

1. Un séquent se présente sous la forme  $\Gamma \vdash B$  où  $\Gamma$  est une liste d'énoncés et de déclaration de variables libres avec leur type et où  $B$  est un énoncé, toute les variables libres étant déclarées à gauche de  $\vdash$ . On écrira aussi  $[\Gamma \vdash B]$  pour distinguer le séquent du reste du texte. Le séquent  $\Gamma \vdash B$  se lit “dans le contexte  $\Gamma$ ,  $B$  est vrai” ou “ Sous les hypothèses données par  $\Gamma$ ,  $B$  est vrai”. Le séquent  $\vdash B$  ( $\Gamma$  est vide) se lit “On a  $B$ ”. Le séquent  $\Gamma \vdash (B \text{ est absent})$  se lit “la liste des énoncés de  $\Gamma$  est contradictoire”

L'écriture

$$\frac{\Gamma_1 \vdash B_1 \quad \Gamma_2 \vdash B_2 \quad \dots}{\Gamma'_1 \vdash B'_1 \quad \dots}$$

signifie qu'on peut passer de la liste de séquents en haut à la liste de séquents en bas par application d'une ou plusieurs règles du calcul des séquents (voir plus bas). L'application successive des règles constitue le calcul des séquents.

On déclare des axiomes ou on rappelle des théorèmes sans leurs preuves par les séquents  $\Gamma \vdash B$  correspondants. Ils induisent des règles de la forme  $\frac{}{\Gamma \vdash B}$ . Un calcul partant des axiomes et théorèmes et aboutissant à  $\Gamma' \vdash B'$  établit  $\Gamma' \vdash B'$  comme nouveau théorème. Un calcul aboutissant à  $\vdash B$  est une preuve de  $B$  : il établit la valeur de vérité  $B \equiv \text{Vrai}$ . Un calcul aboutissant à  $\Gamma \vdash$  est une preuve par l'absurde : il établit que  $\Gamma$  est contradictoire. Si  $\Gamma$  est la liste des énoncés  $A_1, A_2, \dots, A_n$  le calcul établit la valeur de vérité  $(A_1 \text{ et } A_2 \text{ et } \dots \text{ et } A_n) \equiv \text{Faux}$ .

Les règles du calcul des séquents ont deux roles : elles précisent ce que sont les règles de déduction donc ce qu'on admet comme preuve (il y a d'ailleurs plusieurs jeux de règles présents dans la littérature correspondant à des logiques différentes : logique classique pour ce cours, logique intuitionniste,...) ; elles permettent d'établir la valeur de vérité d'un énoncé commençant par un quantificateur  $\forall, \exists$  ce que ne permettent pas les tables de vérité.

## 2. Lien avec les tables de vérité

Les connecteurs logiques  $\neg, \text{et}, \text{ou}, \Rightarrow, \Leftrightarrow$  ont leur table de vérité et relations habituelles. Par exemple  $A \equiv \neg\neg A$  ( $A$  et  $\neg\neg A$  ont même valeurs de vérité d'après la table de vérité de  $\neg$ , quel que soit le contenu de  $A$ ),  $(A \Rightarrow B) \equiv (\neg A \text{ ou } B)$ ,  $(A \text{ et } A \Rightarrow B) \equiv (A \text{ et } B)$ .

On ajoute le lien entre les quantificateurs et la négation :  $\neg(\forall x : \mathcal{T}, P(x)) \equiv (\exists x : \mathcal{T}, \neg P(x))$  où  $\mathcal{T}$  est un type (le type ensemble par exemple) et  $P(x)$  est un énoncé dépendant de  $x : \mathcal{T}$ .

La première règle ci-dessous avec à gauche son nom ( $\vdash V$ ) dit qu'on a  $\Gamma \vdash A$  si on sait  $A \equiv \text{Vrai}$  ; la deuxième (id) dit qu'on a toujours  $\Gamma, A \vdash A$  :

$$(\vdash V) \quad \frac{}{\Gamma \vdash A} \quad (\text{id}) \quad \frac{}{\Gamma, A \vdash A}$$

( $\Gamma$  peut être vide).

## 3. Quelques règles avec à gauche leur nom.

La liste que nous donnons n'est pas minimale : certaines règles se déduisent des autres. Les premières règles sont réversibles : l'écriture obtenue en échangeant le haut et le bas est aussi une règle.

Lorsqu'un énoncé d'un séquent fait intervenir une variable liée (par un quantificateur ou une construction), celle-ci ne doit pas être une variable libre dans le reste du séquent. On évite le conflit de notation en renommant au besoin les variables liées.

$$\begin{array}{lll} (\vdash \text{et}) \quad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \text{ et } B} & (\vdash \Rightarrow) \quad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} & (\vdash \text{ou}) \quad \frac{\Gamma, \neg A \vdash B}{\Gamma \vdash A \text{ ou } B} \\ (\vdash \neg) \quad \frac{\Gamma, A, B \vdash}{\Gamma, A \vdash \neg B} & (\text{et } \vdash) \quad \frac{\Gamma, A, B \vdash C}{\Gamma, A \text{ et } B \vdash C} & (\text{ou } \vdash) \quad \frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \text{ ou } B \vdash C} \end{array}$$

<sup>1</sup>Version du 6 avril 2014

$(\exists \vdash) \frac{\Gamma, (\exists x : \mathcal{T}, P(x)) \vdash B}{\Gamma, x : \mathcal{T}, P(x) \vdash B}$  où  $x$  est une variable (de type  $\mathcal{T}$ ) n'apparaissant pas dans  $\Gamma$  et  $B$  et où  $P(x)$  est un énoncé dépendant de  $x$ .

$(\vdash \forall) \frac{\Gamma, x : \mathcal{T} \vdash P(x)}{\Gamma \vdash (\forall x, P(x))}$  où  $x$  est une variable (de type  $\mathcal{T}$ ) n'apparaissant pas dans  $\Gamma$  et où  $P(x)$  est un énoncé dépendant de  $x$ .

Voici maintenant quelques règles non réversibles :

Affaiblissement à droite  $(ad) \frac{\Gamma \vdash A}{\Gamma \vdash A \text{ ou } B}$ .

Affaiblissement à gauche  $(ag) \frac{\Gamma \vdash B}{\Gamma, A \vdash B}$

Réécritures  $(\Leftrightarrow \vdash) \frac{\Gamma \vdash A \Leftrightarrow B \quad \Gamma, A \vdash C}{\Gamma, B \vdash C} \quad (\vdash \Leftrightarrow) \frac{\Gamma \vdash A \Leftrightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}$

$(\Leftrightarrow \forall) \frac{\Gamma \vdash \forall x : \mathcal{T}, (P(x) \Leftrightarrow Q(x))}{\Gamma \vdash (\forall x : \mathcal{T}, P(x)) \Leftrightarrow (\forall x : \mathcal{T}, Q(x))} \quad (\Leftrightarrow \exists) \frac{\Gamma \vdash \forall x : \mathcal{T}, (P(x) \Leftrightarrow Q(x))}{\Gamma \vdash (\exists x : \mathcal{T}, P(x)) \Leftrightarrow (\exists x : \mathcal{T}, Q(x))}$

Cas particulier à gauche  $(\forall \vdash) \frac{\Gamma, P(t) \vdash B}{\Gamma, (\forall x : \mathcal{T}, P(x)) \vdash B}$  où  $x$  est une variable (de type  $\mathcal{T}$ ) n'apparaissant pas dans  $\Gamma$  et  $B, P$  est un énoncé dépendant de  $x$  et  $t$  est un objet de type  $\mathcal{T}$  donné par une formule faisant intervenir les variables libres de  $\Gamma$  ou les constantes. On peut préciser la valeur prise pour  $x$  en nommant la règle  $(\forall \vdash)[x := t]$ .

Exhiber à droite  $(\vdash \exists) \frac{\Gamma \vdash P(t)}{\Gamma \vdash (\exists x : \mathcal{T}, P(x))}$  où  $x$  est une variable (de type  $\mathcal{T}$ ) n'apparaissant pas dans  $\Gamma$ ,  $P$  est un énoncé dépendant de  $x$  et  $t$  est un objet de type  $\mathcal{T}$  donné par une formule faisant intervenir les variables libres de  $\Gamma$  ou les constantes. On peut préciser la valeur prise pour  $x$  en nommant la règle  $(\vdash \exists)[x := t]$ .

4. Premiers objets : ensembles, entiers et les règles associées.

Axiome associé à la relation d'égalité :  $(=) [x, y : \mathcal{T}, x = y, P(x) \vdash P(y)]$  où  $P(x)$  est un énoncé dépendant d'une variable libre  $x$  de type  $\mathcal{T}$ . Cet axiome semble aller de soi mais il vaut mieux l'explicitier.

Quelques axiomes de la théorie des ensembles (axiomatique de Zermelo). On écrit ici chaque axiome par le séquent  $\Gamma \vdash B$  correspondant plutôt que par l'écriture  $\overline{\Gamma \vdash B}$ .

$(\in) [A, B : \mathcal{E}ns, (\forall x : \mathcal{E}ns, (x \in A \Leftrightarrow x \in B)) \vdash A = B]$ . Le séquent  $[A, B : \mathcal{E}ns, A = B \vdash \forall x, (x \in A \Leftrightarrow x \in B)]$  se déduit de la règle  $(=)$ .

$(\{a, b\}) [a, b : \mathcal{E}ns \vdash \exists X : \mathcal{E}ns, \forall x : \mathcal{E}ns, (x \in X \Leftrightarrow (x = a \text{ ou } x = b))]$

...

$(\{x \in X, P(x)\}) [X : \mathcal{E}ns \vdash \exists E : \mathcal{E}ns, \forall x : \mathcal{E}ns, x \in E \Leftrightarrow (x \in X \text{ et } P(x))]$  où  $P(x)$  est un énoncé dépendant de  $x$  dont  $E$  n'est pas une variable.

Pour  $X$  un ensemble d'objets de type  $\mathcal{T}$  et  $P(x)$  un énoncé dépendant de  $x : \mathcal{T}$ , on écrit  $(\exists x \in X, P(x))$  pour  $(\exists x : \mathcal{T}, (x \in X \text{ et } P(x)))$ . On écrit  $(\forall x \in X, P(x))$  pour  $(\forall x : \mathcal{T}, (x \in X \Rightarrow P(x)))$ .

On dispose des deux "théorèmes" suivants, où  $X \setminus \{x_0\}$  désigne l'ensemble  $\{x \in X, x \neq x_0\}$  et où  $P(x)$  est un énoncé dépendant de la variable  $x$  :

$(x_0 \exists) [X : \mathcal{E}ns, x_0 : X \vdash (\exists x \in X, P(x)) \Leftrightarrow (P(x_0) \text{ ou } \exists x \in X \setminus \{x_0\}, P(x))]$

$(x_0 \forall) [X : \mathcal{E}ns, x_0 : X \vdash (\forall x \in X, P(x)) \Leftrightarrow (P(x_0) \text{ et } \forall x \in X \setminus \{x_0\}, P(x))]$

Type entier et récurrence. On a la règle :

(rec)  $\frac{\Gamma \vdash P(0) \quad \Gamma, n : \mathbb{N}, P(n) \vdash P(n+1)}{\Gamma \vdash \forall n : \mathbb{N}, P(n)}$ , où  $P(n)$  est un énoncé dépendant de l'entier  $n$ .

Exercice : Dédurre de (rec) et de la théorie des ensembles une preuve du séquent

$$[E : \mathcal{P}(N), 0 \in E, (\forall n : \mathbb{N}, (n \in E \Rightarrow n+1 \in E))] \vdash E = \mathbb{N}$$

## 5. Preuves

### 5.1. Quelques Stratégies de Preuve

Ce sont des règles qu'on utilise habituellement pour établir le séquent en bas à partir du ou des séquent en haut. Ces règles se déduisent des règles de la section précédente. Voici les plus usuelles :

– Réécritures ( $\Leftrightarrow \vdash$ ), ( $\vdash \Leftrightarrow$ ), ( $\Leftrightarrow \forall$ ), ( $\Leftrightarrow \exists$ ). Ce sont ces règles qu'on utilise pour traduire un énoncé informel en un énoncé formalisé, pour faire apparaître la définition d'un terme, pour remplacer une définition par une définition équivalente.

– Réduction du séquent à prouver à un ou des séquents plus lisible par application des règles réversibles ( $\vdash \forall$ ), ( $\vdash \Rightarrow$ ), etc.

– Modus Ponens (mp)  $\frac{\Gamma \vdash A \quad \Gamma, A \vdash B}{\Gamma \vdash B}$ . Par affaiblissement à gauche on a aussi  $\frac{\Gamma \vdash A \quad \Gamma', A \vdash B}{\Gamma, \Gamma' \vdash B}$

Lorsque l'énoncé  $A$  n'est pas issu directement de  $\Gamma$  mais est issu de l'imagination de celui qui prouve, on appellera cette stratégie "Observer  $A$ " ou encore "Invoquer  $A$ " si  $\Gamma \vdash A$  est un théorème.

– Distinguer suivant  $H$  (H)  $\frac{\Gamma, H \vdash B \quad \Gamma, \neg H \vdash B}{\Gamma \vdash B}$ . Plus généralement on peut distinguer suivant  $H_1, H_2, \dots, H_n$  si  $(H_1 \text{ ou } \dots \text{ ou } H_n) \equiv V$  :

$$(H_i \vdash) \frac{\Gamma \vdash (H_1 \text{ ou } \dots \text{ ou } H_n) \quad \Gamma, H_1 \vdash B \quad \dots \quad \Gamma, H_n \vdash B}{\Gamma \vdash B}$$

– Séquent plus fort : remplacer le séquent à prouver  $\Gamma \vdash B$  par un séquent  $\Gamma' \vdash B'$  lorsqu'on sait établir la règle  $\frac{\Gamma' \vdash B'}{\Gamma \vdash B}$ . C'est ce qu'on fait notamment avec les règles (ad), (ag), ( $\forall \vdash$ ), ( $\vdash \exists$ ).

– Preuve par l'absurde de  $\Gamma \vdash B$  en prouvant que  $\Gamma, \neg B$  est contradictoire :  $\frac{\Gamma, \neg B \vdash \perp}{\Gamma \vdash B}$ .

– Preuve par récurrence d'un séquent  $[\Gamma \vdash \forall n : \mathbb{N}, P(n)]$ .

La plupart de ces stratégies (réécritures, observer  $A$ , distinguer suivant  $H$ , séquent plus fort) font intervenir un ou des énoncés auxiliaires ad hoc qui ne sont pas issus du séquent à prouver ; c'est ce qui rend les preuves difficiles : le choix d'une telle stratégie n'a rien d'automatique.

Voici pour l'exemple l'établissement de la règle (mp) puis de la règle "Distinguer suivant  $H$ " :

$$\frac{\frac{\frac{\Gamma, A \vdash B}{\Gamma \vdash A \text{ et } (A \Rightarrow B)}{(\vdash \Rightarrow)} \quad \frac{\Gamma \vdash A \text{ et } (A \Rightarrow B)}{\Gamma \vdash A \text{ et } B} (\vdash \text{ et})}{\Gamma \vdash A \text{ et } B} (\vdash \Leftrightarrow) \quad \frac{\Gamma \vdash A \text{ et } B}{\Gamma \vdash A \quad \Gamma \vdash B} (\text{oubl})}{\Gamma \vdash B} (\text{oubl})$$

$$\frac{\frac{\Gamma \vdash H \text{ ou } \neg H}{} (\vdash V) \quad \frac{\Gamma, H \vdash B \quad \Gamma, \neg H \vdash B}{\Gamma, H \text{ ou } \neg H \vdash B} (\text{ou } \vdash)}{\Gamma \vdash B} (\text{mp})$$

Exercices : établir les règles suivantes. Sont elles réversibles ?

$$\frac{}{\Gamma, A, A \Rightarrow B \vdash B} \quad \frac{}{\Gamma, A, A \Rightarrow B \vdash C}$$

## 5.2. Organisation d'une preuve

On écrit le plus souvent une preuve en partant du séquent à prouver et en écrivant les règles (les stratégies de preuve) à l'envers : le séquent du haut se déduit du ou des séquents du bas. L'application successive des stratégies ramène le séquent à prouver à une liste de séquents qu'on sait vrai (les axiomes, les séquents déjà prouvés, le séquent vide).

La preuve d'un séquent n'est pas unique et peut être plus ou moins fastidieuse suivant le choix plus ou moins heureux des stratégies. Il n'est par exemple pas toujours heureux de remplacer un terme par sa définition, etc.

**5.3.** Un exemple : preuve de l'énoncé "Toute partie non vide de  $\mathbb{N}$  admet un plus petit élément" suivant les indications de l'exercice 1 de la feuille de TD 5.

Soit  $S$  une partie non vide de  $\mathbb{N}$ . On note :

–  $H(n)$  l'énoncé " $S$  contient un entier inférieur ou égal à  $n$ " ;  $H(n)$  se formalise comme  $(\exists k : \mathbb{N}, k \in S \text{ et } k \leq n)$

–  $C$  l'énoncé " $S$  admet un plus petit élément" ;  $C$  se formalise partiellement comme  $(\exists n : \mathbb{N}, n \in S \text{ et } n \text{ minore } S)$

On a les équivalences

$$\neg H(n) \Leftrightarrow (\forall k : \mathbb{N}, k \in S \Rightarrow k > n) \Leftrightarrow (\forall k : \mathbb{N}, k \in S \Rightarrow k \geq n + 1) \Leftrightarrow (n + 1 \text{ minore } S)$$

L'exercice 1 de la feuille 5 suggère de montrer par récurrence sur  $n$  l'implication  $H(n) \Rightarrow C$ , ce que nous faisons :

$$\frac{\frac{S : \mathcal{P}(\mathbb{N}) \vdash \forall n : \mathbb{N}, (H(n) \Rightarrow C)}{S : \mathcal{P}(\mathbb{N}) \vdash H(0) \Rightarrow C} (\text{t} \Rightarrow) \quad \frac{S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, H(n) \Rightarrow C \vdash H(n+1) \Rightarrow C}{S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, \neg H(n) \text{ ou } C, H(n+1) \vdash C} (\text{rec})}{\frac{S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, \neg H(n), H(n+1) \vdash C}{S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, C, H(n+1) \vdash C} (\text{ou t})} (\text{t} \Leftrightarrow)}$$

On continue (on écrira — à la place de la répétition des déclarations de variables du séquent du dessus) :

$$\frac{\frac{\frac{S : \mathcal{P}(\mathbb{N}), H(0) \vdash C}{\neg, H(0) \vdash 0 \in S \text{ et } 0 \text{ minore } S} (\text{t} \Leftrightarrow)}{\neg, H(0) \vdash 0 \in S} (\text{t} \text{ et})}{\frac{\frac{\frac{\frac{\neg, k : \mathbb{N}, k \in S, k \leq 0 \vdash 0 \in S}{\neg, k \in S, k = 0 \vdash 0 \in S}}{\neg, k : \mathbb{N}, k \in S, k \leq 0 \vdash 0 \in S} (\text{t} \vee)}{\neg, H(0) \vdash 0 \text{ minore } S} (\text{t} \vee)}{\neg, k : \mathbb{N}, k \in S, k \leq 0 \vdash 0 \in S} (\text{t} \vee)}$$

et

$$\frac{\frac{\frac{S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, \neg H(n), H(n+1) \vdash C}{\neg, \neg H(n), H(n+1) \vdash n+1 \in S \text{ et } n+1 \text{ minore } S}}{\neg, \neg H(n), H(n+1) \vdash n+1 \in S} (\text{t} \vee)}{\frac{\neg, \neg H(n), H(n+1) \vdash n+1 \text{ minore } S}{\neg, \neg H(n), H(n+1) \vdash \neg H(n)} (\text{t} \vee)}$$

On continue encore.

$$\frac{\frac{\frac{\frac{S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, \neg H(n), H(n+1) \vdash n+1 \in S}{\neg, (\forall k : \mathbb{N}, (k \in S \Rightarrow k \geq n+1)), (\exists k : \mathbb{N}, (k \in S \text{ et } k \leq n+1)) \vdash n+1 \in S} (\text{t} \vee)}{\neg, l : \mathbb{N}, (\forall k : \mathbb{N}, (k \in S \Rightarrow k \geq n+1)), l \in S, l \leq n+1 \vdash n+1 \in S} (\text{t} \vee)[k := l]}{\neg, l \in S, l \in S \Rightarrow l \geq n+1, l \leq n+1 \vdash n+1 \in S} (\text{mp})}{\frac{\frac{\frac{\neg, l \in S, l \in S \Rightarrow l \geq n+1 \vdash l \geq n+1}{\neg, l \in S, l \geq n+1, l \leq n+1 \vdash n+1 \in S} (\text{t} \Rightarrow)}{\neg, l \in S \Rightarrow l \geq n+1 \vdash l \in S \Rightarrow l \geq n+1} (\text{t} \Rightarrow)}{\neg, l \in S, l = n+1 \vdash n+1 \in S} (\text{t} \Rightarrow)}$$

Reste bien sûr à déduire  $[\vdash \forall S : \mathcal{P}(\mathbb{N}), (S \neq \emptyset \Rightarrow C)]$  de  $[S : \mathcal{P}(\mathbb{N}) \vdash \forall n : \mathbb{N}, (H(n) \Rightarrow C)]$  :

$$\frac{\frac{\frac{\frac{\vdash \forall S : \mathcal{P}(\mathbb{N}), (S \neq \emptyset \Rightarrow C)}{S : \mathcal{P}(\mathbb{N}), S \neq \emptyset \vdash C}}{S : \mathcal{P}(\mathbb{N}), (\exists n : \mathbb{N}, n \in S) \vdash C}}{S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, n \in S \vdash C}}{S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, n \in S \vdash H(n)} \quad \frac{S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, H(n) \vdash C}{S : \mathcal{P}(\mathbb{N}) \vdash \forall n : \mathbb{N}, (H(n) \Rightarrow C)}$$

Exercice : Prouver  $[S : \mathcal{P}(\mathbb{N}), n : \mathbb{N}, n \in S \vdash H(n)]$ .

Remarque : Rappelons le séquent initial  $[\vdash \forall S : \mathcal{P}(\mathbb{N}), (S \neq \emptyset \Rightarrow C)]$  d'abord après formalisation complète puis après l'application autant de fois que possible des règles  $(\vdash \forall)$ ,  $(\vdash \Rightarrow)$ ,  $(\vdash \text{ et})$ ,  $(\exists \vdash)$ ,  $(\text{ et } \vdash)$ ,  $(\text{ ou } \vdash)$  :

$$\frac{\vdash \forall S : \mathcal{P}(\mathbb{N}), (\exists n : \mathbb{N}, n \in S) \Rightarrow \exists n : \mathbb{N}, (n \in S \text{ et } \forall m : \mathbb{N}, (m \in S \Rightarrow m \geq n))}{\vdots} \\ S : \mathcal{P}(\mathbb{N}), n_0 : \mathbb{N}, n_0 \in S \vdash \exists n : \mathbb{N}, (n \in S \text{ et } \forall m : \mathbb{N}, (m \in S \Rightarrow m \geq n))$$

A ce niveau on est bloqué et la formalisation de l'énoncé C à droite de  $\vdash$  n'aide pas. Toute l'idée de la preuve est d'introduire l'hypothèse  $H(n)$  et de démontrer par récurrence sur  $n$  que  $H(n)$  entraîne C en distinguant dans le pas de récurrence le cas  $(H(n) \text{ et } H(n+1))$  de  $(\neg H(n) \text{ et } H(n+1))$ .