signifie qu'on peut exhiber un objet x et montrer que $x \in E$ et $R(x)$.

$\forall x \in E\ R(x)$ signifie qu'on dispose d'un procédé explicite qui à partir d'une définition d'un objet x et d'une démonstration de $x \in E$ fournit une démonstration de $R(x)$ (tout cela n'ayant bien sûr pas à être formalisable dans un système donné).

Dans l'assertion "il existe x dans E tel que R(x)", la "variable" x est "liée", c'est-à-dire que l'assertion ne dépend pas de la valeur d'un objet noté x : il est donc assez naturel (et techniquement utile) que dans la formalisation de l'expression précédente x n'apparaisse pas. On formalisera l'assertion précédente par $\exists \boxed{\square \in E\ R(\square)}$, c'est-à-dire en écrivant de gauche à droite $\exists, \square, \in$, l'expression (un terme) E et l'expression (une assertion) R dans laquelle on remplace en toutes ses occurrences x par un $\square$, ces $\square$ étant reliées par un lien ou $\square$ qui suit $\exists$. Ces liens servent à indiquer quelles variables sont quantifiées par le $\exists$ initial. On supposera utilisée une technique analogue pour tous les types de variables liées, ce ne sera rappelé dans les règles formatives que par la mention "x est variable liée".

La discussion précédente se formalise en :

<u>Critère formatif</u> : $\in, \forall, \exists, \square$, les liens sont des signes de la théorie.

Si T et U sont des termes, $T \in U$ est une assertion

Si E est un terme, x une lettre, R(x) une assertion (où d'ailleurs x ne doit pas vraiment figurer), alors

$\exists x \in E\ R(x)$ et $\forall x \in E\ R(x)$ sont des assertions (x variable liée).

Schémas d'axiomes.

Q_1 $(R(T)$ et $T \in E) \Rightarrow \exists x \in E R(x)$

Q_2 $(\forall x \in E\ ER\ (x)$ et $T \in E) \Rightarrow R(T)$

Règles de démonstration :

Dans ces règles, la variable libre x est supposée ne figurer ni dans le terme E, ni dans l'assertion C.

$$RQ_1 \quad \frac{\vdash x \in E \text{ et } C \Rightarrow R(x)}{\vdash C \Rightarrow \forall x \in E\ R(x)}$$

$$RQ_2 \quad \frac{\vdash x \in E \text{ et } R(x) \Rightarrow C}{\vdash \exists x \in E R(x) \Rightarrow C}$$

Ce système est recopié de Kleene (1), pg 82, sauf que le champs de variation des variables liées a été borné. On trouvera là l'énoncé et la démonstration de critères permettant de transcrire les démonstrations informelles en démonstrations formelles, notamment le métathéorème de déduction: dans un système possédant exactement les règles de déductions énoncées jusqu'à présent, et possédant tous les axiomes déjà énoncés, si B est un théorème de la théorie obtenue en adjoignant à l'initiale l'axiome supplémentaire A, les lettres figurant dans A devenant des constantes, alors $\vdash A \Rightarrow B$ dans la théorie initiale.

Dorénavant, les conséquences des principes précédents seront librement utilisées. L'habitude montre qu'elles traduisent fidèlement l'interprétation intuitioniste des quantificateurs. Ainsi $\vdash -\exists x \in E\ R(x) \Leftrightarrow \forall x \in E\ -R(x)$ mais par contre $-\forall x \in E\ R(x) \Rightarrow \exists x\ -R(x)$ n'aura pas à être en général vrai.

Le fait qu'aucune nouvelle règle de déduction ne sera introduite permet dès maintenant de montrer comment éliminer les variables libres. J'utiliserai le fait qu'une constante sera introduite dans la théorie ($\mathbb{N}$, ensemble des entiers) mais il suffirait de savoir qu'il existe un terme sans variable libre.

On appellera assertion (terme) limité (1) un texte formel constitué de :

1) une assertion (un terme) R

2) une suite ordonnée d'assertions $x_1 \in \Gamma_1, \cdots, x_n \in \Gamma_n$ où les variables libres x_i sont des lettres distinctes, parmi lesquelles se trouvent toutes les variables libres de R, et où dans Γ_i ne peut figurer que $x_1 \ldots x_{i-1}$.

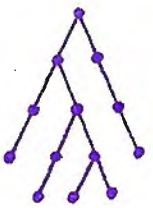
On décrira en abrégé "R($\underline{x}$) pour $\underline{x} \in \underline{\Gamma}$" où la _ rappelle que plusieurs termes sont désignés par un seul.

La fermeture de "R($\underline{x}$) pour $\underline{x} \in \underline{\Gamma}$" (R est une assertion) est l'assertion sensée $\forall x_1 \in \Gamma_1 \cdots \forall x_n \in \Gamma_n R(x_1 \ldots x_n)$, notée aussi $\forall \underline{x} \in \underline{\Gamma}\ R(\underline{x})$
Un axiome limité est un axiome muni d'une "limitation" quelconque. Sa fermeture est un théorème.

---

(1) Cette notion est due à Cohen

Les démonstrations seront toujours considérées comme des "arbres de déduction", où l'assertion figurant en un point de l'arbre est conséquence par une règle de déduction permise de ses prédécesseurs immédiats, ou un axiome s'il n'y a pas de prédécesseur. Un arbre est un ensemble fini ordonné dont toute partie minorée soit totalement ordonnée et qui ait un plus grand éléments (la conclusion).



un arbre

Une démonstration limitée est un arbre d'assertions limitées où les axiomes sont les axiomes limités et les déductions permises sont modus ponens limité

$$\frac{R(\underline{x}) \text{ pour } \underline{x}\in\Gamma,\ R(\underline{x})\Rightarrow S(\underline{x}) \quad \text{pour } \underline{x}\in\Gamma}{S(\underline{x}) \text{ pour } \underline{x}\in\Gamma}$$

ainsi que

$$\frac{(C \text{ et } x_n\in\Gamma_\eta)\Rightarrow R(\underline{x}) \text{ pour } \underline{x}\in\Gamma}{C \Rightarrow \forall x_n\in\Gamma_\eta\ R(\underline{x}) \text{ pour } \underline{x}^\wedge\in\Gamma^\wedge} \quad \text{et} \quad \frac{(R(\underline{x}) \text{ et } x_n\in\Gamma_n)\Rightarrow C \text{ pour } \underline{x}\in\Gamma}{\exists x_n\in\Gamma_\eta(R(\underline{x}))\Rightarrow C \text{ pour } \underline{x}^\wedge\in\Gamma^\wedge}$$

où le $^\wedge$ signifie qu'on omet la nième et dernière limitation $x_n\in\Gamma_\eta$. x_n est supposé ne pas figurer dans C (ni Γ_n).

Proposition : Tout théorème, muni d'une limitation quelconque, admet une démonstration limitée.

Démonstration : Soit D une démonstration de R, limité par $\underline{x}\in\Gamma$ Remplaçant au besoin des variables libres par d'autres et pro-

cédant par récurrence croissante sur D, on vérifie facilement qu'on peut supposer que si une assertion de D (resp. la limitation de R) contient une variable libre l, jamais avant cette assertion (resp.R) l n'a été liée par application de RQ_1 ou RQ_2. Cela fait, on obtient encore une démonstration si pour chaque modus ponens $\dfrac{A \qquad A \Rightarrow B}{B}$ on remplace par $\mathbb{N}$ partout avant B les variables libres de A ne figurant pas dans B.

Par récurrence descendante sur D on vérifie alors qu'il y a une et seule façon de limiter les assertions de D pour obtenir une démonstration limitée de conclusion R pour $\underline{x} \in \Gamma$

Appelons "sensées" les assertions sans variable libre, et "partie sensée de la théorie" la sous-théorie dont les assertions sont les assertions sensées et les théorèmes les théorèmes sensés.

<u>Métathéorème 1.3.2</u> : <u>Les théorèmes de la partie sensée de la théorie sont obtenus, avec pour seule règle de démonstration "modus ponens", à partir des axiomes sensés des types</u> :

a) <u>les fermetures des axiomes limités</u>

b) $\forall \underline{x} \in \Gamma\ A(\underline{x})$ et $\forall \underline{x} \in \Gamma\ (A(\underline{x}) \Rightarrow B(\underline{x})) \Rightarrow \forall \underline{x} \in \Gamma\ B(\underline{x})$

c) $\forall \underline{x} \in \Gamma\ (C \text{ et } x_n \in \Gamma_n \Rightarrow R(\underline{x})) \Rightarrow \forall \underline{x} \in \Gamma\ (C \Rightarrow \forall x_n \in \Gamma_n\ R(\underline{x}))$

c') $\forall \underline{x} \in \Gamma\ (R(\underline{x}) \text{ et } x_n \in \Gamma_n\ C) \Rightarrow \forall \underline{x} \in \Gamma\ (\exists x_n \in \Gamma_n (R(\underline{x})) \Rightarrow C)$

Dans c) et c') a le même sens que précédemment et x_n ne figure pas dans C. Dans b), c) et c') $\underline{x} \in \Gamma$ est une limitation.

Il suffit de remarquer qu'une assertion sensée est limitée par la limitation vide, et que si dans une démonstration limitée on ferme toutes les assertions, les déductions obtenues sont valables dans la théorie décrite dans le métathéorème.

Quelques propriétés du formalisme du calcul propositionnel:

Les assertions suivantes sont des théorèmes :

1) $A \Rightarrow --A$ (quand on a une démonstration de A, il est absurde de démontrer qu'il n'y en a pas)

2) $(A \Rightarrow -B) \Leftrightarrow (-(A \text{ et } B)) \Leftrightarrow (B \Rightarrow -A)$ (déduire une contradiction de B à l'aide de A, c'est déduire une contradiction de A et B)

3) $(--A \Rightarrow -B) \Leftrightarrow (A \Rightarrow -B)$ (1) prouve l'implication $\Rightarrow$; reste à montrer que si $A \Rightarrow -B$ et $--A$, alors B entraîne contradiction : B entraîne alors en effet $-A$.

Scholie : Pour démontrer une assertion négative (c'est-à-dire qu'on sait être équivalente dans la théorie à $-A$ pour un certain A), on peut admettre toute assertion dont la double négation soit un théorème.

En effet, le métathéorème de déduction montre alors que $\vdash H_1 \Rightarrow (H_2 \Rightarrow (\cdots \Rightarrow (H_n \Rightarrow A)))$; 2) montre que si B est négative, $C \Rightarrow B$ est encore négative, et 3) itéré montre alors $\vdash --H_1 \Rightarrow (--H_2 \Rightarrow (\cdots \Rightarrow (--H_n \Rightarrow -A)))$, donc $\vdash -A$ par modus ponens itéré.

Sachant que $\vdash --(B \text{ ou } -B)$, on obtient aisément le

Corollaire : Si on se restreint où la logique sans quantifica-

teurs, une assertion négative est vraie si et seulement si elle l'est classiquement.

En se limitant cette fois au calcul propositionnel complet (règles et schémas d'axiome introduits jusqu'à présent) on peut démontrer un résultat similaire (dont pour l'essentiel la démonstration est dans Kleene (1) § 81).

Proposition : une assertion négative dans laquelle chaque quantificateur universel porte sur une assertion négative est vraie dès qu'elle l'est classiquement.

§ 4. Les ensembles et les définitions imprédicatives.

Pour garantir l'existence d'ensembles, Bourbaki (1) donne sous forme d'axiomes des critères pour affirmer une assertion R(x) "collectivisante", c'est-à-dire dans ses notations. $\exists y \forall x \, (R(x) \Leftrightarrow x \in y)$

Il s'agit des axiomes ou schémas d'axiomes S_8, A_2 (redondant en fait), A_4, et, essentiellement A_5.

Ce procédé est ici inapplicable, car utilise la notion insensée d'ensemble arbitraire. La solution adoptée ici est d'introduire par des symboles primitifs divers procédés clairs et distincts associant à des ensembles et assertions d'autres ensembles.

Notamment :

Règle formative : $\{ \; \} \, \{ \, \} \, \cup$ sont des signes de la théorie, et

a) Si T (X) est un terme, x une lettre, E un terme, R(x) une

assertion alors $\{T(x) \mid x \in E \text{ et } R(x)\}$ est un terme (x est variable liée et pour bien faire on devrait supposer que x ne figure pas dans E)

b) Si T et U sont deux termes, alors $\{T,U\}$ est un terme

c) Si T est un terme, $\bigcup T$ est un terme (intuitivement la réunion des éléments de T

Avant d'énoncer les axiomes correspondant, introduisons = par la

Règle formative : = est un signe de la théorie, et si T et U sont deux termes, T = U est une assertion.

Schémas d'axiomes : T, U, V, E désignant des termes, R une assertion et la variable liée notée x étant censée n'apparaître que là où on l'explicite, on a

E_1 $T = T$

E_2 $(T = U) \Rightarrow (R(T) \Leftrightarrow R(U))$

E_3 $U \in \{T(x) \mid x \in E \text{ et } R(x)\} \Leftrightarrow \exists x \in E\ (R(x) \text{ et } U = T(x))$

E_4 $V \in \{T,U\} \Leftrightarrow V = T \text{ ou } V = U$

E_5 $V \in \bigcup T \Leftrightarrow \exists x \in T\ (V \in x)$

Posons la définition :

$T \subset U$ abrévie $\forall x \in T\ (x \in U)$

L'axiome d'intensionnalité s'écrit alors

E_6 $(T \subset U \text{ et } U \subset T) \Leftrightarrow T = U$

Voici quelques premières conséquences de ces axiomes

proposition 1 : $(T = U \text{ et } U = V) \Rightarrow T = V$; $T = U \Leftrightarrow U = T$

Dém: 1) supposons $T = U$ et $U = V$ (ce qui signifie que pour démontrer $\overset{\cdots\Rightarrow\cdots}{\text{on}}$ va utiliser le métathéorème de déduction); il faut démontrer $T = V$; si on applique E_2 à T, U en prenant pour R $x = V$, on trouve $T = U \Rightarrow (T=V \Leftrightarrow U=V)$ d'où....

2) de même, E_2 appliqué à T, U et $x = T$ donne $T = U \Rightarrow (T = T \Leftrightarrow U = T)$....

proposition 2 : $(\forall x \in T(R(x))$ et $U \subset T) \Rightarrow \forall x \in U(R(x))$

Supposons $\forall x \in T\ R(x)$ et $U \subset T$, c'est-à-dire $\forall z \in U\ (z \in T)$. Soit z quelconque dans U (ce qui signifie qu'on va chercher à appliquer la règle de déduction déduite de RQ_1 :

$$\frac{\vdash z \in U \Rightarrow R(z)}{\vdash \forall z \in U\ R(z)}$$

, et que pour démontrer $z \in U \Rightarrow R(z)$ on applique le métathéorème de déduction en adjoignant provisoirement $z \Rightarrow U$ aux axiomes),

$\forall z \in U\ (z \in T) \Rightarrow (z \in U \Rightarrow z \in T)$ (Q_1)

$\forall x \in T\ R(x)) \Rightarrow (z \in T \Rightarrow R(z))$ (Q_1)

Donc, les premiers membres étant supposés vrais, R(z), comme l'on voulait.

proposition 3 : $T \subset T$. $T \subset U$ et $U \subset V \Rightarrow T \subset V$

Dém: 1) pour $T \subset T$ on peut utiliser E_1 et E_6, ou appliquer la règle dérivée de RQ_1 à $z \in T \Rightarrow z \in T$ pour obtenir $\forall z \in T\ (z \in T)$. On remarque ainsi que l'implication $\Leftarrow$ de E_6 est redondante.

2) Si $\forall z \in U(z \in V)$ et $T \subset U$, la proposition 2 montre $\forall z \in T\ (z \in V)$

La définition qui suit de $\varnothing$ a l'air loufoque car j'y introduis une constante de la théorie, N, qui sera introduite ulté-

rieurement; la raison en est qu'on ne connaît encore aucun terme ou assertion sensée (c'est-à-dire sans variable libre).

$\emptyset$ abrévie $\{x \mid x \in \mathbb{N} \text{ et } x \neq x\}$
est un terme sensé. On a la

proposition 4 : $T \notin \emptyset$. $T \subset \emptyset \Leftrightarrow T = \emptyset$ $\emptyset \subset T$.
où $T \notin U$ abrévie $\neg(T \in U)$. De même $T \neq U$ abréviera $\neg T = U$

Dém: 1) $T \in \emptyset \Leftrightarrow \exists x \in \mathbb{N}(x \neq x \text{ et } x = T)$ qui est absurde par E_3 et E_1

2) la 2ème assertion résulte de la 3e et de E_6

3) résulte par RQ_1 de $z \in \emptyset \Rightarrow z \in T$ (1ère assertion et L_{10})

Les définitions imprédicatives :

La présente discussion est informelle. Voici tout d'abord un exemple de définition imprédicative dont je ne vois vraiment pas comment on pourrait la transformer en définition prédicative. Introduisons d'abord la notation suivante : énumérons les assertions ("arithmétiques") du type
$\forall x_1 \in X \ \exists y_1 \in X \ \forall x_2 \in X \cdots \exists y_n \in X \quad (S(x_1 \ldots y_n))$ où S est combinaison logique (c'est-à-dire par ou, et, $\Rightarrow$, $\neg$) d'assertions $P(x_1 \ldots y_n) = 0$, avec P polynome de $\mathbb{Z}[X, \ldots Y_n]$. Soit $Q(k, X)$ la kième.
L'exemple est alors :

"l'ensemble des entiers k tels qu'il existe $X \subset \mathbb{Z}$ tel que $Q(k,X)$".
Son caractère imprédicatif tient à ce que pour définir une partie d'un ensemble (Z), on utilise un quantificateur (existentiel) portant sur toutes les parties de cet ensemble. De

ce fait, pour montrer qu'un entier k y appartient, on pourrait être amené à utiliser l'existence de parties de Z qu'on ne sache définir qu'à l'aide de cette partie qu'on est en train de définir.

Il n'y a rien à reprocher à cette définition si on admet comme claire et distincte une notion de partie arbitraire de Z (que cette notion soit classique ou constructiviste, arbitraire signifiant alors "définissable"). Ainsi, cette définition pourrait facilement être formalisée dans la présente théorie si on lui adjoignait un symbole $\mathcal{P}$ (ensemble des parties de...) avec l'axiome $T \in \mathcal{P}E \Leftrightarrow T \subset E$.

De mon point de vue intuitioniste, je n'admet pas une telle notion de partie définissable arbitraire; il existe divers procédés de définition, mais un raisonnement diagonal montrerait qu'on ne peut pas "tous" les énumérer; c'est d'ailleurs là l'essentiel du paradoxe de Richard, que je ne connais pas assez pour discuter plus. On ne sait pas expliciter quelles sont tous les objets qu'on voudrait appeler "partie définissable de Z" ou donner un moule pour tous les obtenir.

En conséquence, il n'y aura pas dans cette théorie d'ensemble des parties d'un ensemble donné, même pas d'ailleurs pour un ensemble comme $\{\emptyset\}$ (cf pg.9). Les définitions impredicatives sont automatiquement éliminées.

Ceci n'exclut pas qu'on parle de propriétés vraies pour toutes les parties de E; cela signifiera en fait propriété vraie dans un formalisme qu'on croit pouvoir appliquer chaque fois qu'on aura trouvé dans son chemin un objet qu'on ait envie d'appeler partie de E (cf pg10). Dans la présente théorie cela se traduira par l'étude des conséquences de $l \subset E$, pris comme nouvel axiome, et où l est variable libre.

§ 5. Applications et variantes.

On pose les définitions :

$X \cap Y$	abrévie	$\{x \mid x \in X \text{ et } x \in Y\}$	lu intersection de X et Y
$X \setminus Y$	"	$\{x \mid x \in X \text{ et } x \notin Y\}$	lu complémentaire de Y dans X
$X \cup Y$	"	$\bigcup \{X,Y\}$	lu réunion de X et Y
$\exists ! x \in E\ R(x)$	"	$\exists x \in E\ \forall y \in E (R(y) \Leftrightarrow y = x)$	lu un et un seul objet de E satisfait R
$\iota x \in E\ R(x)$	"	$\bigcup \{x \mid x \in E \text{ et } R(x)\}$	lu l'unique objet de E tel que R
(x,y)	"	$\{\{x\}, \{x,y\}\}$	lu le couple (x,y)
$pr_1\ z$	"	$\iota x \in \bigcup z\ \exists y \in \bigcup z\ z(z=(xy))$	lu première projection de z
$pr_2\ z$	"	$\iota y \in \bigcup z\ \exists x \in \bigcup z\ (z=(xy))$	lu deuxième pro-
$\{T(x) \mid x \in E\}$	"	$\{T(x) \mid x \in E \text{ et } x=x\}$	[-jection de z
$E \times F$	"	$\bigcup \{\{(xy) \mid x \in E\} \mid y \in F\}$	lu produit de E et F

$\{T(x,y) \mid x \in E \text{ et } y \in F \text{ et } R(x,y)\}$
abrévie $\{T(pr_1 z, pr_2 z) \mid z \in E \times F \text{ et } R(pr_1 z, pr_2 z)\}$

De même à plus de variables

$$\bigcup_{z \in E} T(z) \text{ abrévie } \bigcup \{T(z) \mid z \in E\}$$

R est un graphe de E vers F signifie $R \subset E \times F$
la diagonale de E x E signifie $\{(x,x) \mid x \in E\}$ notée Δ_E

On pose aussi des définitions où l'expression abrégée ne contient pas toutes les données, ainsi :
R∘S, si le contexte montre que R est un graphe de F vers G, S un graphe de E vers F
abrévie $\{(x\ z) \mid x \in E \text{ et } z \in G \text{ et } \exists y \in F ((xy) \in S \text{ et } (yz) \in R)\}$

S^{-1} abrévie $\{(yx) \mid x \in E \text{ et } y \in F \text{ et } (xy) \in S\}$
$S\langle X\rangle$ " $\{y \mid y \in F \text{ et } \exists x \in X.\ (x,y) \in S\}$
R est une ralation d'équivalence sur E signifie
R est un graphe de E vers E ("sur E"), $\Delta_E \subset R$ ("réflexivité"), RoR $\subset$ R ("transitivité") et $R^{-1} = R$ ("symétrie")

R est une ralation d'ordre sur E signifie
R est un graphe sur E, $\Delta_E = R \cap R^{-1}$ (réflexivité et "anti-symétrie") et R est transitive.

Je laisse au lecteur le soin de définir les fonctions, injections, surjections, bijections, lois de groupes, structures d'anneaux etc.
Il verra que les définitions proposées signifient bien ce qu'on veut, par exemple $\vdash \exists!\, x \in E\,(R(x)) \Rightarrow R(\iota x \in E\ R(x))$
Il n'a pas être vrai en général que pour une partie Y de X, $Y = X \setminus (X \setminus Y)$, bien que ces deux parties aient même complémentaire.

Pour une équivalence R, on définit la partition E/R par $\{\mathcal{C}_R(x) \mid x \in E\}$ où $\mathcal{C}_R(x)$ est la classe d'équivalence de x pour R, soit $\{y \mid y \in E \text{ et } (x,y) \in R\}$.

Définir une topologie est plus délicat car il y a "trop" d'ouverts pour former un ensemble. Dans tous les cas pratiques cependant, la topologie peut être définie par une base d'ouverts pas "trop" nombreux; T est une prétopologie sur E si a) $\forall X \in T\ (X \in E)$
b) $\forall X \in T\ \forall Y \in T\ (X \cap Y \in T)$

et T et T' "définissent la même topologie" si
a) $\forall x \in E\ \forall X \in T\ (x \in X \Rightarrow \exists Y \in T'\ (x \in Y \subset X)$
et b) réciproquement

Les couples : la définition (très classique) adoptée est très artificielle. Voici comment on pourrait arriver à une théorie logiquement plus satisfaisante, mais donnant lieu à des difficultés techniques sans aucun intérêt mathématique: si on admet d'identifier "ensembles" et "propriétés", il est naturel d'introduire des "ensembles", alias propriétés, ou relations, à plusieurs variables ; $x,y \in E$ signifiera que la propriété (= la relation) E est vraie pour x,y (entre x et y). Désignant alors par (x,y) la relation vraie seulement pour x,y on aurait $x,y \in E \Leftrightarrow (x,y) \subset E$. Les difficultés techniques seraient que

1) il faudrait pour bien faire considérer des "ensembles" à un nombre quelconque de dimension (= nb de variables), et il est difficile d'introduire un nombre quelconque dans un formalisme; cela permettrait cependant d'avoir identité (et non seulement bijection canonique) entre (E x F) xG et Ex(FxG) où E x F est la relation vraie pour $x_1 \ldots x_n\ y_1 \ldots y_m$ si $x_1 \ldots x_n$ satisfait E et $y_1 \ldots y_m$ F.

2) pour pouvoir réunir des ensembles de dimensions différentes, il faudrait admettre des relations ayant un sens pour un nombre quelconque d'arguments.

Les individus : Du fait que par E_6 $E = \{ x \mid x \in E \}$, seuls des ensembles ont droit de cité dans la théorie. On rencontre cependant dans la nature des objets qui n'en sont pas, par exemple une chaise n'est pas un ensemble (au sens mathématique du mot, synonyme de "propriété" et non de "tas"). Cela signifie en pratique que tout ensemble de la théorie doit se construire à partir de $\emptyset$. On aura par exemple
$3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$

On pourrait remédier à cette situation en affaiblissant E_6 pour qu'il ne s'applique pas aux éléments d'un ensemble I, les individus, mais cela n'offre aucun intérêt mathématique.

CHAPITRE II. L'Itération.

§ 1. Principes généraux.

Ce chapitre est consacré aux méthodes de démonstration (et de définition) par récurrence usuelle ou transfinie. Dans le cadre de la présente théorie, où l'on ne dispose pas de l'ensemble des parties d'un ensemble, c'est la force relative de ces méthodes qui fait toute la différence entre une théorie du type de l'arithmétique et une théorie des ensembles; on le verra au § 4.

Brouwers (2) a montré qu'on pouvait sans difficulté définir les ordinaux inférieurs à ω^ω et aller jusqu'à ε_0, le plus petit ordinal tel que $\omega^{\varepsilon_0}=\varepsilon_0$) ou un peu plus loin n'est que plus compliqué; cependant, il n'y a pas à ma connaissance de définition générale de " α est un ordinal" telle que si α et β sont des ordinaux, on ait $\alpha<\beta$, $\alpha=\beta$ ou $\alpha>\beta$. Cela étant peu encourageant, je me suis complètement abstenu d'utiliser les ordinaux dans la théorie. On sait dans les théories classiques que les méthodes de démonstration et de définition par récurrence transfinie restent valables sur un ensemble ordonné vérifiant la condition de chaîne descendante (Bourbaki (2) 1ère éd. §6, ex.27c). Dans le cadre classique toujours, l'axiome de fondation :

$$\forall X \exists x\ (x \in X \text{ et } x \cap X = \emptyset)$$

garantit que le "soubassement" d'un ensemble X, formé des x tels qu'existent $x_0 \ldots x_n$ avec $x = x_0, \ldots x_i \in x_{i+1} \cdots x_n = X$ $(n \geqslant 0)$ est ordonné, et vérifie la condition de chaîne descendante, pour la relation transitive engendrée par l'appartenance.

Dans cette théorie-ci, on combinera ces deux principes pour postuler directement les principes d'itération sur le

soubassement d'un ensemble. La légitimité de ces principes doit être vue comme exprimant une affirmation a priori sur les méthodes dont on peut disposer pour construire des ensembles. Elle me semble en tout cas évidente tant qu'on regarde uniquement les soubassements d'ensembles pouvant être défini dans cette théorie-ci.
Comme d'habitude, il faudra introduire les définitions par récurrence ("transfinie") par un nouveau signe primitif.

Règle formative : $\mathrm{It}(\ ,\ )$ est un signe primitif de la théorie; si E et T(x) sont des termes, x une variable ne figurant pas dans E, alors $\mathrm{It}_x(E,T(x))$ est un terme (x variable liée).

Intuitivement, il s'agit de la valeur en E de la fonction f définie par récurrence transfinie sur le soubassement de E, selon la règle :
la valeur de f en X est T appliqué à la restriction de f à X.
Cela se traduit par l'axiome

I_1 $\quad \mathrm{It}_x(E,T(x)) = T(\{(z,\mathrm{It}_x(z,T(x)))\mid z\in E\})$

Si par exemple on prend pour T : $\{\mathrm{pr}_1(x)\}\cup\bigcup \mathrm{pr}_2(x)$ le terme obtenu s'appelera le soubassement de E noté $\mathrm{Sb}E$ et I_1 signifiera : $\mathrm{Sb}(E)=\{E\}\cup\bigcup_{z\in E}\mathrm{Sb}(z)$ (1)

Les démonstrations par récurrence transfinie seront justifiées par l'axiome

I_2 $\quad \forall F\in \mathrm{Sb}E(\forall x\in F(R(x)) \Rightarrow R(F)) \Rightarrow R(E)$

Un ensemble E est dit complet si $\forall x\in E\,(x\subset E)$.

proposition : 1) Si $z\in \mathrm{Sb}\,E$, alors $\mathrm{Sb}z\subset \mathrm{Sb}E$; en particulier $\mathrm{Sb}E$ est complet.
2) Si E est complet, $\mathrm{Sb}\,E = E\cup\{E\}$
3) $\forall x\in \mathrm{Sb}(E)\quad E\notin x$

Si on démontre une assertion du type $\forall x \in F(R(x)) \Rightarrow R(F)$, F variable libre, I_2 montre que pour tout terme E, R(E); on dira avoir démontré R par récurrence transfinie (absolue) sur E. Utilisons cette méthode pour 1) : si $z \in Sb E$, on aura soit $z = E$, et $Sb z = Sb E$, soit $z \in Sb(x)$ pour un $x \in E$; par récurrence $Sb z \subset Sb x$, et on sait que $Sb x \subset Sb E$. Il résulte encore de (1) que $x \in Sb x$, puis $x \subset Sb x$ et $Sb z \subset Sb E$ implique donc $z \subset Sb E$.

Si on démontre une assertion R(E) par une application de I_2, 1) montre qu'on aura aussi $\forall z \in Sb E\ R(z)$, l'hypothèse de I_2 étant vraie à fortiori pour un $z \in Sb E$ si elle l'est pour E. On dira avoir démontré R(z) $(z \in Sb(E))$ par récurrence transfinie sur z, limitée à $Sb E$. Utilisons cette méthode pour 2), R étant : $x \in E \cup \{E\} \Rightarrow Sb x \subset E \cup \{E\}$

L'hypothèse de récurrence est

$$x \in Sb \text{ et } \forall y \in x\ (y \in E \cup \{E\} \Rightarrow Sb y \subset E \cup \{E\})$$

Si $x \in E \cup \{E\}$, puisque E est complet, $\forall y \in x\ (y \in E)$, donc par récurrence $\forall y \in x\ (Sb y \subset E \cup \{E\})$. Que $x \subset E \cup \{E\}$ résulte alors de (1).

On a donc la conclusion $E \in E \cup \{E\} \Rightarrow Sb E \subset E \cup \{E\}$; l'inclusion inverse résulte de (1) et 2) est démontré.

Pour 3) on va démontrer $\forall z \in Sb E\ (E \notin z)$ par récurrence transfinie absolue sur E. Si $z \in Sb E$, soit $z = E$, soit $\exists x \in E$ tel que $z \in Sb x$. Dans le premier cas, supposons par l'absurde $E \in E$, l'hypothèse de récurrence s'applique dès lors déjà à E, et donne en particulier $E \notin E$. Dans le second cas, de $E \in z$ et $z \in Sb x$ résulterais $E \in Sb x$, absurde par récurrence puisque $x \in E$.

Il est facile de prouver par récurrence transfinie absolue sur E que $\forall z \in Sb E\ (z = E \text{ ou } \exists t \in Sb E(z \in t))$. Cela permet de renforcer 3) en $\forall z \in Sb E(E = z \text{ ou } E \notin Sb z)$, plus parlant

sous la forme $\underline{x \in Sb\ y \text{ et } y \in Sb\ x \Leftrightarrow x = y}$

Notons encore qu'on peut renforcer I_2 en I_2' :

I_2' : $\forall F \in Sb\,E\ (\forall x \in \bigcup_{f \in F} Sb f(R(x)) \Rightarrow R(F)) \Rightarrow R(E)$;

I_2' est conséquence de I_2 appliqué à $R'(X)$: $\forall x \in Sb\,X\ R(x)$

§ 2. Arithmétique.

L'ensemble des nombres entiers sera introduit par une constante de la théorie, $\mathbb{N}$ soumise à des axiomes qui expriment qu'on prend pour suite des entiers la suite $\emptyset = 0, \{\emptyset\} = 1, \{\emptyset, \{\emptyset\}\} = 2, \cdots, n \cup \{n\} = n+1$.

Formellement, on pose les axiomes suivants, ou 0 désigne $\emptyset$ et où $n + 1$ désigne $n \cup \{n\}$:

N_1 $\quad 0 \in \mathbb{N}$

N_2 $\quad \forall n \in \mathbb{N}\ (n + 1 \in \mathbb{N})$

N_3 $\quad \forall n \in \mathbb{N}\ (n = 0 \text{ ou } \exists\, m \in \mathbb{N}\ (n = m + 1))$

Une assertion $R(n)$ étant donnée, appliquons I_2 à l'ensemble $\mathbb{N}$ et à l'assertion $S(X)$: $\forall n \in X\ (n \in \mathbb{N} \Rightarrow R(n))$

On trouve que pour prouver $\forall n \in \mathbb{N}\ R(n)$, il suffit de prouver $\forall X \in F\ (\forall n \in X\ (n \in \mathbb{N} \Rightarrow R(n))) \Rightarrow \forall n \in F (n \in \mathbb{N} \Rightarrow R(n))$ qui est impliqué par

$\forall n \in \mathbb{N}\ (\forall m \in n\ (m \in \mathbb{N} \Rightarrow R(m)) \Rightarrow R(n))$

(faire $X = n$). En vertu de N_3, cette assertion est impliquée par $R(0)$ et $\forall m \in \mathbb{N}\ (R(m) \Rightarrow R(m + 1))$:

Principe de récurrence : $\underline{R(0) \text{ et } \forall n \in \mathbb{N}\ (R(n) \Rightarrow R(n+1))} \Rightarrow \underline{\forall n \in \mathbb{N}\ R(n)}$

Proposition : 1) N est complet
2) tout entier est complet.
3) pour tout entiers n et m, $n \in m$, $n=m$ ou $m \in n$

Démontrons par exemple 3), 1) et 2) étant immédiats par récurrence, de même que l'assertion $o \in n$ ou $o=n$
Procédant par récurrence sur n, on doit prouver

$(n \in m$ ou $n=m$ ou $m \in n) \Rightarrow (n+1 \in m$ ou $n+1=m$ ou $m \in n+1)$ dont la partie non triviale résulte de $n \in m \Rightarrow (n+1 \in m$ ou $n+1=m)$ qu'on va prouver par récurrence sur m. Le cas $m=o$ est trivial. Si $n \in m+1$, on a soit $n=m$ (et $n+1 = m+1$), soit $n \in m$ et dans ce cas par récurrence soit $n+1=m \in m+1$, soit $n+1 \in m \subset m+1$ ce qui termine la démonstration.

La relation $n \in m$ se notera plutôt $n < m$ et la proposition précédente affirme que $\leqslant$ est un ordre total (d'ailleurs identique à $\subset$) et que chaque entier est l'ensemble de ses prédécesseurs. La démonstration du rpincipe de récurrence prouve que l'on a aussi :

$$\forall n \in \mathbb{N}\ (\forall m < n (R(m)) \Rightarrow R(n)) \Rightarrow \forall n \in \mathbb{N}\ \ R(n)$$

En spécialisant I_1 à tous les $n \in \mathbb{N}$ ou à $\mathbb{N}$, on démontre les principes usuels de définition par récurrence; on peut ainsi définir l'addition et la multiplication et vérifier les axiomes de l'arithmétique intuitioniste tels qu'exposés dans Kleene (1), dont les résultats pourront être utilisés.

Dans le cas général, on ne sait pas définir l'ensemble des applications de E dans F; pour $E = [1,n]$, on s'en tire cependant en le définissant par récurrence sur n, et cela permet de poser la définition :

Définition : E est fini net s'il existe n et une bijection entre E et $[1,n]$. n est alors uniquement déterminé et se note card (E).

Pour E fini net on définit par transport l'ensemble des applications de E dans F, Hom (E,F). Pour E et F finis nets, E x F, Hom (E,F), E∪F pour E et F disjoints sont encore finis nets. On prendra garde que E ∪ F n'a pas en général de raison d'être fini net, comme le montre $\{\{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\}$. Tout E fini net est discret, c'est-à-dire que $\forall x \in E \, \forall y \in E$ (x=y ou x≠y). Les parties nettes F de E fini net, c'est-à-dire telles que $\forall x \in E$ (x∈F ou x∉F), sont finies nettes, et on peut définir leur ensemble, identifié à Hom (E,$[1,2]$). Les entiers sont exactement les ensembles finis nets complets totalement ordonnés par "∈ ou = ". Pour E fini net, on définit $\mathcal{P}^n_{net}(E)$ par récurrence comme ensemble des parties nettes de $\mathcal{P}^{n-1}_{net}(E)$; $\mathcal{P}^0_{net}(E)=E$. Le soubassement d'un ensemble E est fini net si E appartient à un des $\mathcal{P}^n_{net}(\emptyset)$, auquel cas E est dit absolument fini net.

Pour les démonstrations, on procède par récurrence et, si cela est nécessaire pour énoncer la récurrence, on se ramène d'abord au cas d'ensembles finis nets "types", comme $[1,n]$. Seule la caractérisation des entiers est un brin plus difficile; on remarque d'abord qu'un ensemble fini net totalement ordonné a un plus petit élément : si f est une bijection $[1,n] \to E$, on pose par récurrence $g(1)= f(1)$, $g(i+1)= f(i+1)$ si $f(i+1) \leqslant g(i)$, $g(i+1)=g(i)$ sinon; g(n) est le plus petit élément. Cela permet, sous les hypothèses faites, de trouver une bijection croissante :

$[1,n] \xrightarrow{h} E$ et une récurrence facile montre $h(i) = i-1$.

§ 3. Un métathéorème d'énumération.

On se propose d'exhiber pour tout terme sensé T un terme sensé Γ qui soit une surjection d'une partie de N dans T. Pour mener à bien la récurrence, on va devoir démontrer plus généralement :

métathéorème d'énumération : Soit T (x) un terme ne contenant pas d'autres variables libres que $\underline{x} = x_1 \cdots x_n$. Soit $\Gamma_1 \cdots \Gamma_n$ des variables libres distinctes des $x_1 \cdots x_n$. On va construire explicitement un terme $\Gamma_T(\underline{x}, \Gamma)$ tel que $\vdash$ Si les Γ_i sont des surjections de parties de N dans les S b x_i, alors $\Gamma_T(\underline{x}, \Gamma)$ est une surjection d'une partie de N dans S b T (x).

La démonstration se fait par récurrence sur la longueur de T. Si T est N ou une variable libre, le résultat est trivial; il faut alors considérer les cas :

a) $T = \{U, V\}$, facile car $SbT = \{T\} \cup SbU \cup SbV$. Le cas $T = \bigcup V$ est plus facile encore.

b) $T = \{U(x) \mid x \in E \text{ et } R(x)\}$. Par récurrence, on dispose d'une surjection d'une partie de N sur SbE, donc aussi de telles surjections sur E et les Sbx pour $x \in E$. L'hypothèse de récurrence, appliquée à U(x) permet alors de construire des surjections $\Gamma[x]$ vers SbU(x) pour $x \in E$. L'assertion résulte alors de l'existence d'une surjection $N \to N \times N$ et de ce que $SbT = \{T\} \cup \bigcup_{x \in E} U(x)$

c) $T = \mathrm{It}_x(E, U(x))$. Le Γ cherché se définira, comme T, par une itération. On dispose déjà de Γ_E (partie de N) $\to$ SbE, et de $\Gamma_U(x, \Gamma)$ (partie de N) $\to$ SbU(x). "Par récurrence", supposons avoir déjà défini Γ^u : partie de $N \to$ Sb $\mathrm{It}_x(u, U(x))$, pour les éléments u de $X \in$ Sb E et définissons Γ^X. En vertu de I_1 $\mathrm{It}_x(X, U(x)) =$ U (graphe de $u \rightsquigarrow \mathrm{It}_x(u, U(x))$, $u \in X$); utilisant Γ_U on voit qu'il suffit de construire Γ_G : (partie de N) $\to$ (Sb du graphe

en question). Cela se fait facilement à l'aide de Γ^{u} et de Γ_{E} qui fournit une surjection vers $Sb X$.

§ 4. Equivalence d'une forme affaiblie de la théorie des ensembles avec l'arithmétique.

n° 1 Equivalences

Une équivalence entre deux théories $\mathcal{T}_0$ et $\mathcal{T}_1$, plus fortes que la logique, est la donnée de lois * associant à chaque assertion de $\mathcal{T}_0$ (resp $\mathcal{T}_1$) une assertion de $\mathcal{T}_1$ (resp $\mathcal{T}_0$) de façon que :

1) * est compatible avec la logique, c'est-à-dire (A ou B)* est A* ou B*, de même pour $\Rightarrow$, et, $\neg$
2) Si A est une assertion de $\mathcal{T}_0$ (resp $\mathcal{T}_1$), $A \Leftrightarrow A^{**}$ est un théorème de $\mathcal{T}_0$ (resp $\mathcal{T}_1$).
3) Si A est un théorème de $\mathcal{T}_0$ (resp $\mathcal{T}_1$), A* est un théorème de $\mathcal{T}_1$ (resp $\mathcal{T}_0$).

Une équivalence limitée entre deux théories $\mathcal{T}_0$ et $\mathcal{T}_1$, du type décrit ici (i.e. ayant au moins les axiomes logiques et quantifiés) est la donnée de lois * associant à chaque assertion (resp. terme) limité de l'une un de l'autre, de façon que :

a) Si (S pour $\underline{z} \in \Gamma$)* est (T pour $\underline{u} \in \Delta$), $\underline{z}$ coïncide avec $\underline{u}$, et (Γ_i pour $z_1 \in \Gamma_1 \cdots z_{i-1} \in \Gamma_{i-1}$)* est Δ_i pour $z_1 \in \Delta_1 \cdots z_{i-1} \in \Delta_{i-1}$
b) Compatibilité avec lalogique et les quantificateurs (par exemple, ($\exists z \in E$ R(z) pour $\underline{x} \in \Gamma$)* est $\exists z \in E^*$ R*(z) pour $\underline{x} \in \Gamma^*$, où, pour définir *, E est limité par $\underline{x} \in \Gamma$ et R par $\underline{x} \in \Gamma$, $z \in E$)
c) Compatibilité avec la substitution de variables libres à d'autres.

d) Si "A pour $\underline{z} \in \Gamma$" est une assertion (un terme) limitée, avec les notations de la pg.13 , on a :

$\vdash \forall \underline{z} \in \Gamma \ (A \equiv A^{**})$

où $\equiv$ désigne $\Leftrightarrow$ (resp.=)

e) Si $\forall \underline{z} \in \Gamma$ A est un théorème, $\forall \underline{z} \in \Gamma^*$ A^* aussi

Les équivalences, ainsi que les équivalences limitées, se composent. Une équivalence limitée induit une équivalence entre les parties sensées des théories (définition pg.15).

Soit $\mathcal{T}$ une théorie qui admet un signe primitif s, et soit $\mathcal{T}$ -s la théorie obtenue en supprimant le signe s (et les axiomes où il figure). On se propose d'expliciter un critère d'élimination limitée de s, c'est-à-dire un critère pour prouver l'équivalence limitée de $\mathcal{T}$ et $\mathcal{T}$ -s, une des lois * étant l'inclusion de $\mathcal{T}$ -s dans $\mathcal{T}$

On suppose que $\mathcal{T}$ a un critère formatif par signe primitif, chacun étant du type suivant

(C.F) Si $\underline{x}$ sont p variables libres disctintes ne figurant pas dans les q termes $\underline{E}$ et si $\underline{V}$ sont r termes et/ ou relations, $t_{\underline{x}}(\underline{E}\ \underline{V})$ est un terme, ou une assertion selon le signe t ($\underline{x}$ variables liées).

Le fait que des variables liées puissent ne pas être limitées va donner lieu à des difficultés. On supposera être dans un des deux cas suivants

(1) cas limité : pour tout signe primitif t et tout terme limité $t_{\underline{x}}(\underline{E},\underline{V})$ pour $\underline{z} \in \Gamma$, si s ne figure ni dans $\underline{E}$, ni dans Γ, on dispose de p termes limités $\underline{H}$ pour $\underline{z} \in \Gamma$ où s ne figure pas, et tels que l'assertion suivante soit un théorème :

$$\forall \underline{z} \in \Gamma \ (\forall \underline{x} \in \underline{H} \ (\underline{V} \equiv \underline{V}') \Rightarrow t_{\underline{x}}(\underline{E},\underline{V}) \equiv t_{\underline{x}}(\underline{E},\underline{V}'))$$

Dans cette formule $\equiv$ représente $\Leftrightarrow$ ou $=$ selon le contexte, et $\underline{V} \equiv \underline{V}'$ représente $V_1 \equiv V_1'$ et ... et $V_r \equiv V_r'$. On suppose $\underline{H}$ choisi une fois pour toutes dans chaque cas.

(q) cas quasi-limité : on définit la notion de terme ou assertion quasi-limitée de façon analogue à celle de terme ou assertion limitée, à cela près que des signes $\in$ peuvent être remplacés par des signes c. On utilisera une notation comme $\underline{z} \in /c\, \underline{\Gamma}$. Pour tout signe primitif t, on suppose encore donné des termes $\underline{H}$ où s ne figure pas et une suite de signes $\in$,c de sorte que

Quelle que soit l'assertion R où $\underline{x}$ ne figure pas, si

$R \Rightarrow (\underline{x} \in /c\, \underline{H}\ (\underline{E}) \Rightarrow \underline{V} \equiv \underline{V}')$ est un théorème, alors

$R \Rightarrow t_{\underline{x}}\ (\underline{E},\underline{V}) \equiv t_{\underline{x}}\ (\underline{E},\underline{V}')$ est un théorème.

Pour éliminer s, on va supposer disposer d'une interprétation limitée ou quasi-limitée de s dans $\mathcal{T}$ -s, selon qu'on est dans le cas (1) ou (q) . Lorsqu'on se donne une assertion (ou terme) limitée (resp. quasi-limitée).

$$s_{\underline{x}}\ (\underline{E},\underline{V}) \text{ pour } \underline{z} \in \underline{\Gamma} \quad (\text{resp pour } \underline{z} \in /c\, \underline{\Gamma})$$

et que s ne figure ni dans $\underline{E}$, ni dans $\underline{V}$, ni dans $\underline{\Gamma}$, il s'agit de disposer dans $\mathcal{T}$ -s de S, dépendant des mêmes variables libres, qui l'interprète. Cela signifie selon le cas

(I1) cas limité : $\quad \vdash \forall \underline{z} \in \underline{\Gamma}\ (s_{\underline{x}}\ (\underline{E}\,;\underline{V}) \equiv S)$

(I_q) cas quasi-limité :

$$\vdash \underline{z} \in /c\, \underline{\Gamma}\ (s_{\underline{x}}\ (\underline{E};\underline{V}) \equiv S)$$

On peut maintenant définir une loi * : $\mathcal{T} \longrightarrow \mathcal{T}$-s en procédant par récurrence sur le nombre de signe s figurant

dans l'assertion ou terme limité (resp quasi-limité) qu'on veut traduire, et de façon à vérifier les conditions suivantes : étant donné T pour $\underline{z} \in \Gamma$ (resp $z \in /c\, \Gamma$)

(1) si s ne figure pas dans Γ_i pour $i < n$, on limite Γ_n par $\underline{z} \in \Gamma_{(i)}$ $(i<n)$ (resp $\underline{z} \in /c\, \Gamma_{(i)}$ $(i<n)$) et
(T pour $\underline{z} \in \Gamma$)* est (T pour $z_1 \in \Gamma_1 \ldots z_n \in \Gamma_n^* \ldots z_k \in \Gamma_k$)*
(resp...)

(2) si s ne figure pas dans Γ et si T est $t_{\underline{x}}$ $(\underline{E},\underline{V})$, on limite $\underline{E}$ par $\underline{z} \in \Gamma$, et
(T pour $\underline{z} \in \Gamma$)* est ($t_{\underline{x}}$ $(\underline{E}^*,\underline{V})$ pour $\underline{z} \in \Gamma$)* (resp...)

(3) si s ne figure pas dans Γ ni $\underline{E}$, on dispose de $\underline{H}$ et on limite $\underline{V}$ par $\underline{z} \in \Gamma$, $\underline{x} \in \underline{H}$ et
($\underline{T}$ pour $\underline{z} \in \Gamma$)* est ($t_{\underline{x}}$ $(\underline{E},\underline{V}^*)$ pour $\underline{z} \in \Gamma$)* (resp...)

(4) si s ne figure pas dans $\underline{E}$, Γ ou $\underline{V}$, soit s ne figure pas dans T, et on ne se fatigue pas, soit T commence pas s, et on prend l'interprétation dont on suppose disposer.

L'idée est donc de commencer la traduction par l'intérieur de la formule, de façon à n'avoir qu'à traiter le cas où s figure seulement en tête.

Les condition a) b) et c) de la définition des équivalences limitées sont remplies. d) et e) sont triviales dans un sens, car $\mathcal{C}$-s $\longrightarrow$ $\mathcal{C}$-s est l'identité. Pour démontrer d), on utilise la même récurrence que plus haut, et dans le cas quasi-limité, on prouve plus généralement que pour A pour $\underline{z} \in /c\, \Gamma$ quasi-limité

$$\underline{z} \in /c\, \Gamma \Rightarrow (A \equiv A^*) \text{ est un théorème.}$$

La démonstration est triviale et la preuve de ce fait laissée

au lecteur. Pour vérifier que le transformé d'un théorème sensé de $\mathcal{T}$ est un théorème, on met sa démonstration sous la forme garantie par le métathéorème 1.3.2. pg.75 et on conclut :

Critère d'élimination limitée : l'élimination limitée de s est possible lorsque (C.F.) est vérifiée, qu'on est dans un des cas (1) ou (q), que selon le cas on dispose d'une interprétation de s vérifiant (I1) ou (Iq) et enfin que la loi * définie plus haut transforme fermeture d'axiomes limités de $\mathcal{T}$ en théorèmes de $\mathcal{T}$ -s.

Dans les applications, la condition C.F. sera triviale, et les conditions (1) ou (q) aisées à vérifier. La loi * change peu la forme des assertions, ce qui rendra aisée la vérification de la dernière condition, spécialement pour les axiomes "non spécifiques à s". Je me contenterai en général d'exhiber l'interprétation, laissant les autres vérifications au lecteur consciencieux.

n°2. La forme affaiblie de la théorie des ensembles.

L'affaiblissement apporté à la théorie des ensembles sera que les définitions par récurrence "transfinie" ne seront permises que pour autant que les valeurs de la fonction définie restent dans un ensemble fixé à l'avance. La définition du soubassement n'étant pas de ce type, on l'introduira par un nouveau signe primitif.

Formellement : la théorie $(Ens.f)_0$ a pour signes primitifs ceux de la théorie précédente, sauf $\mathfrak{U}$, et les nouveaux signes primitifs Sb et $\mathfrak{U}$. Les axiomes autres que d'itération restent inchangés. En outre, si E est un terme, Sb E est un terme et on pose l'axiome

$$\text{I.}\quad \mathrm{Sb}E = \{E\} \cup \bigcup_{z \in E} \mathrm{Sb}z$$

Sb étant entendu à ce nouveau sens, on conserve le principe I_2 de démonstration par récurrence transfinie tel qu'il figure pg.26

Si E, T (x), $\cap$ sont des termes, $\mathrm{Ul}_x(E, T(x), \cap)$ sera un terme. On prend pour axiome :

I_1^1 $\mathrm{Ul}_x(E, T(x), \cap)$ est un graphe fonctionnel d'une partie de SbE dans $\cap$, défini en $X \in \mathrm{Sb}E$ si et seulement si il est défini sur X et que T appliqué à sa restriction à X est dans $\cap$, cet élément de $\cap$ étant alors sa valeur en X.

On se propose de montrer que la partie sensée de $(\mathrm{Ens.f})_0$ est équivalente à l'arithmétique

C'est là un résultat raisonnable, car on s'est arrangé pour tuer l'obstruction la plus évidente, le théorème de Gödel, qui rendrait ce résultat absurde si on pouvait prouver la non-contradiction de l'arithmétique dans $(\mathrm{Ens.f.})_0$.
Dans la théorie initiale, ce peut se faire de deux façons :

A. à chaque assertion arithmétique A, on associe par récurrence une partie de $\mathbb{N}^k$, où k est le nombre de variables qui y figurent. Intuitivement, c'est la partie de $\mathbb{N}^k$ où A est vraie. A tout théorème est associé la partie pleine, et à $o \neq o$ la partie vide

B. Il existe une démonstration plus subtile, due à Gentzen, qui utilise seulement une récurrence transfinie jusqu'à ε_0, le plus petit ordinal tel que $\omega^{\varepsilon_0} = \varepsilon_0$. Si on pose par récurrence $\omega^{[n]} = \omega^{(\omega^{[n-1]})}$ et $\omega^{[0]} = 1$, on a $\varepsilon_0 = \sup \omega^{[n]}$.

Ces deux démonstrations exigent une définition par récurrence d'une fonction dont les valeurs ne restent pas dans un ensemble fini à l'avance, la première parce qu'on ne dispose pas de l'ensemble des parties, la seconde pour définir ε_0.

La démonstration utilise le métathéorème d'énumération, le lemme qui suit, qui montre qu'on n'a à s'occuper que d'ensembles de "type" fini au dessus de N, et enfin un lemme fondamental de codage dû à Gödel.

n° 3. Premières réductions.

lemme : Soit $T(x)$ pour $\underline{z} \in /c\Gamma$ un terme quasi-limité. On peut trouver un entier explicite m tel que l'assertion suivante soit un théorème : $\underline{z} \in /c\Gamma \Rightarrow \mathfrak{U}^m T(x) \subset N$

$\mathfrak{U}^m$ désigne $\mathfrak{U} \ldots \mathfrak{U}$ m fois. On procède par récurrence sur la longueur de T pour $\underline{z} \in /c\Gamma$ (qu'on définit comme la somme des longueurs de T et des Γ_i) et cas par cas selon la forme de T.

Cas 1 : $\{U(z) / z \in E \text{ et } R(z)\}$. Si m convient pour U(z) pour $\underline{z} \in /c\Gamma$, $z \in E$, on prend m+1

Cas 2 $\{U,V\}$ On a $\mathfrak{U}^{m+1} T \subset \mathfrak{U}^m U \cup \mathfrak{U}^m V$

Cas 3 $\mathfrak{U} E$ $\mathfrak{U}^m \mathfrak{U} E \subset N$ si $\mathfrak{U}^m E \subset N$, car $\mathfrak{U} N = N$

Cas 4 $Sb\underline{E}$ $\mathfrak{U}^{m+1} Sb E \subset N$ si $\mathfrak{U}^m E \subset N$, parce que $\mathfrak{U} Sb E = \bigcup_{x \in E} Sb x$ et que si $n \in N$, $Sb n \varphi\, n+1 \subset N$

Cas 5 $\underline{\mathfrak{U}_x(E, T(x), \cap)}$ $\subset Sb E \times \cap$ ce qui ramène aux cas 1, 2, 4

Cas 6 $\underline{N}$ ce cas est trivial.

Cas 7 $\underline{x_i}$ Si $x_i \in \Gamma_i$ ou $x_i \subset \Gamma_i$, $\mathfrak{U}^n \Gamma_i \subset N \Rightarrow \mathfrak{U}^n x_i \subset N$

Proposition : Il existe une équivalence limitée entre $(Ens.f.)_o$ et la théorie obtenue comme suit, (désignée par le sigle $(Ens.f.$

1) On supprime $\mathcal{U}$, Sb, I., I_1^1 et I_2

2) on rajoute un signe $\mathcal{U}^N$. Si T (x) et Λ sont des termes, et si x ne figure pas dans Λ, $\mathcal{U}_x^N(T(x), \Lambda)$ est un terme. On pose l'axiome: I_1^N $\mathcal{U}_x^N(T(x), \Lambda)$ est un graphe fonctionnel d'une partie de N dans Λ , défini en $n \in N$ si et seulement si il est défini sur n $(=[0, n-1])$ et que T appliqué à sa restriction à n $(=[0, n-1])$ est dans Λ , cet élément de Λ étant alors sa valeur en n.

3) de même que $\mathcal{U}^N$ remplace $\mathcal{U}$, on rajoute, à la place de I_2 l'axiome : I_2^N $\forall n \in N((\forall m < n\ R(m)) \Rightarrow R(n)) \Rightarrow \forall n \in N\ R(n)$

Démonstration :

a) Comme chaque fois qu'on voudra remplacer un signe par un autre, apparemment moins puissant, on passera par l'intermédiare de la théorie qui contient les deux (ici $(Ens.f.)'_o$, obtenue en "dédoublant" $\mathcal{U}_x(E, T(x), \Lambda)$ pour $E = N$). Cette théorie est trivialement équivalente à la première, comme on le voit sans devoir utiliser le critère du n°1.

b) On utilisera ici le critère du n°1 dans le cas quasi-limité. Dans $\mathcal{U}_x(E, T(x), \Lambda)$ (resp. $\mathcal{U}_x^N(T(x), \Lambda)$), x est quasi-limité. par x $\in$ SbE $x\Lambda$ (resp. $x \in N$ $x\Lambda$). Le cas des autres signes est trivial. Pour interpréter dans $(Ens.f.)_o^m = (Ens.f.)'_o$-$\mathcal{U}$ un terme
$\mathcal{U}_x(E, T(x), \Lambda)$ pour $\underline{z} \in /\in \Gamma$ où $\mathcal{U}$ ne figure que là où il est explicité, on remarque que I_1^1 fournit une définition de $\mathcal{U}_x(E, T(x), \Lambda)$ en terme des $\mathcal{U}_x(z, T(x), \Lambda)$ pour $z \in E$.

et par récurrence informelle sur n en terme des $\mathcal{U}_x(z, T(x), \cap)$ pour $z \in \mathcal{U}^n E$. Si $z \subset N$, il est facile d'exprimer $\mathcal{U}$ à l'aide de $\mathcal{U}^N$, et on applique le lemme.

c) Pour réduire I_2 à I_2^N il faut montrer que si

(1) $\forall_{\underline{z} \in \Gamma} (\forall F \in SbE (\forall x \in F\, R(x) \Rightarrow R(F)) \Rightarrow R(E))$ est sensé, c'est un théorème de la théorie $(Ens.f.)''_0$ où I_2^N remplace I_2. On montrera ainsi l'équivalence limitée entre $(Ens.f.)''_0$ et $(Ens.f)'''_0$.

De $\forall F \in SbE \quad (\forall x \in F\, R(x) \Rightarrow R(F))$ on déduit

(2) $\forall u \in \mathcal{U}''E (R(u)) \Rightarrow R(E)$ et

(3) $\forall u \in \mathcal{U}''E [\forall F \in u (\forall x \in F (R(x)) \Rightarrow R(F))]$

De plus par le lemme, pour un certain n,

$\forall_{\underline{z} \in \Gamma} (\mathcal{U}^n E \subset N)$ Comme I_2^N implique évidemment

I_2 si on suppose $E \in N$, on déduit de (3) que

$\forall_{\underline{z} \in \Gamma} \forall u \in \mathcal{U}''E (R(u))$ d'où par (2) on déduit (1).

d) Puisque l'équivalence limitée entre théories est transitive, il ne reste plus qu'à exprimer dans $(Ens.f.)_1$ les termes quasi-limités de $(Ens.f.)''_0$ du type SbE pour $z \in / \subset \Gamma$. On applique encore le lemme en remarquant que SbE se définit (sans Sb) en fonction des Sbz pour $z \in \mathcal{U}^n E$ et que si $z \in N$, $Sbz = z+1 (z \cup \{z\})$

n°4 Variante au métathéorème d'énumération.

On se propose de donner une variante de métathéorème d'énumération du § 3 qui ait un sens et soit vraie dans les théories affaiblies qu'on sera amené à considérer.

Variante : Il existe un procédé explicite qui à chaque terme limité :

$$T\,(z_1 \dots z_k) \text{ pour } z_1 \in \Gamma_1 \,,\quad z_2 \in \Gamma_2\,(z_1) \dots z_k \in \Gamma_k(z_1 \dots z_{k-1})$$

associe une famille de termes

$$\varphi^{T}_{\iota_1 \dots \iota_k \iota}(\underline{n}_1 \dots \underline{n}_k\, \underline{\ell})$$

de sorte que

1) a) φ n'a pas d'autres variables libres que celles indiquées (toutes distinctes, et qui en pratique parcoureront $\mathbb{N}$)

b) chaque indice parcourt un segment $[1, u]$ des entiers, où u dépend des valeurs des indices antérieurs.

c) la suite de variables groupées sous le symbole $\underline{n}_p$ (resp $\underline{l}$) dépend de $(i_1 \dots i_p)$ (resp $(\iota_1 \cdots \iota_k \iota)$)

d) dans $\varphi^{\Gamma_p}_{i_1 \dots i_{p-1} \iota}\,,(i_1 \dots i_{p-1}, i)$ a même domaine de variation que $(i_1 \dots i_p)$ dans φ^{T}, et les paquets correspondant de variables $(\underline{n}_1 \dots \underline{n}_{p-1}\, \underline{l})$ et $(\underline{n}_1 \dots \underline{n}_p)$ coïncident.

2) Pour $(i_1 \dots i_k)$ dans le domaine de variation, posons

$\widetilde{T}_{i_1 \dots \iota_k} \equiv T\,(\varphi^{\Gamma_1}_{\iota_1}, \varphi^{\Gamma_2}_{\iota_1 \iota_2} \dots)$; les seules variables libres de $\widetilde{T}$ sont donc $\underline{n}_1 \dots \underline{n}_k$.

L'assertion suivante est un théorème :

$$\vdash \forall \underline{n}_1 \in \underline{N} \cdots \forall \underline{n}_k \in \underline{N} \quad \forall z \in \widetilde{T}_{\iota_1 \cdots \iota_k} \quad \bigvee_{\iota} \; \exists \underline{\ell} \in N\,(z = \varphi^{T}_{\iota_1 \cdots \iota_k \iota}(\underline{n}_1 \cdots \underline{n}_k\, \underline{\ell}))$$

(quels que soient $\iota_1 \cdots \iota_k$)

où V désigne une disjonction itérée (finie).

Démonstration :

Intuitivement, on veut donc que les φ_i^T énumèrent T pour la valeur des z_j correspondant (par les $\varphi^{\overline{r}}$) aux $\underline{n}_j$. Pour mener à bien une récurrence sur la longueur du terme limité, on devra définir simultanément des

$$\varphi^{T,m}_{i_1 \cdots i_k j_0 \cdots j_m} \quad (\underline{n}_1 \cdots \underline{n}_k \underline{l}_0 \cdots \underline{l}_m) \qquad (m \text{ entier} \geqslant 0)$$

On vérifiera par après que ces termes ne sont autre que

(1) $\varphi^{T,m+1} \equiv \varphi^{\varphi^{T,m}} \qquad \varphi^{T,0} \equiv \varphi^T$

ce qui a un sens car $\varphi^{T,m}$ est considéré comme limité par $\underline{n} \in \underline{\mathbb{N}}$, $\underline{l} \in \underline{\mathbb{N}}$. Les $\varphi^{T,m}$ énuméreront donc $\dot{U}^m$ T. On procède cas par cas selon la forme de T; le résultat ne sera utilisé que dans une théorie ne contenant pas $\mathcal{U}^{\mathbb{N}}_0$ et je laisse donc sans scrupule le cas $\mathcal{U}^{\mathbb{N}}$ au lecteur; les cas où T est une variable libre ou $\mathbb{N}$ sont traités pg. 48 (cas 3 et 4).

Cas 1 : T est $\dot{U}$ V. On dispose déjà de $\varphi^{V,m+1}_{i_1 \cdots i_k j_0 \cdots j_{m+1}}$. Pour obtenir $\varphi^{\dot{U}V,m}_{i_1 \cdots i_k j_0 \cdots j_m}$, on prend le φ précédent où on collapse les indices j_0 et j_1 (par exemple en ordonnant lexicographiquement le domaine de variation de $(j_0 j_1)$

Cas 2 : T est $\{U, V\}$. Pour m = o, $\varphi^T_{i_1 \cdots i_k 1}(\underline{n}_1 \cdots \underline{n}_k \underline{l}_1)$ est $\widetilde{U}_{i_1 \cdots i_k}(\underline{n}_1 \cdots \underline{n}_k$, 2 pour V (o variables dans $\underline{l}_1$ et $\underline{l}_2$).

Pour m > o, $\varphi^{T,m}_{i_1 \cdots i_k 1 j_1 \cdots j_m}$ est $\varphi^{U,m-1}_{i_1 \cdots i_k j_1 \cdots j_m}$, 2 pour V. Par la suite, ce genre de précision sur la façon de se débrouiller avec les indices sera omis.

Cas 3 : T est $\{V(\underline{z},t) : t \in E(\underline{z}) \text{ et } R(\underline{z},t)\}$

on dispose déjà de φ pour le terme limité
$V(z,t)$ pour $t \in E(\underline{z}), \underline{z}$

$m = o$: on prend $\widetilde{V}$
$m \neq o$: on prend φ convenant pour V et $m-1$

Que φ a bien les propriétés requises se vérifie par une récurrence facile. On prouve d'abord (1) par récurrence sur la longueur du terme limité. On prouve alors 1) par récurrence sur T encore pour tous les $\varphi^{T,m}$ simultanément, puis 2).

n° 5 Elimination de $\mathcal{U}\ell^N$

Les opérations + et . dans N ont été définies par récurrence. Avant d'éliminer $\mathcal{U}\ell^N$, il faut les introduire par de nouveaux signes primitifs:
la théorie $(\text{Ens.}f.)_1$ est équivalente à la théorie $(\text{Ens.}f)'_1$ obtenue en adjoignant deux signes primitifs S et P et les axiomes A_0 A_1 A_2 A_3.

a) Si n, m, p sont trois termes, alors
$S(n,m,p)$ et $P(n,m,p)$ sont des assertions
b) <u>axiomes</u> :

A_0 $\quad S(E,F,G)$ ou $P(E,F,G) \quad \Rightarrow \quad E \in N$ et $F \in N$ et $G \in N$

A_1 $\quad \forall n \in N \; \forall m \in N \; (\exists! s \in N \; S(n,m,s)$ et $\exists! p \in N \; P(n,m,p))$

A_2 $\quad \forall n \in N \quad S(n,o,n)$ et $\forall n \in N \; \forall m \in N \; \forall s \in N \; (S(n,m,s) \Rightarrow S(n,m+1,s+1))$

A_3 $\quad \forall n \in N \quad P(n,o,o)$ et $\forall n \in N \; \forall m \in N \; \forall p \in N \; \forall q \in N$
$P(n,m,p)$ et $P(n,m+1,q) \Rightarrow S(n,p,q)$

Le lecteur aura deviné que $S(n,m,S)$ (resp $P(n,m,p)$) signifie $s = n + m$ (resp $p = nm$).
$m + 1$ signifie comme d'habitude $m \cup \{m\}$
Le lemme suivant, qui résume les procédés de codage de

Gödel, va permettre de définir une équivalence limitée entre $(Ens.f)'_1$ et la théorie $(Ens.f)_2$ obtenue en supprimant $\mathcal{U}^{\mathbb{N}}$

Lemme : On peut dans $(Ens.f)_2$ définir un terme H(n) tel que $H(o) = \{\emptyset\}$ et que

$$\forall_{n\in\mathbb{N}}\ H(n+1) = \{f \cup \{(n+1,m)\} \mid f \in H(n) \text{ et } m \in \mathbb{N}\}$$

Intuitivment, H(n) sera l'ensemble des fonctions de $[1,n]$ Dans $\mathbb{N}$. Considérons avec Gödel l'assertion arithmétique B(n,m,i,w,) : "w est le reste de la division de n par 1 + im" i.e. $\exists d \quad n = d(1+im) + w.$ et $w < 1+im$
Cette assertion est fonctionnelle en w, et toujours vraie ou fausse. Il est clair, informellement, que pour $1 \leqslant i \leqslant k$, n et m variables, w(i) énumère toutes les fonctions $[1,k] \longrightarrow \mathbb{N}$, et on va le démontrer en arithmétique formelle intuitionniste.

Voici les points essentiels de la démonstration :

a) Si une assertion R(n) est décidable (i.e. $\forall n\, R(n)$ ou $\neg R(n)$) et si $\exists n\, R(n)$, il existe un plus petit entier tel que R [par récurrence sur n, on voit $\forall k \leqslant n \neg R(k)$ ou $\exists k \leqslant n (R(k)$ et $\forall k' < k\ (\neg R(k)))$]

b) Formule de Bezout pour le pgcd de n et m

[pgcd (n,m) = inf an $\dot{-}$ bm pour $a<m$, $b<n$]

c) Existence d'un plus petit facteur premier. Théorème d'Euclide pour un nombre premier divisant un produit.

d) $\forall n \exists m$ dont les facteurs premiers sont les nombres premiers $\leqslant n$ [récurrence sur n]

e) Pour un tel m, les (1 + im) sont deux à deux premiers entre eux pour $1 \leqslant i \leqslant n$ [tout nombre premier divisant deux d'entre eux divise la différence donc est $\leqslant n$ - absurde].

f) Soit un terme $\Psi(i)$ tel que les $\Psi(i)$ soient deux à deux premiers entre eux pour $1 \leqslant i \leqslant n$. $\forall i \leqslant n \ \exists d$ divisible par $\Psi(j)$ pour $1 \leqslant j \leqslant n$, $i \neq j$ et premier avec $\Psi(i)$ [par récurrence sur n, il existe d dont les facteurs premiers sont exactement...]

g) Même hypothèse que (f). Il existe d divisible par les $\Psi(j)$ pour $1 \leqslant j \leqslant n$, $i \neq j$, dont le reste de la division par $\Psi(i)$ est un nombre donné quelconque $< \Psi(i)$ (utiliser Bezout pour $\Psi(i)$ et le d trouvé en (f): prendre un multiple de ce dernier).

h) Même hypothèse que (f). On se donne de plus un terme $\Psi(i)$ et on suppose $\Psi(i) < \Psi(i)$ pour $1 \leqslant i \leqslant n$. Il existe d dont le reste de la division par $\Psi(i)$ est $\Psi(i)$ pour $1 \leqslant i \leqslant n$ (par récurrence sur $1 \leqslant j \leqslant n$, il existe d divisible par $\Psi(i)$ pour $i > j$ et ayant le bon reste pour $i \leqslant j$)

i) On se donne un terme $\Psi(i)$ et k

$\exists n \exists m \forall i \leqslant k \quad B(n, m, i, \Psi(i))$

j) $\forall w \ \exists n \ \exists m \quad B(n, m, 1, w)$

k) $\forall w \ \forall k \ \forall n \ \forall m \ \exists n' \ \exists m' \ (\forall 1 \leqslant i \leqslant k \ \forall v \ B(n,m,i,v) \Leftrightarrow B(n',m',i,v)$ et $B(n', m', k+1, w)$

On a ainsi fait ce qu'il fallait pour pouvoir définir H (k) comme :

$$\left\{ \left\{ (i\,w) \,;\, 1 \leqslant i \leqslant k, w \in N \text{ et } B(n,m,i,w) \right\} ;\ n, m \in N \right\}$$

Il est aisé maintenant de définir l'ensemble Hom $([pq], N^1)$ des applications de $[pq]$ dans N^1. Pour éliminer $\mathcal{U}^N$, ainsi que pour toutes les éliminations ultérieures, on utilisera le

critère du n°1 sous la forme limitée. Soit donc un terme limité $\mathcal{U}\ell_x^N(T(x),\Lambda)$ pour $\underline{z}\in\Gamma$.

a) si $\mathcal{U}\ell_N$ ne figure pas ni dans Λ, ni dans Γ, il s'agit de limiter la variable liée x. Les résultats du n°4 permettent de trouver $\varphi(\underline{n})$, terme de $(Ens.f)_2 = (Ens.f)'_1 - \mathcal{U}\ell^N$, tel que $\forall \underline{z}\in\Gamma\ \forall w\in\Lambda\ \exists \underline{n}\in\mathbb{N}\ (w=\varphi(\underline{n}))$

On peut alors définir Hom $([o,n],\Lambda)$ et limiter x par $\bigcup_{n\in\mathbb{N}} \mathrm{Hom}\,([o,n],\Lambda)$ $(\mathrm{Hom}([o,n],\Lambda)\subset\{\varphi\circ f / f\in \mathrm{Hom}([o,n],\underline{\mathbb{N}})\})$

b) si $\mathcal{U}\ell^N$ ne figure que là où il est explicité, il s'agit d'en trouver une interprétation :

$\{(n,y) / n\in\mathbb{N},\ y\in\Lambda,$ et $\exists f\in \mathrm{Hom}([o,n],\Lambda)$ tel que $f(n)=y$ et que $\forall i<n\ f(i)=T(f|[o,i[)\}$

n°6 Nouvelles éliminations.

La théorie $(Ens.f)_2$ est équivalente à $(Ens\,f)_2^\circ$ obtenue en supprimant $\{T,U\}$, mais en adjoignant un signe primitif pour U ∪ V, car $\{T,U\} = \{T\} \cup \{U\}$ et $\{T\} = \{T / n\in\mathbb{N} \text{ et } o=o\}$. Elle est encore équivalente à $(Ens.f.)_2^\pi$ obtenue en adjoignant à $(Ens.f.)_2^!$ des signes primitifs pour exprimer $\{T(n_1,\ldots,n_k) / n_1\in\mathbb{N}\ldots$ $\ldots, n_k\in\mathbb{N};\ R(\underline{n})\}$ $(k\geqslant o)$ le tout avec des axiomes évidents. Pour établir une équivalence limitée entre $(Ens.f.)_2^\pi$ et $(Ens.f)_2^{\pi\circ}$ obtenue en supprimant le signe $\{\ /\ \}$ initial, il s'agit d'exprimer dans $(Ens.f.)_2^{\pi\circ}$ les termes limités

$$\{T(x) / x\in E \text{ et } R(x)\} \quad \text{pour } \underline{z}\in\Gamma \quad (1)$$

où $\{\ /\ \}$ n'apparaît qu'à l'endroit où il est explicité. La variante du métathéorème d'énumération est vraie dans $(Ens.f)_2^{\pi\circ}$ (le nouveau cas dans la récurrence est traité pg48 (cas2). L'appliquant à : E pour $\underline{z}\in\Gamma$ (k termes dans Γ)

on trouve $\varphi^1_{i_1}(\underline{n}_1), \cdots \varphi^k_{i_1 \cdots i_k}(\underline{n}_1 \cdots \underline{n}_k), \varphi_{i_1 \cdots i_k}(\underline{n}_1 \cdots \underline{n}_k \underline{n})$ comme il est expliqué au n°3.(1) s'interprète comme la réunion (∪) étendue au domaine de variation de $(\underline{i}, i)$ des
$\{T(\varphi(\underline{\underline{n}}\ \underline{n}))\ /\ \underline{\underline{n}} \in \underline{\underline{N}}, \underline{n} \in N; \underline{z} = \underline{\varphi}(\underline{\underline{n}}) \text{ et } \varphi(\underline{\underline{n}}\ \underline{n}) \in E \text{ et } R(\varphi(\underline{\underline{n}}, \underline{n}))\}$

De même, pour éliminer $\bigcup$, on interprète $\bigcup E$ pour $\underline{z} \in \underline{\Gamma}$ comme la réunion (u) des
$\{\psi(\underline{\underline{n}}, \underline{n})\ /\ \underline{\underline{n}} \in \underline{\underline{N}}, \underline{n} \in \underline{N}; \underline{z} = \underline{\varphi}(\underline{\underline{n}}) \text{ et } \exists x \in E(\psi(\underline{\underline{n}}, \underline{n}) \in x)\}$

où, avec les notations du n°3, ψ est $\varphi^{E,1}$.

On a jusqu'ici établi l'équivalence limitée de (Ens.f.), avec une théorie $(\text{Ens.f.})''_2$.
Il est standart qu'on peut pousser la réduction un peu plus loin en supprimant le signe = et en définissant l'égalité par l'axiome d'extensionabilité. E_1 (T = T) devient alors trivial et E_2 donne

E'_2 $\quad \forall x \in T(x \in U) \text{ et } \forall x \in U(x \in T) \quad \Rightarrow \quad R(T) \Leftrightarrow R(U)$

Finalement, on s'est ramené à considérer la théorie $(\text{Ens.f.})_3$ ayant pour signes primitifs ou, et, $\Rightarrow, -\ ; \forall, \exists; \in, \cup, \{\ /\ \in N, \cdots \in N;\ \}$; N, S, P.
et pour axiomes, outre ceux de la logique quantifiée :

Extensionalité : $T = U \Rightarrow (R(T) \Leftrightarrow R(U))$
où par définition $T = U$ désigne $\forall x \in T(x \in U) \text{ et } \forall x \in T(x \in U)$

U $\quad T \in \bigcup V\ W \Leftrightarrow T \in V \text{ ou } T \in W$

$\{\ /\ \}$ $\quad T \in \{V\ /\ \underline{n} \in \underline{N}; R\} \Leftrightarrow \exists \underline{n} \in \underline{N}\ (R \text{ et } T = V)$

N $\quad$ Les axiomes N_1, N_2, N_3 (pg28), I_2^N (pg 39) et

A_0, A_1, A_2, A_3, (pg43)

n° 7 L'hallali :

A) Pour pouvoir tirer profit de toutes les particularités de la situation, donnons dans (Ens.f.)$_3$ la démonstration de la variante du métathéorème d'énumération. On garde les notations et méthodes du n°4.

Cas 1 : $V \cup W$ on prend, ensemble, les φ qui conviennent pour V pour $\underline{z} \in \Gamma$ et W pour $\underline{z} \in \Gamma$ et la même valeur de m. On additionne donc les domaines de variation de l'indice j_0

Cas 2 : $\{V(z,n) \mid n \in \mathbb{N}$ et $R\}$ Distinguons les cas

m = o : on prend $\widetilde{V}$

m = p+1 : on prend les φ qui convenaient pour ρ et $V(\underline{z},\underline{n})$ pour $\underline{n} \in \mathbb{N}$, $\underline{z} \in \Gamma$

Cas 3 : $\underline{1}$ (une lettre). Cette lettre est limitée par un $1 \in \Gamma_i$: on prend les φ qui convenaient pour m+1 et Γ_i pour $z_1 \in \Gamma_1 \cdots z_{i-1} \in \Gamma_{i-1}$, soit $\varphi_{i_1 \cdots i_{i-1} j_0 \cdots j_{m+1}}(\underline{n}_1 \cdots \underline{n}_{i-1}\, p_0 \cdots p_{m+1})$ qu'on lit

en interprétant j_0 comme le nouveau i_i, j_{i+1} comme le nouveau j_i, et en regardant φ comme dépendant aussi de variables $\underline{n}_{i+1} \cdots \underline{n}_k$ qui n'y apparaissent pas explicitement.

Cas 4 : $\underline{\mathbb{N}}$ (k quelconque) - les j parcourent $[1,1]$

$\varphi_{i_1 \cdots i_k 1 \cdots 1}(\underline{n}, p_0 \cdots p_m) = p_m$

On vérifie alors :

(1) $\varphi^{T,m+1} = \varphi^{\varphi^{T,m}}$ (où $\varphi^T = \varphi^{T,0}$)

on garde la même récurrence sur T, et on fait à chaque stade la démonstration pour tous les m simultanément. Les cas autres que 2 pour $m = o$ sont triviaux. Il faut montrer l'identité entre φ^V et $\varphi^{\widetilde{V}}$

Distinguons les cas selon la forme de V. Les cas 1 et 3 résultent de l'hypothèse de récurrence, le cas 4 est trivial, et enfin dans le cas 2, $V \equiv \{W(\underline{z},\underline{n}) / \underline{n} \in \underline{N} \text{ et } R\}$ pour $\underline{z} \in \Gamma$

φ^V est $\widetilde{W}$, $\widetilde{V}$ est $\{\widetilde{W}(\varphi(\underline{n}),\underline{n}) / \underline{n} \in \underline{N} \text{ et } \widetilde{R}\}$ pour $\underline{n} \in \underline{N}$

et $\varphi^{\widetilde{V}} = \widetilde{W}$

(2) <u>énoncé de la variante</u> (même récurrence, facile)

<u>Définition : un terme (resp.une assertion) N -limité(e) est un terme (resp. une assertion) limité(e) dont la limitation est du type $\underline{n} \in \underline{N}$.</u>

(3) <u>si T est un terme N limité, la longueur des φ^T est $\leqslant$ à celle de T</u>

(contrairement à l'habitude, il s'agit ici de la longueur du terme, limitation non comprise). Récurrence standart (gardant toujours $m = o$). Lors des cas 1 et 2 on a même inégalité stricte.

(4) La loi qui à $T(\underline{n})$ N-limité associe $\varphi_i^T(\underline{n},\underline{l})$ est compatible avec les substitutions de variable, par exemple avec le remplacement de n_1 par n_2.

Récurrence standart; en fait il y a ici un grain de sable inessentiel, car on ne peut pas par exemple remplacer n_i par 1 . Dans (3) et (4) on utilise que la définition par récurrence de φ n'amène pas à sortir de la classe des termes N-limités.

Des raisons techniques amènent à associer à chaque terme ou assertion limité T pour $\underline{z} \in \Gamma$ un entier r, selon les règles

a) r est additif pour les signes logiques, u, $\in$, S et P (ainsi r (UuV pour $\underline{z} \in \Gamma$) = r (U pour $\underline{z} \in \Gamma$) + r (V pour $\underline{z} \in \Gamma$))

b) $r(\exists x \in E \ R(x)$ pour $\underline{z} \in \Gamma) = 1 + r$ (R(x) pour $\underline{z} \in \Gamma$, $\underline{x} \in E$) $+ r$ (E pour $\underline{z} \in \Gamma$)

c) $r(\{V \mid \underline{n} \in \underline{N}$ et $R\}$ pour $\underline{z} \in \Gamma) = 1 + r$ (V pour $\underline{z} \in \Gamma$, $\underline{n} \in N$) $+ r$ (R pour $\underline{z} \in \Gamma, n \in N$

d) r (N) = 1

e) $r(Z_i$ pour $\underline{z} \in \Gamma) = r(\Gamma_i)$

(5) $\underline{r(\varphi^T) \leqslant r(T)}$ (pour tous les φ^T associés à T)

Récurrence standart sur la longueur de T pour $\underline{z} \in \Gamma$ (pour tous les m simultanément).

Cas 2 : m = o : il suffit de montrer $r(\tilde{V}) \leqslant r(V)$; cela va se montrer par récurrence, limitée à la longueur de T, sur V pour $\underline{z} \in \Gamma$ (V terme ou assertion). On distingue les cas a) à e) de la définition de r.a), d) sont triviaux,

e) résulte de la récurrence principale pour Γ_i, b) résulte de la récurrence secondaire pour R pour $x \in E$, $\underline{z} \in \Gamma$ et de la formule $\varphi^E = \varphi^{\tilde{E}}$ démontrée en (1). c) résulte de la récurrence secondaire pour V et R.

(6) $\underline{r(R(\varphi^E)) < r(\exists x \in E(R))}$
$\underline{\text{pour } \exists x \in E(R) \text{ N-limité}}$

$r(\exists x \in E \ R$ pour...) > $r(R$ pour $x \in E, \ldots) \geqslant r(\hat{R}) =$ $r(R(\varphi^E))$

B) On se propose d'associer à chaque assertion N-limitée R pour $\underline{n} \in \underline{N}$ une assertion a R dans l'arithmétique formelle,

dépendant des mêmes variables, qui l'interprète. Il faudra simultanément s'occuper des termes N-limités; si T pour $\underline{n} \in \underline{\mathbb{N}}$ (k N) est un tel terme, dans les $\varphi^{T,m}$ les indices $\iota_1 \cdots \iota_k$ ne parcourent que [illegible],$\underline{l}$; on s'intéresse seulement au cas m = o et les φ s'écriront donc simplement $\varphi^T_j(\underline{n}, \underline{l})$.
On définira $L^T_j(\underline{n},\underline{l})$, en arithmétique encore, tel que pour $\underline{n}$ fixe, les $\varphi^T_j(\underline{n},\underline{l})$ définissent une surjection de la somme sur j des ensembles de $\underline{l}$ tels que L dans T (rien de trop, rien de trop peu).

La récurrence se fait cas par cas, selon la forme de T ou R.

Cas 1. R est combinaison logique de relations R_i
On prend la même combinaison logique des interprétations.

Cas 2. $\exists x \in E \ R(x)$ pour $\underline{n} \in \mathbb{N}$ On prend :
$\bigvee_j \exists \underline{l} \quad (L^E_j(\underline{n},\underline{l})$ et $a(R(\varphi^E_j(\underline{n},\underline{l}))))$
ou V est une disjonction finie. Idem pour $\forall$.

Cas 3. $\underline{n_i}$ pour $\underline{n} \in \mathbb{N}$ φ est une lettre l: on prend pour $L^{n_i}(\underline{n},\underline{l})$: $l < n_i$ (rappelons que < en arithmétique correspond à $\in$ en théorie des ensembles)

Cas 4. $\underline{\mathbb{N}}$ φ est une lettre. On prend une limitation vide (o = o)

Cas 5. $\underline{V \cup W}$. Les φ sont ceux de V et W, on garde les limitations correspondantes.

Cas 6. $\underline{\{V(n,m) \mid m \in \mathbb{N}, R(n,m)\}}$ pour $\underline{n \in \mathbb{N}}$
φ est $V(n,m,)$, la limitation sera a R

Cas 7. $\underline{S(U,V,W)}$ s'interprète comme
a (U∈N) et a(V∈N) et a(W∈N) et $\exists n,m,s,$ (n+m=s et
$\forall n' \ \forall m' \ \forall s'$ ($n' < n \Leftrightarrow$ a (n'∈U) et $m' < m \Leftrightarrow a(m' \in V)$ et
$s' < s \Leftrightarrow s(s' \in W)$)
Idem pour P.

Cas 8. Reste à considérer les assertions T∈V, où on distinguera plusieurs cas selon la forme de V

8.a. $\underline{T \in V \cup W}$ s'interprète comme a(T∈V) ou a (T∈W)

8.b; $T \in \{V(\underline{n}) / \underline{n} \in \mathbb{N} \text{ et } R(\underline{n})\}$ s'interprète comme
$\exists \underline{n}$ (a R(n) et a ($T = V(\underline{n})$ où, selon les dénitions,
a($T=V(\underline{n})$) est a $\forall x \in T$ ($x \in V(\underline{n})$) et a $\forall x \in V(\underline{n})$ ($x \in T$)

8.C. Si U est N ou n, et si

8.c.a. T aussi est N ou n, on prend les interprétations :
$\mathbb{N} \in \mathbb{N}$ et $\mathbb{N} \in n$ sont faux, $n \in \mathbb{N}$ est vrai, $n \in m$ signifie
$n < m$

8.C.B. Dans les autres cas $T \in \mathbb{N}$ (resp $T \in n$) s'interprète
comme a $T \subset \mathbb{N}$ et $\exists k\ \forall l$ ($al \in T \Leftrightarrow l < k$)
(resp a $T \subset \mathbb{N}$ et $\exists k$ ($k < n$ et $\forall l$ (a $l \in T \Leftrightarrow l < k$)))
Ceci suppose déjà interprétés $l \in T$ et $T \subset \mathbb{N}$. D'après le
cas 2, a $T \subset \mathbb{N}$ n'est autre que
$\bigwedge_l \forall \underline{l}$ $(L_l^T(\underline{l}) \Rightarrow a(\varphi_l^T(\underline{l}) \in \mathbb{N}))$

Montrons que cette longue récurrence n'est pas vicieuse.
Cela résulte de :

(1) dans le cas 2, le nombre r défini en A) décroît strictement quand on passe de l'expression initiale aux expressions supposées déjà traitées par récurrence.

(2) dans tous les cas, sauf le 2, la longueur diminue (strcitement), tout au moins après un nombre fini de stades(cas 8.c.b, à cause de $T \in \mathbb{N} \rightarrow l \in T$)

(3) dans aucun cas, r n'augmente.

C) Il n'est pas difficile d'associer à chaque assertion A de l'arithmétique formelle une assertion $\mathbb{N}$-limitée A* de $(Ens.f.)_3$ qui l'interprète, et dans B) on est parvenu à aussi définir une opération * en sens inverse. On laisse au lecteur le soin de ne pas vérifier.

1) pour tout A arithmétique, $\forall \underline{n}$ (A $\Leftrightarrow$ A**) est un théorème

2) pour tout A $\mathbb{N}$-limité de $(Ens.f.)_3$, $\forall \underline{n} \in \underline{\mathbb{N}}$ (A $\Leftrightarrow$ A**) est un théorème

3) pour tout A arithmétique, si A est un théorème, $\forall \underline{n} \in \mathbb{N}\ A^*$ est un théorème.

Pour établir l'équivalence entre les parties sensées de $(Ens.f)_0$ et de l'arithmétique, il reste à prouver

4) pour tout théorème sensé A de $(Ens.f)_3$, A* est un théorème de l'arithmétique.

On s'appuyera sur le métathéorème 1.3.2 (page 15).

Si R pour $\underline{z} \in \Gamma$ est une assertion limitée, $(\forall \underline{z} \in \Gamma\ R)^*$ peut s'obtenir comme suit (B) cas 2 itéré) :

on pose : $\widetilde{\Gamma}'_{\ell, i_1 \cdots i_{\ell-1}} (\underline{n}_1 \cdots \underline{n}_{\ell-1}) \equiv \Gamma_\ell \left(\varphi^{\Gamma_1}_{i_1}(\underline{n}_1), \varphi^{\widetilde{\Gamma}_{2,i_1}}_{i_2}(\underline{n}_1, \underline{n}_2), \cdots, \varphi^{\widetilde{\Gamma}_{\ell-1, i_1 \cdots i_{\ell-2}}}_{i_{\ell-1}}(\underline{n}_1 \cdots \underline{n}_{\ell-1}) \right)$

$R(\varphi^{\Gamma_1}_{i_1}(\underline{n}_1), \cdots \varphi^{\widetilde{\Gamma}_\ell}_{i_\ell}(\underline{n}_1 \cdots \underline{n}_\ell))$ n'est d'ailleurs autre que $\widetilde{R}_{i_1 \cdots i_k}(\underline{n}_1 \cdots \underline{n}_k)$ déjà défini. Avec ces notations, $(\forall \underline{z} \in \Gamma\ R)^*$ n'est autre que

$$\bigwedge_{i_1 \cdots i_k} \forall \underline{n}_1 \cdots \forall \underline{n}_k \left(L^{\Gamma_1}(\underline{n}_1) \text{ et } L^{\widetilde{\Gamma}_{2,i_1}}(\underline{n}_1\, \underline{n}_2) \text{ et } \cdots\ L^{\widetilde{\Gamma}_{k, i_1 \cdots i_{k-1}}}(\underline{n}_1 \cdots \underline{n}_k) \Rightarrow a\, \widetilde{R}_{i_1 \cdots i_k}(\underline{n}_1 \cdots \underline{n}_k) \right)$$

Se rappelant que lorsque dans un axiome on remplace une lettre par un terme, on obtient encore un axiome, on trouve

5) Pour vérifier que l'interprétation arithmétique de la cloture d'un axiome limité est toujours un théorème, il suffit de vérifier que l'interprétation d'un axiome N-limité est toujours un théorème.

Vérifions maintenant que pour A du type indiqué dans le métathéorème 1.3.2 c), A* est un théorème. On garde les notations du métathéorème.

Comme * est compatible à la logique, le résultat précédent, qui donne la forme de $(\forall \underline{z}^\circ \in \Gamma^\circ(\ldots))^*$, montre qu'il s'agit de prouver :

$$\bigwedge_{i_1 \cdots i_{k-1}} \forall \underline{n}^\circ \left(\underline{\widetilde{L}}^{\widetilde{\Gamma}^\wedge}(\underline{n}^\circ) \Rightarrow a(\forall x_n \in \widetilde{\Gamma}_n (\widetilde{C} \text{ et } x_n \in \widetilde{\Gamma}_n \Rightarrow \widetilde{R}(x_n))) \Rightarrow \right.$$

$$\left. \bigwedge_{i_1 \cdots i_{k-1}} \forall \underline{n}^\circ \left(\underline{\widetilde{L}}^{\widetilde{\Gamma}^\wedge}(\underline{n}^\circ) \Rightarrow a(\widetilde{C} \Rightarrow \forall x_n \in \widetilde{\Gamma}_n\ \widetilde{R}(x_n)) \right) \right.$$

qui résulterait du cas particulier où n = 1, où il n'y a

plus de Γ ° : prouvons donc

$\vdash a\,(\forall x \in \Gamma \;\; (C \text{ et } x \in \Gamma \Rightarrow R(x)) \Rightarrow a\,(C \Rightarrow \forall x \in \Gamma \;\; R(x))$

identique à

$\bigwedge_i \forall n\,(L_i^{\Gamma}(n) \Rightarrow ((aC \text{ et } a(\varphi_i^{\Gamma}(n) \in \Gamma)) \Rightarrow aR(\varphi_i^{\Gamma}(n))))$

$aC \Rightarrow \bigwedge_i \forall n\,(L_i^{\Gamma}(n) \Rightarrow a\,R(\varphi_i^{\Gamma}(n)))$

qui est un théorème pourvu que

(6) en soit un

(6) pour tout terme N-limité,

$\vdash L_i^{\Gamma}(n) \Rightarrow a(\varphi_i^{\Gamma}(n) \in \Gamma)$

Exactement le même raisonnement montre que de (6) on peut déduire que les interprétations des assertions c') sont des théorèmes. On laisse au lecteur le soin de vérifier que l'interprétation de b) est un théorème.

Pour prouver par récurrence que l'interprétation de tout théorème est un théorème, reste à prouver (6), (7) et (8).

(7) si A* et (A⇒B)* sont des théorèmes, B* est un théorème.

(8) si A est un axiome N-limité, A* est un théorème.

(7) est trivial, puisque (A⇒B)* n'est autre que $A^* \Rightarrow B^*$. Le même raisonnement prouve (8) pour les axiomes logiques. Les axiomes "arithmétiques" N_1, N_2, N_3, A_2, A_3, A_4, ne contiennent ni terme ni assertion indéterminée, ce qui permet de vérifier (8) par un calcul explicite. Le cas des axiomes A_1 I_2^N et des axiomes caractérisant $\cup$ ou $\{\,\}$ résulte aussitôt des cas 7,2 et 8.c, 8a et 8b de la récurrence qui définit l'interprétation.

Restent les axiomes Q_1 et Q_2 relatifs aux quantificateurs, et l'axiome "d'extensionnalité" sous la forme :

$$(T \subset U \text{ et } U \subset T) \Rightarrow (R(T) \Leftrightarrow R(U))$$

Pour Q_1, il s'agit de prouver (en arithmétique) :

$\vdash$ ((R(T) et T$\in$E)$\Rightarrow$ $\exists$ x$\in$E R(x))*

soit $\vdash$ (a (R(T)) et a (T$\in$ E))$\Leftrightarrow \forall_i \exists \underline{1}(L_i^E(\underline{1})$ et a(R ($\varphi_i^E(1)$))

qui résulte de la conjonction des:

(6 bis) $\vdash$ a (T$\in$E) $\Rightarrow \forall_i \exists \underline{1}\ (L_i^E(\underline{1})$ et a(T=$\varphi_i^E(1)$))

(9) a (T = U)$\Rightarrow$ (a (R(T)) $\Leftrightarrow$ a(R(U)))

Où (9) est l'interprétation de l'axiome d'extensionnalité.
idem pour Q_2

D) Preuve de (6), (6 bis) et (9)

Preuve de (6) : on procède par récurrence sur la longueur de Γ, distinguant les cas selon la forme de Γ. Les cas "N" et "n" sont triviaux, et le cas V $\cup$ W résulte de l'hypothèse de récurrence appliquée à V et W. Si Γ est $\{V(\underline{m},\underline{n})/\ \underline{n}\in\underline{N};\ R(\underline{m},\underline{n})\}$, il s'agit de prouver :
$\forall n$ (aR($\underline{m},\underline{n}$) $\Rightarrow$ a(V($\underline{m},\underline{n}$)$\in$ $\{V(\underline{m},\underline{n})/\underline{n}\in\underline{N};\ R(\underline{m},\underline{n})\}$))
soit (cas 8b)
$\forall n$ (aR($\underline{m},\underline{n}$)$\Rightarrow \exists$ n' (a R(m,n') et a($\forall$m,n) = V(m,n')))
qui résulte de a(V(m,n) = V(m,n)) parce que l'interprétation est compatible avec les substitutions de variables. Il faut prouver :

$\forall 1$ ($L_i^V(1) \Rightarrow$ a $\varphi_i^V(1)\in$ V)

et cela résulte de l'hypothèse de récurrence.

Corollaire : $\vdash$(T = T)*

Preuve de (6 bis) : certains des cas de la récurrence qu'on va utiliser seront repris dans la démonstration de (9). On eut pu éviter des redites en démon-

trant (6 bis) et (9) par une récurrence simultanée, mais on eut ainsi compliqué la vérification de l'absence de cercle vicieux dans la récurrence.

Si E est réunion (u) des E_k, (6 bis) pour T et E :

$$a\ T \in E \Rightarrow \forall_i \exists \underline{l}\ (L_i^E\ (\underline{l}) \text{ et } a\ T = \varphi_i^E(l))$$

résulte des énoncés (6 bis) pour les T et E_k.
Pour E du type $\{V(\underline{n},\underline{m}) /\!/ \underline{n} \in \mathbb{N} \text{ et } R(\underline{n},\underline{m})\}$, l'assertion est vraie, car $a\ T \in E$ est :

$$\exists \underline{n} \in \mathbb{N}\ (a\ R(\underline{m},\underline{n}) \text{ et } a\ T = V(\underline{m},\underline{n})), \text{ identique à}$$

$$\exists \underline{n} \in \mathbb{N}\ (L^E\ (\underline{n}) \text{ et } a\ T = \varphi^E(\underline{n})).$$

Enfin, si E est N ou n, $T \in E$ s'interprète cas par cas selon la forme de T; (6 bis) est évident si T est N ou m et sinon l'interprétation est :

$$q\ (T \subset \mathbb{N}) \text{ et } \exists l\ \forall p\ (a(p \in T) \Leftrightarrow p < l$$ et dans le second cas, $l < n$)

Il suffit de prouver :

$$a\ T \subset \mathbb{N} \text{ et } \forall p\ (a(p \in T) \Leftrightarrow p < l) \Rightarrow a\ (T \subset l \text{ et } l \subset T)$$

La seconde inclusion est facile, la première résulte de :

$$(L_i^T(\underline{n}) \Rightarrow a\ (\varphi_i^T(\underline{n}) \in \mathbb{N}) \text{ et } \forall p\ (a\ p \in T \Rightarrow p < l)) \Rightarrow$$

$$L_i^T\ (\underline{n}) \Rightarrow a\ (\varphi_i^T(\underline{n}) \in l)$$

Par (6) $L_i^T(\underline{n}) \Rightarrow a\ (\varphi_i^T(\underline{n}) \in T)$ et si on admet (6 bis) pour $\varphi_i^T(\underline{n}) \in \mathbb{N}$: $a\ \varphi_i^T(\underline{n}) \in \mathbb{N} \Rightarrow \exists p (a\ \varphi_i^T(\underline{n}) = p)$

Il reste à prouver :

$$\left[a\ (\varphi_i^T(\underline{n}) = p)\ \text{ et } \varphi_i^T(\underline{n}) \in T \text{ et } a\ (p \in T) \Rightarrow p < l\right] \Rightarrow a\ (\varphi_i^T(\underline{n}) \in l)$$

En résumé, (6 bis) pour $T \in E$ est vrai si T est N ou n, ou si aucun des E_k n'est N ou m; sinon, c'est en tout cas une

conséquence de (6 bis) pour $\varphi^T \in \mathbb{N}$ plus :

$$a(\varphi_i^T(\underline{n}) = \rho) \Rightarrow (a(\varphi_i^T(\underline{n}) \in T) \Leftrightarrow a(\rho \in T))$$
et $$a(\varphi_i^T(\underline{n}) = \rho) \Rightarrow (a(\varphi_i^T(\underline{n}) \in 1) \Leftrightarrow a(\rho \in 1))$$

Ces assertions sont des cas particuliers de (9) du type

(10) $$a(T = U) \Rightarrow (a(T \in X) \Leftrightarrow a(U \in X))$$

(6 bis) et (10) vont être prouvés par une récurrence simultanée: il suffit de prouvés que (10) pour (T,U,X) résulte de (6 bis) pour les $V \in K$ avec lg (V) $\leq$ (lgT,lgU,lgX) et de (10) pour les (T', U', X') avec $\sup(lgT', lgU', lgX') \leqslant \sup(lgT, lgU, lgX)$ et $lg(T') + lg(U') + lg(X') < lg(T) + lg(U) + lg(X)$. [lg : longueur]

Cas 1 : X est $X_1 \cup X_2$: trivial

Cas 2 : X est $\{V(\underline{n}) / \underline{n} \in \underline{\mathbb{N}}$ et R$\}$ a $(T \in X)$ est

$\exists \underline{m}$ (aR et $aT = V(\underline{n})$), ce qui ramène à prouver :
$a(T = U) \Rightarrow (a(T = V) \Leftrightarrow a(U = V))$. Il suffit de remarquer que $a(A \subset B)$ et $a(B \subset C) \Rightarrow a(A \subset C)$ résulte de (6bis) pour $\varphi^A \in B$ et (1o) pour $(\varphi^A, \varphi^B, C)$:
$(L_i^A(\underline{n})) \Rightarrow (\varphi_i^A(\underline{n}) \in B) \Rightarrow (\bigvee_j \exists \underline{m}\ (L_j^B(\underline{m})$ et $\varphi_i^A(\underline{n}) = \varphi_j^B(\underline{m}))$
pour cet m, $(L_j^B(\underline{m})) \Rightarrow (\varphi_j^B(\underline{m}) \in C) \Rightarrow (\varphi_i^A(\underline{n}) \in C)$

Cas 3 : X est $\mathbb{N}$ ou n. Comme démontré plus haut,
$a\ T = U \Rightarrow (a\ T \subset \mathbb{N} \Leftrightarrow a\ U \subset \mathbb{N})$ résulte de (6 bis) pour $\varphi^T \in V$, $\varphi^U \in T$ et (10) pour $(\varphi^T, \varphi^U, \mathbb{N})$; (10) est ici trivial pour T et U des types $\mathbb{N}$ ou n.
$a\ n \in T \Rightarrow \forall \exists \underline{1}(n = \varphi_i^T(\underline{1})$ et $L_i^T(\underline{1}))$ (6 bis pour $n \in$),
(10) pour $(n, \varphi_i^T(\underline{1}), U)$ fournit donc $a\ T \subset U \Rightarrow a\ n \in T \Rightarrow a\ n \in U$.
$a\ T = U \Rightarrow (a(n \in T) \Leftrightarrow a(n \in U))$ résulte donc de l'hypothèse de récurrence, et cela achève la démonstration de (6 bis).

On a vu au cours de la démonstration, ou on voit par les mêmes méthodes :

Corollaire : (10) $\underline{a\ T = U \quad (a\ T \in X \Leftrightarrow a\ U \in X)}$

(11) $\underline{a\ T = U \quad (a\ X \in T \Leftrightarrow a\ X \in U)}$

(12) $\underline{a\ T \subset U \Rightarrow \bigwedge \forall n\ (L_i^T(n) \Rightarrow \bigvee \exists\ m\ (L^U(m) \text{ et } a\ \varphi_i^T(n) = \varphi_i^U(m))}$

Preuve de (9) :

On prouvera (9) et (9bis) par une récurrence simultanée :

(9) $a\ T = U \Rightarrow (a(R(T)) \Leftrightarrow a(R(U)))$

(9bis) $a\ T = U \Rightarrow a(E(T) = E(U))$

Cas 1: R est combinaison logique de relation R_i, ou E est réunion de E_i : (9) (resp.(9bis)) pour (T,U,R) (resp (T, U, E)) résulte de (9) (resp (9bis)) pour les (T, U, R_i) (resp (T, U, E_i))

Cas 2: R est $\exists x \in E\ (S(x))$: a R (T) est $\bigvee_i \exists \underline{1}\ (L_i^{E(T)}(\underline{1})$ et a $S_T\ (\varphi_i^{E(T)}(\underline{1}))$: 1' équivalence, par (12), résulte de (9bis) pour (T,U,E) et (9) pour $(\varphi^{E(T)}, \varphi^{E(U)}, S_{\varphi}(\ ))$ et

$(T, U, S.(\varphi^{E(U)}))$ Idem pour $\forall$

Cas 3: R est S (X,Y,Z) d'interprétation
$aX \in \mathbb{N}$ et $a\ Y \in \mathbb{N}$ et $aZ \in \mathbb{N}$ et $\exists n, m, p\ (n + m = p$ et

$\forall 1 (a\ 1 \in X \Leftrightarrow 1 < n, a\ 1 \in Y \Leftrightarrow 1 < m, a\ 1 \in Z \Leftrightarrow 1 < p)$:

(9) pour R résulte de (9bis) pour

(T,U,X), (T,U,Y), (T,U,Z) car par (10) et (11)

$X(T) = X(U) \Rightarrow (a\ X(T) \in \mathbb{N} \Leftrightarrow a\ X(U) \in \mathbb{N})$ et
$(a1 \in X(T) \Leftrightarrow a\ 1 \in X(U))$
idem pour P

Cas 4 : R est $X \in Y$ a $X(T) \in Y(T) \Leftrightarrow$ a $X(U) \in Y(U)$ résulte de a $X(T) \in Y(T) \Leftrightarrow$ a $X(T) \in Y(U)$, et a $X(T) \in Y(U)$ a $X(U) \in Y(U)$, donc, par (10) et (11), (9) résulte ici de (9bis) pour (T, U, X) et (T, U, Y)

Cas 5 : E est $\{V(n) / n \in \mathbb{N}, R(n)\}$

(9 bis) pour E résulte de (9 bis) pour (T,U,V) et (9) pour (T,U,R).

Cas 6 : Désignons par t la variable de R ou E à laquelle on substitue T ou U. Si E est t ou si t ne figure pas dans R (resp E), l'assertion est triviale.

Que (9) et (9 bis) sont effectivement démontrés ainsi par récurrence se voit en faisant une première récurrence sur le nombre r attaché à $R(T) \Leftrightarrow R(U)$ (resp $r(E(T)) + r(E(U))$) et une seconde, si besoin est, sur la longueur.
Ceci termine la démonstration.

n° 8 La curée.

On a démontré :

métathéorème : La partie sensée de la théorie des ensembles affaiblie ($Ens._{\in}$), est équivalente à la partie sensée de l'arithmétique.

Un tel résultat n'est possible que parce que ($Ens._{\in}$), est une théorie très faible; rappelons que ses caractéristiques essentielles sont :

a) on n'admet pas d'axiome d'ensemble des parties.

b) les définitions par récurrence transfinie ne sont admises que pour définir une fonction prenant ses valeurs dans un ensemble fixé à l'avance.

Le mot "transfini" est d'ailleurs du bluff, car tous les ensembles qu'on peut définir sont "dénombrables", et de type fini au-dessus de N, et toutes les récurrences qu'on peut effectivement mener se réduisent à des récurrences usuelles (n°3 lemme)

Il est vraisemblable que le métathéorème est encore vrai pour une théorie un peu plus forte que $(\text{Ens.}f)_0$, où l'on puisse parler de l'ensemble des ensembles absolu ment finis nets et où tout ordinal strictement plus petit que ε_0 soit définissable.

ε_0 désigne le plus petit ordinal tel que $\omega^{\varepsilon_0} = \varepsilon_0$

Je n'ai pas sérieusement cherché à le démontrer, l'intérêt de ce perfectionnement me paraissant d'autant plus mince qu'on peut dans $(\text{Ens.}f)_0$, pour tout ordinal informel $\alpha < \varepsilon_0$, définir un ensemble ordonné $(E, \leqslant)$ de $(\text{Ens.}f)_0$ de cet ordinal et faire dessus de la récurrence transfinie; cela traduit simplement que la récurrence jusque $\alpha < \varepsilon_0$ est "arithmétique".

De façon intuitive, on peut considérer que $(\text{Ens.}f)_0$ est une théorie des ensembles "jusque ε_0", tandis que la théorie initiale est à peu près, si cela avait un sens, une théorie "jusque tout ordinal constructible".

Nulle part n'a été utilisé le caractère intuitioniste de $(\text{Ens.}f)_0$, et le métathéorème reste vrai dans sa variante classique, où l'axiome logique L_{10} est remplacé par L'_{10}.
Bien sûr, la pauvreté de $(\text{Ens.}f)_0$ paraît plus drastique encore dans ce cadre.

Le métathéorème permet d'utiliser librement en arithmétique un langage ensembliste élémentaire, ce qui évite contorsions ou scrupules éventuels en parlant en arithmétique formelle des divers corps de nombres, de passage au quotient par un idéal etc.

De façon plus substantielle, il fournit une démonstration rigoureuse du fait évident que les raisonnements d'analyse

prédicative (quand on aura bien défini ce que c'est) peuvent se traduire en arithmétique. cf. S. Feferman: systems of predicative analysis. Journal of Symbolic Logic. Vol 29 n°1 (1964)
Comme il semble vraisemblable que les théorèmes d'analyse complexe classique ont des équivalents en analyse prédicative (c'est là le problème difficile), on voit que les théorèmes de théorie analytique des nombres doivent être vrais en arithmétique formelle.

CHAPITRE III : L'analyse.

§ 1. La thèse de Church intuitionniste.

n° 1. Rappel sur les fonctions récursives.

Un algorithme est un "procédé mécanique" qui se met en branle quand on lui présente un entier explicite n, et qui s'il s'arrête, ce qui n'est pas exigé, fournit en réponse un entier $f(n)$; f est une fonction non partout définie $\mathbb{N} \longrightarrow \mathbb{N}$. C'est là une notion informelle. On peut donner diverses définitions formelles de la classe des fonctions "définissable par un algorithme"; ces définitions sont équivalentes entre elles, et la thèse de Church est qu'elles rendent parfaitement compte de l'intuition qu'on a de la notion d'algorithme.

Une des définitions possibles consiste à décrire un certain type de "machines" (les machines de Turing); qui chacunes calculent un algorithme; on peut les énumérer, et traduire en arithmétique l'assertion : "quand à la eième machine de Turing on présente un entier n, elle s'arrête après S stades et fournit en réponse l'entier m" , soit R(e, s, n, m). Ce qui précède peut être résumé en la

Scholie : On peut en arithmétique formelle intuitioniste construire un prédicat $\mathbb{R}$ (e, s, n, m) tel que :

a) $\mathbb{R}$ est effectivement décidable

b) $\forall e \forall n$ il existe au plus un couple (s,m) tel que $\mathbb{R}$

c) thèse de Church : pour toute fonction (informelle) f définie par un algorithme, il existe e tel que pour tout n, f est définie en n si et seulement si il existe s et m (explicite) pour lesquels $\mathbb{R}$ (e,s,n,m), m étant alors la valeur de f en n.

En fait, R sera définie par une succession de définitions par récurrence du type le plus simple ("récursions primitives"); en supplément de a) on aura $\vdash \forall e\, \forall s\, \forall n\, \forall m\, (R(e,s,n,m) \text{ ou } \neg R(e,s,n,m))$, et en supplément de b) on aura :
$\vdash \forall e\, \forall n\, \forall s\, \forall s'\, \forall m\, \forall m'\, (\ldots(e,s,n,m) \text{ et } R(e,s',n,m') \Rightarrow (s=s' \text{ et } m=m'))$.
c) est vraie dans tous les cas particuliers connus.

Cela permet en théorie des ensembles de définir des fonctions non nécessairement partout définies f_e , $\mathbb{N} \to \mathbb{N}$, de graphe $\{(n,m) \mid \exists s\ R(e,s,n,m)\}$. Ces fonctions sont les fonctions partiellement récursives, et celles qui sont partout définies seront appelées fonctions récursives; e est appelé un "nombre de Gödel" de f_e . On peut parler de l'ensemble de toutes les fonctions partiellement récursives, défini comme $\{f_e \mid e \in \mathbb{N}\}$

N°2. La thèse de Church intuitioniste.

En intuitionisme, une assertion du type $\forall x \in E\ \exists\ y \in F\ R(x,y)$ signifie qu'on dispose d'un procédé explicite qui, chaque fois qu'on se donne x et une démonstration de $x \in E$, fournit y, une démonstration de $y \in F$ et une de $R(x,y)$. Si pour E on a pris $\mathbb{N}$, on peut pour chaque entier explicité $n = o + 1 + \ldots + 1$ donner une démonstration type de $n \in \mathbb{N}$, et le procédé prédédent associe, à chaque entier explicité n, y et les démonstrations de $y \in E$ et $R(n,y)$. Si pour F aussi on a pris $\mathbb{N}$, la thèse de Church affirme que y doit être fonction récursive de n. D'où l'axiome

T.C. $\forall n \in \mathbb{N}\ \exists m \in \mathbb{N}\ R(n,m) \Rightarrow \exists\ e$ (e est le nombre de Gödel d'une fonction récursive et $\forall n \in \mathbb{N}\ R(n, f_e(n))$

On prendra garde avec plaisir que cet axiome est faux

classiquement. Kleene a donné dans (1) ch.XV §&2 une interprétation de l'arithmétique formelle intuitioniste augmentée de T.C.; en particulier ce sytème est cohérent (si l'arithmétique l'est). Les raisonnements du ch.II. § 4 s'appliquent encore à (Ens.f)$_o$ et à l'arithmétique tous deux augmentés de T.C., et (Ens.f.)$_o$ + T.C. est donc cohérent (si l'arithmétique l'est).

Application au principe de Mostowski.

Le principe suivant, dû à Mostowski, est sujet à caution, mais a des conséquences intéressantes :

P.M $(\forall n\ (S(n)$ ou $-S(n))$ et $-\forall n\ S(n)) \Rightarrow \exists n - S(n)$

De T.C. résulte que P.M. implique le principe apparemment plus fort

P.M! $(\forall n\ (R(n)$ ou $S(n))$ et $-\forall n\ R(n)) \Rightarrow \exists n\ S(n)$

Si en effet on applique T.C. à

(R(n) et m = o) ou (S(n) et m = 1), la première hypothèse de P.M! implique l'existence de e tel que

$f_e(n) = o$ ou 1, $f_e(n) = o \Rightarrow R(n)$, $f_e(n) = 1 \Rightarrow S(n)$. P.M. fournit alors $-\forall n\ f_e(n) = o \Rightarrow \exists n\ f_e(n) \neq o$

et pour un tel n, S(n), ce qui achève la démonstration.

Comme conséquence de P.M. citons déjà

proposition P.M. : $(\forall n\ (R(n)$ ou $-R(n)$ et $\forall n(S(n)$ ou $-S(n))) \Rightarrow$
$(\forall n\ R(n) \Rightarrow \exists m\ S(m)) \Rightarrow (-\forall n\ R(n)$ ou $\exists m\ S(m))$

Ici comme plus tard, le sigle P.M. mis après proposition, lemme etc. signifie qu'il est fait usage du pincipe de Mostowski.

$(\forall n\ R(n) \Rightarrow \exists m\ S(m)) \Rightarrow -\forall n\ (R(n)$ et $-S(n))$ donc (P.M.)

$\exists n$ $-R(n)$ et $-S(n)$), équivalent ici à $\exists n - R(n)$ ou $\exists m$ $S(m)$ qui implique $-\forall n$ $R(n)$ ou $\exists m$ $S(m)$.

P.M. signifie que la seule façon de montrer absurde une assertion $\forall n$ $S(n)$ avec S décidable est de donner un contre-exemple, ou encore, en termes incorrects, que si "en fait" pour tout n $S(n)$, on ne peut déduire aucune contradiction de l'hypothèse qu'on sache prouver $\forall$ n $S(n)$.

n° 3. Application à la construction d'ensembles.

Des raisonnements standarts permettent de déduire du métathéorème d'énumération (Ch II § 3) la

Scholie : Une assertion sensée est un théorème lorsqu'elle est impliquée par une conjonction d'assertions " Γ est une surjection d'une partie de N dans U_i" où les variables libres Γ sont distinctes entre elles et de toutes les variables libres apparaissant dans les termes U_i.

Tant qu'on ne s'intéresse qu'aux assertions sensées, on peut donc supposer dans les démonstrations que pour tout terme T on dispose d'un terme U qui soit une surjection d'une partie de N sur T, c'est ce qu'on fera.

Lemme : Soit Γ une surjection d'une partie de N dans E, et f une fonction de N dans E. Il existe e, nombre de Gödel d'une fonction récursive, tel que $f = \Gamma \circ f_e$

Par hypothèse, $\forall n \in N \; \exists m \in N \; (f(n) = \Gamma(m))$; l'assertion résulte de T.C.

Si est une surjection d'une partie de N sur E, cela permet de définir l'ensemble des applications de N dans E par Hom (N,E) = $\{\Gamma \circ f_e \}$ $e \in N$ et e est le nombre de Gödel d'une fonction récursvie prenant ses valeurs dans le domaine de définition de Γ }

Dès lors :

Proposition : il existe une équivalence limitée entre la théorie des ensembles et la théorie des ensembles à laquelle on a adjoint un signe primitif Hom(E,) avec l'axiome $T \in \mathrm{Hom}(N,E) \Leftrightarrow$ T est une fonction de N dans E

On ne précisera plus désormais si on travaille dans la théorie initiale ou augmentée ni si on fait usage de la scholie pour dénommer théorème des assertions dont toutes les conséquences sensées le sont.

Définition : un ensemble E est récursivement énumérable s'il existe une surjection de N sur E.

Lorsque E est récursivement énumérable, on peut définir Hom (E,F) pour tout ensemble F : si S est une surjection de N sur E, S identifiera en effet Hom (E,F) à une partie de Hom (N,F).

Théorème (axiome du choix intuitioniste)

Toute surjection $F \xrightarrow{S} G$ induit une surjection $\mathrm{Hom}(N,F) \xrightarrow{S}$ Hom (N,G)

Démonstration :

Soit Γ une surjection d'une partie de N sur F; $S \circ \Gamma$ est une

surjection d'une partie de $\mathbb{N}$ sur G, et d'après la lemme toute fonction $g : \mathbb{N} \longrightarrow G$ est du type $s \circ \Gamma \circ f_e$; $\Gamma \circ f_e : \mathbb{N} \longrightarrow F$, est un relèvement de g.

Ce théorème est peut-être plus parlant sous la forme équivalente :

Corollaire : Soit E_n une famille d'ensembles indexée par $\mathbb{N}$; si chaque E_n a au moins un élément, alors $\prod_{n \in \mathbb{N}} E_n$ a au moins un élément.

Bien sur, la morale de ce résultat est non point qu'on peut tirer des conséquences mirobolantes de ce que chaque E_n ait au moins un élément, mais au contraire que cette assertion sera difficile à prouver.
En outre, les propriétés spéciales de $\mathbb{N}$ jouent un rôle essentiel; on peut cependant remplacer $\mathbb{N}$ par un ensemble du type $\{n \mid n \in \mathbb{N} \text{ et } \exists p \in \mathbb{N}\ R(n,p)\}$ pour R décidable, i.e. tel que $\forall n\ \forall p\ (R(n,p) \text{ ou } \neg R(n,p))$: la somme de $\mathbb{N}$ et d'un tel ensemble est en bijection avec $\mathbb{N}$.

§ 2. Les nombres réels.

n° 1. Définition

On laisse au lecteur le soin de définir à sa guise l'ensemble $\mathbb{Z}$ des entiers rationnels et l'ensemble $\mathbb{Q}$ des nombres rationnels. Il existe des bijections entre ces ensembles et $\mathbb{N}$. Les résultats du § précédent permettent de recopier la construction de Cantor des nombres réels.

On appelle suite de Cauchy de nombres rationnels un élément (q_n) de Hom $(\mathbb{N}, \mathbb{Q})$ tel que $\forall n>0\ \exists m\ \forall r \geqslant m\ \forall s \geqslant m\ |q_r - q_s| \leqslant \frac{1}{n}$

et deux suites de Cauchy sont équivalentes si

$$\forall n>0\ \ \exists\ m\ \forall\ r \geqslant m\ \ |q_r - q'_r| \leqslant \frac{1}{n}$$

Définition : l'ensemble $\mathbb{R}$ des nombres réels est le quotient de l'ensemble des suites de Cauchy de nombres rationnels par l'équivalence définie plus haut.

On laisse au lecteur le soin de définir la somme, la différence et le produit de deux nombres réels.

Définition : deux nombres réels x,y sont nettement différents, en abrégé $x \# y$, s'il existe $q \in \mathbb{Q}$ strictement positif tel que $|x-y| \geqslant q$.

Par définition, la relation $x \leqslant y$ entre nombres réels signifie qu'il existe des suites q_n , q'_n de nombres rationnels tendant vers x et y telles que $q_n \leqslant q'_n$

$x \geqslant y$, $x<y$, $x>y$, $x \not< y$, $x \not> y$ signifient respectivement $y \leqslant x$, $x \leqslant y$ et $x \# y$, $y \prec x$, $x \leqslant y$ et $x \neq y$, $y \not< x$.

Si on admet le principe de Mostowski, la situation se simplifie car :

proposition P.M. $\forall x, y \in \mathbb{R}\ ,\ x \not\leqslant y \Leftrightarrow x \# y$

Par translation, il suffit de prouver $x \not\leqslant 0 \Rightarrow x \# 0$.

Soit $x = \lim q_n$ $(q_n \in \mathbb{Q})$; q_n est une suite de Cauchy,

i.e. $\forall n>0\ \exists m\ \forall m' \geqslant m\ (|q_m - q_{m'}| \leqslant \frac{1}{n}$

Appliquons T.C. : il existe une fonction récursive f telle que $\forall n > 0 \quad \forall m' > f(n) \quad (|q_{f(n)} - q_{m'}| \leqslant \frac{1}{n}$)

$x = o$ est alors équivalent à

$\forall n > o \; (|q_{f(n)}| \leqslant \frac{1}{n} \;)$ D'après P.M.

$x \neq o \Rightarrow \exists n > o \; (|q_{f(n)}| > \frac{1}{n})$, donc pour cet n

$x \geqslant |q_{f(n)} - \frac{1}{n}| > o$ et $x \neq o$.

Proposition : toute suite de Cauchy de nombres réels est convergente

Soit x_n de Cauchy; soit pour chaque n $q_n \in Q$ tel que $|x_n - q_n| < \frac{1}{n}$ (on applique ici le § 1 n° 3 Cor au Th). q_n est une suite de Cauchy de nombres rationnels et $\lim x_n = \lim q_n$.

On peut munir $\mathbb{R}$ d'une topologie (Ch I § 5) en prenant pour base d'ouverts les $]x, y[= \{ z \} \quad z \in \mathbb{R}$ et $x < z < y \}$ pour $x, y \in \mathbb{R}$.
Cela revient à prendre pour système fondamental de voisinage de chaque point x les $]x - q , x + q[$ pour q strictement positif dans Q.

Théorème (développement d'un nombre réel selon une base)
Soit b un entier $\geqslant 2$. Tout nombre réel $x \geqslant o$ peut s'écrire

$$x = \sum_{i \in \mathbb{Z}} c_i b^i \qquad \text{où}$$

a) les c_i sont des entiers, nuls pour i assez grand

b) $o \leqslant c_i \leqslant b$

c) c_i ne peut être égal à b que pour $i < o$, et si $c_{-i} = b$, alors $c_{-i-1} = o$

Les c_i sont les chiffres du développement; le grain de sel de ce théorème est qu'on admet qu'un chiffre soit égal à la base b !

Lemme : si $x \geqslant o$, il existe $n \in \mathbb{N}$ tel que $n \leqslant x < n + 1 + b^{-2}$

Soit q rationnel $\geqslant o$ tel que $|x - q| < \frac{1}{2} b^{-2}$ et soit $[q]$ la partie entière de q. On prend $n = o$ si $[q] = o$, $n = [q]$ si $q - [q] \geqslant \frac{1}{2} b^{-2}$, $n = [q] - 1$ dans les autres cas.

Le théorème se voit par une récurrence facile si $x \in \mathbb{N}$, auquel cas on peut prendre $c_i = o$ pour $i < o$.
Appliquons ce résultat au n dont le lemme garantit l'existence :

On est ramené à prouver que si $o \leqslant x < 1 + b^{-2}$, x a un développement avec $c_i = o$ pour $i \geqslant o$. Soit q_n une suite de rationnels telle que $o \leqslant q_n \leqslant x < q_n + b^{-n-2}$. Par récurrence, on pose, pour $i > o$, $c_{-i} = \sup (o, \; [(q_i - \sum_{j=o}^{i-1} c_{-j} b^{-j}) b^i])$.

$[\,]$ désigne la partie entière d'un rationnel.
On montre successivement par récurrence

a) $\sum_{i>o}^{n} c_{-i} b^i \leqslant x$

b) $x < \sum_{i>o}^{n} c_{-i} b^{-i} + b^{-n} + b^{-n-2}$ si $o \leqslant c_{-n} < b$

et $x < \sum_{i>o}^{n} c_{-i} b^{-i} + b^{-n-1}$ si $c_{-n} = b$

une de ces hypothèses étant vérifiée.
Dès lors, $x = \sum c_{-i} b^{-i}$ convient

On prendra garde à ce que

proposition : $\neg \forall x \in \mathbb{R} \; (x \geqslant o \text{ ou } x \leqslant o)$ et

$\neg \forall x \in \mathbb{R} \; (x = o \text{ ou } x \neq o)$

Soit S(n) décidable (i.e. $\forall n \in \mathbb{N} (S(n) \text{ ou } \neg S(n))$) et posons

$S_n = \begin{cases} o \text{ si} & \forall p \leqslant n \; \neg S(p) \quad \text{et sinon} \\ (-1)^p \frac{1}{p} & \text{où } p \text{ est le plus petit entier tel que } S \end{cases}$

s_n est une suite de Cauchy, soit s sa limite.

$s = o$ ou $s \neq o$ signifie $\forall p\, S(p)$ ou $-\forall p\ -S(p)$

$s \geqslant o$ ou $s \leqslant o$ signifie $\exists n\ S(n) \Rightarrow$ le plus petit p tel que S est pair ou

$\exists n\ S(n) \Rightarrow$ le plus petit p tel que S est impair

Si S dépend d'un second paramètre m, les assertions à montrer absurde entrainent respectivement

$\forall m\ (-\forall p\ -S(p,m)$ ou $\forall p\ -S(p,m))$

$\forall m\ (\exists q = o$ ou $1\ (\exists n\ S(nm) \Rightarrow$ le plus petit p tel que $S(p,m)$ est congru à $q \bmod 2)$

D'après T.C., ces assertions entraînent chacune l'existence d'une fonction récursive f telle que respectivement

$\forall m\ ((\forall p - S(p,m)) \Leftrightarrow f(m) = o)$

$\forall m\ (\exists n\ S(n,m) \Rightarrow$ le plus petit p tel que $S(p,m)$ est congru à $f(m) \bmod 2)$

Définition : une partie P de N est dite décidable si $\forall n \in N (n \in P$ ou $n \notin P)$, ou encore s'il existe une fonction $f : N \longrightarrow N$ (automatiquement récursive) valant o sur P et 1 sur le complémentaire.

Prenant pour S $m \notin A_p$, la première assertion signifie qu'une intersection dénombrable de parties décidables est décidable. Prenant pour $\exists_n S$ $\exists n$ pair tel que $m = f(\frac{n}{2})$ ou n impair tel que $m = g(\frac{n-1}{2})$, la seconde assertion signifie que si P et Q sont deux parties récursivement énumérables disjointes de N, il existe une partie décidable D de N telle que $P \subset D \subset \complement Q$; il suffit de donner un contre-exemple à cela, l'autre contre-exemple requis s'obtient en considérant $\complement Q$.

Lemme : Il existe deux parties récursivement énumérables disjointes P et Q de $\mathbb{N}$ telles que pour toute partie décidable D de $\mathbb{N}$, soit $D \cap P$, soit $\complement D \cap Q$ ait au moins un élément

Avec les notations du § 1 n° 1, soit P et Q les parties disjointes

$$P = \{e \mid \exists s \exists m \neq o \, \mathbb{R}(e,s,e,m)\}$$
$$Q = \{e \mid \exists s \; \mathbb{R}(e,s,e,o)\}$$

Si D est décidable, il existe qui soit nombre de Gödel de sa fonction caractéristique :

Si $e \in D$, $\exists s \, \mathbb{R}(e,s,e,1)$ et $e \in P$: $D \cap P$ a un élément
Si $e \notin D$ $\exists s \, \mathbb{R}(e,s,e,o)$ et $e \in Q$: $D \cap Q$ a un élément

Enfin P et Q sont non vides (car P (resp Q) contient tout nombre de Gödel de la fonction 1 (resp o)), donc récursivement énumérables en vertu du lemme :

Lemme : Si $\exists n \in \mathbb{N} \; \exists m \in \mathbb{N} \; S(n,m)$ et si $\forall n \in \mathbb{N} \, \forall m \in \mathbb{N}$ (Sou -S) alors $\{n \mid \exists m \in \mathbb{N} \; S(n,m)\}$ est récursivement énumérable.

On sait qu'un élément n_o appartient à l'ensemble ; comme surjection $\mathbb{N} \to \cdots$ il suffit de prendre le composé d'une surjection $\mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$ et de f défini par :

$$f(n,m) = \begin{cases} n_o \text{ si } \sim S(n,m) \\ n \text{ si } S(n,m) \end{cases}$$

N° 2. Théorème de continuité.

Dans un cadre essentiellement différent de celui-ci, Brouwers (2m) a "démontré" que toute fonction $[0,1] \to \mathbb{R}$ est uniformément continue. Il admettait une notion de nombre réel plus proche de la notion classique, de sorte que l'assertion "pour tout nombre réel x, S(x)" était beaucoup plus puissante que l'assertion, "pour toute suite récursive et convergente q_n de rationnels, S(lim q_n) ". Les deux étapes essentielles de sa démonstration étaient :

A) Se donner une fonction $f : (0,1) \to \mathbb{R}$, c'est se donner un procédé explicite qui a un nombre réel $x \in (0,1)$ associe $y \in \mathbb{R}$ (c'est le sens intuitioniste de $\forall x \exists y\ f(x) = y$. Utilisant les développements décimaux, on voit encore qu'il faut à toute suite de chiffres c_i $(0 \leq c_i \leq 10, i > 0)$ et tout n associer un rationnel q tel que $|y - q| < 10^{-n}$

Les nombres rationnels étant paramétrés par $\mathbb{N}$, le problème de Brouwers était d'étudier les assertions du type
$\forall c \in Hom(\mathbb{N}, [0,10])\ \exists q \in \mathbb{N}\ S(c,q)$

Dans son cadre, il était raisonnable d'admettre que la seule façon d'associer à une suite c_i un entier q était de se donner des lois $F_n(c_1 \cdots c_n)$ $(n \in \mathbb{N})$ qui a certaines suites $c_1 \ldots c_n$ associent un entier, de façon que

1) si $F_n(c_1 \cdots c_n) = q$, $F_{n+k}(c_1 \cdots c_n \cdots c_{n+k}) = q$ (en particulier est défini)
2) pour toute suite c, il existe n tel que $F_n(c_1 \cdots c_n)$ soit défini.

Cela signifiait qu'un calcul explicite ne peut tenir compte que d'un nombre fini d'objets, ce nombre ne devant toutefois pas être fixé à priori.

Considérant les suites $c_1 \ldots c_n$ où F est définie, on voit que le théorème résulte de (B).

B) Si P est un ensembles de suites finies $(c_1 \ldots c_n)$ $(n \in \mathbb{N}, c_i \in [0,10]$

et si (1) $(c_1 \ldots c_n) \in P \Rightarrow (c_1 \ldots c_{n+k}) \in P$

(2) pour toute suite infinie c_i, $\exists n$ tel que

$(c_1 \ldots c_n) \in P$

Alors il existe l tel que pour toute suite $c_1 \ldots c_l$, on a

$(c_1 \ldots c_l) \in P$ (Principe de Brouwers)

Ce principe est vrai classiquement, et était raisonnable du point de vue de Brouwers. Ici, il est faux, ainsi que Kleene l'a fait remarquer.

Ceci explique pourquoi je n'ai pas été capable de démontrer le théorème de continuité sous la forme forte rappelée au début de ce numéro.

J'obtiens cependant un résultat partiel, en perfectionnant et formalisant les premières méthodes utilisées par Brouwers (voir (2m))

Lemme 1: Si une partie décidable P de N est telle que pour toute partie décidable Q de N, on ait $P \subset Q$ ou $\neg(P \subset Q)$, alors il existe $m \in \mathbb{N}$ tel que P ait au plus m éléments.

L'hypothèse est que pour toute assertion décidable S(p,m) pouvant dépendre d'un paramètre n, l'assertion $\forall p \in P\ (S(p,n))$ est décidable, et l'idée de la démonstration est de tirer le maximum de l'argument diagonal qui prouve que l'intersection d'une suite de parties décidables n'est plus toujours décidable.

Prenons pour S(p,m) l'assertion :

" $\neg\, \mathbb{R}(n,m,n,1)$, où m est le nombre d'éléments de P plus petits que p " (cf. page 62 , Scholie)

Soit e un nombre de Gödel de la fonction caractéristique de l'ensemble D des n tels que $\forall p\ S(p,n)$.
Si $e \in D$, d'une part, pour un certain m, $\mathbb{R}(e,m,e,1)$ et d'autre part, $\forall p \in P$ (p est le $m+1$-ième élément de $P \Rightarrow$ $\neg \mathbb{R}(e,m,e,1)$), donc P n'a pas de $m+1$-ième élément.
Si $e \notin D$, pour tout m $\neg \mathbb{R}(e,m,e,1)$, donc à fortiori $\forall p \in P\ S(p,e)$ ce qui est absurde (signifie $e \in D$).

Il en résulte bien que P n'a pas de $m+1$ ième élément pour un certain m.

Lemme 2 : Si f est une fonction $\mathbb{R} \to \mathbb{R}$, si x_n est une suite d'éléments de $\mathbb{R}$ convergeant vers x, et si de plus $f(x)$ et les $f(x_n)$, sont rationnels, alors pour tout $\varepsilon > 0$ existe m tel que l'ensemble des n où $|f(x_n) - f(x)| \geqslant \varepsilon$ ait au plus m éléments.

On ne restreint pas la généralité en supposant ε rationnel; l'ensemble P des n où $|f(x_n) - f(x)| \geqslant \varepsilon$ est alors décidable, et il suffit de prouver qu'il satisfait l'hypothèse du lemme 1. Soit donc Q décidable dans $\mathbb{N}$; remplaçant Q par $P \cap Q$, on peut supposer $Q \subset P$ puisque $P \subset Q \Leftrightarrow P \subset P \cap Q$. Posons alors

$y_n = x$ si $[0,n] \cap P \subset [0,n] \cap Q$

$y_n = x_p$ si $[0,n] \cap P \not\subset [0,n] \cap Q$ et si p est le plus petit élément de $P \setminus Q$.

y_n est une suite de Cauchy, car si pour $p \geqslant N$ $|x_p - x| < \eta$, alors pour $p,q \geqslant N$, $|y_p - y_q| < \eta$. Soit $y = \lim y_n$; $f(y)$, comme tout nombre réel, peut être approché d'aussi près qu'on veut par des rationnels, donc soit $f(y) \neq f(x)$ soit $|f(y) - f(x)| < \varepsilon$. Si $f(x) \neq f(y)$, $x \neq y$ et donc il est absurde de supposer $P \subset Q$. Au contraire, si $|f(y) - f(x)| < \varepsilon$ et $p \in P$, il est absurde de supposer $p \notin P$ car on aurait alors $y = x_q$ pour un $q \in P (q < p)$, donc $|f(y) - f(x)| \geqslant \varepsilon$

Q étant décidable, on trouve donc que

$\neg(P \subset Q)$ ou $\forall p \in P (p \in Q)$ i.e. $P \subset Q$ ou $\neg(P \subset Q)$

Théorème : *Si f est une fonction $\mathbb{R} \to \mathbb{R}$ et si $\lim x_n = x$, alors $\lim f(x_n) = f(x)$*

On ne restreint pas la généralité en supposant $f(x) = 0$
Remarquons tout d'abord que si $\lim x_n = x$, il existe une fonction continue $\eta : \mathbb{R} \to \mathbb{R}$ telle que $\eta(1/n) = x_n$ et $\eta(0) = x$. Il suffit de définir η par interpolation linéaire. On sait que $\forall n \exists q_n \in Q \ (|f(x_n) - q_n| < 1/n)$

D'après T.C. et l'argument précédent, il existe $h : \mathbb{R} \to \mathbb{R}$ tel que $h(1/n) = q_n - f(x_n)$ et $h(0) = 0$. Prenant $f_1 = h + f \circ \eta$, on voit qu'il existe f_1 satisfaisant

(1) $f_1(0) = 0$, $f_1(1/n) \in Q$

(2) $|f_1(1/n) - f(x_n)| < 1/n$ $f_1(0) = f(0) = 0$.

Une première conclusion est que le lemme 2 est valable sans supposer $f(x)$ et les $f(x_n)$ rationnels, et qu'il suffit de démontrer le Th. pour f satisfaisant aux hypothèses du lemme 2, dont on reprend les notations.
On a soit $|f(y) - f(x)| < \varepsilon$, auquel cas $P \subset Q$, soit $|f(y) - f(x)| > \frac{\varepsilon}{2}$. Puisque $y = \lim y_n$, il existe au plus m valeurs de n pour lesquelles $|f(y) - f(y_n)| > \frac{\varepsilon}{2}$; on ne peut donc avoir $(0, m+1) \cap P \subset (0, m+1) \cap Q$, qui impliquerait $f(y_m) = f(x)$ pour $n \leqslant m+1$ et $|f(y) - f(y_m)| > \frac{\varepsilon}{2}$ pour m + 1 valeur de n au moins. Le résultat obtenu est un peu meilleur que l'hypothèse du lemme 1 :

Si $f(x)$, les $f(x_n)$ et ε sont rationnels, l'ensemble P des p tels que $|f(x_p) - f(x)| \geqslant \varepsilon$ est décidable, et pour toute partie décidable Q, soit $P \subset Q$, soit il existe un élément dans $P \setminus Q$.

On va en déduire que P est borné, ce qui achèvera la démonstration du théorème. On procède par récurrence sur l'entier m que,

dans le lemme 2, on a montré exister.
Si $m = o$, $P = \emptyset$. Si $m > o$, soit $P \subset \emptyset$, donc $P = \emptyset$, soit $\exists p \in P$ et $P = \{p\} \cup P \setminus \{(\}$) où $P \setminus \{p\}$ satisfait à l'hypothèse pour m-1, donc est borné.

Corollaire : Deux fonctions $\mathbb{R} \to \mathbb{R}$ coïncidant sur $\mathbb{Q}$ sont égales.

On peut maintenant définir l'ensemble des fonction de $\mathbb{R}$ dans $\mathbb{R}$. $\mathbb{Q}$ étant en bijection avec $\mathbb{N}$, on peut définir Hom $(\mathbb{Q}, \mathbb{R})$; à chaque $f : \mathbb{Q} \to \mathbb{R}$, on associe $\tilde{f}$, défini en $x \in \mathbb{R}$ si chaque fois que $\lim q_n = x$, $\tilde{f}(q_n)$ converge, $\tilde{f}(x)$ étant une limite (indépendante de la suite q_n choisie).

Définition : $\mathrm{Hom}(\mathbb{R}, \mathbb{R}) = \{f \mid f \in \mathrm{Hom}(\mathbb{Q}, \mathbb{R})$ et $\tilde{f}$ partout défini$\}$

Il est facile de montrer que toute fonction $f : \mathbb{R} \to \mathbb{R}$ est somme d'une fonction f_1 uniformément continue et d'une fonction f_2 telle que $f_2(\mathbb{Q}) \subset \mathbb{Q}$. Pour prouver que toute fonction $[o,1] \to \mathbb{R}$ est uniformément continue, il suffirait donc de prouver que toute fonction (récursive) $[o,1] \cap \mathbb{Q} \longrightarrow \mathbb{Q}$ qui se prolonge par continuité à $[o,1] \longrightarrow \mathbb{R}$ est uniformément continue. Bien que ce problème semble très explicite, je n'ai pas été capable de le résoudre, ni même de prouver la fonction bornée.

BIBLIOGRAPHIE.

Bourbaki N . (1) Théorie des ensembles . Chap. 1 et 2 . Act.Sc.et Ind. 1212 Hermann 1954.

Brouwers L.E.J. (1) De onbetrouwbaarheid der logische principes Tijdschrift voor wijsbegeerte vol.2 (1908) pg.152 - 158.

(2) Zur Begründung der intuitionistischen Mathematik
I. Math. Ann.93 (1924) pg. 244 - 258
II.Math. Ann.95 (1925) pg. 453 - 473
III.Math.Ann.96 (1926) pg. 451 - 489

Heyting A. (1) Die formalen Regeln der intuitionistischen Logik.Sitzungberichte der Preussischen Akademie der Wissenschaften -Physikalisch - mathematische Klasse (1930) pg 42 -56

(2) Die formale Regeln der intuitionistischen Mathematik
Ibid. p.57 - 71, 158 - 169 .

(3) Intuitionism, an introduction. Noord-Holl. Uitg.mij. Amsterdam 1956

Kleene S.C. (1) Introduction to métamathematics. Noord. Holl. Publ.Co. Amsterdam 1952

Kleene S.C. and Vesley R.E. (2) The foundations of intuitionistic mathematics Noord.Holl. Uitg.Mij. Amsterdam 1965

Mc Kinsey (1) Proof of the independence of the primitive symbols of Heytings's calculus of proposition Jour.symb.logic vol.4 p.155 - 158.

Table des matières.