Rapport de stage de M1 à l'Université de McMaster à Hamilton, Canada

Elyes Boughattas
École Normale Supérieure de Paris

Septembre 2018

Table des Matières

I Déroulement du stage **4**

II Travail mathématique **6**

1 Première partie du stage **6**
1.1 Groupe de travail: élimination des imaginaires 6
1.2 Cours: o-minimalité 6

2 Deuxième partie du stage **7**
2.1 Groupe de travail: groupes stables 7
2.2 Groupe de lecture: analyse p-adique 7

III Élimination des imaginaires dans un cadre abstrait **8**

1 Le modèle monstre **8**
1.1 Définition 8
1.2 Propriétés 8

2 Élimination des imaginaires dans un cadre abstrait **9**
2.1 Codes 9
2.2 Élimination des imaginaires 10
2.3 Construction et propriétés de T^{eq} 11
2.4 Élimination des imaginaires et automorphismes du monstre 12
2.4.1 Un lemme de Svenonius 13
2.4.2 Codes et automorphismes du monstre 13
2.4.3 Caractérisations de l'élimination des imaginaires 15

3 Étude de quelques théories **16**
3.1 Quelques critères 16
3.2 Arithmétique de Peano 16
3.3 Corps réels clos 17
3.4 Ordres totaux denses sans extrémités 17
3.5 Corps algébriquement clos 18

IV Cas d'étude des corps algébriquement clos valués **19**

1 Langage et théorie des corps valués algébriquement clos **19**
1.1 Première approche naïve 19
1.2 Un langage plus adapté 19
1.3 Un langage tri-sorté 20

2 Élimination des quantificateurs et parties définissables **21**
2.1 Élimination des quantificateurs 21
2.1.1 Un critère d'élimination des quantificateurs 21
2.1.2 Application aux corps algébriquement clos valués 22
2.2 Conséquences les opération de clôture et les ensembles définissables 24
2.2.1 Complétions 24
2.2.2 Opérations de clôtures 24
2.2.3 Parties définissables 25

3 Premières remarques sur l'élimination des imaginaires **26**
3.1 Insuffisance du langage uni-sorté 26

3.2 Notations et sortes géométriques 26
3.3 Un critère d'élimination des imaginaires 27

4 Élimination des imaginaires **28**
4.1 Opérations sur les types définissables et quelques définitions 28
4.1.1 Produit et poussé en avant 28
4.1.2 Les types génériquement stables 28
4.1.3 Une notion d'indépendance 29
4.2 Démonstration du troisième point du critère 30
4.2.1 Relèvements définissables 30
4.2.2 Démonstration du théorème 31
4.3 Retour aux sortes géométriques "naturelles" 34

Appendices **35**

A Généralités sur les corps valués **35**
A.1 Une construction catégorique 35
A.2 Corps valués 36
A.2.1 Première approche via les valuations 36
A.2.2 Deuxième approche via les anneaux de valuation 37
A.2.3 Les catégories $\overline{\textbf{ValField}}$ et **ValRing** sont isomorphes 38
A.3 Topologie d'un corps valué 38
A.4 Rang d'un groupe abélien ordonné 39
A.4.1 Définition 39
A.4.2 Groupes ordonnés de rang 1 39
A.5 Complétion d'un corps valué 40

B Extensions d'une valuation **42**
B.1 Définitions 42
B.2 Existence d'une extension 42
B.3 Cas des extensions algébriques 43
B.3.1 Description des extensions d'un anneau valué 43
B.3.2 Majoration du nombre d'extensions 45

C Corps henséliens **46**
C.1 Définition 46
C.2 Caractérisations et propriétés 46
C.2.1 Définitions équivalentes 46
C.2.2 Quelques propriétés des corps henséliens 48
C.2.3 Le lemme de Krasner 49

Références **51**

Partie I
Déroulement du stage

Je suis arrivé à Hamilton le dimanche 4 février au soir et j'ai rencontré Deirdre Haskell le mercredi 7 février. Nous avions déjà échangé par courrier électronique si bien que Deirdre connaissait mes prérequis et m'avais précisé ce sur quoi elle souhaitait que nous commencions à travailler: une étude, sous la forme d'un groupe de travail, de l'élimination des imaginaires dans le cadre de plusieurs théories de corps valués. Dès le lendemain, je commençai à lire le premier article du groupe de travail concernant le cas des corps algébriquement clos valués: mon stage avait donc commencé.

Un avantage particulier durant ce stage fut la disponibilité de Deirdre que je voyais en moyenne chaque semaine – d'abord pour le groupe de travail sus-évoqué, ensuite pour un groupe de lecture que j'évoquerai plus bas. J'ai également pu discuter avec d'autres théoriciens des modèles de l'université, notamment Patrick Speissegger et Bradd Hart, puis quelques doctorants qui participaient aux cours et groupes de travail que je suivais.

Logement J'avais fait le choix de ne pas louer de chambre avant d'être sur place, afin d'éviter d'éventuelles escroqueries. J'ai donc réservé une chambre via Airbnb pour quelques jours, puis j'ai fini par trouver une chambre en colocation où je me suis installé quelques jours après mon arrivée: seul inconvénient, elle était vide de meubles, ce qui m'a obligé à faire un détour chez le fameux fabriquant de meubles suédois (j'ai d'ailleurs réussi à revendre le mobilier avant mon départ).

J'étais dans une colocation assez grande dans le quartier d'Ainslie Wood, à l'extrême-ouest d'Hamilton, soit à une demi-heure de marche de l'université. Le cadre était très agréable, d'autant plus que je disposais d'une vue inspirante sur le jardin de la maison où écureuils et lapins se baladaient nonchalamment.

Je me trouvais en compagnie de 4 canadiens, tous étudiants à l'université de McMaster: bien que fort sympathiques, j'ai eu peu d'occasions de leur parler et ce certainement parce que leurs us diffèrent des nôtres en ce qu'ils restent dans leurs chambres et ne cuisinent presque jamais.

L'université de McMaster Le campus de l'université est très verdoyant: il jouit d'une position en bordure du coin sud-ouest du lac Ontario et ses jardins forment une zone naturelle protégée où on peut trouver de nombreux animaux qu'il n'est pas coutume de voir en liberté dans les pays européens.

Le département de mathématiques est quant à lui situé au sein du campus. J'ai obtenu la clé d'un bureau au sous-sol où je me suis peu rendu en raison du vacarme qu'y faisait une poignée d'étudiants de niveau master. Le département propose des cours dans plusieurs domaines: théorie des modèles, topologie algébrique, équations aux dérivées partielles et statistique. Il y avait également des séminaires, en particulier un séminaire de théorie des modèles qui avait lieu en moyenne une semaine sur deux.

En ce qui concerne la bibliothèque, je m'y suis peu aventuré, surtout parce que j'avais accès aux références nécessaires en ligne, mais aussi parce que la densité y était trop importante.

Je note enfin qu'en guise de restauration, le campus est majoritairement rempli de commerces des restauration rapide, ce qui peut dérouter en prime abord.

La ville et ses environs La ville de Hamilton est une ville de 550 000 habitants anciennement connue pour son industrie de sidérurgie: une industrie florissante d'autant plus que la ville dispose d'un accès au lac Ontario et d'un système ferroviaire la reliant aux grandes villes. La désindustrialisation y a amené beaucoup de pauvreté dans le début des années 1990, notable au nord-est du centre-ville. Depuis, la ville a réussi à diversifier son économie et l'université joue un rôle dans la redynamisation des quartiers pauvres.

Le cadre est néanmoins très agréable puisque la ville est entourée de paysages verdoyants et est traversée au sud par l'escarpement du Niagara qui donne lieu à de très jolies cascades. Il y a en outre des sentiers très agréables pour qui souhaite se promener, en particulier de très belles portions de la transcanadienne, qui représente un complexe de sentiers reliant la côté occidentale à la côte pacifique du Canada.

Partie II
Travail mathématique

Au niveau mathématique, mon stage s'est divisé en deux grandes parties au cours desquelles j'ai étudié deux principaux sujets:

1 Première partie du stage

1.1 Groupe de travail: élimination des imaginaires

J'ai commencé mon stage par l'étude de l'élimination des imaginaires. Cette étude s'est faite sous la forme d'un groupe de travail constitué de Deirdre, deux étudiants dont elle encadre la thèse, Paul et moi-même.

Dire qu'une théorie ayant suffisamment de constantes élimine les imaginaires revient à dire que les quotients par des relations d'équivalences $\emptyset$-définissables sont $\emptyset$-définissables, ainsi que les surjections canoniques. Les imaginaires ont tout d'abord été introduits par Shelah dans [She78] puis par Poizat dans [Poi83]: ce dernier montra alors que la théorie des corps algébriquement clos les élimine.

Les théories de corps munis d'une valuation ont le bon goût d'avoir de bonnes propriétés modèle-théoriques: lorsque les corps sont supposés algébriquement clos, elles éliminent les quantificateurs comme le montra Robinson dans [Rob56]. Néanmoins, un argument simple assure que les corps algébriquement clos n'éliminent pas les imaginaires dans le langage de Robinson.
Après que Holly eut montré dans [Hol97] qu'en rajoutant des imaginaires pour les boules on pouvait coder les sous-ensembles définissables du corps, Haskell, Hrushovksi et Macpherson ont réussi à montrer dans [HHM06] qu'on peut éliminer les imaginaires pour les corps algébriquement clos valués en rajoutant des sortes dites géométriques qu'on peut voir comme des boules de dimensions supérieures. J'ai donc commencé par étudier une version raccourcie de cette preuve, établie par Johnson dans [Joh14].

Il est alors naturel de se demander ce qui advient dans d'autres théories de corps valués. Un résultat positif a été donné par Hils Kamensky et Rideau dans [HKR18] dans le cas des corps séparablement clos valués de degré d'imperfection fini, avec les sortes géométriques. Les auteurs réduisent le problème au cas semi-algébrique en utilisant des λ-fonctions puis se ramènent au résultat analogue dans le cas des corps algébriquement clos valués d'équicaractéristique p.

Il a également été montré par Hrushovski, Martin et Rideau dans [HMRC07] que la théorie des corps p-adique élimine les imaginaires en rajoutant les sortes géométriques.

1.2 Cours: o-minimalité

Au cours de cette première moitié du stage, j'ai également suivi un cours sur l'o-minimalité donné par Patrick Speissegger. Une structure o-minimale est une extension des ordres linéaires denses sans extrémités où toute partie définissable est une réunion finie d'intervalles: un premier exemple est celui des corps réels clos. Une particularité des structures o-minimale est qu'on est capable de décrire ses parties définissables (de dimension quelconque), ce qui constitue le théorème de décomposition cellulaire.

L'o-minimalité d'une structure permet d'obtenir des résultats analytiques parfois spectaculaires: Miller a par exemple montré que dans une extension o-minimale du corps ordonné des réels, toute fonction définissable est bornée si et seulement si l'exponentielle est définissable.

2 Deuxième partie du stage

2.1 Groupe de travail: groupes stables

En sentant la fin du premier groupe de travail arriver et ayant été piqué de curiosité par une branche de la théorie des modèles qu'on appelle la théorie des modèles géométrique, j'ai souhaité consacrer la deuxième partie de mon stage à ce sujet. J'ai donc discuté avec Deirdre qui a fini par me diriger vers Bradd Hart, lequel me fit un petit exposé sur le sujet et me proposa d'organiser un groupe de travail. Nous commençâmes donc, début mai, un groupe de travail sur les groupes stables, où il y avait entre trois et cinq participants.

La théorie des modèles géométriques est née avec une conjecture que Zil'ber proposa au début des années 1970 selon laquelle toute structure fortement minimale est porteuse d'une géométrie qui est: soit triviale; soit modulaire non triviale; soit non-modulaire. La conjecture s'est avérée fausse vingt ans plus tard, un contre-exemple ayant été apporté par Hrushovski dans [Hru93]. Elle reste néanmoins fondamentale car porteuse d'une intuition qui s'est avérée vraie dans de nombreux cas.

Durant le groupe de travail, il a surtout été question de groupes stables. Nous avons étudié le théorème de configuration de groupes et suivi partiellement [WWH97].

Une ouverture a été donnée lors de la dernière séance sur la théorie de la classification, un projet entrepris et développé par Shelah depuis la seconde moitié des années 1970 et qui vise à étudier le comportement du spectre d'une théorie, c'est-à-dire la fonction qui à un cardinal κ associe le nombre de modèles deux à deux non isomorphes de cardinal κ, pourvu que la théorie ait des propriété combinatoires raisonnables.

2.2 Groupe de lecture: analyse p-adique

En parallèle, j'ai participé à un groupe de lecture organisé par Deirdre qui rassemblait quelques étudiants, Paul et moi-même. Après quelques rappels sur les corps p-adiques et la complétion de leur clôture algébrique, nous avions étudié les propriétés de l'exponentielle, du logarithme, puis d'autres fonctions analytiques telles que la fonction gamma. Nous avons fini par voir comment interpoler la fonction Zeta pour obtenir une fonction Zeta p-adique. Ce groupe de lecture se résume en fait à une étude non linéaire de [Kob77].

Partie III
Élimination des imaginaires dans un cadre abstrait

On se propose ici de poser les jalons théoriques de l'élimination des imaginaires. On étudie également le cas de quelques théories usuelles et on renvoie le lecteur à la partie IV du mémoire pour l'étude d'une théorie plus élaborée.

1 Le modèle monstre

Dans cette section, nous évoquons un point de vue qu'on adoptera souvent par la suite et qui permet d'éviter des lourdeurs de raisonnement.

1.1 Définition

Si T est une théorie complète dont les modèles sont infinis, il est commode de travailler dans un modèle saturé de cardinal suffisamment grand pour que tout modèle s'y injecte élémentairement.

Dans le cas des théories stables, il est aisé d'obtenir des modèles saturés de cardinal arbitrairement grand: le lecteur intéressé pourra se référer à [TZ12, Lemme 5.2.9].

Dans le cas général, en se plaçant dans **BGC** (Bernays-Gödel+Choix global), qui est une extension conservative de **ZFC**, on dispose du théorème suivant:

Théorème 1.1.1. *Il existe une classe* $\mathbf{C}$ *qui est un modèle de* T *et qui réalise tout type à paramètres dans un sous-ensemble. Cette classe est unique à isomorphisme près.*

Démonstration. Le choix global fournit une chaîne croissante $(M_\alpha)_{\alpha\in\mathrm{On}}$ de modèles de T telle que tout type de M_α est réalisé dans $M_{\alpha+1}$. La réunion croissante de cette chaîne convient clairement.

L'unicité relève d'arguments usuels de saturation. □

Définition 1.1.1. *La classe* $\mathbf{C}$ *est alors appelée un modèle monstre de* T.

1.2 Propriétés

Proposition 1.2.1. *Un modèle monstre d'une théorie complète* T *jouit des propriétés suivantes:*

(i) Le modèle $\mathbf{C}$ *est* κ*-saturé pour tout cardinal* κ*;*

(ii) Tout modèle de T *s'injecte élémentairement dans* $\mathbf{C}$*;*

(iii) Toute bijection élémentaire entre sous-ensembles de $\mathbf{C}$ *s'étend en un automorphisme de* $\mathbf{C}$.

La commodité du modèle monstre se traduit par le fait suivant:

Fait 1.2.1. *Soit* A *un ensemble inclus dans* $\mathbf{C}$*. Deux éléments de* $\mathbf{C}$ *ont le même type à paramètres dans* A *si et seulement si il existe un automorphisme de* $\mathbf{C}$ *qui fixe* A *et qui envoie l'un sur l'autre.*

2 Élimination des imaginaires dans un cadre abstrait

Dans la suite, T désigne une théorie dans un langage $\mathcal{L}$. On travaille dans le cadre d'un langage éventuellement multi-sorte.

2.1 Codes

Commençons par définir la notion de code:

Définition 2.1.1. *Soit X une partie définissable d'une $\mathcal{L}$-structure $\mathcal{M}$.*

Un code de X est la donnée d'un tuple c de $\mathcal{M}$ et d'une $\mathcal{L}$-formule $\varphi(\overline{x},\overline{y})$ tels que $X=\varphi\left(\mathcal{M}^{\overline{x}},c\right)$ et pour tout $c'\neq c$ on ait $X\neq\phi\left(\mathcal{M}^{\overline{x}},c'\right)$. On dit encore que c est un code de X via $\varphi(\overline{x},\overline{y})$.

Le pendant uniforme de la notion de code est défini comme suit:

Définition 2.1.2. *Soit $\mathcal{M}$ une $\mathcal{L}$-structure et $\theta(\overline{x},\overline{y})$ une $\mathcal{L}$-formule. Un code uniforme de $\theta(\overline{x},\overline{y})$ est la donnée d'une $\mathcal{L}$-formule $\varphi(\overline{x},\overline{z})$ telle que pour tout $a\in\mathcal{M}^{\overline{y}}$ l'ensemble $\theta\left(\mathcal{M}^{\overline{x}},a\right)$ admet un code via $\varphi(\overline{x},\overline{z})$.*

La définition précédente peut se reformuler de la façon suivante:

Fait 2.1.1. *Soit $\mathcal{M}$ une $\mathcal{L}$-structure et $\theta(\overline{x},\overline{y})$ une $\mathcal{L}$-formule. Une $\mathcal{L}$-formule $\varphi(\overline{x},\overline{z})$ est un code uniforme de $\theta(\overline{x},\overline{y})$ si et seulement si il existe une unique fonction $\emptyset$-définissable f telle que pour tout tuple a de sortes adéquates, $\theta\left(\mathcal{M}^{\overline{x}},a\right)=\varphi\left(\mathcal{M}^{\overline{x}},f(a)\right)$.*

Si l'existence d'un code uniforme pour toute formule assure l'existence d'un code pour toute partie définissable, la réciproque est vraie si on dispose de deux constantes $\emptyset$-définissables:

Proposition 2.1.1. *Soit $\mathcal{M}$ une $\mathcal{L}$-structure telle que* $\mathrm{dcl}(\emptyset)$ *contient au moins deux éléments d'une même sorte et un élément de chaque sorte et soit $\theta(\overline{x},\overline{y})$ une $\mathcal{L}$-formule. Si pour tout tuple a l'ensemble définissable $\theta\left(\mathcal{M}^{\overline{x}},a\right)$ admet un code, alors $\theta(\overline{x},\overline{y})$ admet un code uniforme.*

Démonstration. Supposons que pour tout tuple a l'ensemble $\theta\left(\mathcal{M}^{\overline{x}},a\right)$ admet un code.

En ce cas, le $\emptyset$-type

$p(\overline{y}):=\{$"l'ensemble défini par $\theta(\overline{x},\overline{y})$ n'est pas codé par $\varphi(\overline{x},\overline{z})$" : $\varphi(\overline{x},\overline{z})$ est une $\mathcal{L}$-formule$\}$

est incohérent avec $\mathrm{Th}(\mathcal{M})$. Par compacité il existe donc $(\varphi_i(\overline{x},\overline{z_i}))_{i=1,\ldots,n}$ telle que, pour tout tuple a de sorte adéquate, il existe $i\in\{1,\ldots,n\}$ tel que $\theta\left(\mathcal{M}^{\overline{x}},a\right)$ admet un code via $\varphi_i(\overline{x},\overline{z_i})$. De plus, quitte à interposer de nouvelles variables qu'on décrète égales à des constantes $\emptyset$-définissables, on peut supposer que les $\overline{z_i}$ sont tous égaux à un même tuple de variables $\overline{z}$.

En outre, quitte à remplacer $\varphi_i(\overline{x},\overline{z})$ par

$$\varphi_i(\overline{x},\overline{z})\wedge\left(\bigwedge_{j<i}\neg\left(\exists!\overline{z'}\forall\overline{x}\left(\varphi_j\left(\overline{x},\overline{z'}\right)\longleftrightarrow\varphi_i(\overline{x},\overline{z})\right)\right)\right)$$

on peut supposer que pour tout tuple a de sorte adéquate, il existe un unique $i\in\{1,\ldots,n\}$ tel que $\theta(\mathcal{M},a)$ est codé via $\varphi_i(\overline{x},\overline{z})$.

Notons c et d deux constantes $\emptyset$-définissables d'une même sorte. En notant u_i le tuple $(c, \ldots, d, \ldots, c)$ où d est à la ième place, posons

$$\psi(\overline{x}, \overline{z}, \overline{u}) := \bigvee_i \overline{u} = \overline{u_i} \wedge \varphi_i(\overline{x}, \overline{z})$$

qui est une $\mathcal{L}$-formule.

Il est alors clair que $\psi(\overline{x}, \overline{z}, \overline{u})$ code uniformément $\theta(\overline{x}, \overline{y})$. En effet, si a est un tuple de sorte adéquate, il existe un unique i tel que $\theta(\mathcal{M}, a)$ est codé via $\varphi_i(\overline{x}, \overline{z})$: en notant b le tuple associé à ce code, on obtient que bu_i code $\theta(\mathcal{M}, a)$ via $\psi(\overline{x}, \overline{z}, \overline{u})$, ce qui conclut. □

Remarque 2.1.1. *En particulier, s'il n'y a qu'une sorte et qu'il y a deux constantes définissables, l'existence d'un code uniforme est assurée.*

Il y a également une notion de code faible:

Définition 2.1.3. *Soit X une partie définissable d'une $\mathcal{L}$-structure $\mathcal{M}$ et c un tuple de $\mathcal{M}$. On dit que c est un code faible de $\mathcal{M}$ s'il existe une $\mathcal{L}$-formule $\varphi(\overline{x}, \overline{z})$ vérifiant $X = \varphi\left(\mathcal{M}^{\overline{x}}, c\right)$ et telle qu'il existe un nombre fini de tuples c' vérifiant $X = \varphi\left(\mathcal{M}^{\overline{x}}, c'\right)$.*

Comme avant, on définit également une notion de code faible uniforme.

2.2 Élimination des imaginaires

Définition 2.2.1. *La théorie T élimine les imaginaires si l'une des propriétés équivalentes suivantes est vérifiée:*

(i) Toute partie définissable d'un modèle de T admet un code;

(ii) Pour tout modèle $\mathcal{M}$ de T et toute $\mathcal{L}$-formule $E(\overline{x}, \overline{y})$ qui définit une relation d'équivalence modulo T, les classes d'équivalence de E dans M admettent un code.

Dans ce cas, on écrira que T admet (EI).

Démonstration. Le sens $(i) \longrightarrow (ii)$ étant évident, il suffit de montrer que $(ii) \longrightarrow (i)$.

Soit X une partie définissable d'un modèle $\mathcal{M}$ de T et $\theta(\overline{x}, \overline{y})$ une $\mathcal{L}$-formule ainsi que a un tuple de $\mathcal{M}$ tels que $X = \theta\left(\mathcal{M}^{|\overline{x}|}, a\right)$.

Posons $E(\overline{y}, \overline{z}) := \forall \overline{x} \theta(\overline{x}, \overline{y}) \longleftrightarrow \theta(\overline{x}, \overline{z})$ qui définit une relation d'équivalence modulo T. Par hypothèse, la classe de a admet donc un code c via une $\mathcal{L}$-formule $\varphi(\overline{y}, \overline{u})$. En posant $\psi(\overline{x}, \overline{u}) := \exists \overline{y} \theta(\overline{x}, \overline{y}) \wedge \varphi(\overline{y}, \overline{u})$, il est alors aisé de vérifier que c est un code de X via $\psi(\overline{x}, \overline{u})$. □

On dispose de la version uniforme de la définition précédente:

Définition 2.2.2. *La théorie T élimine uniformément les imaginaires si l'une des propriétés équivalentes suivantes est vérifiée:*

(i) Dans tout modèle de T, toute $\mathcal{L}$-formule admet un code uniforme;

(ii) Dans tout modèle de T, toute $\mathcal{L}$-formule $E(\overline{x}, \overline{y})$ qui définit une relation d'équivalence modulo T admet un code uniforme.

(iii) Pour tout modèle $\mathcal{M}$ de T et toute relation d'équivalence définie par une $\mathcal{L}$-formule $E(\overline{x}, \overline{y})$ il existe une fonction $\emptyset$-définissable f telle que pour tous a, b de sortes adéquates, $f(a) = f(b)$ si et seulement si $E(a, b)$.

Dans ce cas, on écrira que T admet (EUI).

Démonstration. L'équivalence $(i) \longleftrightarrow (ii)$ se montre de façon analogue à celle de la preuve précédente, tandis que l'équivalence $(ii) \longleftrightarrow (iii)$ est conséquence du fait 1.1.1. □

Enfin, on peut également définir une élimination faible des imaginaires de la façon suivante:

Définition 2.2.3. *La théorie T élimine faiblement les imaginaires si l'une des propriétés équivalentes suivantes est vérifiée:*

(i) Dans tout modèle de T, toute $\mathcal{L}$-formule admet un code faible;

(ii) Dans tout modèle de T, toute $\mathcal{L}$-formule $E(\overline{x}, \overline{y})$ qui définit une relation d'équivalence modulo T admet un code faible.

Dans ce cas, on écrira que T admet (EFI).

En vertu du paragraphe précédent:

Proposition 2.2.1. *Si T admet* (EUI) *alors elle admet* (EI). *De plus, si la théorie définit une constante par sorte et deux constantes d'une même sorte, la réciproque est vraie.*

2.3 Construction et propriétés de $\mathbf{T^{eq}}$

On construit ici une extension de T qui élimine les imaginaire, après enrichissement du langage $\mathcal{L}$.

Notons $\mathbf{Eq}(T)$ l'ensemble des $\mathcal{L}$-formules $E(\overline{x}, \overline{y})$ telles que

$$T \vdash \text{"}E(\overline{x}, \overline{y}) \text{ est une relation d'équivalence".}$$

Ajoutons pour tout $E(\overline{x}, \overline{y}) \in \mathbf{Eq}(T)$ une sorte S_E et un symbole de fonction $f_E : S_=^{\overline{x}} \longrightarrow S_E$. Associons les symboles de $\mathcal{L}$ à la sorte $S_=$ et notons $\mathcal{L}^{eq}$ le langage ainsi obtenu.

On pose alors:

$$T^{eq} := T \cup \{\text{"}f_E \text{ est surjective et } f_E(\overline{x}) = f_E(\overline{y}) \longleftrightarrow E(\overline{x}, \overline{y})\text{"} : E(\overline{x}, \overline{y}) \in \mathbf{Eq}(T)\}.$$

On peut décrire, à isomorphisme près, les modèles de T^{eq}:

Fait 2.3.1. *Les modèles de T^{eq} sont, à isomorphisme près, en correspondance bijective avec ceux de T de la façon suivante:*

À tout modèle $\mathcal{M}$ de T on associe la $\mathcal{L}^{eq}$-structure $\mathcal{M}^{eq}$ définie par $M_=^{eq} := M$ et pour $E \in \mathbf{Eq}(T)$ on pose $M_E^{eq} := M/E$ et on interprète f_E par la projection canonique.

Réciproquement, tout modèle $\mathcal{N}$ de T^{eq} est déterminé de manière unique par $N_=$.

Le lemme suivant est utile pour montrer que T^{eq} hérite des propriétés de stabilité et de saturation de T:

Lemme 2.3.1. *Si $\varphi(x_1, \ldots, x_n)$ est une $\mathcal{L}^{eq}$-formule, où chaque x_i sont des singletons de sorte S_{E_i}, il existe une $\mathcal{L}$-formule $\psi(w_1, \ldots, w_n)$, où les w_i sont des tuples de sortes adéquates, telle que:*

$$T^{eq} \vdash \varphi(f_{E_1}(w_1), \ldots, f_{E_n}(w_n)) \longleftrightarrow \psi(w_1, \ldots, w_n).$$

Démonstration. L'ensemble des formules vérifiant une telle propriété est clairement clos par négation, conjonction et quantification existentielle. Il suffit donc de montrer que les $\mathcal{L}^{eq}$-formules atomiques y sont.

Notons que les termes sur $\mathcal{L}^{eq}$ sont soit des $\mathcal{L}$-termes, soit de la forme $f_E(\tau(\overline{x}))$ où $\tau(\overline{x})$ est un tuple de $\mathcal{L}$-termes.

On en déduit que les $\mathcal{L}^{eq}$-formules atomiques sont de l'une des formes suivantes:

- soit des $\mathcal{L}$-formules atomiques, auquel cas il suffit de prendre pour ψ la même formule;
- soit de la forme $f_E(\tau(\overline{x})) = f_E(\sigma(\overline{y}))$, où $\tau(\overline{x})$ et $\sigma(\overline{y})$ sont des $\mathcal{L}$-termes, auquel cas il suffit de poser $\psi(\overline{x}, \overline{y}) := E(\tau(\overline{x}), \sigma(\overline{y}))$;
- soit de la forme $f_E(\tau(\overline{x})) = y$, où $\tau(\overline{x})$ est un $\mathcal{L}$-terme, auquel cas il suffit de poser $\psi(\overline{x}, y) := \exists w E(\tau(\overline{x}), y)$.

□

La proposition suivante découle du lemme précédent:

Proposition 2.3.1. *On dispose des propriétés suivantes:*

(i) Si T est complète alors T^{eq} l'est aussi;

(ii) Si $\mathcal{M} \models T$ est κ-saturé alors $\mathcal{M}^{eq}$ est κ-saturé;

(iii) La théorie T est λ-stable si et seulement si T^{eq} est $\lambda - stable$.

La propriété fondamentale de T^{eq} est qu'elle élimine les imaginaires:

Théorème 2.3.1. *La théorie T^{eq} élimine les imaginaires.*

Démonstration. Soit $E(\overline{x}, \overline{y})$ une $\mathcal{L}^{eq}$-formule qui définit une relation d'équivalence modulo T^{eq} et soit b un tuple de sortes adéquates d'un modèle $\mathcal{M}^{eq}$ de T: on cherche à coder $E(\mathcal{M}^{eq}, b)$.

Par le lemme 2.3.1 il existe une $\mathcal{L}$-formule $\theta(\overline{u}, \overline{v})$ et un tuple de $f_{E'}$, noté F, tels que:

$$T^{eq} \vdash E(F(\overline{u}), F(\overline{v})) \longleftrightarrow \theta(\overline{u}, \overline{v}).$$

Ainsi, θ est une relation d'équivalence modulo T.

Soit a un tuple de $\mathcal{M}$ tel que $F(a) = b$ et $c := a/\theta$. Notons d'emblée que $\theta\left(\mathcal{M}^{\overline{u}}, a\right)$ est codé par c via $\varphi(\overline{u}, t) := (f_\theta(\overline{u}) = t)$. On en déduit que $E\left(\mathcal{M}^{eq\overline{x}}, b\right)$ est codé par c via:

$$\psi(\overline{x}, t) := \exists \overline{u}\,(F(\overline{u}) = \overline{x} \wedge \varphi(\overline{u}, t)).$$

□

Enfin, on remarquera le point suivant:

Fait 2.3.2. *Si T est complète, alors $\mathbf{C}^{eq}$ est un monstre de T^{eq}.*

Si T est complète et si X est une partie définissable du monstre on notera dans la suite $\ulcorner X \urcorner$ un code de X dans $\mathbf{C}^{eq}$.

2.4 Élimination des imaginaires et automorphismes du monstre

Dans la suite, T est supposée complète et on choisit un monstre $\mathbf{C}$ de T.

2.4.1 Un lemme de Svenonius

Le lemme suivant, en général attribué à Svenonius, permet de caractériser les paramètres sur lesquels on peut définir une partie définissable d'un modèle, pourvu que celui-ci jouisse d'une hypothèse raisonnable de saturation.

Lemme 2.4.1. *Soit $\mathcal{M}$ une $\mathcal{L}$ structure saturée, $A \subseteq M$ telle que $|A| < |M|$ et $X \subseteq M^n$ un ensemble définissable. Alors, X est A-définissable si et seulement si X est stable par tout élément de* $\mathrm{Aut}(\mathcal{M}/A)$.

Démonstration. Le sens direct est évident. Supposons donc que X est stable par tout élément de $\mathrm{Aut}(\mathcal{M}/A)$ et montrons que X est A-définissable.

Puisque X est définissable, il existe une $\mathcal{L}$-formule $\psi(\overline{u}, \overline{y})$ et $\overline{m}$ un tuple de $\mathcal{M}$ tels que $\psi(\overline{u}, \overline{m})$ définit X. Considérons le type $p(\overline{x}, \overline{y})$ défini par

$$p(\overline{u}, \overline{v}) := \{\psi(\overline{u}, \overline{m}), \neg\psi(\overline{v}, \overline{m})\} \cup \{\varphi(\overline{u}) \longleftrightarrow \varphi(\overline{v}) : \varphi(\overline{u}) \text{ est une } \mathcal{L}\text{-formule}\}.$$

Notons que $p(\overline{u}, \overline{v}) \cup \mathrm{Th}_{M}(M)$ est incohérent. Autrement, puisque M est saturé, il aurait une réalisation $(\overline{a}, \overline{b})$ dans M si bien que $tp(\overline{a}/A) = tp(\overline{b}/A)$ d'où l'existence de $\sigma \in \mathrm{Aut}(\mathcal{M}/A)$ qui envoie $\overline{a}$ sur $\overline{b}$: ainsi, par hypothèse, $\overline{a} \in X$ si et seulement si $\overline{b} \in X$ ce qui contredit que $\mathcal{M} \models \psi(\overline{a}, \overline{m})$ et $\mathcal{M} \not\models \psi(\overline{b}, \overline{m})$.

Il existe donc un nombre fini de $\mathcal{L}(A)$-formules $\varphi_1, \ldots, \varphi_r$ telles que

$$\mathcal{M} \models \forall\overline{u}\forall\overline{v}\left(\bigwedge_{i=1}^{r}(\varphi_i(\overline{u}) \longleftrightarrow \varphi_i(\overline{v})) \longrightarrow (\psi(\overline{u}, \overline{m}) \longleftrightarrow \psi(\overline{v}, \overline{m}))\right). \tag{1}$$

En posant pour $\tau : \{1, \ldots, n\} \longrightarrow 2$ la $\mathcal{L}(A)$-formule définie par

$$\theta_\tau(\overline{u}) := \bigwedge_{\tau(i)=0} \varphi_i(\overline{u}) \wedge \bigwedge_{\tau(i)=1} \neg\varphi_i(\overline{u})$$

la formule (1) assure que si $\mathcal{M} \models \theta_\tau(\overline{a}) \wedge \theta_\tau(\overline{b})$ alors $\overline{a} \in X$ si et seulement si $\overline{b} \in X$.

On en déduit que si S désigne l'ensemble des τ tels que $\mathcal{M} \models \theta_\tau(\overline{a})$ pour un certain $\overline{a} \in X$, alors la $\mathcal{L}(A)$-formule

$$\varphi(\overline{u}) := \bigvee_{\tau \in S} \theta_\tau(\overline{u})$$

définit X, ce qui conclut. □

2.4.2 Codes et automorphismes du monstre

On peut caractériser les codes d'un ensemble définissable via les automorphismes du monstre:

Proposition 2.4.1. *Soit X un ensemble définissable de $\mathbf{C}$. Un tuple c de $\mathbf{C}$ est un code de X si et seulement si pour tout $f \in$* $\mathrm{Aut}(\mathbf{C})$

$$f(X) = X \longleftrightarrow f(c) = c. \tag{2}$$

Démonstration. Le sens direct étant évident, il s'agit de montrer l'autre sens. Donnons-nous donc un tuple c tel que (2) est vérifié pour tout $f \in \mathrm{Aut}(\mathbf{C})$.

Par le lemme de Svenonius, X est alors c-définissable d'où l'existence de $\varphi(x, c)$ qui définit X. L'hypothèse (2) assure alors que

$$tp(c) \cup \{y \neq c, \forall x\varphi(x, c) \longleftrightarrow \varphi(x, y)\}$$

est incohérent d'où l'existence de $\theta(y) \in tp(c)$ telle que

$$\mathbf{C} \models (\theta(y) \wedge \forall x\varphi(x, c) \longleftrightarrow \varphi(x, y)) \longrightarrow y = c$$

d'où on déduit que c code X via $\theta(y) \wedge \varphi(x, y)$. □

Une conséquence immédiate est que tout tuple inter-définissable avec un code de X dans $\mathbf{C}^{eq}$ est encore un code de X:

Proposition 2.4.2. *Soit X une partie définissable de $\mathbf{C}$ et c un tuple de $\mathbf{C}$. Pour que c soit un code de X, il faut et il suffit que* $\mathrm{dcl}^{\mathrm{eq}}(c) = \mathrm{dcl}^{\mathrm{eq}}(\ulcorner X \urcorner)$.

On dispose d'un résultat analogue à la proposition précédente:

Proposition 2.4.3. *Un ensemble définissable X de $\mathbf{C}$ admet un code faible si et seulement si il existe un ensemble fini A de $\mathbf{C}$ tel que pour tout $f \in \mathrm{Aut}(\mathbf{C})$*

$$f(X) = X \longleftrightarrow f(A) = A. \tag{3}$$

Démonstration. Le sens direct étant évident, donnons-nous un ensemble définissable X vérifiant (3). Écrivons $a_1, \ldots, a_r$ les éléments de A et considérons le tuple $c := a_1 c_2 \ldots a_r$. Le lemme de Svenonius associé à (3) assure alors que X est c-définissable si bien qu'il existe une formule $\varphi(x, c)$ qui définit X.

Le point (3) assure également que c est algébrique sur $\ulcorner X \urcorner$: notons $c_1, \ldots, c_n$ ses $\ulcorner X \urcorner$-conjugués. L'hypothèse (3) assure alors que le type

$$tp(c) \cup \{y \neq c_1, \ldots, c_n, \forall x \varphi(x, c) \longleftrightarrow \varphi(x, y)\}$$

est incohérent d'où l'existence de $\theta(y) \in tp(c)$ telle que

$$\mathbf{C} \models (\theta(y) \wedge \forall x \varphi(x, c) \longleftrightarrow \varphi(x, y)) \longrightarrow \bigvee_{i=1}^{n} y = c_i$$

d'où on déduit que c code faiblement X via $\theta(y) \wedge \varphi(x, y)$. □

Le lecteur se convaincra que le résultat suivant découle de la preuve précédente:

Proposition 2.4.4. *Soit X un ensemble définissable de $\mathbf{C}$. Un tuple c de $\mathbf{C}$ code faiblement X si et seulement si $\ulcorner X \urcorner \in \mathrm{dcl}^{\mathrm{eq}}(c)$ et $c \in \mathrm{acl}^{\mathrm{eq}}(\ulcorner X \urcorner)$.*

Enfin, on dispose du critère suivant d'élimination faible des imaginaires:

Proposition 2.4.5. *Un ensemble définissable X de $\mathbf{C}$ admet un code faible si et seulement si il admet un plus petit ensemble de définition algébriquement clos.*

Démonstration. Si X admet un code faible, il existe A fini tel que (3) est vérifié. L'ensemble $\mathrm{acl}(A)$ est alors algébriquement clos et X est défini sur A. En outre, si B est un ensemble de définition algébriquement clos de X alors pour tout $a \in A$ et $f \in \mathrm{Aut}_B(\mathbf{C})$, l'assertion (3) assure que $f(a) \in A$ ce qui signifie que a est algébrique sur B et donc que $a \in B$, d'où $A \subseteq B$.

Réciproquement, supposons que X admet un plus petit ensemble de définition A algébriquement clos et soit a un tuple de A tel que X soit défini par une formule $\varphi(x, a)$. Par minimalité de A on a déjà $A = \mathrm{acl}(a)$.

Supposons par l'absurde qu'il existe une infinité de b tels que $tp(a) = tp(b)$ et $\varphi(x, b)$ définit X. Par compacité, on dispose alors de b non algébrique sur a tel que $tp(a) = tp(b)$ et $\mathbf{C} \models \varphi(x, a) \longleftrightarrow \varphi(x, b)$. Puisque A est minimal, on a en outre que $a \in \mathrm{acl}(b)$.

On dispose alors d'un automorphisme f tel que $f(b) = a$. Du fait que $b \notin \mathrm{acl}(a)$ et $a \in \mathrm{acl}(b)$ on déduit que $a \notin \mathrm{acl}(f(a))$ et $f(a) \in \mathrm{acl}(a)$ et donc que $\mathrm{acl}(f(a)) \subsetneq \mathrm{acl}(a)$. De plus, puisque $\mathbf{C} \models \varphi(x, a) \longleftrightarrow \varphi(x, b)$ on a $\mathbf{C} \models \varphi(x, a) \longleftrightarrow \varphi(x, f(a))$, ce qui assure que X est définissable sur $\mathrm{acl}(f(a)) \subsetneq \mathrm{acl}(a)$ d'où une contradiction du fait que A est un plus petit ensemble vérifiant cette propriété.

On en déduit qu'il existe une formule $\theta(y) \in tp(a)$ et $a_1, \ldots, a_n$ des tuples de $\mathbf{C}$ tels que

$$\mathbf{C} \models (\theta(y) \wedge \forall x \varphi(x, a) \longleftrightarrow \varphi(x, y)) \longrightarrow \bigvee_{i=1}^{n} y = a_i$$

et donc que X admet un code faible via $\theta(y) \wedge \varphi(x, y)$. $\square$

2.4.3 Caractérisations de l'élimination des imaginaires

On rassemble les propositions 2.4.2 et 2.4.4 au sein du théorème suivant:

Théorème 2.4.1. *On a:*

1. *Si pour tout* $e \in \mathbf{C}^{eq}$ *il existe un tuple* c *de* $\mathbf{C}$ *tel que* $\mathrm{dcl}^{\mathrm{eq}}(e) = \mathrm{dcl}^{\mathrm{eq}}(c)$ *alors* T *admet* (EI).
2. *Si pour tout* $e \in \mathbf{C}^{eq}$ *il existe un tuple* c *de* $\mathbf{C}$ *tel que* $e \in \mathrm{dcl}^{\mathrm{eq}}(c)$ *et* $c \in \mathrm{acl}^{\mathrm{eq}}(e)$ *alors* T *admet* (EFI)

Le résultat suivant s'en déduit aisément:

Proposition 2.4.6. *La théorie* T *admet* (EI) *si et seulement si tout ensemble fini de* $\mathbf{C}$ *a un code et* T *admet* (EFI).

3 Étude de quelques théories

Nous nous proposons ici d'étudier les résultats d'élimination des imaginaires pour quelques théories usuelles.

3.1 Quelques critères

Commençons par le critère suivant pour l'élimination uniforme des imaginaires:

Critère 3.1.1. *Soit T une théorie complète. Si toute formule $\varphi(x, \overline{y})$, où x est un singleton, admet un code uniforme et si T admet des fonctions de Skolem $\emptyset$-définissables, alors T admet* (EUI).

Démonstration. Soit $E(\overline{x}, \overline{y})$ une $\mathcal{L}$ formule qui définit une relation d'équivalence modulo T et soit $\mathcal{M}$ un modèle de T. On se propose de construire une fonction $\emptyset$-définissable f qui satisfait au point (iii) de la définition 2.2.2.

Plus précisément, en notant n la longueur du tuple $\overline{x}$ on montre par récurrence descendante sur $k \in \{-1, \ldots, n-1\}$ qu'il existe une fonction $\emptyset$-définissable f_k telle que f_k soit constante sur les classes de E et pour tout tuple $\overline{a}$ on ait

$$\mathcal{M} \models \exists x_{n-k}, \ldots, x_n E\left(f_k(\overline{a}), x_{n-k}, \ldots, x_n, \overline{a}\right). \tag{4}$$

Pour $k = n-1$, l'hypothèse d'élimination uniforme des imaginaires pour les formules définissant des parties de M assure qu'il existe $\varphi(x_1, \overline{z})$ qui code uniformément $\exists x_2, \ldots, x_n E(x_1, x_2, \ldots, x_n, \overline{y})$. On vérifie alors que toute fonction de Skolem en x_1 pour $\exists x_1, x_2, \ldots, x_n E(x_1, x_2, \ldots, x_n, \overline{y})$ convient pour f_{n-1}.

On itère le procédé de façon naturelle pour $k < n-1$ ce qui donne une fonction $\emptyset$-définissable $f := f_{-1}$ qui vérifie (4). □

On a le critère suivant d'élimination faible des imaginaires:

Critère 3.1.2. *Supposons que T soit une théorie complète qui satisfait les conditions suivantes:*

- *il n'existe pas de suite strictement décroissante $A_0 \supsetneq A_1 \supsetneq \cdots \supsetneq A_n \supsetneq \ldots$ où chaque A_n est la clôture algébrique d'un ensemble fini de paramètres;*
- *si A et B sont des clôtures algébriques d'ensembles finis, le groupe* $\mathrm{Aut}(\mathbf{C}/A \cap B)$ *est engendré par* $\mathrm{Aut}(\mathbf{C}/A)$ *et* $\mathrm{Aut}(\mathbf{C}/B)$*;*

alors T admet (EFI).

Démonstration. Le premier point assure que tout ensemble définissable X admet un ensemble de définition algébriquement clos minimal pour cette propriété. Ces éléments minimaux étant la clôture algébrique d'ensembles finis, le second point assure que si A et B sont de tels éléments minimaux, X est également $A \cap B$-définissable où $A \cap B$ est algébriquement clos, d'où $A = A \cap B = B$ par minimalité de A et B. Il existe donc un plus petit ensemble de définition algébriquement clos pour X. On déduit alors de la proposition 2.4.5 que T admet (EFI). □

3.2 Arithmétique de Peano

Soit $\mathcal{L}_{\text{Peano}} := \{+, ., 0, 1\}$ le langage de Peano et $E(\overline{x}, \overline{y})$ une $\mathcal{L}_{\text{Peano}}$-formule qui définit une relation d'équivalence modulo l'arithmétique de Peano et notons n la longueur du tuple $\overline{x}$. Notons $<$ l'ordre $\emptyset$-définissable de l'arithmétique de Peano et $\prec$ l'ordre $\emptyset$-définissable lexicographique sur M^n. Rappelons que tout partie définissable de $\mathcal{M}$ incluse dans M^n admet un plus petit élément pour l'ordre lexicographique.

Considérons la fonction $\emptyset$-définissable f donnée par $f(\overline{y}) :=$ "le plus petit $\overline{x}$ pour $\prec$ tel que $E(\overline{x}, \overline{y})$". Il est alors clair que

$$T_{\text{Peano}} \vdash E(\overline{x}, \overline{y}) \longleftrightarrow f(\overline{x}) = f(\overline{y})$$

d'où on déduit, en combinant la proposition 2.2.1 ainsi que le fait que le langage de Peano contient deux constantes:

Théorème 3.2.1. *La théorie de l'arithmétique de Peano admet* (EUI).

3.3 Corps réels clos

La théorie des corps réels clos élimine les quantificateurs: on en déduit qu'elle vérifie les hypothèses du critère 3.1.1 (voir [Hod93, section 3.1, Exemple 3]). En conséquence:

Théorème 3.3.1. *La théorie des corps réels clos admet* (EUI).

3.4 Ordres totaux denses sans extrémités

Soit $\mathbf{C}$ un monstre de DLO: l'ordre assure que les parties finies de M sont codées. Pour montrer que DLO admet (EI) il suffit donc, selon la proposition 2.4.6, de montrer que DLO admet (EFI). Pour ce faire, nous allons utiliser le critère 3.1.2.

L'élimination des imaginaires pour DLO assure que tout ensemble de $\mathbf{C}$ est algébriquement clos, si bien que le premier point du critère est vérifié.

Pour ce qui est du second point, il s'agit de montrer que si A et B sont des parties finies de $\mathbf{C}$ alors $\mathrm{Aut}_{A\cap B}(\mathbf{C})$ est engendré par $\mathrm{Aut}_A(\mathbf{C})$ et $\mathrm{Aut}_B(\mathbf{C})$. Ordonnons les éléments de B sous la forme $b_1 < \cdots < b_r$ et posons $b_0 := -\infty$ et $b_{r+1} := +\infty$.

On va montrer par récurrence sur la taille de A que tout élément de $\mathrm{Aut}_{A\cap B}(\mathbf{C})$ est produit d'un élément de $\mathrm{Aut}_A(\mathbf{C})$ et d'un élément de $\mathrm{Aut}_B(\mathbf{C})$.

- Si $A = \emptyset$, le résultat est évident.
- Si $A = \{a\}$, commençons par distinguer deux cas:
  - si $a \in B$: le résultat est évident;
  - si $a \notin B$: soit $f \in \mathrm{Aut}(\mathbf{C})$. Si $f(a) = a$ le résultat est évident: supposons que $f(a) \neq a$ et par exemple que $f(a) < a$. Soit i tel que $a \in]b_i, b_{i+1}[$ et $c < f(a)$.

    On vérifie alors que $tp(c, b_{i+1}/a) = tp(b_i, b_{i+1}/a)$ si bien qu'il existe $g \in \mathrm{Aut}_a(\mathbf{C})$ tel que $g(cb_{i+1}) = b_i b_{i+1}$. Ainsi, gf envoie a sur un élément de $]b_i, b_{i+1}[$.

    On en déduit que $tp(a/B) = tp(gf(a)/B)$ et donc qu'il existe $h \in \mathrm{Aut}_B(\mathbf{C})$ qui envoie $gf(a)$ sur a. De là, $hgf \in \mathrm{Aut}_a(\mathbf{C})$ et donc f est produit d'un éléments de $\mathrm{Aut}_a(\mathbf{C})$ et d'un élément de $\mathrm{Aut}_B(\mathbf{C})$.
- Si $|A'| \geq 1$ et $a \notin A'$, soit $f \in \mathrm{Aut}_{A'a\cap B}(\mathbf{C})$. Distinguons deux cas:
  - si $a \in B$: puisque $f \in \mathrm{Aut}_{A'\cap B}(\mathbf{C})$ l'hypothèse de récurrence assure l'existence de $g \in \mathrm{Aut}_{A'}(\mathbf{C})$ et $h \in \mathrm{Aut}_B(\mathbf{C})$ tels que $f = gh$. Puisque $f(a) = h(a) = a$, on a $g(a) = a$ d'où $g \in \mathrm{Aut}_{A'a}(\mathbf{C})$, ce qui conclut.
  - si $a \notin B$: soit i tel que $a \in]b_i, b_{i+1}[$.

De façon analogue au cas où $|A| = 1$, on construit $g \in \mathrm{Aut}_{A'a}(\mathbf{C})$ qui envoie $f(a)$ dans $]b_i, b_{i+1}[$.

Ainsi, $tp(A'a/B) = tp(A'gf(a)/B)$ d'où l'existence de $h \in \mathrm{Aut}_B(\mathbf{C})$ qui envoie $A'gf(a)$ sur $A'a$. En conséquence, $hgf \in \mathrm{Aut}_{A'a}(\mathbf{C})$, ce qui conclut.

Le second point du critère 3.1.2 est donc vérifié. On en déduit donc, en vertu des arguments donnés au début du paragraphe, le résultat suivant:

Théorème 3.4.1. *La théorie des ordres totaux denses sans extrémités admet* (EI).

Remarque 3.4.1. *Notons néanmoins que* DLO *n'admet pas* (EUI).
De fait, considérons la formule $\varphi(x, yz) := (y = z)$ et supposons par l'absurde qu'elle admet un code uniforme $\psi(x, u)$. Suivant les paramètres, $\varphi(x, yz)$ définit soit $\mathbf{C}$ soit $\emptyset$. On a donc des tuples c et d uniques tels que $\psi(x, c) = \mathbf{C}$ et $\psi(x, d) = \emptyset$. Ainsi, $c, d \in \mathrm{dcl}(\emptyset)$ alors que $\mathrm{dcl}(\emptyset) = \emptyset$, ce qui est absurde.

3.5 Corps algébriquement clos

Une première démonstration de l'élimination des imaginaires dans les corps algébriquement clos a été donnée par Poizat dans [Poi83, Théorème 7]. On donne ici une preuve différente qui repose sur [TZ12, Lemme 8.4.11], attribué à Lascar et Pillay:

Lemme 3.5.1. *Si T est une théorie complète fortement minimale telle que* $\mathrm{acl}(\emptyset)$ *est infinie, alors T admet* (EFI).

Démonstration. En vertu du point 2. du théorème 2.4.1 il suffit de montrer que pour tout élément imaginaire $e = c/E$ il existe un élément de e algébrique sur e, ou encore que pour toute partie définissable $X \subseteq \mathbf{C}^n$, l'ensemble $\mathrm{acl}^{\mathrm{eq}}(\ulcorner X \urcorner)$ rencontre X. On raisonne par récurrence sur n.

Si $n = 1$, la stricte minimalité nous invite à distinguer deux cas. Si X est fini, X est inclus dans $\mathrm{acl}^{\mathrm{eq}}(\ulcorner X \urcorner)$ ce qui conclut. Si X est cofini, $\mathrm{acl}(\emptyset)$ est infini, donc rencontre X ce qui conclut.

Si $n > 1$, soit X_1 la projection de X sur la première coordonnée. Par initialisation il existe $x \in X_1$ qui est dans $\mathrm{acl}^{\mathrm{eq}}(\ulcorner X_1 \urcorner) \subseteq \mathrm{acl}^{\mathrm{eq}}(\ulcorner X \urcorner)$. En posant X_x la fibre de X au-dessus de x, l'hypothèse de récurrence assure l'existence de $y \in X_x$ qui est dans $\mathrm{acl}^{\mathrm{eq}}(\ulcorner X_x \urcorner) \subseteq \mathrm{acl}^{\mathrm{eq}}(\ulcorner X \urcorner)$. Ainsi, le couple (x, y) est à la fois dans X et dans $\mathrm{acl}^{\mathrm{eq}}(\ulcorner X \urcorner)$ ce qui conclut. □

De plus, les corps algébriquement clos codent les ensembles finis:

Lemme 3.5.2. *Les corps algébriquement clos codent les ensembles finis.*

Démonstration. Il suffit de montrer l'assertion pour chaque monstre de ACF_p où p est premier ou nul. Soit donc $\mathbf{C}$ un tel monstre.

Soit A un ensemble fini de k-tuples $c_1, \ldots, c_n$ où $c_i = (c_{i,j})_{j<k}$. Considérons $f_i \in K[X, Y_1, \ldots, Y_k]$ défini par

$$X - \sum_{j<k} c_{i,j} Y_j$$

et $f := \prod_i f_i$. En notant S le tuple des coefficients de s et en se rappelant que $K[X, Y_1, \ldots, Y_k]$ est factoriel, on vérifie qu'un automorphisme de $\mathbf{C}$ stabilise A si et seulement si il fixe s point par point. On en déduit que s est un code de A. □

L'existence de deux constantes dans le langage des anneaux et les deux lemmes précédents combinés à la proposition 2.4.6 conduisent donc au:

Théorème 3.5.1. *La théorie des corps algébriquement clos admet* (EUI).

Partie IV
Cas d'étude des corps algébriquement clos valués

La théorie des corps algébriquement clos valués, notée ACVF, n'élimine les imaginaires ni dans le langages $\mathcal{L}_{\text{div}}$ ni dans le langage tri-sorté. Néanmoins, en rajoutant des sortes dites *géométriques*, Haskell, Hrushovski et Macpherson on montré dans [HHM06] qu'on dispose d'un résultat d'élimination des imaginaires.

On se propose ici de donner un schéma de la partie technique d'une version raccourcie de la démonstration de [HHM06], exposée par Johnson dans [Joh14]. Pour ce faire, on commence par introduire les résultats fondamentaux d'élimination des quantificateurs et de description des ensembles définissables dans ACVF.

1 Langage et théorie des corps valués algébriquement clos

1.1 Première approche naïve

Une première idée est de prendre pour langage $\mathcal{L}_1$ celui des anneaux $\mathcal{L}_{\text{ann}}$ et de rajouter un prédicat unaire P pour l'anneau de valuation. On définit alors la théorie des corps valués par T_1 :="axiomes de corps"+"P est un anneau de valuation".

On peut alors définir la théorie des corps algébriquement clos valués de la façon suivante:

Définition 1.1.1. *La $\mathcal{L}_1$-théorie des corps algébriquement clos valués, notée* ACVF_1*, est la théorie des corps à valuation non triviale dans ce même langage à laquelle on ajoute l'axiome de clôture algébrique du corps.*

L'inconvénient de la signature $\mathcal{L}_1$ est que ACVF_1 n'y élimine pas les quantificateurs, ce qui rend délicate la description des parties définissables.

1.2 Un langage plus adapté

Commençons donc par définir le langage $\mathcal{L}_{\text{div}} := \{0, 1, +, -, \cdot, \text{div}\}$ où div est un prédicat binaire qu'on interprète dans le cas d'un corps valué (K, v) par

$$x \,\text{div}\, y \Longleftrightarrow v(x) \leq v(y).$$

La théorie des corps valués dans le langage $\mathcal{L}_{\text{div}}$ est alors axiomatisée de la façon suivante:

(i) Tout d'abord les axiomes de corps;

(ii) $1 \,\text{div}\, 1 \wedge 1 \,\text{div}\, 0$;

(iii) $\forall x \forall y\, (1 \,\text{div}\, x \wedge 1 \,\text{div}\, y) \longrightarrow 1 \,\text{div}\, x + y \wedge 1 \,\text{div}\, xy$;

(iv) $\forall x \forall y\, (xy = 1) \longrightarrow (1 \,\text{div}\, x \vee 1 \,\text{div}\, y)$;

(v) $\forall x \forall y \forall z\, (xy = 1) \longrightarrow (x \,\text{div}\, z \Longleftrightarrow 1 \,\text{div}\, yz)$.

On peut alors définir la théorie des corps algébriquement clos valués de la façon suivante:

Définition 1.2.1. *La $\mathcal{L}_{\text{div}}$-théorie des corps algébriquement clos valués, notée* ACVF*, est la théorie des corps à valuation non triviale dans ce même langage à laquelle on rajoute l'axiome de clôture algébrique du corps.*

Chaque $\mathcal{L}_1$-modèle $\mathcal{M}_1$ de $ACVF_1$ est clairement définissablement interprétable dans le modèle $\mathcal{M}$ de ACVF défini par $\mathcal{M} := (M_1, 0, 1, +, \cdot, \{x : 1 \operatorname{div} x\})$. Réciproquement, tout $\mathcal{L}_{\text{div}}$-modèle $\mathcal{M}$ de ACVF est définissablement interprétable dans le modèle $\mathcal{M}_1$ de ACVF_1 défini par $\mathcal{M}_1 := \left(M, 0, 1, +, \cdot, \left\{(x, y) : P\left(yx^{-1}\right)\right\}\right)$. Cette bi-interprétabilité conduit à la conclusion suivante:

Fait 1.2.1. *Les parties $\mathcal{L}_1$-définissables d'un corps algébriquement valué sont ses parties $\mathcal{L}_{\text{div}}$-définissables.*

On montre dans la suite que ACVF élimine le quantificateurs ce qui donne une description des parties $\mathcal{L}_{\text{div}}$-définissables d'un corps algébriquement clos valué et donc, en vertu du fait précédent, une description de ses parties $\mathcal{L}_1$-définissables.

1.3 Un langage tri-sorté

On peut également penser au langage muni de trois sortes K, Γ_∞, k et des symboles suivants:

- $\{0, 1, +, -, \cdot\}$ sur K et k;
- $\{0, +, -, \leq, \infty\}$ sur Γ_∞;
- un symbole de fonction $v : K \longrightarrow \Gamma_\infty$;
- un symbole de fonction $\text{res} : K \longrightarrow k$.

Dans ce langage, la théorie des corps algébriquement clos à valuation non triviale élimine également les quantificateurs. On en déduit que les parties définissables de la sorte K sont les mêmes que celles pour les langages des sections précédentes.

2 Élimination des quantificateurs et parties définissables

2.1 Élimination des quantificateurs

Robinson a montré dans [Rob56] que la théorie des corps algébriquement clos valués dans le langage $\mathcal{L}_1$ est modèle-complète. Sa preuve a ensuite été adaptée pour montrer qu'il y a élimination des quantificateurs dans le langage $\mathcal{L}_{\text{div}}$.

On suit ici la démonstration d'élimination des quantificateurs donnée dans [Cha08]. Elle repose sur le critère donnée dans la section suivante. Une autre preuve utilisant le critère donné durant le cours d'introduction à la logique mathématique de l'ENS, qui est également énoncé dans [Mar02, Corollaire 3.1.6], est présentée dans [Rid13].

2.1.1 Un critère d'élimination des quantificateurs

Lemme 2.1.1. *Si T une théorie et $\varphi(x)$ une formule qui n'est pas équivalente à une formule sans quantificateurs modulo T, alors il existe un modèle $\mathcal{M}$ de T et deux tuples a et b de $\mathcal{M}$ qui ont le même type sans quantificateurs et tels que*

$$\mathcal{M} \models \varphi(a) \wedge \neg\varphi(b).$$

Démonstration. Soient T et $\varphi(x)$ comme dans l'énoncé et a, b des tuples de constantes. Il s'agit de montrer que la théorie

$$T \cup \{\psi(a) \Longleftrightarrow \psi(b) : \psi(x) \text{ est sans quantificateurs}\} \cup \{\varphi(a) \Longleftrightarrow \neg\varphi(b)\}$$

est cohérente. □

Critère 2.1.1. *Soit T une théorie. Les assertions suivantes sont équivalentes:*

(i) *La théorie T élimine les quantificateurs.*

(ii) *Pour tous modèles $\aleph_1$-saturés $\mathcal{M}$ et $\mathcal{N}$ de T, pour toutes sous-structures $\mathcal{A}$ et $\mathcal{B}$ engendrées par des parties dénombrables de $\mathcal{M}$ et $\mathcal{N}$ respectivement, tout isomorphisme $f : \mathcal{A} \longrightarrow \mathcal{B}$ et tout $c \in \mathcal{M}$, on peut étendre f à un isomorphisme entre la structure engendrée par Ac et une sous-structure de $\mathcal{N}$.*

Démonstration. Commençons par noter que si $\mathcal{M}$ est une $\mathcal{L}$-structure et $\mathcal{A}$ est une sous-structure de $\mathcal{M}$ engendrée par une partie A_0, alors le type d'isomorphisme de $\mathcal{A}$ est déterminé par l'ensemble des $\mathcal{L}(A_0)$-énoncés sans quantificateurs vérifiés par $(\mathcal{M}, A_0)$.

$(i) \longrightarrow (ii)$: En prenant les notations du point (ii), soit A_0 une partie dénombrable engendrant $\mathcal{A}$ et p l'ensemble des $\mathcal{L}(A_0c)$-énoncés sans quantificateurs vrais dans $\mathcal{M}$. Posons $q(x) := \{\varphi(x) \in \mathcal{L}(A_0) : \varphi(c) \in p\}$.

Pour $\varphi(x) \in q$, l'élimination des quantificateurs dans T assure qu'il existe un $\mathcal{L}(A_0)$-énoncé ψ tel que

$$T \models \exists x\varphi(x) \Longleftrightarrow \psi.$$

Puisque $(\mathcal{M}, A_0) \models \exists x\varphi(x)$, on en déduit que $(\mathcal{M}, A_0) \models \psi$. L'isomorphisme f assure donc que $(\mathcal{N}, f(A_0)) \models \psi$ et donc que $(\mathcal{N}, f(A_0)) \models \exists x\varphi(x)$.

Le type q est donc un type à paramètres dénombrables qui est cohérent dans la $\mathcal{L}(A_0)$-structure $(\mathcal{N}, f(A_0))$, laquelle est $\aleph_1$-saturée. On en déduit qu'il est réalisé par un élément d de $\mathcal{N}$.

La remarque faite en début de preuve assure donc qu'on peut étendre f à un isomorphisme entre la structure engendrée par Ac et celle engendrée par Bd.

$(ii) \longrightarrow (i)$ Il s'agit de montrer que si $\varphi(x, y)$ est une formule sans quantificateurs, alors $\exists x \varphi(x, y)$ est équivalente à une formule sans quantificateurs.

En supposant par l'absurde que ce n'est pas le cas, le lemme 1.1.1 assure qu'il existe un modèle $\mathcal{M}$ de T et deux tuples a et b de M ayant même type sans quantificateurs tels que $\mathcal{M} \models \exists x \varphi(x, a)$ et $\mathcal{M} \models \neg \exists x \varphi(x, b)$. Quitte à prendre une extension élémentaire, on peut supposer que $\mathcal{M}$ est $\aleph_1$-saturée.

La remarque faite au début de la démonstration assure qu'il existe un isomorphisme entre la structure engendrée par a et celle engendrée par b qui envoie a sur b. En notant c un tuple tel que $\mathcal{M} \models \varphi(c, a)$, le point (ii) assure alors qu'on peut étendre cette isomorphisme à un isomorphisme g entre la structure engendrée par ac et une structure étendant celle engendrée par b. On en déduit que $\mathcal{M} \models \varphi(g(c), b)$, ce qui contredit que $\mathcal{M} \models \neg \exists x \varphi(x, b)$. □

2.1.2 Application aux corps algébriquement clos valués

On prend pour langage $\mathcal{L}_{\text{div}}$ et on montre que les corps algébriquement clos valués éliminent les quantificateurs dans ce langage:

Théorème 2.1.1. *La $\mathcal{L}_{\text{div}}$-théorie* ACVF *élimine les quantificateurs.*

Démonstration. On souhaite utiliser le critère 1.1.1. Soient (K, v) et (L, w) deux corps algébriquement clos valués $\aleph_1$-saturés, A et B des sous-anneaux dénombrables de K et L respectivement. Soit $f : A \longrightarrow B$ un isomorphisme de $\mathcal{L}_{\text{div}}$-structures et $c \in K$. Commençons par remarquer qu'on peut supposer que A et B sont des corps.

Distinguons trois cas:

- **Cas 1**: c est algébrique sur A.

  On peut étendre f à un isomorphisme de corps g entre A^{alg} et B^{alg}. Ainsi, $g\left(\mathcal{O}_v \cap A^{\text{alg}}\right)$ est un anneau de valuation de B^{alg} qui étend $\mathcal{O}_w \cap B$. On en déduit qu'il existe $\sigma \in \operatorname{Gal}\left(B^{\text{alg}}/B\right)$ qui envoie $g\left(\mathcal{O}_v \cap A^{\text{alg}}\right)$ sur $\mathcal{O}_w \cap B^{\text{alg}}$. Ainsi, l'isomorphisme $\sigma \circ f$ convient.

  Ayant vu qu'on peut étendre f aux clôtures algébriques respectives de A et B, on peut supposer dans la suite que ces derniers sont algébriquement clos. On suppose également que c est transcendant sur A.

- **Cas 2**: il existe $d \in A(c)$ tel que $\gamma := v(d) \notin \Gamma_A$.

  Puisque A est algébriquement clos, Γ_A est un groupe divisible. On en déduit que que $\Gamma_A \cap \mathbf{Z}\gamma = \emptyset$ puis que pour $\sum_{i \geq 0} a_i d^i \in A(d)$ on a $v\left(\sum_{i \geq 0} a_i d^i\right) = \min_{i \geq 0} v(a_i) + i\gamma$ et donc que $v\left(A(c)^{\times}\right) = \Gamma_A \oplus \mathbf{Z}\gamma$.

  Notons $\varphi : \Gamma_A \longrightarrow \Gamma_B$ l'isomorphisme de groupes ordonnés associé à f et considérons le Γ_B-type $p(\xi) := \{\xi > \alpha : \alpha \in \Gamma_A \text{ et } \gamma > \alpha\} \cup \{\xi < \alpha : \alpha \in \Gamma_A \text{ et } \gamma < \alpha\}$. Puisque φ respecte l'ordre et $\Gamma_L \models$ DLO, le type p est cohérent. Enfin, du fait que L est $\aleph_1$-saturé, on déduit qu'il existe $e \in L$ tel que $\epsilon := w(e)$ satisfait p dans L.

  Notons tout d'abord que puisque $\epsilon \notin \Gamma_B$ et puisque Γ_B est divisible, on a $\Gamma_B \cap \mathbf{Z}\epsilon = \emptyset$. On définit alors $\psi : \Gamma_A \oplus \mathbf{Z}\gamma \longrightarrow \Gamma_B \oplus \mathbf{Z}\epsilon$ par $\psi(\alpha + m\gamma) := \varphi(\alpha) + m\epsilon$ qui est un isomorphisme de groupes. Ce morphisme respecte également l'ordre puisque pour $m \neq m'$ (supposons par exemple $m < m'$) on a

  $$\alpha + m\gamma < \alpha' + m'\gamma \Longleftrightarrow \alpha - \alpha' < (m' - m)\gamma \Longleftrightarrow \frac{\alpha - \alpha'}{m' - m} < \gamma \Longleftrightarrow \frac{\varphi(\alpha) - \varphi(\alpha')}{m' - m} < \epsilon$$

ce qui équivaut à $\psi(\alpha + m\gamma) < \psi(\alpha' + m'\gamma)$.

En outre, puisque $w(e) \notin \Gamma_B$ on en déduit que $e \notin B$ et donc que e est transcendant sur B. On peut donc étendre f à un isomorphisme $g : A(d) \longrightarrow B(e)$ qui envoie d sur e. On vérifie aisément que $\psi \circ v = w \circ g$ si bien que g est un isomorphisme de corps valués.

Puisque $A(c)^{\mathrm{alg}} = A(d)^{\mathrm{alg}}$, le cas précédent assure qu'on peut étendre g à un isomorphisme entre $A(c)^{\mathrm{alg}}$ et une sous-structure de L, ce qui conclut.

- **Cas 3**: il existe $d \in A(c) \cap \mathcal{O}_v$ tel que $\mathrm{res}(d) \notin k_A$.

  Puisque k_A est algébriquement clos, cette hypothèse assure que $\mathrm{res}(d)$ est transcendant sur k_A et donc que d est transcendant sur A. Par $\aleph_1$-saturation de L on trouve $e \in \mathcal{O}_L$ tel que $\mathrm{res}(e) \notin k_B$. On étend alors f en un isomorphisme de corps $g : A(d) \longrightarrow B(e)$ qui envoie d sur e. Il reste à vérifier que g est un morphisme de corps valués.

  Pour le montrer, il suffit de remarquer que $v\left(\sum_{i\geq 0} a_i d^i\right) = \min_{i\geq 0} v(a_i)$: en effet, il suffit de le montrer dans le cas où tous les a_i sont nuls ou de valuation nulle, auquel cas $\mathrm{res}\left(\sum_{i\geq 0} a_i d^i\right) = \sum_{i\geq 0} \mathrm{res}(a_i)\,\mathrm{res}(d)^i$ est non nul par transcendance de $\mathrm{res}(d)$ d'où on déduit que $v\left(\sum_{i\geq 0} a_i d^i\right) = 0$. Il en va de même dans $B\,(e)$.

  On en déduit que g réalise bien un isomorphisme de corps valués. Le cas 1 permet de l'étendre à $A(c)^{\mathrm{alg}}$.

- **Cas 3**: l'extension $A(c)/A$ est immédiate.

  Commençons par remarquer que l'ensemble $\{v(c-a) : a \in A\}$ n'a pas de maximum. En effet, soit $a \in A$ et $a' \in A$ tel que $v(c-a) = v(a')$: puisque $v\left(\frac{c-a}{a'}\right) = 0$ on a alors $a'' \in A$ tel que $v\left(\frac{c-a}{a'} - a''\right) > 0$, d'où on déduit que $v\,(c - a - a'a'') > v(a') = v(c-a)$.

  On en déduit alors que le A-type

  $$p(x) := \{v\,(x-a) = v\,(a') : a, a' \in A \text{ et } v(c-a) = v(a')\}$$

  est cohérent avec $\mathrm{Th}(A)$.

  En effet, si $a_1, a_1', \ldots, a_n, a_n' \in A$ sont tels que $v(c-a_i) = v(a_i')$ alors en choisissant a tel que pour tout i on ait $v(c-a) > v(c-a_i)$, on obtient par ultramétricité que $v(a-a_i) = v(a-c+c-a_i) = v(c-a_i) = v(a_i')$.

  Puisque f est un isomorphisme de $\mathcal{L}_{\mathrm{div}}$-structure entre A et B, on en déduit que $fp(x)$ est un B-type cohérent avec $\mathrm{Th}(B)$. Par $\aleph_1$-saturation de L, considérons d une réalisation de fp dans L et remarquons qu'elle n'est pas dans B, donc qu'elle est transcendante sur B.

  On dispose alors d'un isomorphisme de corps $g : A(c) \longrightarrow B(d)$ qui étend f et qui envoie c sur d. Il s'agit de montrer qu'il respecte la valuation.

  Soit $\varphi : \Gamma_A \longrightarrow \Gamma_B$ l'isomorphisme de groupes correspondant à f. Puisque tout polynôme d à coefficients dans A est scindé dans A, tout élément de $A\,[c]$

s'écrit sous la forme $\lambda \prod_i (c - a_i)$ où $\lambda, a_i \in A$. En prenant $a'_i \in A$ tel que $v(c - a_i) = v(a'_i)$, on a alors

$$wg\left(\lambda \prod_i (c - a_i)\right) = wg(\lambda) + wg\left(\prod_i (c - a_i)\right) = \varphi f(\lambda) + \sum_i w\left(d - f(a_i)\right)$$

si bien que

$$wg\left(\lambda \prod_i (c - a_i)\right) = \varphi f(\lambda) + \sum_i w\left(f(a'_i)\right) = \varphi f(\lambda) + \sum_i \varphi v(a - a_i) = \varphi v\left(\lambda \prod_i (c - a_i)\right)$$

d'où on déduit que f est un isomorphisme de corps valués.

□

2.2 Conséquences les opération de clôture et les ensembles définissables

2.2.1 Complétions

En notant, pour un couple d'entiers (m, n), $\mathrm{ACVF}_{(m,n)}$ la $\mathcal{L}_{\mathrm{div}}$-théorie axiomatisée par:

ACVF +"le corps est de caractéristique m"+"le corps résiduel est de caractéristique n"

on a la description suivante des différentes complétions de ACVF:

Proposition 2.2.1. *Les différentes complétions de* ACVF *sont données par les* $\mathrm{ACVF}_{(0,0)}$*,* $\mathrm{ACVF}_{(0,p)}$ *et* $\mathrm{ACVF}_{(p,p)}$*, où p désigne un nombre premier.*

Démonstration. Il est clair que tout modèle de ACVF est modèle d'une des théories décrites dans l'énoncé et que deux de ces théories n'ont pas de modèles communs. Il s'agit donc de montrer que chacune de ces théories est complète:

- $\mathrm{ACVF}_{(0,0)}$: tout modèle de ACVF de caractéristique nulle et dont le corps résiduel est de caractéristique nulle a comme sous-structure $\mathbf{Q}^{\mathrm{alg}}$ muni de la valuation triviale. On en déduit, par élimination des quantificateurs, qu'ils ont tous la même théorie.
- $\mathrm{ACVF}_{(0,p)}$: tout modèle de ACVF de caractéristique nulle et dont le corps résiduel est de caractéristique p a comme sous-structure le corps valué $\mathbf{Q}_p^{\mathrm{alg}}$. L'élimination des quantificateurs assure alors qu'ils ont tous la même théorie.
- $\mathrm{ACVF}_{(p,p)}$: tout modèle de ACVF de caractéristique p et dont le corps résiduel est de caractéristique p a comme sous-structure le corps valué $\mathbf{F}_p$ muni de la valuation triviale. L'élimination des quantificateurs assure alors qu'ils ont tous la même théorie.

□

2.2.2 Opérations de clôtures

L'élimination des quantificateurs donne également une description des clôtures algébrique et définissable dans un modèle de ACVF:

Proposition 2.2.2. *Si $K \models$ ACVF et $A \subseteq K$, alors $\mathrm{acl}(A)$ est la clôture algébrique du sous-corps de K engendré par A.*

Démonstration. En notant K' le corps décrit par l'énoncé, il est d'emblée clair que $K' \subseteq \mathrm{acl}(A)$. De plus, puisque ACVF élimine les quantificateurs, elle est modèle-complète d'où $K' \preceq K$. On en déduit alors aisément que $\mathrm{acl}(A) \subseteq K'$ si bien que $K' = \mathrm{acl}(A)$. □

En ce qui concerne la clôture définissable on admettra le résultat suivant dont une preuve est donnée dans [Rid13, Remarque 1.32]:

Proposition 2.2.3. *Si $K \models \mathrm{ACVF}$ et $A \subseteq K$ alors $\mathrm{dcl}(A)$ est l'hensélianisé du corps des fractions de l'anneau engendré par A.*

2.2.3 Parties définissables

Une description canonique des parties définissables d'un corps algébriquement clos valués est donnée par Holly dans [Hol95]. Sans en donner la preuve, donnons cette description.

Définition 2.2.1. *Si (K, v) est un corps valué, un fromage suisse de K est une partie de la forme $B - \bigcup_{i=1}^{n} B_i$ où B et les B_i sont des boules de K telles que $B_i \subseteq B$ et $B_i \cap B_j = \emptyset$ pour $i \neq j$.*

On dit que deux fromages suisses sont trivialement emboîtés si la boule extérieure de l'un est un trou de l'autre.

On dispose alors de la description suivante, que le lecteur intéressé peut retrouver dans [Hol95, Théorème 3.26]:

Théorème 2.2.1. *Si $K \models \mathrm{ACVF}$ alors toute partie définissable s'écrit de manière unique comme une union de fromages suisses non trivialement emboîtés.*

Enfin, l'élimination des quantificateurs donne la cardinalité des parties définissables non finies:

Fait 2.2.1. *Si $(K, v) \models \mathrm{ACVF}$ alors toute partie définissable non finie a le cardinal de K.*

Démonstration. Il est clair qu'il suffit de le montrer pour les parties définissables incluses dans K. Soit donc $X \subseteq K$ une partie définissable: par le théorème précédent X contient un fromage suisse infini. Ce dernier est alors d'intérieur non vide, si bien que X contient une boule fermée non triviale B. Or, il est clair que le cardinal de B est celui de $\mathcal{O}_v$ et donc de son corps des fractions K, ce qui conclut. □

3 Premières remarques sur l'élimination des imaginaires

Dans cette section, on pose les jalons du langage qui sera utilisé puis on donne un critère d'élimination des imaginaires pour une théorie à laquelle on rajoute quelques sortes imaginaires. Ce critère est celui de [Joh14] dont on modifie légèrement la démonstration.

3.1 Insuffisance du langage uni-sorté

Il est légitime de se demander si la $\mathcal{L}_{\text{div}}$-théorie ACVF élimine les imaginaires. La réponse étant négative, donnons un certain nombre de relations d'équivalences dont on ne peut éliminer les imaginaires.

Fait 3.1.1. *En posant $E(x,y) := (v(x) = v(y))$, il n'existe pas de fonction $\emptyset$-définissable f telle que* $\mathrm{ACVF} \vdash E(x,y) \iff (f(x) = f(y))$.

Démonstration. Supposons par l'absurde qu'il existe une telle fonction $\emptyset$-définissable f et considérons le corps valué $K := \mathbf{Q}_p^{\text{alg}}$ dont on rappelle que le groupe de valuation est isomorphe à $\mathbf{Q}$.

Puisque K a la puissance du continu, on aurait alors $|K| > |\Gamma_K| = |f(K)|$ ce qui contredit le fait 1.2.1. □

On prouve de façon analogue les fait suivants:

Fait 3.1.2. *En posant $E(x,y) := (res(x) = res(y))$, il n'existe pas de fonction $\emptyset$-définissable f telle que* $\mathrm{ACVF} \vdash E(x,y) \iff (f(x) = f(y))$.

Fait 3.1.3. *En posant $E((x_1,x_2),(y_1,y_2)) := (B(x_1, v(x_1 - x_2)) = B(y_1, v(y_1 - y_2)))$, il n'existe pas de fonction $\emptyset$-définissable f telle que* $\mathrm{ACVF} \vdash E((x_1,x_2),(y_1,y_2)) \iff (f(x_1,x_2) = f(y_1,y_2))$.

En vertu des faits précédents, il est légitime de penser que puisqu'on ne peut coder les boules dans le langage $\mathcal{L}_{\text{div}}$, il serait suffisant de rajouter des sortes pour les boules.

En réalité, Holly a montré dans [Hol97] qu'en rajoutant de telles sortes, on peut coder les parties définissables du corps ambiant. Néanmoins, il s'avère que ces sortes ne sont pas suffisantes: il faut en réalité introduire des "boules de dimension n".

3.2 Notations et sortes géométriques

Si on considère un corps algébriquement clos valué $(K, \mathcal{O})$, dont on note k le corps résiduel, on peut considérer les sortes suivantes qu'on qualifiera de "géométriques":

- Une sorte K pour le corps.
- Pour chaque n une sorte S_n qui est l'ensemble des (codes des) $\mathcal{O}$-réseaux de K^n, c'est-à-dire les $\mathcal{O}$-sous-modules de K^n qui sont libres de rang n.
- Pour chaque n une sorte T_n qui est l'ensemble des couples (Λ, ξ) où $\Lambda \in S_n$ et $\xi \in \operatorname{res} \Lambda := \Lambda \otimes_{\mathcal{O}} k$: tout élément de T_n est appelé un *torseur*.
- Pour chaque (n,l) une sorte R_{nl} qui est l'ensemble des couples (Λ, V) où $\Lambda \in S_n$ et V est un sous-espace de dimension l de $\operatorname{res} \Lambda$.

Chacune de ces sortes est interprétable dans ACVF: montrons-le et tâchons de décrire les premiers termes de chacune de ces sortes.

Par exemple, S_n s'identifie à $\mathrm{GL}_n(K)/\mathrm{GL}_n(\mathcal{O})$ et donc à une sorte de K^{eq}. On notera alors que S_1 s'identifie à $\Gamma_K = K^\times/\mathcal{O}^\times$ et que la surjection canonique $v : K \longrightarrow K^\times/\mathcal{O}^\times \simeq S_1$ s'identifie à la valuation. Notons que S_1 s'identifie aux boules fermées centrées en 0 si bien que celles-ci sont codées. Le fait suivant assure que toute boule fermée est codée dans $S_2 \cup K$ (une boule triviale étant codée par l'élément correspondant dans K) et plus généralement que tout translaté d'un n-réseau est codé dans S_{n+1}:

Fait 3.2.1. *Si $s \in S_n$ et $a \in K$ alors le sous-module de K^{n+1} engendré par $(a+s)\times\{1\}$ est un $n+1$-réseau qui code $a+s$.*

Démonstration. Le fait qu'il s'agit d'un $n+1$-réseau est aisé à vérifier. La fonction h qui à $a+s$ associe le $n+1$-réseau engendré par $(a+s)\times\{1\}$ est en outre $\emptyset$-définissable, ce qui se voit en remarquant que $h(a+s) \cap K^n \times \{1\} = (a+s) \times \{1\}$. $\square$

De plus, T_n s'identifie à $\biguplus_{s\in S_n} s/\mathfrak{m}s$ si bien que T_n est dans K^{eq} puisque ses éléments sont des classes de s (qui est dans K^{eq} par le sous-groupe définissable $\mathfrak{m}s$. Remarquons également que puisque $\mathcal{O}$ est un réseau de rang 1, $k = \mathcal{O}/\mathfrak{m} \subseteq T_1$ et l'application res qui à $a \in \mathcal{O}$ associe sa classe résiduelle $a + \mathfrak{m}$ est définissable.

On montre d'abord que la théorie ACVF élimine les imaginaires dans les sortes K et R_{nl}. En guise de conclusion, on finira par en déduire qu'elle élimine également les imaginaires dans les sortes géométriques "standards" K, S_n et T_n.

3.3 Un critère d'élimination des imaginaires

Critère 3.3.1. *Soit T une théorie dans un langage avec sorte de base K et soit $\mathcal{G}$ une famille de sortes de K^{eq}. Supposons que:*

1. *pour toute partie définissable non vide $X \subseteq K^1$ il existe un type $\mathrm{acl}^{\mathrm{eq}}(\ulcorner X \urcorner)$-définissable inclus dans X;*

2. *tout type définissable de K^n a un code (éventuellement infini) dans $\mathcal{G}$, au sens où si p est un type définissable de K^n alors l'ensemble des codes des définitions de p est interdéfinissable avec un ensemble (éventuellement infini) de tuples de sortes dans $\mathcal{G}$.*

3. *tout ensemble fini de tuples de $\mathcal{G}$ a un code dans $\mathcal{G}$.*

Alors T admet l'élimination des imaginaires dans les sortes $\mathcal{G}$.

On se propose de donner un schéma de démonstration:

Démonstration. Commençons par montrer par récurrence sur n que toute partie définissable non vide $X \subseteq K^n$ contient un type $\mathrm{acl}^{\mathrm{eq}}(\ulcorner X \urcorner)$-définissable, l'initialisation étant donnée par 1.

En projetant X sur les $n-1$ première coordonnées on a par hypothèse de récurrence un type $\mathrm{acl}^{\mathrm{eq}}(\ulcorner \pi(X) \urcorner)$-définissable inclus dans $\pi(X)$. En notant a_i une réalisation de ce type, considérons sa fibre F dans K^1 qui est $\ulcorner X \urcorner a_1$-définissable. Par 1., F contient un type $\mathrm{acl}^{\mathrm{eq}}(\ulcorner X \urcorner a_1)$-définissable dont on note a_2 une réalisation. On en déduit aisément qu'il existe un type $\mathrm{acl}^{\mathrm{eq}}(\ulcorner X \urcorner)$-définissable réalisé par (a_1, a_2), si bien qu'il est inclus dans X.

Soit e un élément imaginaire qui code une partie définissable $X \subseteq K^n$, p un type $\mathrm{acl}^{\mathrm{eq}}(e)$-définissable inclus dans X et, par 2., un code t de p issu de $\mathcal{G}$. On a alors $e \in \mathrm{dcl}^{\mathrm{eq}}(t)$ et $t \in \mathrm{dcl}^{\mathcal{G}}(e)$. On peut se ramener au cas où t est un tuple fini t_0: puisque l'ensemble des conjugués de t_0 est fini, il est par 3. codé par un certain s de $\mathcal{G}$. On vérifie alors que $s \in \mathrm{dcl}^{\mathcal{G}}(e)$ et $e \in \mathrm{dcl}^{\mathrm{eq}}(s)$, ce qui conclut.

$\square$

4 Élimination des imaginaires

Rappelons que nous commençons par considérer l'ensemble des sortes $\mathcal{G} := K \cup \bigcup_{n,l} R_{nl}$. On se propose ici de montrer que le point 3. du critère 3.3.1 est vérifié par ACVF pour les sortes $\mathcal{G}$, à savoir:

3. tout ensemble fini de tuples de $\mathcal{G}$ a un code dans $\mathcal{G}$.

Dans la suite, on travaille dans un monstre $\mathbf{U}$ de ACVF.

4.1 Opérations sur les types définissables et quelques définitions

4.1.1 Produit et poussé en avant

Commençons par présenter le poussé en avant d'un type définissable:

Définition 4.1.1. *Soit $p(\overline{x})$ un type C-définissable et $f : X \subseteq \mathbf{U}^{\overline{x}} \longrightarrow Y$ une fonction C-définissable. Le poussé en avant $f_*p(\overline{y})$ de p par f est le type C-définissable donné par:*

$$\mathrm{d}_{f_*p}\left(\varphi(\overline{y}, \overline{z})\right) := \mathrm{d}_p\left(\varphi\left(f(\overline{x}), \overline{z}\right)\right).$$

Avec les notations de la définition, on a:

Fait 4.1.1. *Si $B \supseteq C$ et $a \in \mathbf{U}$ alors:*

$$a \models p \restriction B \Longrightarrow f(a) \models f_*p \restriction B.$$

Dans le cas où la réciproque est vraie, on dit que p est dominé le long de f.

Passons à la définition du produit de deux types définissables:

Définition 4.1.2. *Si p et q sont des types C-définissables alors le produit $p \otimes q$ est le C-type définissable donné par:*

$$\mathrm{d}_{p\otimes q}\left(\varphi(\overline{x}, \overline{y}, \overline{z})\right) := \mathrm{d}_q\left(\mathrm{d}_p\left(\varphi(\overline{x}, \overline{y}, \overline{z})\right)\right).$$

Le produit est également caractérisé par:

$$(a, b) \models p \otimes q \restriction B \Longleftrightarrow a \models p \restriction Bb \text{ et } b \models q \restriction B$$

dès que $B \supseteq C$.

Fait 4.1.2. *On a les propriétés suivantes:*

1. *Le produit des types définissables est associatif.*
2. *Le poussé en avant d'un produit est le produit des poussés en avant.*

On retiendra néanmoins que le produit n'est en général pas commutatif.

4.1.2 Les types génériquement stables

Définition 4.1.3. *Un type $p(\overline{x})$ est génériquement stable si $p(\overline{x}) \otimes q(\overline{y}) = q(\overline{y}) \otimes p(\overline{x})$ pour type définissable $q(\overline{y})$.*

Proposition 4.1.1. *On dispose des propriétés suivantes:*

1. *un produit de types génériquement stables est génériquement stable.*
2. *le poussé en avant d'un type génériquement stable est génériquement stable.*
3. *si p est dominé le long de f et f_*p est génériquement stable alors p est génériquement stable.*

4. *si p et q sont génériquement stables et dominés le long de f et g respectivement, alors $p \otimes q$ est dominé le long de $f \times g$.*

Démonstration. Les points 1. et 2. résultent du fait 4.1.2.

Pour montrer 3., soit q un type définissable et B un ensemble. Si a et b sont tels que $(b, a) \models q \otimes p \restriction B$ alors:

$$(b, a) \models q \otimes p \restriction B \Longrightarrow (b, f(a)) \models q \otimes f_* p \restriction B \Longrightarrow (f(a), b) \models f_* p \otimes q \restriction B.$$

Puisque p est dominé le long de f on en déduit que $(a, b) \models p \otimes q \restriction B$. Ceci étant vrai pour tout B, il vient que $p \otimes q = q \otimes p$.

La preuve du point 4 utilise des arguments analogues à ceux utilisés pour montrer le point 3. □

4.1.3 Une notion d'indépendance

On donne ici une définition ad-hoc de la notion d'indépendance, dont une étude plus approfondie est faite dans [TZ12].

Définition 4.1.4. *Soit $\overline{a}$ est un tuple fini et B, C des parties du monstre. Les assertions suivantes sont équivalentes:*

1) *le type $tp(\overline{a}/BC)$ admet une extension globale C-définissable.*

2) *pour tout ensemble D il existe une extension C-définissable de $tp(\overline{a}/BC)$ à un BCD-type.*

3) *pour tout ensemble D il existe $D' \equiv_{BC} D$ tel que $tp(\overline{a}/BCD')$ est C-définissable.*

4) *il existe un model $M \supseteq BC$ tel que $tp(\overline{a}/M)$ est C-définissable.*

On dit dans ce cas que A est indépendant avec B au-dessus de C, et on note $A \mathop{\smile\!\!\!\!\!\!\mid}\nolimits_C B$.

Démonstration. 1) $\longrightarrow$ 2): il suffit de restreindre la définition globale.

2) $\longrightarrow$ 3): si D est un ensemble, soit $tp(\overline{a}'/BCD)$ un type C-définissable qui étend $tp(\overline{a}/BC)$. Par saturation, il existe D' tel que $\overline{a}'D \equiv_{BC} \overline{a}D'$ d'où on déduit que $tp(A/BCD')$ est C-définissable avec $D \equiv_{BC} D'$.

3) $\longrightarrow$ 4) et 4) $\longrightarrow$ 1) sont évidents. □

Pour la prochaine proposition nous avons besoin du fait suivant:

Fait 4.1.3. *Soient $C \subseteq B$ des ensembles et a_1, a_2 des tuples. Si $p_1 := tp(a_1/B)$ est C-définissables et $p_2 := tp(a_2/Ba_1)$ est Ca_1-définissable alors $q := tp(a_1 a_2/B)$ est C-définissable.*

Démonstration. Il suffit de remarquer que $q = p_1 \otimes p_2$. □

On dispose de la propriété de *transitivité à gauche*:

Proposition 4.1.2. *Si $a_1 \mathop{\smile\!\!\!\!\!\!\mid}\nolimits_C B$ et $a_2 \mathop{\smile\!\!\!\!\!\!\mid}\nolimits_{Ca_1} B$ alors $a_2 a_1 \mathop{\smile\!\!\!\!\!\!\mid}\nolimits_C B$.*

Démonstration. On utilise le point 3) de la définition. Soit D un ensemble.

Puisque $a_1 \mathop{\smile\!\!\!\!\!\!\mid}\nolimits_C B$, il existe $D' \equiv_{BC} D$ tel que $tp(a_1/BCD')$ est C-définissable.

De même, puisque $a_2 \mathop{\smile\!\!\!\!\!\!\mid}\nolimits_{Ca_1} B$, il existe $D'' \equiv_{Ca_1B} D'$ tel que $tp(a_2/BCa_1D'')$ est Ca_1-définissable. Puisque $D'' \equiv_{CB} D'$, il vient également que $tp(a_1/BCD'')$ est C-définissable.

Le fait précédent assure alors que $tp(a_2 a_1/BCD'')$ est C-définissable où $D'' \equiv_{BC} D' \equiv_{BC} D$, ce qui conclut. □

4.2 Démonstration du troisième point du critère

Commençons par rappeler le point 3. du critère 3.3.1, point qu'il s'agit de vérifier dans ACVF avec $\mathcal{G}$ qui est la collection de K est des R_{nl} (qu'on appellera également les sortes géométriques):

Théorème 4.2.1. *Tout ensemble fini de tuples de $\mathcal{G}$ a un code dans $\mathcal{G}$.*

Définition 4.2.1. *Si X est un ensemble, on définit $\mathrm{Sym}^n(X) := X^n/\mathfrak{S}_n$ où S_n agit sur X_n par $\sigma(x_1, \ldots, x_n) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. On notera $\sigma : X^n \longrightarrow \mathrm{Sym}^n(X)$ la surjection canonique.*

Avec cette définition, il suffit de montrer le résultat suivant:

Théorème 4.2.2. *Soit G un produit fini de sortes géométriques. Tout élément de $\mathrm{Sym}^n(G)$ a un code géométrique, c'est-à-dire un code dans les sortes géométriques.*

En effet, le théorème 4.2.1 se déduit aisément du théorème 4.2.2 via le fait suivant:

Fait 4.2.1. *Si $S = \{x_1, \ldots, x_n\}$ est un ensemble fini vérifiant $S \subseteq G$ alors $\sigma(x_1, \ldots, x_n)$ est un code de S.*

Démonstration. Un automorphisme de $\mathbf{U}^{\mathrm{eq}}$ stabilise S si et seulement si il fixe $\sigma(x_1, \ldots, x_n)$ point par point. □

La suite de cette section est donc vouée à la démonstration du théorème 3.2.2.

On sera amené à admettre le résultat suivant, dont une preuve est donnée dans [Joh14, Théorème 4.5]:

Théorème 4.2.3. *Tout type définissable qui est dans K^n admet un code géométrique.*

4.2.1 Relèvements définissables

Définition 4.2.2. *On dit qu'une application $\emptyset$-définissable $\pi : X \longrightarrow Y$ admet un relèvement définissable si pour tout $b \in Y$ il existe un type b-définissable p_b dans $\pi^{-1}(\{b\})$.*

On dit que l'application π admet un relèvement génériquement stable si p_b peut être choisi génériquement stable.

Remarque 4.2.1. *Quitte à modifier l'application $b \mapsto p_b$, on peut supposer qu'elle est $\mathrm{Aut}(\mathbf{U})$-équivariante, c'est-à-dire que $p_{\sigma(b)} = \sigma(p_b)$ pour tout $\sigma \in \mathrm{Aut}(\mathbf{U})$.*

On dispose du résultat suivant de relèvement des types via des applications ayant un relèvement définissable:

Proposition 4.2.1. *Soient une application $\pi : X \longrightarrow Y$ ayant un relèvement définissable, q un type dans Y qui est C-définissable. Il existe un type p dans X qui est C-définissable et tel que $q = \pi_* p$.*

Démonstration. Soit π et q comme dans l'énoncé et $\mathcal{M}$ un modèle inclus dans le monstre et qui contient C.

Soit b tel que $b \models q{\restriction}M$: on a alors $b \downarrow_C M$.

Considérons $\mathcal{N}$ un modèle qui contient Mb et prenons $a \in \pi^{-1}(\{b\})$ qui réalise $p_b{\restriction}M$. Le type $tp(a/N)$ est alors b-définissable d'où on déduit que $a \downarrow_{Cb} M$ (car $MbC \subseteq N$).

Par le résultat de transitivité à gauche de la proposition 4.1.2 on en déduit que $ba \downarrow_C M$ et donc que $a \downarrow_C M$ d'où $a \models p{\restriction}M$ pour un type C-définissable p. Du fait 4.1.1, il vient donc que $\pi(a) = b \models \pi_* p{\restriction}M$.

Ainsi, $\pi_* p{\restriction}M = q{\restriction}M$ pour tout modèle $\mathcal{M}$) qui contient C, si bien que $q = \pi_* p$. □

On en déduit un résultat de transfert de l'existence de codes géométriques pour les types:

Proposition 4.2.2. *Si $\pi : X \longrightarrow Y$ admet un relèvement définissable et si tout type définissable dans X admet un code dans les sortes géométriques, alors tout type définissable dans Y admet un code dans les sortes géométriques.*

Démonstration. Soit q un type définissable dans Y. D'après la proposition précédente, il existe un type p dans X qui est $\lceil q \rceil$-définissable et tel que $q = \pi_* p$.

Puisque p est $\lceil q \rceil$-définissable, on a $\lceil q \rceil \in \operatorname{dcl}(\lceil p \rceil)$. De plus, puisque $q = \pi_* p$, on a également $\lceil p \rceil \in \operatorname{dcl}(\lceil q \rceil)$. Ainsi, $\lceil p \rceil$ et $\lceil q \rceil$ sont interdéfinissables, ce qui conclut. □

Fait 4.2.2. *On dispose des opérations suivantes sur les application ayant un relèvement définissable:*

1) *Si $\pi : X \longrightarrow Y$ et $\pi' : X' \longrightarrow Y'$ ont un relèvement définissable (respectivement génériquement stable) alors $\pi \times \pi'$ admet un relèvement définissable (respectivement génériquement stable).*

2) *Si $\pi : X \longrightarrow Y$ admet un relèvement génériquement stable, alors l'application $\operatorname{Sym}^n \pi : \operatorname{Sym}^n X \longrightarrow \operatorname{Sym}^n Y$ admet un relèvement génériquement stable.*

Démonstration. Pour 1), si $b \mapsto p_n$ et $b' \mapsto p_{b'}$ sont des relèvements définissables (respectivement génériquement stables)de π et π' respectivement, alors $(b, b') \mapsto p_b \otimes p_{b'}$ est un relèvement définissable (respectivement génériquement stable) de $\pi \times \pi'$.

Pour 2), si $b \mapsto p_b$ est un relèvement génériquement stable équivariant de π, alors $\sigma(b_1, \ldots, b_n) \mapsto p_{b_1} \otimes \cdots \otimes p_{b_n}$ est bien défini et est un relèvement définissable de $\operatorname{Sym}^n \pi$. □

4.2.2 Démonstration du théorème

Soit G un produit de sortes géométriques: il s'agit de montrer que tout élément de $\operatorname{Sym}^n G$ a un code géométrique.

On va en fait montrer que tout type définissable dans $\operatorname{Sym}^n G$ a un code géométrique: le résultat en découle en considérant les types constants. Commençons par remarquer qu'en vertu du fait 4.2.2 on peut supposer que G est une des sortes géométriques.

L'idée de la démonstration est de trouver une application $\emptyset$-définissable $G' \longrightarrow G$ ayant un relèvement génériquement stable et telle que tout élément de $\operatorname{Sym}^n G'$ admet un code géométrique: en utilisant la proposition 4.2.2, cela suffit à conclure.

Pour construire un tel G' et une telle application, nous avons besoin du lemme suivant, dont on reporte la démonstration à plus tard:

Lemme 4.2.1. *Les types définissables de* $\operatorname{Sym}^n \left(K^m \times k^l\right)$ *ont des codes géométriques.*

Il suffit donc de construire $G' \longrightarrow G$ qui admet un relèvement génériquement stable, ainsi qu'une injection $\emptyset$-définissable $G' \hookrightarrow K^m \times k^l$:

- **Si** $G = K$: Il suffit de prendre $G' := K$ et les applications d'identité.
- **Si** $G = R_{nl}$: En posant $\widetilde{R_{nl}} := \left\{ \left(\vec{b}, \Lambda, V\right) : (\Lambda, V) \in R_{nl} \text{ et } \vec{b} \text{ est une } \mathcal{O}\text{-base de } \Lambda \right\}$ on admettra que l'application suivante a un relèvement génériquement stable (voir par exemple [Joh14, Section 2.3]):

$$\begin{array}{ccc} \widetilde{R_{nl}} & \hookrightarrow & R_{nl} \\ \left(\vec{b}, \Lambda, V\right) & \longmapsto & (\Lambda, V) \end{array}$$

On peut également injecter $\widetilde{R_{nl}}$ dans un $K^M \times k^L$. En effet, en notant $\mathrm{Gr}(V,p)$ la grassmanienne d'ordre p de V, on a un plongement

$$\begin{aligned} \widetilde{R_{nl}} &\hookrightarrow K^{n^2} \times \mathrm{Gr}\left(\Lambda/\mathfrak{m}\Lambda, l\right) \\ \left(\vec{b}, \Lambda, V\right) &\longmapsto (\Lambda, V) \end{aligned}$$

qu'on peut composer par le plongement de Plücker

$$K^{n^2} \times \mathrm{Gr}\left(\Lambda/\mathfrak{m}\Lambda, l\right) \hookrightarrow K^{n^2} \times \mathbf{P}\left(\bigwedge\nolimits^l \left(\Lambda/\mathfrak{m}\Lambda\right)\right)$$

puis on note qu'on a un isomorphisme

$$K^{n^2} \times \mathbf{P}\left(\bigwedge\nolimits^l \left(\Lambda/\mathfrak{m}\Lambda\right)\right) \xrightarrow{\sim} K^{n^2} \times \mathbf{P}\left(k^L\right)$$

avec $L := \binom{n}{l}$. Enfin, puisque k est algébriquement clos et ACF élimine uniformément les imaginaires, on a un plongement $\emptyset$-définissable de $\mathbf{P}\left(k^L\right)$ dans un certain k^M. On en déduit l'existence d'un plongement $K^{n^2} \times \mathbf{P}\left(k^L\right) \hookrightarrow K^{n^2} \times k^M$. En composant dans l'ordre toutes les applications ainsi obtenues, on finit donc par avoir un plongement

$$\widetilde{R_{nl}} \hookrightarrow K^{n^2} \times k^M$$

ce qui conclut.

Il s'agit maintenant de montrer le lemme 3.2.1.

Preuve du lemme 4.2.1: Soit p un type définissable qui est dans $\mathrm{Sym}^n\left(K^m \times k^l\right)$ et $\lceil p \rceil$ un imaginaire qui le code. Il s'agit de montrer que $\lceil p \rceil$ est interdéfinissable avec un tuple géométrique.

Nous allons pour l'instant admettre le lemme suivant:

Lemme 4.2.2. *Si S est une partie finie C-définissable de K, alors il existe α dans une puissance de K tel que $\alpha \mathop{\downarrow}_C C$ ainsi qu'une injection de S dans une puissance de k qui est $\alpha\lceil S \rceil$-définissable.*

On va raisonner en deux temps:

- **Montrons d'abord que $\lceil p \rceil$ code également un type dans un produit de puissances de K et k:**

  Soit β une réalisation de p dans $\mathrm{Sym}^n\left(K^m \times k^l\right)$ et $\mathcal{M}$ un modèle qui contient $\beta\lceil p \rceil$. Écrivons $\beta = \sigma(a_1, b_1, \ldots, a_n b_n)$, où $a_i \in K^m$ et $b_i \in k^l$, et posons $S := \{\text{coordonées des } a_i\} \subseteq K$. L'ensemble fini S est alors β-définissable et donc $\beta\lceil p \rceil$-définissable.

  En vertu du lemme 4.2.2, on a alors α qui est un tuple de K tel que $\alpha \mathop{\downarrow}_{\beta\lceil p \rceil} M$ ainsi qu'une injection f de S dans $k^{l'}$ qui est $\alpha\lceil S \rceil$-définissable.

  Puisque $\beta \mathop{\downarrow}_{\lceil p \rceil} M$ et $\alpha \mathop{\downarrow}_{\beta\lceil p \rceil} M$, la transitivité à gauche (proposition 3.1.2) assure que $\alpha\beta \mathop{\downarrow}_{\lceil p \rceil} M$, d'où on déduit que $tp\left(\alpha\beta/M\right)$ et $tp\left(\beta/M\right) = p$ ont les mêmes codes.

Fait 4.2.3. *L'élément β est interdéfinissable au-dessus de α avec l'élément*

$$\omega := (\sigma(a_1, \ldots, a_n), \sigma(f(a_1)b_1, \ldots, f(a_n)b_n)) \in \mathrm{Sym}^n(K^m) \times \mathrm{Sym}^n\left(k^{l'm+l}\right).$$

Démonstration. Il est évident que ω est définissable sur $\alpha\beta$.

Réciproquement, β est définissable sur $\alpha\omega$. En effet, les premières coordonnées de ω déterminent S; puis S et α déterminent f laquelle, injective, permet de retrouver β à partir des secondes coordonnées de ω. □

Puisque ACF admet l'élimination uniforme des imaginaires et puisque K et k sont algébriquement clos, on peut coder tout élément de $\mathrm{Sym}^n(K^m)$ par un élément d'un certain K^M et tout élément de $\mathrm{Sym}^n\left(k^{l'm+l}\right)$ par un élément d'un certain k^L. On en déduit qu'on peut identifier ω à un élément $\gamma\delta \in K^M \times k^L$.

Le fait assure que $\alpha\beta$ et $\alpha\omega$ sont interdéfinissables. On en déduit que $\alpha\beta$ et $\alpha\gamma\delta$ sont également interdéfinissables.

En conséquence, $tp(\alpha\gamma\delta/M)$ et $tp(\beta/M) = p$ ont les mêmes codes. Puisque $\alpha\gamma$ est un tuple de K et δ un tuple de k, cela conclut.

- **Montrons maintenant que tout type définissable qui est dans un produit d'une puissance de K et d'une puissance de k admet un code géométrique:**

  On cherche essentiellement à construire une application à valeur dans $K^n \times k^l$ qui admet un relèvement définissable.

  Commençons par remarquer que $\mathrm{res} : \mathcal{O} \longrightarrow k$ admet un relèvement définissable donné par $b \mapsto p_b(x) :=$ "$x \in b + \mathfrak{m}$ mais n'appartient à aucune sous-boule stricte".

  En considérant le produit de res avec id_K, on obtient donc une application $K^n \times \mathcal{O}^l \longrightarrow K^n \times k^l$. Puisque $\mathcal{O} \subseteq K$ est définissable et puisque le théorème 4.2.3 assure que les types définissables de K^{n+L} ont un code géométrique, la proposition 4.2.2 permet de conclure quant à l'existence de codes géométriques pour les types définissables de $K^n \times k^l$.

Les deux points précédents assurent donc que p admet un code géométrique, ce qui conclut la démonstration du lemme 4.2.1.

Preuve du lemme 4.2.2: Considérons S un ensemble fini C-définissable de K.

Notons $\widetilde{\mathcal{B}} := \{(x, y) \in K^2 : x \neq y\}$ et $\mathcal{B} := \{\text{boules fermées non triviales}\}$. L'application $\beta : \widetilde{\mathcal{B}} \longrightarrow \mathcal{B}$ qui envoie (x, y) sur la plus petite boule fermée contenant x et y admet un relèvement génériquement stable (voir par exemple [Joh14, Section 2.3]).

Posons $T := \{\beta(x, y) : (x, y) \in S^2 \text{ et } x \neq y\} \subseteq \mathcal{B}$ et $n := |T|$, si bien que l'élément $\lceil T \rceil \in \mathrm{Sym}^n \mathcal{B}$ est C-définissable. Puisque β admet un relèvement génériquement stable, il existe un type C-définissable au-dessus du type constant associé à $\lceil T \rceil$ dans $\mathrm{Sym}^n \widetilde{\mathcal{B}}$: soit $\alpha \in \mathrm{Sym}^n \widetilde{\mathcal{B}} \subseteq \mathrm{Sym}^n\left(K^2\right)$ un élément réalisant ce type C-définissable.

On a alors $\alpha \mathop{\smile\!\!\!\!\!\!\;\;|}_C C$; de plus, puisque α code un sous-ensemble fini T' de K^2 et puisque ACF élimine les imaginaires, on peut supposer que α est un tuple de K.

Il reste à montrer qu'il existe une injection $\alpha\lceil S \rceil$-définissable de S dans une puissance de k. Pour ce faire, il suffit (voir [CH99, Appendice]) de montrer que tout automorphisme du monstre qui fixe α et k point par point et qui stabilise S fixe également S point par point.

En supposant par l'absurde qu'il existe $z \in S$ et un automorphisme σ qui ne fixe pas z. En considérant $B := \beta(z, \sigma(z)) \in T$ on a alors $\sigma(z) \in B \cap \sigma B$ d'où on déduit que $B = \sigma B$.

En outre, puisque α code T' et $\beta(\alpha) = \lceil T \rceil$, il existe un unique $(x, y) \in T'$ tel que $B = \beta(x, y)$. On en déduit alors que si B est la plus petite boule contenant x et y, $x = \sigma(x)$ et $y = \sigma(y)$.

Fait 4.2.4. *L'ensemble* $\operatorname{res} B$ *des sous-boules ouvertes de* B *de même rayon que* B *admet une structure de droite affine sur* k.

On en déduit que $\operatorname{res} B$ est $\{x, y\}$-définissablement isomorphe à k: puisque σ fixe k, x et y, elle fixe $\operatorname{res} B$ point par point. On en déduit que $\operatorname{res} z = \operatorname{res} \sigma(z)$ et donc que $\beta(z, \sigma(z)) \subsetneq B$ ce qui est absurde.

4.3 Retour aux sortes géométriques "naturelles"

En ayant montré que le critère 3.3.1 est vérifié, nous avons donc obtenu que ACVF élimine les imaginaires dans les sortes K, R_{nl}. Pour montrer que ACVF élimine les imaginaires dans les sortes K, S_n et T_n, on suit l'argument de [HHM06, Lemme 2.6.4].

Commençons par remarquer qu'on peut coder R_{nl} à l'aide des $R_{m0} (= S_m)$ et R_{m1}. En effet, si Λ est un réseau de K^n et V un sous-espace de dimension l de $\operatorname{res} \Lambda$, alors V est codé par le sous-espace $\bigwedge^l V$, de dimension 1, de $\bigwedge^l \operatorname{res}(\Lambda) = \operatorname{res}\left(\bigwedge^l \Lambda\right)$ ainsi que le réseau $\bigwedge^l \Lambda$. On peut donc coder R_{nl} par un élément de R_{N0} et un élément de R_{N1} où $N = \binom{n}{l}$.

Il s'agit maintenant de montrer que R_{n1} peut être codé à l'aide des S_n et T_n, ce qu'on montre par récurrence sur n, les cas $n = 0$ et $n = 1$ étant évidents.

Considérons un réseau Λ de K^n, V un sous-espace de dimension 1 de $\operatorname{res}(\Lambda)$ et notons π la projection sur la première coordonnée. Le module $\pi(\Lambda)$ est alors libre et la suite

$$0 \longrightarrow \Lambda' \longrightarrow \Lambda \longrightarrow \pi(\Lambda) \longrightarrow 0$$

est exacte et scindée; Λ' est en outre un réseau de K^{n-1}. En tensorisant par k on obtient encore une suite exacte scindée

$$0 \longrightarrow \operatorname{res}(\Lambda') \longrightarrow \operatorname{res}(\Lambda) \longrightarrow \operatorname{res}(\pi(\Lambda)) \longrightarrow 0\ .$$

Si V est inclus dans $\operatorname{res}(\Lambda')$, qui est de dimension $n-1$, il a un code géométrique par hypothèse de récurrence.

Sinon, l'application $V \longrightarrow \operatorname{res}(\pi(\Lambda))$ est un isomorphisme: pour code V, il suffit donc de coder l'application $\operatorname{res}(\pi(\Lambda)) \longrightarrow V \longrightarrow \operatorname{res}(\Lambda)$. Or, puisque tous les $\mathcal{O}$-modules en jeu sont libres, on a les identifications

$$\operatorname{Hom}_k(\operatorname{res}(\pi(\Lambda)), \operatorname{res}(\Lambda)) = \operatorname{Hom}_k(\pi(\Lambda) \otimes k, \Lambda \otimes k) = \operatorname{Hom}_{\mathcal{O}}(\pi(\Lambda), \Lambda) \otimes k.$$

Puisque $\operatorname{Hom}_{\mathcal{O}}(\pi(\Lambda), \Lambda)$ est un réseau de $\operatorname{Hom}_K(K, K^n) \simeq K^n$, on en déduit qu'un morphisme de $\operatorname{res}(\pi(\Lambda))$ dans $\operatorname{res}(\Lambda)$ peut être codé par un élément de T_n.

Appendices

Il est de bon aloi de commencer par poser le cadre d'étude des objets qui apparaissent dans le mémoire: cet appendice répond à cette attente.

A Généralités sur les corps valués

Nous allons évoquer deux approches d'étude des corps valués: pour exprimer le fait que ces deux approches se recouvrent, nous allons faire appel à un formalisme catégorique. Ce formalisme doit être considéré comme une curiosité et il est conseillé de passer outre pour le lecteur non habitué à la théorie de la valuation.

A.1 Une construction catégorique

Supposons donnée une catégorie $\mathscr{C}$ telle que

(i) La classe des objets est partitionnée via des classes U_i $(i \in I)$;

(ii) Pour tous $i \in I$ et $x, x' \in U_i$ supposons donné un isomorphisme $\varphi_{x,x'} : x \longrightarrow x'$. Supposons en outre que $\varphi_{x,x} = id_x$ et que ces isomorphismes sont compatibles, c'est-à-dire que pour $x, x', x'' \in U_i$ on a $\varphi_{x',x''} \circ \varphi_{x,x'} = \varphi_{x,x''}$.

Remarque A.1.1. *Le lecteur pourra vérifier que si $\mathscr{C}$ est localement petite, si les U_i sont des ensembles et si (ii) est remplacée par*

(ii') Pour $i \in I$ les objets de U_i sont deux à deux isomorphes;

alors (ii) peut être réalisée.

Il s'agit de construire une catégorie $\overline{\mathscr{C}}$ obtenue à partir de $\mathscr{C}$ en identifiant les objets isomorphes donnés par la partition et en définissant soigneusement la composition.

Définition A.1.1. *On décrit la catégorie $\overline{\mathscr{C}}$ par ses objets et ses flèches:*

(i) Les objets sont les U_i;

(ii) Pour $(i,j) \in I^2$ on pose $\overline{\mathscr{C}}(U_i, U_j) := \left(\bigcup_{(x,y) \in U_i \times U_j} \mathscr{C}(x,y) \right) / \sim$ où la relation d'équivalence $\sim$ est définie comme suit: pour $x, x' \in U_i$, $y, y' \in U_j$, $f : x \longrightarrow y$ et $f' : x' \longrightarrow y'$ on pose $f \sim f'$ si le diagramme suivant commute

$$\begin{tikzcd} x \arrow[r, "f"] \arrow[d, "\varphi_{x,x'}"'] & y \arrow[d, "\varphi_{y,y'}"] \\ x' \arrow[r, "f'"'] & y' \end{tikzcd}$$

Pour $(i,j,k) \in I^3$, $(x, y, y', z) \in U_i \times U_j \times U_j \times U_k$, $f : x \longrightarrow y$ et $g : y' \longrightarrow z$ on pose $g \boxtimes f := g \circ \varphi_{y,y'} \circ f$.

On vérifie naturellement que si $f \sim f'$ et $g \sim g'$ alors $g' \boxtimes f' \sim g \boxtimes f$ si bien que $\boxtimes$ induit une composition sur les flèches de $\overline{\mathscr{C}}$.

On notera que la catégorie ainsi définie dépend de la partition fournie par (i) ainsi que de la famille d'isomorphismes compatibles fournie par (ii).

A.2 Corps valués

A.2.1 Première approche via les valuations

Commençons par introduire la notion de valuation:

Définition A.2.1. *Soit K un corps. Une valuation sur K est une application surjective $v : K \longrightarrow \Gamma \cup \{\infty\}$, où Γ est un groupe abélien ordonné et ∞ est un ensemble n'appartenant pas à Γ, satisfaisant aux conditions suivantes:*

(i) pour tout $x \in K$, $v(x) = \infty$ si et seulement si $x = 0$;

(ii) pour tout $(x, y) \in K^2$ on a $v(xy) = v(x) + v(y)$;

(iii) pour tout $(x, y) \in K^2$ on a $v(x + y) \geq min\,(v(x), v(y))$;

où on convient que ∞ soit infiniment grand par rapport à Γ et l'on convient également que pour tout $\gamma \in \Gamma$ on ait $\gamma + \infty = \infty$.

On notera que:

Remarque A.2.1. *Le point (ii) est équivalent au fait que v induit un morphisme de groupes de $K^\times$ vers Γ.*

Le propriété (iii) est en général qualifiée de *propriété ultramétrique*: elle traduit le fait que tous les triangles sont isocèles. Plus précisément, on a l'énoncé suivant, dont la preuve relève de manipulations élémentaires:

Proposition A.2.1. *Soit K un corps et v une valuation sur K. Pour tous $x, y \in K$ l'un des trois cas de figures suivants est réalisé:*

1. *$v(x + y) \geq v(x)$ et $v(x) = v(y)$;*
2. *$v(x) \geq v(y)$ et $v(y) = v(x + y)$;*
3. *$v(y) \geq v(x)$ et $v(x) = v(x + y)$.*

On dispose alors d'une première définition d'un corps valué:

Définition A.2.2. *Un corps valué est alors la donnée de (K, v) où K est un corps et v est une valuation sur K.*

Dans la suite, on adoptera la notation suivante:

Notations A.2.1. *Si (K, v) est un corps valué, on notera vK ou Γ_K l'image de $K^\times$ par v. On l'appelle le groupe de valuation de (K, v) ou, s'il n'y a pas d'ambiguïté, le groupe de valuation de K.*

Définissons les morphismes entre corps valués:

Définition A.2.3. *Soient (K, v) et (L, w) des corps valués. Un morphisme de (K, v) dans (L, w) est la donnée d'une paire (f, ϕ), où $f : K \longrightarrow L$ est un morphisme de corps et $\phi : vK \longrightarrow wL$ est un morphisme de groupes ordonnés, telle que le diagramme suivant commute:*

$$\begin{array}{ccc} K & \xrightarrow{f} & L \\ {\scriptstyle v}\big\downarrow & & \big\downarrow{\scriptstyle w} \\ vK & \xrightarrow[\phi]{} & wL \end{array}$$

Si $(f, \phi) : (K, v) \longrightarrow (L, w)$ et $(g, \psi) : (L, w) \longrightarrow (M, r)$ sont des morphismes de corps valués, alors $(gf, \psi\phi)$ est un morphisme de (K, v) dans (M, r): on définit de la sorte la composée de deux morphismes $(g, \psi) \circ (f, \phi) := (gf, \psi\phi)$.

On définit de la sorte la catégorie des corps valués:

Définition A.2.4. *La catégorie des corps valués, notée* **ValField***, est la catégorie dont les objets sont les corps valués et les flèches les morphismes de corps valués.*

A.2.2 Deuxième approche via les anneaux de valuation

On commence par définir ce qu'est un anneau de valuation d'un corps:

Définition A.2.5. *Soit K un corps. Un anneau de valuation de K est un sous-anneau $\mathcal{O}$ de K tel que pour tout $x \in K^\times$ on ait $x \in \mathcal{O}$ ou $x^{-1} \in \mathcal{O}$.*

Le lecteur notera que si $\mathcal{O}$ est un anneau de valuation d'un corps K alors K est isomorphe au corps des fractions de $\mathcal{O}$ si bien qu'il serait possible de définir ce qu'est un anneau de valuation sans invoquer *a priori* le corps qui le contient.

Il est toutefois à noter que l'évocation du corps ambiant sera cruciale pour le paragraphe suivant.

Un anneau de valuation est un anneau local:

Proposition A.2.2. *Soit K un corps et $\mathcal{O}$ un anneau de valuation de K. L'anneau $\mathcal{O}$ est un anneau local d'idéal maximal $\mathfrak{m} := \{0\} \cup \big\{x \in \mathcal{O} : x^{-1} \in K - \mathcal{O}\big\}$.*

Notations A.2.2. *Si $\mathcal{O}$ est un anneau de valuation, on notera $\mathfrak{m}_{\mathcal{O}}$ son idéal maximal.*

Plus précisément, l'ensemble les idéaux d'un anneau de valuation est totalement ordonné par l'inclusion:

Fait A.2.1. *Si K est un corps et $\mathcal{O}$ est un anneau de valuation de K, l'ensemble des idéaux de $\mathcal{O}$ est totalement ordonné par l'inclusion.*

Un premier exemple d'anneau de valuation est celui associé à un corps valué:

Fait A.2.2. *Si (K, v) est un anneau valué, alors $\mathcal{O}_v := \{x \in K : v(x) \geq 0\}$ est un anneau de valuation de K, d'idéal maximal $\mathfrak{m} := \{x \in K : v(x) > 0\}$.*

On remarquera que pour un corps valué (K, v), la valuation induit une bijection croissante entre les idéaux de $\mathcal{O}_v$ et les segments finaux de vK.

Réciproquement, on peut associer une valuation à tout anneau de valuation d'un corps comme suit:

Proposition A.2.3. *Soit K un corps et $\mathcal{O}$ un anneau de valuation de K. Le groupe $K^\times/\mathcal{O}^\times$ peut être muni de l'ordre suivant: pour $x, y \in K^\times$, $\overline{x} \geq \overline{y}$ si et seulement si $xy^{-1} \in \mathcal{O}^\times$ (où $\overline{x}$ et $\overline{y}$ désignent les classes respectives de x et y modulo $\mathcal{O}$).*

L'application $v : K \longrightarrow K^\times/\mathcal{O}^\times \cup \{\infty\}$, qui coïncide avec l'application quotient sur $K^\times$ et qui envoie 0 sur ∞, est une valuation sur K.

On dispose d'une catégorie dont les objets sont les couples formés d'un corps et d'un anneau de valuation définie comme suit:

Définition A.2.6. *La catégorie* **ValRing** *est la catégorie dont les objets sont les couples $(K, \mathcal{O})$, où K est un corps et $\mathcal{O}$ est un anneau de valuation de K, et les flèches sont les morphismes de corps qui induisent des morphismes sur les anneaux de valuation.*

Les liens entre **ValField** et **ValRing** sont décrits au paragraphe suivant, à l'aide de la sous-section $A.1$.

On clôt ce paragraphe en définissant le corps résiduel associé à un anneau de valuation:

Définition A.2.7. *Si $\mathcal{O}$ est un anneau de valuation d'un corps K, on définit le corps résiduel de $\mathcal{O}$ comme étant $\mathcal{O}/\mathfrak{m}_{\mathcal{O}}$. On le notera $k_{\mathcal{O}}$ ou k s'il n'y a aucune ambiguïté.*

A.2.3 Les catégories $\overline{\textbf{ValField}}$ et ValRing sont isomorphes

Nous allons appliquer la construction de la sous-section $A.1$ à **ValField**.

Commençons par définir une relation d'équivalence sur les objets de **ValField**, notée $\equiv$, de la façon suivante: $(K, v) \equiv (L, w)$ lorsque $K = L$ et lorsqu'il existe un isomorphisme de groupes ordonnés $\phi : vK \longrightarrow wL$ tel que (id_K, ϕ) soit un morphisme de corps valués de (K, v) vers (L, w).

Cette relation d'équivalence induit une partition $(U_i)_{i \in I}$ sur la classe des objets de **ValField**.

En outre, remarquons que si $(K, v) \equiv (K, w)$, alors il existe un unique isomorphisme de groupes ordonnés $\phi : vK \longrightarrow wK$ tel que (id_K, ϕ) soit un isomorphisme de corps valués: notons-le $\varphi_{(K,v),(K,w)}$.

De la sorte, les U_i et les $\varphi_{(K,v),(K,w)}$ vérifient les conditions (i) et (ii) de la sous-section $A.1$: on en déduit une catégorie $\overline{\textbf{ValField}}$ selon le procédé de construction de ladite sous-section.
Notons qu'on dispose d'un foncteur "quotient" Π : **ValField** $\longrightarrow$ $\overline{\textbf{ValField}}$ qui envoie un objet (K, v) sur sa classe modulo $\equiv$ et une flèche $(K, v) \longrightarrow (L, w)$ sur celle qu'elle induit dans $\overline{\textbf{ValField}}$.

Définissons le foncteur F : **ValRing** $\longrightarrow$ **ValField** qui envoie:

- le couple $(K, \mathcal{O})$ sur le couple (K, v) où v est la valuation associée à $(K, \mathcal{O})$ selon la proposition $A.2.3.$;
- une flèche $f : (K, \mathcal{O}_K) \longrightarrow (L, \mathcal{O}_L)$ sur la flèche $(id, \overline{f})$ où $\overline{f} : \overline{x} \mapsto \overline{f(x)}$;

puis posons $G := \Pi \circ F$.

Définissons ensuite H : $\overline{\textbf{ValField}}$ $\longrightarrow$ **ValRing** qui envoie:

- la classe $[(K, v)]$ sur $(K, \mathcal{O}_v)$;
- une flèche $\theta : [(K, v)] \longrightarrow (L, w)$ sur l'unique morphisme $(f, \phi) : (K, v) \longrightarrow (L, w)$ tel que $(f, \phi) \in \theta$;

dont on vérifiera qu'il est bien défini.

De façon immédiate, les définitions de G et H fournissent que $H \circ G = id_{\textbf{ValRing}}$ et $G \circ H = id_{\overline{\textbf{ValField}}}$, d'où on déduit:

Proposition A.2.4. *Les catégories* **ValRing** *et* $\overline{\textbf{ValField}}$ *sont isomorphes.*

En vertu de ce résultat et plus précisément du fait que les foncteurs G et H sont des isomorphismes, il nous arrivera assez souvent de considérer qu'un corps valué est la donné d'un anneau de valuation $\mathcal{O}$ inclus dans un corps K, le groupe de valuation étant $K^\times/\mathcal{O}^\times$.

A.3 Topologie d'un corps valué

Dans cette sous-section, (K, v) désigne un corps valué et on note $\Gamma := vK$.

On pose $\mathcal{B}$ la famille des $B(a, \gamma) := \{x \in K : v(x - a) > \gamma\}$ où $(a, \gamma) \in K \times \Gamma$. C'est une base puisque pour $(a, b) \in K^2$ et $(\gamma, \delta) \in \Gamma^2$ tels que $B(a, \gamma) \cap B(b, \delta) \neq \emptyset$ on a

$$B(a, \gamma) \cap B(b, \delta) = B\left(a, \max(\gamma, \delta)\right).$$

La topologie induite par $\mathcal{B}$ munit alors K d'une structure de *corps topologique*. On laisse au lecteur le loisir de vérifier que $\mathcal{B}$ est constituée d'ouverts-fermés si bien que:

Proposition A.3.1. *La topologie sur K est séparée et totalement discontinue.*

A.4 Rang d'un groupe abélien ordonné

Dans cette sous-section, Γ désigne un groupe abélien ordonné.

A.4.1 Définition

Définition A.4.1. *On dit qu'un sous-groupe Δ de Γ est convexe lorsque pour tout $(\delta, \epsilon) \in \Delta^2$ et $\gamma \in \Gamma$, si $\delta \leq \gamma \leq \epsilon$ alors $\gamma \in \Delta$.*

Remarque A.4.1. *On obtient une définition équivalent en remplaçant δ par 0.*

L'ensemble des sous-groupes convexes de Γ est alors totalement ordonné par l'inclusion:

Fait A.4.1. *L'inclusion est un ordre total sur l'ensemble des sous-groupes convexes de Γ.*

On obtient alors un invariant de groupes abéliens ordonnés:

Définition A.4.2. *Le rang de l'ordre qu'induit l'inclusion sur l'ensemble des sous-groupes convexes de Γ est appelé le rang de Γ. On le note $rg\,(\Gamma)$.*

A.4.2 Groupes ordonnés de rang 1

On montre ici que les groupes de rang 1 sont précisément les sous-groupes de $\mathbf{R}$:

Proposition A.4.1. *Le groupe Γ est de rang 1 si et seulement si il est isomorphe à un sous-groupe de $\mathbf{R}$.*

Démonstration. Le sens réciproque étant évident, on montre le sens direct. Supposons donc que Γ est de rang 1.

Tout d'abord, l'ordre est archimédien puisque pour $\epsilon > 0$, $\Delta := \{\gamma \in \Gamma : \forall n \geq 0, |n\gamma| \leq \epsilon\}$ est un sous-groupe convexe strict de Γ: ce dernier étant de rang 1 on en déduit que $\Delta = 0$ et donc que l'ordre est archimédien.

Pour définir un monomorphisme de Γ dans $\mathbf{R}$, fixons $\epsilon > 0$ et posons pour $\gamma \in \Gamma$ les ensembles $U(\gamma) := \left\{\frac{m}{n} \in \mathbf{Q} : n > 0 \text{ et } m\gamma < n\epsilon\right\}$ et $L(\gamma) := \left\{\frac{m}{n} \in \mathbf{Q} : n > 0 \text{ et } m\gamma \geq n\epsilon\right\}$. Notons que pour $\gamma \in \Gamma$, les ensembles $L(\gamma)$ et $U(\gamma)$ définissent des coupures dans $\mathbf{Q}$.

Le caractère archimédien de l'ordre assurant en outre que ces ensembles sont non vides, on en déduit que l'application $\Phi : \Gamma \longrightarrow \mathbf{R}$ qui envoie γ sur $\inf U(\gamma)$ est bien défini. Il est aisé de vérifier que c'est un morphisme et qu'il préserve l'ordre.

De plus, Φ est injective puisque si $\gamma \in \ker \Phi$, alors pour tout entier $n \neq 0$ on a $|n\gamma| \leq \epsilon$: le caractère archimédien de l'ordre assure donc que $\gamma = 0$.

Ainsi, Φ est un plongement de Γ dans $\mathbf{R}$. $\square$

Les corps valués dont le groupe de valuation est de rang 1 ont des propriétés intéressantes que nous évoquerons dans la suite.

A.5 Complétion d'un corps valué

Dans cette section, (K, v) désigne un corps valué dont on note Γ son groupe de valuation.

Notons κ la cofinalité de Γ, c'est-à-dire le plus petit cardinal λ tel qu'il existe une partie $U \subseteq \Gamma$ de cardinal λ qui soit non bornée. Soit $U \subseteq \Gamma$, de cardinal κ et qui est non bornée.

On dit qu'une suite $(a_\nu)_{\nu<\kappa} \in K^\kappa$ est de Cauchy si pour tout $\gamma \in U$ il existe $\nu < \kappa$ tel que $\lambda, \mu > \nu \Longrightarrow v(a_\lambda - a_\mu) > \gamma$. Nous aurons besoin du fait suivant:

Fait A.5.1. *Si $(a_\nu)_{\nu<\kappa} \in K^\kappa$ est une suite de Cauchy alors l'une des deux situations suivantes est réalisée:*

- *la suite $(a_\nu)_{\nu<\kappa}$ tend vers 0;*
- *la suite $(v(a_\nu))_{\nu<\kappa}$ est stationnaire.*

Définition A.5.1. *Un corps valué est dit complet si toute suite de Cauchy est convergente.*

On peut construire de façon fonctorielle le complété d'un corps valué. Plus précisément, on a la propriété universelle suivante:

Proposition A.5.1. *Il existe un corps valué complet $(\overline{K}, \overline{v})$ et un monomorphisme de corps valués $\iota : (K, v) \longrightarrow (\overline{K}, \overline{v})$ tel que pour tout corps valué complet (L, w), tel que Γ et Γ_L ont même cofinalité, et tout morphisme $(f, \phi) : (K, v) \longrightarrow (L, w)$ où ϕ est cofinale, il existe un unique $(\overline{f}, \overline{\phi}) : (\overline{K}, \overline{v}) \longrightarrow (L, w)$ qui fasse commuter le diagramme suivant:*

$$\begin{tikzcd} (K,v) \arrow[r, "\iota"] \arrow[dr, "(f,\phi)"'] & (\overline{K},\overline{v}) \arrow[d, "(\overline{f},\overline{\phi})"] \\ & (L,w) \end{tikzcd}$$

Le corps valué $(\overline{K}, \overline{v})$ est unique à unique isomorphisme près. On l'appelle le complété de (K, v).

Démonstration. L'unicité à unique isomorphisme près relève d'arguments usuels. Démontrons l'existence d'un tel objet.

Notons $A := \{(a_\nu)_{\nu<\kappa} \in K^\kappa : (a_\nu)_{\nu<\kappa} \text{ est de Cauchy}\}$ qui est un anneau. Le fait 0.5.1. assure que A est un anneau local d'idéal maximal $\mathfrak{m} := \{(a_\nu)_{\nu<\kappa} \in K^\kappa : (a_\nu)_{\nu<\kappa}\}$.

On pose donc $\overline{K} := A/\mathfrak{m}$ et $\overline{v} : \overline{K} \longrightarrow \Gamma \cup \{\infty\}$ définie par $\overline{v}(\mathfrak{m}) = \infty$ et $\overline{v}\left(\left[(a_\nu)_{\nu<\kappa}\right]\right) = lim\,(v(a_\nu))_{\nu<\kappa}$ si $(a_\nu)_{\nu<\kappa} \notin \mathfrak{m}$: le fait 0.5.1 assure que $\overline{v}$ est bien définie.

On pose également ι l'injection canonique qui à un élément de K associe la classe de la suite constante associée.

Soit (L, w) un corps valué complet tel que Γ et Γ_l ont même cofinalité, et (f, ϕ) : $(K, v) \longrightarrow (L, w)$ où ϕ est cofinale. Le morphisme f envoie alors toute suite de Cauchy de K sur une suite de Cauchy de L.

On en déduit que l'application $\overline{f} : \overline{K} \longrightarrow L$ qui envoie la classe de $(a_\nu)_{\nu<\kappa}$ sur $lim\,(f(a_\nu))_{\nu<\kappa}$ est bien définie: on vérifie par ailleurs que c'est un morphisme de corps. En reprenant la définition de $\overline{f}$, on laisse alors le lecteur s'assurer qu'en posant $\overline{\phi} := \phi$ que $(\overline{f}, \overline{\phi})$ fait commuter le diagramme de l'énoncé de la proposition.

Ce morphisme est en outre unique puisque tout morphisme faisant commuter le diagramme est confondu avec (f, ϕ) sur la partie dense $\operatorname{Im} \iota$. $\square$

B Extensions d'une valuation

On cherche ici à comprendre comment étendre une valuation. On s'intéresse *a fortiori* au cas des extensions algébriques pour lesquelles on a une description des extensions possibles.

B.1 Définitions

Définition B.1.1. *Si* $K \hookrightarrow L$ *est une extension de corps,* v *une valuation sur* K *et* w *une valuation sur* L*, on dit que* w *étend* v *si* $w{\restriction}K = v$*.*

Définition B.1.2. *Si* $K \hookrightarrow L$ *est une extension de corps,* $\mathcal{O}_K$ *un anneau de valuation de* K *et* $\mathcal{O}_L$ *un anneau de valuation de* L*, on dit que* $\mathcal{O}_L$ *étend* $\mathcal{O}_K$ *lorsque* $\mathcal{O}_K = \mathcal{O}_L \cap K$*.*

De façon équivalente, $\mathcal{O}_L$ *étend* $\mathcal{O}_K$ *si et seulement si* $\mathcal{O}_K^\times = \mathcal{O}_L^\times \cap K$*, ce équivaut à* $\mathfrak{m}_K = \mathfrak{m}_L \cap K$*.*

On se convaincra que si $K \hookrightarrow L$ est une extension de corps et v une valuation sur K, alors celle-ci s'étend en une valuation de L si et seulement si $\mathcal{O}_v$ s'étend en un anneau de valuation de L.

Remarquons que si $K \hookrightarrow L$ est une extension de corps, $\mathcal{O}$ un anneau de valuation de K et $\mathcal{O}'$ un anneau de valuation de L qui étend $\mathcal{O}$, alors:

(i) l'inclusion $K \hookrightarrow L$ induit un plongement de groupes $K^\times/\mathcal{O}^\times \hookrightarrow L^\times/\mathcal{O}'^\times$ et on notera $e(L:K) := (L^\times/\mathcal{O}'^\times : K^\times/\mathcal{O}^\times)$, appelé *l'indice de ramification* de l'extension L/K (dont on notera qu'il dépend du choix des anneaux de valuation);

(ii) l'inclusion $\mathcal{O} \hookrightarrow \mathcal{O}'$ induit un plongement de corps $k_K \hookrightarrow k_L$ et on notera $f(L:K) := [k_L : k_K]$, appelé *le degré résiduel* de l'extension L/K.

B.2 Existence d'une extension

Commençons par montrer le résultat général suivant:

Théorème B.2.1. *Soit* A *un sous-anneau d'un corps* K *et* $\mathfrak{p}$ *un idéal premier de* A*. Il existe un anneau de valuation* $\mathcal{O}$ *de* K *tel que:*

(i) $A \leq \mathcal{O}$*;*

(ii) $\mathfrak{m}_{\mathcal{O}} \cap A = \mathfrak{p}$*;*

(iii) le corps résiduel $k_{\mathcal{O}}$ *de* $\mathcal{O}$ *est une extension algébrique du corps des fractions de* $A/\mathfrak{p}$*.*

Démonstration. Notons I l'ensemble des couples $(R, \mathfrak{m})$ où R est un sous-anneau de K et $\mathfrak{m}$ un idéal maximal de R tels que:

1. $A \leq R$;
2. $\mathfrak{m} \cap A = \mathfrak{p}$;
3. $R/\mathfrak{m}$ est algébrique sur le corps des fractions de $A/\mathfrak{p}$.

L'ensemble I est non vide puisqu'il contient $(A_\mathfrak{p}, \mathfrak{p}A_\mathfrak{p})$. Muni, de l'inclusion, il est en outre inductif: le lemme de Zorn fournit donc un élément maximal $(R_0, \mathfrak{m}_0)$. Montrons que R_0 est un anneau de valuation de K.

Supposons par l'absurde qu'il existe $a \in K^\times$ tel que $a \notin R_0$ et $a^{-1} \notin R_0$.

Considérons les anneaux $R_0[a]$ et $R_0\left[a^{-1}\right]$ ainsi que leurs idéaux $\mathfrak{m}_0[a]$ et $\mathfrak{m}_0\left[a^{-1}\right]$.

Montrons que l'un de ces idéaux est propre. Si ce n'est pas le cas, on dispose d'entier m et n minimaux tels qu'existent $b_i, c_j \in \mathfrak{m}_0$ vérifiant:

$$1 = b_0 + b_1 a + \cdots + b_n a^n \tag{5}$$

$$1 = c_0 + c_1 a^{-1} + \cdots + c_m a^{-m} \tag{6}$$

et on peut supposer que $m \leq n$. En multipliant (1) par $1 - c_0$ et (2) par $b_n a^n$ on obtient respectivement:

$$1 = c_0 + (1-c_0)b_0 + (1-c_0)b_1 a + \cdots + (1-c_0)b_n a^n \tag{7}$$

$$(1-c_0)b_n a^n = (1-c_0)b_n c_1 a^{n-1} + \cdots + (1-c_0)b_n c_m a^{n-m} \tag{8}$$

puis en injectant (4) dans (3) on trouve:

$$1 = [c_0 + (1-c_0)b_0] + \cdots + (1-c_0)(b_{n-m} + b_n c_m)a^{n-m} + \cdots + (1-c_0)(b_{n-1} + b_n c_1)a^{n-1} \tag{9}$$

ce qui contredit la minimalité de n. En conséquence, l'un des idéaux $\mathfrak{m}_0[a]$ et $\mathfrak{m}_0\left[a^{-1}\right]$ est propre.

On peut par exemple supposer que $\mathfrak{m}_0[a]$ est un idéal propre de $R_0[a]$ et posons $\mathfrak{m}$ un idéal maximal de $R_0[a]$ contenant $\mathfrak{m}_0$. Montrons que $(R_0[a], \mathfrak{m})$ est dans I:

1. puisque $A \leq R_0$ et $R_0 \leq R_0[a]$ on obtient que $A \leq R_0[a]$;
2. puisque $\mathfrak{m} \cap R_0$ est un idéal premier de R_0 qui contient $\mathfrak{m}_0$, qui est maximal, on en déduit que $\mathfrak{m} \cap R_0 = \mathfrak{m}_0$. Du fait que $A \cap \mathfrak{m}_0 = \mathfrak{p}$ on conclut que $A \cap \mathfrak{m} = \mathfrak{p}$;
3. pour montrer que $R_0[a]/\mathfrak{m}$ est algébrique sur le corps des fractions de $A/\mathfrak{p}$, il suffit de montrer qu'il est algébrique sur $R_0/\mathfrak{m}_0$ (puisque ce dernier est lui-même algébrique sur le corps des fraction de $A/\mathfrak{p}$).

   Il s'agit donc de montrer que $a + \mathfrak{m}$ est algébrique sur $R_0/\mathfrak{m}_0$. Distinguons deux cas:

   - si $a \in \mathfrak{m}$, le résultat est évident;
   - sinon, il existe $b \in R_0[a]$ tel que $ab - 1 \in \mathfrak{m}$: écrivons $b = f(a)$ où $f \in R_0[X]$. En réduisant la relation $ab - 1 \in \mathfrak{m}$ modulo $\mathfrak{m}$ et en notant $\overline{f}$ le réduit de f modulo $\mathfrak{m}_0$ on en déduit que le polynôme non nul $X\overline{f} - 1$ annule $a + \mathfrak{m}$. Ainsi, $a + \mathfrak{m}$ est algébrique sur $R_0/\mathfrak{m}_0$.

Ainsi, $(R_0[a], \mathfrak{m})$ est dans I ce qui contredit la maximalité de $(R_0, \mathfrak{m}_0)$. □

Une conséquence immédiate de ce théorème est le résultat d'extension des valuations suivant:

Corollaire B.2.1. *Si $K \hookrightarrow L$ est une extension de corps, alors tout anneau de valuation de K s'étend en un anneau de valuation de L.*

B.3 Cas des extensions algébriques

B.3.1 Description des extensions d'un anneau valué

On prétend montrer que les extensions d'un anneau de valuation son précisément les localisés de sa clôture intégrale selon les idéaux maximaux.

Commençons par montrer un premier lemme:

Lemme B.3.1. *Si A est un sous-anneau d'un corps K, alors la clôture intégrale de A dans K est l'intersection des anneaux de valuation de K qui contiennent A.*

Démonstration. Soient A un sous anneau d'un corps K et R sa clôture intégrale dans K.

Soit $x \in R$ et $\mathcal{O}$ un anneau de valuation qui contient R. Si $x \notin \mathcal{O}$ alors $x^{-1} \in \mathcal{O}$ et donc $A\left[x^{-1}\right] \leq \mathcal{O}$. Mais puisque x est entier sur A on a $x \in A\left[x^{-1}\right] \leq \mathcal{O}$, ce qui est contradictoire. Donc $x \in \mathcal{O}$.

Soit $x \notin R$: puisque x n'est pas entier sur A, on a $x \notin A\left[x^{-1}\right]$. Cette dernière relation assure qu'il existe un idéal maximal $\mathfrak{m}$ de $A\left[x^{-1}\right]$ qui contient x^{-1}. Le théorème B.2.1. fournit un anneau de valuation $\mathcal{O}$ de K tel que $\mathfrak{m}_{\mathcal{O}} \cap K = \mathfrak{m}$, si bien que $x \notin \mathcal{O}$. Donc x n'est pas dans l'intersection des anneaux de valuation de K contenant A. □

On utilisera également le fait suivant:

Fait B.3.1. *Si $A \leq B$ une extension entière d'anneaux et $\mathfrak{m}$ est un idéal maximal de B alors $\mathfrak{m} \cap A$ est un idéal maximal de A.*

Théorème B.3.1. *Soit $\mathcal{O}$ un anneau de valuation d'un corps K et L une extension algébrique de K. En notant R la clôture intégrale de $\mathcal{O}$ dans L:*

1. *Si $\mathcal{O}_1$ est un anneau de valuation de L qui étend $\mathcal{O}$, alors $\mathfrak{m}_0 := \mathfrak{m}_{\mathcal{O}_1} \cap R$ est un idéal maximal de R et $\mathcal{O}_1 = R_{\mathfrak{m}_0}$;*
2. *Si $\mathfrak{m}_0$ est un idéal maximal de R alors $R_{\mathfrak{m}_0}$ est un anneau de valuation de L qui étend $\mathcal{O}$.*

Démonstration. Commençons par remarquer que le second point est conséquence du premier.

En effet si $\mathfrak{m}_0$ est un idéal maximal de R, le théorème B.2.1. fournit un anneau de valuation $\mathcal{O}_1$ de L tel que $R \leq \mathcal{O}_1$ et $\mathfrak{m}_{\mathcal{O}_1} \cap R = \mathfrak{m}_0$. Le point 1. assure l'existence d'un idéal maximal $\mathfrak{m}_1$ de R tel que $\mathcal{O}_1 = R_{\mathfrak{m}_0}$, si bien que $R_{\mathfrak{m}_0}$ est un anneau de valuation de L: de plus il étend $\mathcal{O}$ puisque le fait B.3.1. assure que $\mathfrak{m}_0 \cap \mathcal{O} = \mathfrak{m}_{\mathcal{O}}$.

Pour montrer le point 1., considérons donc $\mathcal{O}_1$ un anneau de valuation de L qui étend $\mathcal{O}$ et posons $\mathfrak{m}_0 := \mathfrak{m}_{\mathcal{O}_1} \cap R$.

Du fait que $\mathfrak{m}_{\mathcal{O}_1} \cap \mathcal{O} = \mathfrak{m}_{\mathcal{O}}$ on tire que $\mathfrak{m}_0 \cap \mathcal{O} = \mathfrak{m}_{\mathcal{O}}$. Le fait B.3.1. assure donc que $\mathfrak{m}_0$ est un idéal maximal de R.

Par le lemme B.3.1., on sait que $R \leq \mathcal{O}_1$. Puisque $\mathfrak{m}_0 = R \cap \mathfrak{m}_{\mathcal{O}_1}$, on en déduit que $R_{\mathfrak{m}_0} \leq \mathcal{O}_1$.

Pour montrer l'inclusion réciproque, considérons $a \in \mathcal{O}_1$ et montrons que $a \in R_{\mathfrak{m}_0}$. Puisque L est algébrique sur K, on dispose de $n \geq 1$ et de $a_0, \ldots, a_n \in K$ non tous nuls tels que:

$$a_n a^n + \cdots + a_0 = 0 \tag{10}$$

Choisissons $j \leq n$ maximal tel que $v(a_j)$ soit minimal. En divisant (6) par $a_j x^j$, on obtient:

$$\left(b_{n-j} a^{n-j} + \cdots + b_1 a + 1\right) + x^{-1}\left(b_{-1} + b_{-2} a^{-1} + \cdots + b_{-j} a^{-j}\right) \tag{11}$$

où $b_k = a_j^{-1} a_{k+j}$. En posant $b := \left(b_{n-j} a^{n-j} + \cdots + b_1 a + 1\right)$ et $c := \left(b_{-1} + b_{-2} a^{-1} + \cdots + b_{-j} a^{-j}\right)$ on a donc $ba = -c$.

Pour montrer que les éléments b et c sont dans R, il suffit de montrer qu'ils sont dans tout anneau de valuation $\mathcal{O}'$ contenant $\mathcal{O}$. On distingue deux cas:

- si $a \in \mathcal{O}'$: puisque $b_k \in \mathcal{O} \leq \mathcal{O}'$, l'expression de b fournit que $b \in \mathcal{O}'$ et donc que $c = -bx \in \mathcal{O}'$;
- sinon $a^{-1} \in \mathcal{O}'$: puisque $b_k \in \mathcal{O} \leq \mathcal{O}'$, l'expression de c fournit que $c \in \mathcal{O}'$ et donc que $b = -cx^{-1} \in \mathcal{O}'$.

Montrons enfin que $b \notin \mathfrak{m}_0$. En effet, pour $k \geq 1$ le choix de j assure que $b_k \in \mathfrak{m}_{\mathcal{O}_1}$: du fait que $x \in \mathfrak{O}_1$, l'expression de b donne donc que $b - 1 \in \mathfrak{m}_{\mathcal{O}_1}$. Mais puisque $b - 1 \in R$ on en déduit que $b - 1 \in \mathfrak{m}_0$ et donc que $b \notin \mathfrak{m}_0$.

Ainsi, $x = -cb^{-1} \in R_{\mathfrak{m}_0}$, ce qui conclut. □

Remarque B.3.1. *Adoptons les notations et les hypothèses du théorème. Puisque l'intersection des localisés de R en ses idéaux maximaux est égale à R, on en déduit que la clôture intégrale de $\mathcal{O}$ dans L est l'intersection des anneaux de valuations de L qui l'étendent.*

B.3.2 Majoration du nombre d'extensions

Énonçons, sans preuve, le *going-up* de Cohen-Seidenberg. Le lecteur intéressé en trouvera une dans [Mat89, Théorème 9.3].

Proposition B.3.1. *Soit A un anneau intégralement clos, K son corps des fractions et L une extension normale de K.*

Si $\mathfrak{p}$ est un idéal premier de A et R est la clôture intégrale de A dans L alors les idéaux premier de R qui étendent $\mathfrak{p}$ sont conjugués sur K.

On en déduit le résultat suivant:

Proposition B.3.2. *Soit $\mathcal{O}$ un anneau de valuation d'un corps K, L une extension normale de K.*

Les extensions de $\mathcal{O}$ à un anneau de valuation de L sont conjuguées sur K.

Démonstration. Il suffit d'appliquer la proposition précédente avec $A := \mathcal{O}$ et R sa clôture intégrale dans L. Les idéaux maximaux de R sont alors conjugués sur K, si bien que les extensions de $\mathcal{O}$ sont conjuguées sur K, puisqu'elle sont décrites comme les localisés de R suivant ses idéaux maximaux en vertu du théorème B.3.1. □

On en déduit une borne du nombre d'extensions d'un anneau de valuation à une extension algébrique:

Corollaire B.3.1. *Si $\mathcal{O}$ est un anneau de valuation d'un corps K et L est une extension algébrique de K alors le nombre d'extension de $\mathcal{O}$ à un anneau de valuation de L est majoré par $[\mathrm{clnorm}_K(L) : K]_s$.*

Pour les extensions finies, on peut en réalité borner le nombre d'extensions d'un anneau de valuation par le degré de séparabilité de l'extension de corps. On renvoie le lecteur intéressé à [EP05, Théorème 3.2.9].

On clôt cette sous-section par le fait suivant, dont la preuve est laissée au lecteur:

Fait B.3.2. *Si $\mathcal{O}$ est un anneau de valuation d'un corps K et L une extension purement inséparable de K, alors l'anneau de valuation $\mathcal{O}' := \left\{x \in L : \exists n \geq 0 \ x^{p^n} \in \mathcal{O}\right\}$ de L est l'unique extension de $\mathcal{O}$ à L.*

C Corps henséliens

Le lemme de Hensel est certainement connu par le lecteur dans le cas des corps p-adiques, que ce soit sous sa forme "faible" ou "forte". Il est en réalité équivalent à un énoncé d'unicité d'extension des anneaux de valuation: nous développons ce propos dans la suite.

C.1 Définition

Définition C.1.1. *Un anneau de valuation $\mathcal{O}$ d'un corps K est dit hensélien s'il admet une unique extension à la clôture algébrique de K.*

En vertu du fait 1.3.2, on a la remarque suivante:

Remarque C.1.1. *Soit $\mathcal{O}$ un anneau de valuation d'un corps K. Les propriétés suivantes sont équivalentes:*

1. *L'anneau $\mathcal{O}$ est hensélien.*
2. *L'anneau de valuation $\mathcal{O}$ s'étend de manière unique à toute extension algébrique de K.*
3. *L'anneau de valuation $\mathcal{O}$ s'étend de manière unique à toute extension galoisienne finie de K.*
4. *L'anneau de valuation $\mathcal{O}$ s'étend de manière unique à la clôture séparable K^s de K.*

C.2 Caractérisations et propriétés

C.2.1 Définitions équivalentes

Le théorème qui suit fournit des définition équivalentes d'un corps valué hensélien. Avant de continuer, effectuons la remarque suivante:

Remarque C.2.1. *Soit $(K, \mathcal{O})$ un corps valué dont on notera, v une valuation. En définissant w sur $K[X]$ par $w\left(\sum_{i\geq 0} a_i X^i\right) := \min_{i\geq 0} v(a_i)$ on définit une valuation.*

On en déduit le résultat suivant: tout polynôme f de $\mathcal{O}[X]$ qui a une décomposition $f = g_1 \ldots g_r$ en polynômes non constants de $K[X]$ admet également une décomposition $f = h_1 \ldots h_r$ en polynômes non constants de $\mathcal{O}[X]$.

Théorème C.2.1. *Soit $(K, \mathcal{O})$ un corps valué dont on notera respectivement $\mathfrak{m}$ l'idéal maximal de $\mathcal{O}$, k le corps résiduel, Γ un groupe de valuation et $v : K \longrightarrow \Gamma \cup \{\infty\}$ une valuation. On notera également $a \mapsto \overline{a}$ le morphisme résiduel $\mathcal{O} \longrightarrow k$ et $f \mapsto \overline{f}$ celui qu'il induit sur $\mathcal{O}[X]$.*

Les assertions suivantes sont équivalentes:

(i) *L'anneau de valuation $\mathcal{O}$ est hensélien.*

(ii) *Pour tout polynôme $f \in \mathcal{O}[X]$ sur K tel que $\overline{f} \notin k$, il existe $g \in \mathcal{O}[X]$ et $s \geq 1$ tels que $\overline{g}$ est irréductible et $\overline{f} = \overline{g}^s$.*

(iii) *Pour tous $f, g, h \in \mathcal{O}[X]$ vérifiant $\overline{f} = \overline{g}.\overline{h}$, où $\overline{g}$ et $\overline{h}$ sont étrangers, il existe $g_1, h_1 \in \mathcal{O}[X]$ tels que $f = g_1 h_1$, $\overline{g_1} = \overline{g}$, $\overline{h_1} = \overline{h}$ et $\deg g_1 = \deg \overline{g}$.*

(iv) *Soit $f \in \mathcal{O}[X]$. Pour tout $\alpha \in k$ tel que $\overline{f}(\alpha) = 0$ et $\overline{f}'(\alpha) \neq 0$, il existe $a \in \mathcal{O}$ tel que $\overline{a} = \alpha$ et $f(a) = 0$.*

(v) *Soit $f \in \mathcal{O}[X]$. Pour tout $a \in \mathcal{O}$, si $v(f(a)) > 2v(f'(a))$ alors il existe $b \in K$ tel que $f(b) = 0$ et $v(a - b) > v(f'(a))$.*

(vi) *Tout polynôme de la forme* $X^n+X^{n-1}+a_{n-2}X^{n-2}+\cdots+a_0$ *où* $a_0,\ldots,a_{n-2}\in\mathfrak{m}$ *a une racine dans* K.

(vii) *Tout polynôme de la forme* $X^n+a_{n-1}X^{n-1}+\cdots+a_0$ *où* $a_0,\ldots,a_{n-2}\in\mathfrak{m}$ *et* $a_{n-1}\notin\mathfrak{m}$ *a une racine dans* K.

Démonstration. $(i)\Longrightarrow(ii)$ Soit $f\in\mathcal{O}[X]$ irréductible sur K. Écrivons le polynôme f sous la forme $f=\prod_{i=1}^{r}(\gamma X-\alpha_i)$ où γ et les α_i sont dans la clôture algébrique K^{a} de K. Notons $\mathcal{O}'$ l'unique extension de $\mathcal{O}$ à K^{a}.

Commençons par remarquer que du fait que f est à coefficients dans $\mathcal{O}$ on déduit que $\gamma,\alpha_i\in\mathcal{O}'$ si bien que dans $k'_{\mathcal{O}}$ (qui est une extension de k) on a $\overline{f}=\prod_{i=1}^{r}(\overline{\gamma}X-\overline{\alpha_i})$: de plus, puisque $\overline{f}\notin k$ on a $\overline{\gamma}\neq0$. Remarquons également que si σ est un automorphisme de K^{a} alors le caractère hensélien de $\mathcal{O}$ assure que $\sigma(\mathcal{O}')=\mathcal{O}'$ si bien que $\sigma(\mathfrak{m}_{\mathcal{O}'})=\mathfrak{m}_{\mathcal{O}'}$: en particulier, σ induit un automorphisme $\overline{\sigma}$ de $k_{\mathcal{O}'}$.

Soient $i,j\leq r$: du fait que f est irréductible, on déduit qu'il existe un automorphisme σ de K^{a} tel que $\sigma\left(a_i\gamma^{-1}\right)=a_j\gamma^{-1}$. De là, $\overline{\sigma}\left(\overline{a_i}.\overline{\gamma}^{-1}\right)=\overline{a_j}.\overline{\gamma}^{-1}$.

Ainsi, les racines de $\overline{f}$ sont deux à deux conjuguées, si bien qu'il existe $h\in k[X]$ irréductible et $s\geq1$ tels que $\overline{f}=h^s$: tout relèvement $g\in\mathcal{O}[X]$ de h vérifie alors $\overline{f}=\overline{g}^s$.

$(ii)\Longrightarrow(iii)$ Écrivons $f=p_1\ldots p_r$ où $p_i\in\mathcal{O}[X]$ est irréductible sur K. Par hypothèse, il existe $q_i\in\mathcal{O}[X]$ et $s_i\geq0$ tels que les $\overline{q_i}$ soient irréductibles et $\overline{p_i}=\overline{q_i}^{s_i}$.

Puisque $\overline{g}$ et $\overline{h}$ sont étrangers, il existe (quitte à renuméroter les p_i) un $j<k\leq r$ et $a,b\in\mathcal{O}^\times$ tels qu'on ait $\overline{a}.\overline{g}=\prod_{1\leq i<j}\overline{p_i}$ ainsi que $\overline{b}.\overline{h}=\prod_{j\leq i<k}\overline{p_i}$ et $\overline{c}=(\overline{a}\overline{b})^{-1}\prod_{k\leq j\leq r}p_i$.

Il est alors clair que $g_1:=a^{-1}\prod_{1\leq i<j}p_i$ et $h_1:=a\prod_{j\leq i\leq r}p_i$ conviennent.

$(iii)\Longrightarrow(iv)$ Ce sens est immédiat.

$(iv)\Longrightarrow(v)$ Soient f et a comme dans (v). Puisque $a,f'(a)\in\mathcal{O}$, on a un développement de $f(a-f'(a)X)$ sous la forme

$$f(a-f'(a)X)=f(a)-f'(a)^2X+f'(a)^2X^2g(X)\tag{12}$$

où $g\in\mathcal{O}[X]$. En divisant (8) par $f'(a)^2$ (ce qui est possible étant donné que $v(f'(a))<\infty$), l'hypothèse sur a assure que $h:=\dfrac{f(a-f'(a)X)}{f'(a)^2}$ est à coefficients dans $\mathcal{O}$. En outre, puisque $\frac{f(a)}{f'(a)^2}\in\mathfrak{m}$, on a $\overline{h}=X(Xg-1)$ si bien que 0 est une racine simple de $\overline{h}$. Par (iv), il existe donc $a'\in\mathfrak{m}$ tel que $h(a')=0$, c'est à dire tel que $f(a-f'(a)a')=0$.

En posant $b:=a-f'(a)a'$ on obtient donc que $f(b)=0$ et $v(b-a)=v(f'(a))+v(a')>v(f'(a))$.

$(v)\Longrightarrow(vi)$ Il suffit d'appliquer (v) avec $a:=-1$.

$(vi)\Longrightarrow(vii)$ Il suffit d'effectuer le changement de variable $X:=a_{n-1}Y$, de diviser par a_{n-1}^n puis d'appliquer (vi).

$(vii)\Longrightarrow(i)$ Supposons que $\mathcal{O}$ n'est pas hensélien et considérons une extension galoisienne finie N de K où $\mathcal{O}$ ne s'étend pas de manière unique.

Appelons $\mathcal{O}_1,\mathcal{O}_2,\ldots,\mathcal{O}_r$ ses différentes extensions à N, si bien que $r\geq2$. On notera $\mathfrak{m}_i$ l'idéal maximal de $\mathcal{O}_i$. Considérons $H:=\{\sigma\in\mathrm{Gal}(N/K):\sigma(\mathcal{O}_1)=\mathcal{O}_1\}$. Puisque la proposition $B.3.2.$ assure que les $\mathcal{O}_i$ sont conjugués sur K et puisque $r\geq2$

on en déduit que $H < \mathrm{Gal}(N/K)$ et donc que $L := N^H$ est une extension stricte de K.

Posons $\mathcal{O}'_i := L \cap \mathcal{O}_i$ si bien que les $\mathcal{O}'_i$ sont les extensions de $\mathcal{O}$ à L (non nécessairement deux à deux distinctes). Notons alors que pour $i \geq 2$ on a $\mathcal{O}'_1 \neq \mathcal{O}'_i$, sinon la proposition $B.3.2.$ assure que $\mathcal{O}_1$ et $\mathcal{O}_i$ sont conjugués sur L et donc que $\mathcal{O}_1 = \mathcal{O}_i$ en vertu de la définition de L.

Posons $R := \mathcal{O}'_1 \cap \cdots \cap \mathcal{O}'_r$. D'après la remarque $B.3.1.$, l'anneau R est la clôture intégrale de $\mathcal{O}$ dans L et en posant $\mathfrak{m}'_i := \mathfrak{m}_{\mathcal{O}'_i} \cap R$, le théorème $B.3.1.$ assure que $\mathcal{O}'_i = R_{\mathfrak{m}'_i}$.

Du fait que les $\mathfrak{m}'_i$ sont maximaux et que pour $i \geq 2$ on a $\mathcal{O}'_1 \neq \mathcal{O}'_i$ on déduit que pour $i \geq 2$ on a $\mathfrak{m}'_1 \neq \mathfrak{m}'_i$. Le lemme chinois fournit donc $\alpha \in R$ tel que $\alpha \in 1 + \mathfrak{m}'_1$ et $\alpha \in \mathfrak{m}'_i$ $(i \geq 2)$. En particulier, puisque $r \geq 2$ on en déduit que $\alpha \notin K$ si bien qu'en notant $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$ le polynôme irréductible de α sur K, f n'a pas de racine dans K.

Soit $\beta \neq \alpha$ un conjugué de α: il existe $\sigma \in \mathrm{Gal}(N/K)$ tel que $\sigma\alpha = \beta$. Notons d'abord que $\sigma(\mathcal{O}_1) \neq \mathcal{O}_1$ sans quoi σ fixerait L et donc $\alpha = \beta$. Ainsi, σ permute les $\mathcal{O}_i$ sans fixer $\mathcal{O}_1$. Puisque $\alpha \in 1+\mathfrak{m}_1$ et $\alpha \in \mathfrak{m}_i$ $(i \geq 2)$, on en déduit que $\beta = \sigma\alpha \in \mathfrak{m}_1$.

En conséquence, $a_{n-1} \in (1+\mathfrak{m}_1) \cap K = 1 + \mathfrak{m}$ et pour $i < n-1$, $a_i \in \mathfrak{m}_1 \cap K = \mathfrak{m}$ si bien que f vérifie les conditions de (vii) sans avoir de racine sur K.

□

C.2.2 Quelques propriétés des corps henséliens

On énonce ici des propriétés de transitivité du caractère hensélien d'un corps valué.

Proposition C.2.1. *Soient $\mathcal{O} \leq \mathcal{O}_1$ des anneaux de valuation d'un corps K. Notons $\mathfrak{m}$ et $\mathfrak{m}_1$ les idéaux maximaux respectifs de $\mathcal{O}$ et $\mathcal{O}_1$, si bien que $\mathfrak{m}_1 \leq \mathfrak{m}$. Notons également k le corps résiduel de $(K, \mathcal{O})$ et k_1 celui de $(K, \mathcal{O}_1)$.*

Alors, $\mathcal{O}/\mathfrak{m}$ est un anneau de valuation de k_1 et $(K, \mathcal{O})$ est hensélien si et seulement si $(K, \mathcal{O}_1)$ et $(k_1, \mathcal{O}/\mathfrak{m}_1)$ sont henséliens.

Démonstration. La preuve de la première assertion est laissée au lecteur.

Supposons que $(K, \mathcal{O})$ est hensélien.

Soit $f = X^n + X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_0 \in \mathcal{O}_1[X]$ où $a_i \in \mathfrak{m}_1$. Alors $a_i \in \mathfrak{m}$ si bien que f admet une racine d'après le point (vi) du théorème $C.2.1$: ce même point assure donc que $(K, \mathcal{O}_1)$ est hensélien.

De même, si $\overline{f} = X^n + X^{n-1} + \overline{a_{n-2}}X^{n-2} + \cdots + \overline{a_0} \in k_1[X]$ où $\overline{a_i} \in \mathfrak{m}/\mathfrak{m}_1$ alors on peut relever $\overline{f}$ en un polynôme $f = X^n + X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_0 \in K[X]$ où $a_i \in \mathfrak{m}$. Puisque $(K, \mathcal{O})$ est hensélien, on dispose d'une racine de f dans $\mathcal{O}$ dont le réduit modulo $\mathfrak{m}_1$ induit donc une racine de $\overline{f}$. Le point (vi) du théorème $C.2.1$ assure donc que $(k_1, \mathcal{O}/\mathfrak{m}_1)$ est hensélien.

Réciproquement, supposons que $(K, \mathcal{O}_1)$ et $(k_1, \mathcal{O}/\mathfrak{m}_1)$ sont henséliens. Soit $f \in \mathcal{O}[X]$ et $\alpha \in k$ une racine simple de $\overline{f} \in k[X]$. Puisque k est isomorphe au corps résiduel de $(k_1, \mathcal{O}/\mathfrak{m}_1)$ le point (iv) du théorème $C.2.1.$ assure qu'il existe un relèvement $\beta \in k_1$ de α qui annule le réduit de f modulo $\mathfrak{m}_1$: du fait que α est une racine simple de $\overline{f}$ on déduit que β est une racine simple du réduit de f modulo $\mathfrak{m}_1$. De même, puisque $(K, \mathcal{O}_1)$ est hensélien, on peut relever β en $\gamma \in \mathcal{O}$ qui annule f. On en déduit donc que $(K, \mathcal{O})$ est hensélien. □

Si la définition du caractère hensélien assure que toute extension algébrique d'un corps hensélien est hensélienne, le lecteur peut se demander ce qu'il en est de ses sous-extensions: on verra par la suite, dans le cadre de l'hensélisation d'un corps, que les sous-extensions algébriques ne sont pas toujours henséliennes.

On dispose néanmoins du résultat suivant:

Proposition C.2.2. *Soit $(K, \mathcal{O}_K) \leq (L, \mathcal{O}_L)$ une extension de corps valués. Si L est hensélien et K est séparablement clos dans L alors K est hensélien.*

Démonstration. Commençons par remarquer que dans la preuve de $(vii) \implies (i)$ nous avons seulement utilisé (vii) dans le cas où le polynôme de l'assertion est séparable.

Montrons que K vérifie (vii) avec l'hypothèse de séparabilité. Soit $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$ un polynôme séparable où $a_{n-1} \in \mathcal{O}_K^\times$ et $a_0, \ldots, a_{n-2} \in \mathfrak{m}_K$. Puisque L est hensélien, f a une racine dans L: celle-ci étant séparable sur K on en déduit qu'elle est dans K. Ainsi, $(K, \mathcal{O}_K)$ est hensélien. □

C.2.3 Le lemme de Krasner

Enchaînons avec le théorème suivant, dont l'implication $(i) \implies (iii)$ est connue sous le nom de lemme de Krasner:

Théorème C.2.2. *Soit K un corps muni d'une valuation v. En notant $K^{\mathbf{alg}}$ la clôture algébrique de K, les assertions suivantes sont équivalentes:*

(i) Le corps valué (K, v) est hensélien;

(ii) Si v' est une valuation de $K^{\mathbf{alg}}$ qui étend v, si x est algébrique sur K de polynôme minimal $f = (X - x_1) \ldots (X - x_n)$ sur K et si y est tel que

$$v(y - x) > \max \{v(x - x_i) : x_i \neq x\}$$

alors $K(x, y)$ est purement inséparable sur $K(y)$;

(iii) Si v' est une valuation de $K^{\mathbf{alg}}$ qui étend v, si x est séparable sur K de polynôme minimal $f = (X - x_1) \ldots (X - x_n)$ sur K et si y est tel que

$$v(y - x) > \max \{v(x - x_i) : x_i \neq x\}$$

alors $K(x) \subseteq K(y)$.

Démonstration. $(i) \implies (ii)$ Soit N une extension normale de K qui contient $K(x, y)$. Pour montrer l'inséparabilité de l'extension $K(y) \hookrightarrow K(x, y)$ il suffit de montrer que tout élément de $\mathrm{Gal}(N/K(y))$ fixe x.

Supposons par l'absurde qu'il existe $\sigma \in \mathrm{Gal}(N/K(y))$ tel que $\sigma(x) \neq x$. Puisque (K, v) est hensélien, il existe un unique anneau valué $\mathcal{O}_N$ de N qui étend $\mathcal{O}_v$. Notons que puisque $\sigma(\mathcal{O}_N) = \mathcal{O}_N$, on a $v \circ \sigma = v$. Puisque $v(\sigma(x) - y) = v(\sigma(x - y)) = v(x - y)$ et puisque $\sigma(x)$ est un conjugué de x sur K distinct de x, on a:

$$v(\sigma(x) - x) = v((\sigma(x) - y) - (x - y)) \geq \min \{v(\sigma(x) - y), v(x - y)\} = v(x - y) > v(\sigma(x) - x)$$

ce qui constitue une contradiction.

$(ii) \implies (iii)$ Ce sens est immédiat.

$(iii) \implies (i)$ Pour montrer le caractère hensélien de K, on va montrer que le point (vii) du théorème $C.2.1$ est vérifié. Commençons par poser $\mathcal{O} := \mathcal{O}_v$ et $\mathcal{O}' := \mathcal{O}_{v'}$, d'idéaux maximaux $\mathfrak{m}$ et $\mathfrak{m}'$ respectivement.

Soit $f = X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_0 \in K[X]$ où $a_{n-1} \in \mathcal{O}^\times$ et $a_0, \ldots, a_{n-2} \in \mathfrak{m}$. Les relations entre coefficients et racines assurent que f admet une unique racine x telle que $v'(x) = 0$, les autres se trouvant dans $\mathfrak{m}'$. Notons g

son polynôme minimal sur K et y l'opposé du coefficient de $X^{\deg(g)-1}$. En notant $x_1, \ldots, x_d$ les racines de g, le lecteur vérifiera aisément que puisque les racines de g distinctes de x sont également racines de f, on a que $v'(x-y) > \max\{v'(x-x_i) : x_i \neq x\}$.

Par (iii), on a donc $K(x) \subseteq K(y) = K$ si bien que f admet une racine $x \in K$: le point (vii) du théorème $C.2.1.$ est donc vérifié. $\square$

Références

[CH99] Zoé Chatzidakis and Ehud Hrushovski. Model theory of difference fields. *Trans. Amer. Math. Soc.*, 351(8):2997–3071, 1999.

[Cha08] Zoé Chatzidakis. Théorie des modèles des corps valués, 2008.

[EP05] Antonio J. Engler and Alexander Prestel. *Valued fields*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2005.

[HHM06] Deirdre Haskell, Ehud Hrushovski, and Dugald Macpherson. Definable sets in algebraically closed valued fields: elimination of imaginaries. *J. Reine Angew. Math.*, 597:175–236, 2006.

[HKR18] Martin Hils, Moshe Kamensky, and Silvain Rideau. Imaginaries in separably closed valued fields. *Proc. Lond. Math. Soc. (3)*, 116(6):1457–1488, 2018.

[HMRC07] E. Hrushovski, B. Martin, S. Rideau, and R. Cluckers. Definable equivalence relations and zeta functions of groups. *ArXiv Mathematics e-prints*, December 2007.

[Hod93] Wilfrid Hodges. *Model theory*, volume 42 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1993.

[Hol95] Jan E. Holly. Canonical forms for definable subsets of algebraically closed and real closed valued fields. *J. Symbolic Logic*, 60(3):843–860, 1995.

[Hol97] Jan E. Holly. Prototypes for definable subsets of algebraically closed valued fields. *J. Symbolic Logic*, 62(4):1093–1141, 1997.

[Hru93] Ehud Hrushovski. A new strongly minimal set. *Ann. Pure Appl. Logic*, 62(2):147–166, 1993. Stability in model theory, III (Trento, 1991).

[Joh14] W. Johnson. On the proof of elimination of imaginaries in algebraically closed valued fields. *ArXiv e-prints*, June 2014.

[Kob77] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, Vol. 58.

[Mar02] D. Marker. *Model Theory : An Introduction*. Graduate Texts in Mathematics. Springer New York, 2002.

[Mat89] Hideyuki Matsumura. *Commutative ring theory*, volume 8. Cambridge university press, 1989.

[Poi83] Bruno Poizat. Une théorie de Galois imaginaire. *J. Symbolic Logic*, 48(4):1151–1170 (1984), 1983.

[Rid13] Silvain Rideau. Élimination des imaginaires dans les corps valués. Master's thesis, École Normale Supérieure, 2013.

[Rob56] Abraham Robinson. *Complete theories*. North-Holland Publishing Co., Amsterdam, 1956.

[She78] Saharon Shelah. *Classification theory and the number of nonisomorphic models*, volume 92 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam-New York, 1978.

[TZ12] Katrin Tent and Martin Ziegler. *A course in model theory*, volume 40 of *Lecture Notes in Logic*. Association for Symbolic Logic, La Jolla, CA; Cambridge University Press, Cambridge, 2012.

[WWH97] F. Wagner, F.O. Wagner, and N.J. Hitchin. *Stable Groups.* Lecture note series / London mathematical society. Cambridge University Press, 1997.