Logique fadélienne

DMI

Pour JYG et B

1 Introduction

Voilà un exercice amusant de type taupe :

Exercice 1. Soit A un anneau commutatif unitaire. Pour I un idéal de A, on note $Ann(I)$ l'idéal des $x \in A$ tels que $xI = 0$.
Alors pour tout I, $I \subset Ann(Ann(I))$ et $Ann(Ann(Ann(I))) = Ann(I)$.

Pour celleux qui ont fait un peu de logique, la preuve de cette exercice doit leur rappeler la preuve en logique constructive que $p \vdash \neg\neg p$ et $\neg\neg\neg p \vdash \neg p$. Ce n'est pas une coïncidence. On va explorer le fait que ce n'en soit pas une, et voir ce que cette exploration donne sur les anneaux fadéliens; on obtiendra une logique qui méritera de s'appeler logique fadélienne.

2 Logique annelée

On se fixe un ensemble de variables (plus tard il faudra voir ce qu'on entend par ensemble, si on veut faire de la logique infinitaire; pour le moment on s'en tient à des connecteurs d'arité finie) V. L'idée va être d'interpréter les variables par des idéaux d'anneaux, et les différents connecteurs par des opérations sur ces idéaux. Dans la suite, "idéal" voudra dire "idéal à gauche", sauf mention du contraire (on peut bien sûr faire le truc dual avec des idéaux à droite; c'est un peu plus subtil pour les idéaux bilatères par contre - mais ils ne nous intéressent pas vraiment pour les fadéliens, qui sont simples); et "anneau" veut dire "anneau unitaire"
En logique on a d'habitude un certain nombre de connecteurs : et, ou, non, implique, vrai, faux, en sont les principaux.
On se débarasse déjà de "non" car c'est en réalité "implique faux" donc il n'est pas nécessaire. Pour savoir comment intérpréter les autres il va falloir réfléchir un peu, et on va voir apparaître une nuance sur le "et".

On va vouloir déjà que la prouvabilité se traduise en inclusion d'idéaux : si je note par exemple $||p||$ l'idéal interprétant p, on va vouloir que si le séquent $p \vdash q$ est prouvable (il faudra voir ce que "prouvable" veut dire ici), alors pour toute interprétation, $||p|| \subset ||q||$. Se rappelant que "et" devrait vérifier quelque chose comme "p prouve q et r si et seulement si p prouve q et p prouve r", on a une interprétation toute trouvée : $||p\&q||$ devrait être $||p|| \cap ||q||$. Je note & et non pas le classique $\wedge$ parce qu'il va y avoir un deuxième "et", et choisir lequel mérite $\wedge$ est au-delà de mes forces, alors que mes choix actuels sont relativement intuitifs.

Une analyse similaire donne $||p \vee q|| = ||p|| + ||q||$ (là je ne sais pas s'il y a d'autres "ou", c'est bien possible. En attendant, je mets le classique $\vee$). Clairement, $||\bot||$ devrait être 0 et $||\top||$ devrait être R où R est l'anneau dans lequel on interprète. Reste à voir ce qu'est $\rightarrow$ (et qui est le deuxième "et", mais il viendra naturellement, ne vous inquiétez pas ;)).

Rappelons nous qu'on veut $Ann(||p||) = ||\neg p|| = ||p \rightarrow \bot|| = (||p|| : 0)$ où (:) est l'opération sur les idéaux qui correspondra à $\rightarrow$ (la notation n'est pas anodine, celleux qui connaissent assez de théorie des anneaux la reconnaîtront). Un brin de réflexion montre alors qu'une définition raisonnable est $(I : J) = \{x \in R \mid xI \subset J\}$ (qui est bien un idéal à gauche lorsque J en est un). Ainsi $||p \rightarrow q|| = \{x \in R \mid x||p|| \subset ||q||\}$.

MAIS on se rend compte assez vite qu'on a là un problème, vu qu'on a pas de modus ponens : $||p\&(p \rightarrow q)||$ n'est pas toujours inclus dans $||q||$. Et une logique sans modus ponens... C'est là qu'on se souvient que "et" a une autre définition que celle que j'ai donnée; "et" a une définition en termes de $\rightarrow$: en termes de preuves, on devrait avoir "p et q prouve r" si et seulement si "p prouve que $q \rightarrow r$" (adjonction tenseur/hom si on veut utiliser des mots savants). Ca + quelques idées d'opérations sur les idéaux nous donne l'idée de définir $||p \otimes q|| = ||p||||q||$ (et oui, lorsque I, J sont des idéaux, $IJ = \{\sum_i a_i b_i, a_i \in I, b_i \in J\}$ en est un aussi (attention, contrairement au cas commutatif on n'a a priori pas $IJ \subset I$)

Cette définition est cool puisqu'il y a une multiplication, et que la définition de l'interprétation de $\rightarrow$ a aussi une multiplication. Et remarquez : si I, J sont des idéaux, $(I : J)I \subset J$ (petite inversion, due à la non-commutativité, mais c'est pas grave, ça a quand même la gueule d'un modus ponens).
En fait on a la full-adjonction tenseur/hom : $IJ \subset K$ si et seulement si $I \subset (J : K)$. Récapitulons, plus proprement :

Définition 1 (Formule annelée)**.** En partant de l'ensemble de variables V, on définit les formules par induction :

- Une variable est une formule
- $\bot, \top$ sont des formules
- Si p, q sont deux formules, alors $p\&q, p \rightarrow q, p \otimes q, p \vee q$ en sont aussi

L'ensemble des formules est le plus petit ensemble contenant les variables et vérifiant les trucs du dessus

Exemples 1.

- $p \otimes (q \to r)$
- $((p \otimes q) \& r) \vee (r \to s)$

Définition 2. Un modèle de la logique annelée sur les variables V est un anneau R muni d'une application $|| - || : V \to \{I \subset R \mid I \text{ idéal }\}$. On étend cette application à l'ensemble des formules via les règles décrites plus tôt, qu'on rappelle :

- $||p \& q|| = ||p|| \cap ||q||$
- $||p \vee q|| = ||p|| + ||q||$
- $||\bot|| = 0, ||\top|| = R$
- $||p \to q|| = (||p|| : ||q||)$
- $||p \otimes q|| = ||p|| ||q||$

On définit aussi l'abbréviation $\neg p := p \to \bot$, de sorte que $||\neg p|| = Ann(||p||)$

Définition 3. Soit C une classe d'anneaux; une formule φ est *valable dans* C si quel que soit le modèle de la logique annelée avec pour anneau sous-jacent $R \in C$, $||\varphi|| = R$.
Si Γ est un ensemble de formules, on note $\Gamma \models_C \varphi$ l'assertion que pour tout modèle avec anneau sous-jacent $R \in C$ dans lequel $||\psi|| = R$ pour tout $\psi \in \Gamma$, on $||\varphi|| = R$. Une formule est alors valable dans C si et seulement si $\models_C \varphi$ (on omet "$\emptyset$")

Exemples 2.

- Pour toute formule p, la formule $p \to p$ est valable pour tous les anneaux.
- En omettant l'indice lorsque la classe C est celle de tous les anneaux, on a $\{p, p \to q\} \models q$ (une autre forme de modus ponens)

Un séquent est un couple de formules (p, q) , qu'on note en général $p \vdash q$ (je n'ai pas encore réussi à gérer des séquents avec plusieurs hypothèses ou plusieurs conclusions, c'est une piste à explorer), à comprendre comme "p prouve q".
Un séquent $p \vdash q$ est satisfait dans un modèle $(R, || - ||)$ si on a $||p|| \subset ||q||$
On définit de manière évidente le fait qu'un séquent soit satisfait par une classe d'anneaux C.

Une règle de déduction est un couple $(\Gamma, p \vdash q)$ où Γ est une liste (en réalité un multiensemble puisqu'on a commutativité à ce niveau là) de séquents, et $p \vdash q$ est un autre séquent. Une règle de déduction $(\Gamma, p \vdash q)$ est dite admissible pour (ou "dans" ou n'importe quelle préposition qui rend la chose claire) une classe d'anneaux C si quel que soit le modèle $(R, || - ||)$ avec $R \in C$, si les séquents de Γ sont satisfaits dans $(R, || - ||)$, alors $p \vdash q$ l'est aussi.

Remarque 1. Si $(\Gamma, p \vdash q)$ est admissible pour C, alors évidemment en substituant des formules pour des variables dans l'ensemble des séquents considérés, on obtient une autre règle admissible.

Notation 1. On note en général les règles de déduction sous la forme $\frac{\Gamma}{p \vdash q}$

Maintenant si on a des règles de déduction admissibles pour une classe d'anneaux C et qu'on fait une preuve suivant ces règles de déduction, tout séquent qu'on prouvera sera satisfait dans tout modèle avec un anneau sous-jacent $\in C$; on le prouve de manière évidente par récurrence (bon, faudrait définir la notion de preuve mais c'est bon vous êtes des adultes vous pouvez imaginer la définition et j'ai la flemme de l'écrire).
Un objectif pourrait alors être de trouver un ensemble relativement minimal de règles de déduction admissibles qui "engendrent" l'ensemble des règles de déduction admissibles; engendrent au sens où les autres règles de déduction admissibles s'en déduisent par preuve ou par substitution suivant la remarque qu'on a faite plus haut; typiquement voir si l'ensemble des règles de déduction admissibles a des propriétés de calculabilité etc. Pour le moment je n'en ai aucune idée.

Dans ce qui suit je fais une petite liste de règles de déductions admissibles que j'ai trouvées avec des commentaires sur celles que j'espérais mais qui n'étaient pas au rendez-vous.
Avant d'y aller, petite remarque : attention à la non commutativité de $\otimes$!

Je rajoute une remarque que j'ai oubliée de mentionner plus haut : on pourrait croire que le fait qu'on n'a pas de modus ponens/pas d'adjonction tenseur/hom avec & est un signe de la mauvaise définition de l'interprétation de $\to$; mais ce n'est pas le cas. & ne saurait avoir de " $\implies$ " lui correspondant puisque $a\&-$ ne préserve pas $\vee$, qui est un coproduit, donc $a\&-$ n'a pas d'adjoint à droite, i.e. pas de " $\implies$ " correspondant.

2.1 Règles de déduction admissibles pour la classe de tous les anneaux

- Identité : $\frac{}{p \vdash p}$
- Modus ponens : $\frac{r \vdash p \quad s \vdash p \to q}{s \otimes r \vdash q}$
  C'est pas commutatif, attention !
- Explosion : $\frac{p \vdash \perp}{p \vdash q}$
- Disjonction : $\frac{r \vdash p \quad s \vdash p}{r \vee s \vdash p}$.
  Ici on peut renverser la barre aussi, si je savais LaTeXer je mettrais une double-barre pour l'indiquer. Cette règle montre en particulier que $\vee$ est commutatif

- Conjonction "additive" [le fait qu'il y ait deux "et" me rappelle la logique linéaire mais je n'y connais rien donc je mets "additive" à moitié au pif à moitié parce que j'ai une interprétation du mot] : $\frac{r \vdash p \quad r \vdash q}{r \vdash p \& q}$.
Même remarque, on peut renverser la barre et ça marche. Et aussi pareil, & est commutatif.

- Conjonction "multiplicative" [même remarque] : $\frac{r \vdash p \quad s \vdash q}{r \otimes s \vdash p \otimes q}$.
Attention à respecter l'ordre !

- Cas particulier du truc au-dessus, montrant un peu un lien avec la logique linéaire : $\frac{r \vdash p \quad r \vdash q}{r \otimes r \vdash p \otimes q}$

- Affaiblissement : $\frac{}{r \otimes s \vdash s}$
Toujours pas de commutativité, c'est un peu triste.. Mais si on y pense en terme de ressources, on peut le voir comme "ah j'avais r, j'ai mis $r \otimes s$ et ça me bloque l'accès à r"

- Faux : $\frac{}{\neg p \otimes p \vdash \bot}$.
Amusant : en général on n'a pas $p \otimes \neg p \vdash \bot$!

- Vrai : $\frac{}{p \vdash \top}$

- Vrai 2 : $\frac{}{p \& \top \vdash p}$

- Adjonction et/implique : $\frac{r \otimes s \vdash p}{r \vdash s \to p}$
On peut à nouveau renverser la double barre

- Distributivité : $\frac{}{p \otimes (c \vee b) \vdash p \otimes c \vee p \otimes b}$
Celle-là j'ai hésité à la mettre parce que la réciproque est prouvable à partir des autres, et donc je me demande si elle ne l'est pas. Pareil, si on échange l'ordre (donc $(c \vee b) \otimes p$) on peut prouver l'équivalence à partir des autres règles; donc ça m'attriste un peu.

Petite remarque : $(R : I)$ pour un idéal I est le plus gros idéal bilatère inclus dans I, ce qui montre que $\top \to p$ est assez loin de p dans ce monde, ce qui est assez surprenant. En particulier, ce n'est pas parce que $q \vdash p$ est satisfait que $q \vdash \top \to p$ l'est (si on se souvient de l'adjonction plus haut, $q \vdash \top \to p$ est équivalent à $q \otimes \top \vdash p$, mais voilà $q \otimes \top$ est assez loin de q, puisque q est un idéal à gauche, et que là on multiplie à droite.

3 Petit interlude loin des fadéliens : logique annelée commutative

On se concentre maintenant sur la classe des anneaux commutatifs, qui est évidemment de peu d'intérêt si on s'intéresse aux fadéliens, mais qui simplifie vachement la vie. En effet, on va avoir la commutativité de $\otimes$ et donc plein de trucs super chouettes.

Je ne le fais pas, mais on peut s'intéresser dans ce cas là à voir quels anneaux satisfont la logique intuitionniste (il faut choisir un "et", ou bien demander qu'ils coïncident), la logique classique etc. et il y a des réponses plutôt explicites.

4 Logique fadélienne

On en vient au coeur du sujet. Je ne l'ai pas étudiée vachement donc je n'ai quasi rien à dire, mais déjà une première remarque : si I, J sont deux idéaux d'un anneau fadélien A, et $x \in I \cap J$, alors ou bien $x = 0$ auquel cas $x \in IJ$, ou bien on peut diviser fadéliennement 1 par x, $1 = ax + xb$; et alors $x = ax^2 + xbx, x^2 \in IJ, bx \in J$ et donc $ax^2 \in IJ, xbx \in IJ$, de sorte que $x \in IJ$: $I \cap J \subset IJ$ (la situation inverse du cas commutatif !)
A noter qu'on n'a pas toujours $IJ \subset I \cap J$ (prendre I un idéal propre, donc non bilatère, alors on n'a pas $IR \subset I$). En particulier, la première règle de déduction fadélienne qui n'est pas une règle de déduction annelée est : $\frac{}{p\&q \vdash p \otimes q}$

Je répète donc un objectif possible de cette étude : trouver un ensemble "minimal" de règles de déduction fadéliennes qui engendrent toutes les règles de déduction. Si on a ça, on a une idée d'à quoi ressemble la logique fadélienne et donc d'à quoi ressemble la structure des idéaux d'un anneau fadélien "générique". Si j'ai le temps et que je trouve des trucs, cette section devrait grandir.

5 Logique infinitaire ?

Jusque là on a tout fait en logique finitaire (tous les connecteurs sont d'arité finie), et on pourrait se dire que $\vee$ et & ont tout à fait le droit de porter sur des ensembles infinis puisque si j'ai une famille quelconque d'idéaux je peux bien prendre leur somme et leur intersection sans me soucier de sa taille.
Je ne suis pas certain de comment bien définir ça, c'est certain qu'il y a moyen mais après le système de déduction devient très chaotique (on ne peut plus dire "oh une preuve c'est un objet fini" puisqu'il faut avoir la possibilité de conjonctions/disjonctions infinies). A voir