EQUATIONS EN UN GRAND NOMBRE DE VARIABLES

26 avril 2021

GROUPE MAT04
Sigui DRO
Rémi LESBATS
Kai MAO
Adrien POULALION
Ababacar SEMBENE
Armel Randy ZEBAZE


l'
ÉCOLE
POLYTECHNIQUE
IP PARIS

Remerciements

Nous tenons à remercier tous les personnels de l'Ecole qui nous ont permis, dans un contexte particulier, de mener ce projet dans les meilleures dispositions.

Nous sommes en particulier extrêmement reconnaissants envers notre tuteur, Diego Izquierdo, qui nous a accompagnés à la perfection tout au long de ce périple mathématique. Sa bienveillance et sa disponibilité à toute épreuve nous ont rendu la tâche très agréable. Il a de plus su nous aiguiller vers de nombreuses pistes passionnantes, et nous sensibiliser à une approche moins académique, plus proche de la recherche mathématique. Il nous a par ailleurs conféré ce plaisir de lire, de découvrir des théories mathématiques de notre propre chef, ce qui est un trésor inestimable et une des grandes leçons que nous tirerons de ce travail.

Nous remercions enfin l'ensemble du département de mathématiques, et en particulier le coordinateur du département Javier Fresán, qui nous a conseillés à bon escient et dans une constante bonne humeur.

Motivation

Résoudre des équations est une préoccupation majeure en mathématiques. Dès nos premiers pas dans cette discipline, au lycée, nous avons appris à trouver les racines de polynômes de degré 1, puis de degré 2, principalement dans l'ensemble des réels. On commence dès le second ordre à toucher du doigt des notions d'existence de solutions à de telles équations, et à effleurer par exemple le concept de clôture algébrique en introduisant le corps des nombres complexes.
En effet, avant même de savoir résoudre des équations polynomiales, la question de l'existence de solutions se pose naturellement. Et si le cadre des réels et des complexes nous est familier et est relativement aisé à traiter, on peut étudier les équations polynomiales sur des structures plus élaborées et abstraites. En effet, le cadre naturel d'étude des polynômes est celui des corps, ce qui englobe les réels, les complexes, les rationnels mais aussi tant d'autres objets moins communs.
Ainsi, une des questions qui a taraudé les mathématiciens, mais aussi des scientifiques spécialisés dans d'autres disciplines, tout au long du vingtième siècle est de savoir déterminer avec certitude s'il existe une solution à une équation polynomiale sur un corps donné. Par exemple, Hilbert a énoncé dans ses 23 problèmes pour les mathématiques du vingtième siècle, un problème portant sur la possibilité de décider algorithmiquement si un polynôme à coefficients entiers possède une racine entière. Le russe Youri Matiyasevich y a répondu par la négative avec une approche logicienne. Une telle approche peut d'ailleurs s'avérer fructueuse pour d'autres problèmes du même type, aussi nous verrons comment la logique fondamentale peut éclairer les mathématiques (via le principe d'Ax-Kochen). Ceci met en évidence la difficulté de ces questions, auxquelles il est parfois tout simplement impossible de répondre de manière systématique. C'est aussi cela qui rend ce domaine si excitant, il s'agit d'un véritable défi pour la raison humaine.
Chercher des critères garantissant l'existence de zéros à un polynôme a donc galvanisé les forces des mathématiciens du siècle dernier. Un des angles d'attaque les plus prometteurs a été introduit dans les années 1950 par Artin et Lang, qui ont mis en évidence le fait que dans beaucoup de corps, il existe une relation très simple reliant le degré et le nombre de variables d'un polynôme homogène, qui, si elle est vérifiée, systématise l'existence de zéros non triviaux. La théorie des corps C_i est née, et elle s'est avérée très robuste pour étudier la plupart des corps usuels. Elle a connu de nombreux développements jusqu'à ce jour, et des outils algébriques et géométriques plus récents sont venus corroborer les résultats existants, et éclairer les points d'ombre restants. Il s'agit encore d'un sujet de recherche actif.
L'objectif de ce projet est de se saisir de la propriété C_i d'Artin et Lang, et plus généralement d'étudier l'existence de zéros à des polynômes homogènes sur des corps donnés.

Plan détaillé

Nous avons choisi de découper notre étude en quatre moments principaux.
Dans un premier temps, nous allons chercher à comprendre comment fonctionne la propriété C_i, et pour quelles raisons il est pertinent de l'introduire. Après quelques éléments de définition, nous allons étudier le cas des corps finis, puis voir de quelle manière le caractère C_i d'un corps peut être transmis à certaines de ses extensions, via le théorème de Tsen. Ces premiers éléments permettront d'entrevoir la puissance de la propriété d'Artin et Lang.
Ensuite, nous allons construire un premier exemple de corps dont le comportement échappe à la propriété C_i, avec les corps p-adiques $\mathbb{Q}_p$, pour p premier. Plus généralement, nous allons construire les corps de valuation discrète, ainsi que leurs complétés, et étudier leurs propriétés. Nous construirons $\mathbb{Q}_p$ par ce prisme, et nous en déduirons des résultats fondamentaux sur les zéros des polynômes homogènes, avec par exemple le lemme d'Hensel. Nous nous focaliserons alors sur le comportement des corps $\mathbb{Q}_p$ vis-à-vis de la propriété C_2, et prouverons que malgré des éléments encourageants, aucun corps $\mathbb{Q}_p$ n'est C_2, ni même C_i pour un i quelconque.
Nous continuerons l'étude des corps p-adiques en présentant le théorème d'Ax-Kochen, qui requiert une approche tout à fait différente puisque sa démonstration repose sur des outils de logique et de théorie des modèles. Nous étudierons en particulier les similitudes profondes entre les corps $\mathbb{Q}_p$ et les séries de Laurent formelles à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. Après avoir redéfini les éléments de logique du premier ordre nécessaires, la démonstration du théorème sera découpée en deux temps. Nous introduirons d'abord la notion d'ultraproduit, cadre naturel de cette preuve, avant d'établir l'équivalence au premier ordre entre deux de ces ultraproduits. Nous présenterons ensuite le théorème et ce qu'il change dans notre façon d'envisager la théorie des corps C_i.
Enfin, nous aborderons le problème par un tout nouvel angle emprunté à l'algèbre moderne, en évoquant la notion de cohomologie. L'objectif de cette ultime partie sera de faire le lien entre ce que l'on appelle la dimension cohomologique et la propriété C_i. Nous présenterons d'abord les prémices de la cohomologie sur différentes structures de groupes, et définirons la dimension cohomologique. Nous construirons ensuite la cohomologie galoisienne, ce qui nous donnera suffisamment d'outils pour étudier la cohomologie sur les corps C_1. Nous verrons brièvement le cas des corps C_2, ce qui nous permettra de faire le lien avec toutes les notions vues dans les trois premières parties.

Table des matières

1
LA PROPRIÉTÉ C_i ET SON INTÉRÊT

Nous allons tout d'abord définir la propriété C_i, puis mettre en évidence l'intérêt qu'elle revêt dans le cadre de l'étude de l'existence de racines à des polynômes en beaucoup de variables dans certains corps.

1.1 DÉFINITIONS PRÉLIMINAIRES

On rappelle qu'un polynôme (en éventuellement plusieurs variables) sur un corps K est dit homogène s'il est non constant et que tous ses monômes sont de même degré. On l'appelle aussi "forme". Nous nous focaliserons essentiellement sur des polynômes de ce type.

Définition 1. Soient K un corps et $i \geqslant 0$ un entier. On dit que le corps K vérifie la propriété C_i si pour tous entiers strictement positifs N et d vérifiant $N > d^i$, tout polynôme homogène à coefficients dans K, de degré d, en N variables possède un zéro non trivial (c'est-à-dire distinct de 0) sur K.

C'est cette propriété qu'Artin et Lang ont introduite, nous verrons par la suite qu'elle est intéressante en ce que de nombreux corps la vérifient pour un certain i. Notons par exemple que les corps algébriquement clos sont trivialement C_0, c'est en particulier le cas de $\mathbb{C}$. A l'inverse que le corps des réels $\mathbb{R}$ n'est C_i pour aucun i (il suffit pour s'en rendre compte de considérer la somme de N variables élevées au carré et de faire tendre N vers l'infini). On peut aussi définir une propriété analogue mais plus faible :

Définition 2. Soient K un corps, et $i \geqslant 0$ et $d \geqslant 1$ des entiers. Le corps K est dit de classe $C_i(d)$, ou encore faiblement C_i en le degré d, si pour tout entier strictement positif N vérifiant $N > d^i$, tout polynôme homogène à coefficients dans K, de degré d, en N variables possède un zéro non trivial sur K.

Remarque 1. Le corps K est alors C_i si et seulement s'il est $C_i(d)$ pour tout entier d strictement positif.

Revenons au cas du corps des réels. Si ce corps n'est C_i pour aucun entier i, on peut se rendre compte que pour un degré d impair, le corps $\mathbb{R}$ est $C_0(d)$. Cela vient simplement de l'étude des limites en l'infini d'une forme de degré impaire, ainsi que d'une application du théorème des valeurs intermédiaires.
En revanche, ce sont les degrés pairs qui posent problème. Considérons d un entier pair strictement positif, le polynôme $X_1^d + \ldots + X_N^d$ ne peut avoir de zéro autre que le zéro trivial, puisque c'est une somme de carrés. Ainsi, $\mathbb{R}$ n'est $C_i(d)$ pour aucun entier i.
Le cas des corps $\mathbb{R}$ ou $\mathbb{C}$ relève tout au plus d'un jeu de notations pour bien comprendre comment fonctionne la propriété C_i. Nous allons maintenant voir en quoi cette théorie est réellement robuste, en étudiant des corps qui sont C_1 : les corps finis.

1.2 LES CORPS FINIS SONT C_1

Soit k un corps fini à q éléments et soit p sa caractéristique. On rappelle que q est nécessairement de la forme p^n pour un certain entier strictement positif n. Tous les corps finis ont pour ordre la puissance d'un nombre premier.

On introduit k^* le groupe multiplicatif des éléments non nuls de k, qui possède $q-1$ éléments. On veut prouver que k^* est cyclique d'ordre $q-1$. Ceci peut être démontré comme suit. Supposons que k^* n'est pas cyclique. La théorie élémentaire des groupes abéliens finis nous dit que m, le plus petit commun multiple des ordres des éléments de k^*, est l'ordre d'au moins un élément y dans k. Comme k^* est supposé non cyclique, l'ordre de y est strictement plus petit que $q-1$, ce qui implique $m < q-1$. Par conséquent, l'équation $x^m = 1$, vérifiée par les $q-1$ éléments de k^*, possède strictement plus de m racines distinctes dans k^*, ce qui est impossible. k^* est donc cyclique.
On va prouver le lemme 1 par application de ce résultat.

Lemme 1. Soit m un entier strictement positif. On a : $\sum_{x\in k} x^m = \begin{cases} -1 & \text{si } q-1 \text{ divise } m \\ 0 & \text{sinon} \end{cases}$

Démonstration. La fonction $x \longmapsto x^m$ est un endomorphisme de k^*. Puisque k^* est cyclique d'ordre $q-1$, cet endomorphisme est trivial seulement si m est divisible par $q-1$, et dans ce cas la somme vaut $(q-1)\cdot 1 = -1$. Si m n'est pas divisible par $q-1$, le résultat est une conséquence du lemme suivant : □

Lemme 2. Soit Ω un corps, et $h : k^* \longrightarrow \Omega^*$ un homomorphisme non trivial du groupe multiplicatif de k vers celui de Ω . Alors $\sum_{x\in k^*} h(x) = 0$.

Démonstration. Par hypothèse, il existe $y \in k^*$ tel que $h(y) \neq 1$. Ainsi, utilisant le changement de variable bijectif sur k^* qui à x, associe xy :

$$\sum_{x\in k^*} h(x) = \sum_{x\in k^*} h(xy) = h(y) \sum_{x\in k^*} h(x)$$

puisque h est un homomorphisme. Utilisant l'intégrité du corps, on en déduit que soit $h(y) - 1 = 0$, soit la somme des images des éléments du groupe par h est nulle. Mais le premier cas est exclu par hypothèse, ce qui conclut la démonstration. □

L'objectif est de prouver que k est C_1, c'est-à-dire que tout polynôme homogène dont le nombre de variables est supérieur à son degré a un zéro non nul dans k. Pour y parvenir, nous allons utiliser un argument de comptage des zéros, qui donne un résultat plus général que celui qui nous intéresse.

Théorème 1. [CHEVALLEY-WARNING]
Soit f un polynôme à n variables et à coefficients dans un corps fini k de caractéristique p, soit d le degré de ce polynôme et $N(f)$ le nombre de zéros de f dans k. Si $n > d$, alors $N(f) \equiv 0[p]$. En particulier, si f n'a pas de terme constant alors f a un zéro non trivial dans k.

Démonstration. Pour tout $n-$uplet $x \in k^n$, on a d'après le théorème de Lagrange :

$$1 - f(x)^{q-1} = \begin{cases} 1 & \text{si } f(x) = 0 \\ 0 & \text{sinon.} \end{cases}$$

En sommant sur tous les éléments de k^n, on a : $\overline{N(f)} = \sum_{x \in k^n} \left(1 - f(x)^{q-1}\right) = -\sum_{x \in k^n} f(x)^{q-1}$

où $\overline{N(f)}$ est la classe résiduelle modulo p de $N(f)$, considéré comme un élément de k. Ainsi il reste à montrer que pour tout polynôme f avec $d < n$, on a $\sum_{x \in k^n} f(x)^{q-1} = 0$.

Or f^{q-1}, étant de degré $d(q-1)$, est une k-combinaison linéaire de monômes de degré au plus $d(q-1)$. Si $X^\mu = X_1^{\mu_1} X_2^{\mu_2} \dots X_n^{\mu_n}$ est parmi ces monômes, on a $\sum_{X \in k^n} X^\mu = \prod_{i=1}^{n} \sum_{X_i \in k} X_i^{\mu_i}$.

Puisque $d < n$, il existe au moins un i tel que μ_i est strictement plus petit que $q-1$, et donc non divisible par $q-1$. D'après le Lemme 1, le $i-$ième terme du produit est nul. Ainsi la somme $\sum_{X \in k^n} X^\mu$ est nulle. Il en est donc de même pour $\sum_{x \in k^n} f(x)^{q-1}$ par conséquent, d'où le résultat.

En outre, si le terme constant de f est nul, le polynôme f est au moins annulé par le zéro trivial, il vient $N(f) \geqslant p > 1$. Par conséquent, f doit nécessairement posséder un autre zéro que le zéro trivial. Ceci s'applique notamment aux polynômes homogènes, permettant d'affirmer le caractère C_1 du corps k. □

Nous avons donc trouvé un premier exemple de corps vérifiant la propriété C_i pour $i \geqslant 1$. En particulier, le résultat établi ci-dessus concerne le corps $\mathbb{Z}/p\mathbb{Z}$, pour p premier. Nous verrons par la suite comment itérer une telle propriété pour des corps plus grands, en particulier des extensions de corps ou des corps de fractions rationnelles.

1.3 THÉORÈME DE TSEN ET INTÉRÊT DES CORPS C_i

Nous venons d'exhiber, avec le théorème de Chevalley-Warning, des premiers corps satisfaisant une propriété C_i pour un certain entier i. Pour donner de l'intérêt à la théorie d'Artin et Lang, il faut encore que de nombreux autres corps entrent dans ce cadre et soient aussi C_j pour j entier. Le théorème de Tsen va permettre le tour de force de démontrer que partant d'un corps K qui est C_i, d'autres corps (parmi lesquels ses extensions algébriques, ses extensions transcendantes de degré fini, ainsi que son corps de fractions rationnelles) sont C_{i+j} pour un entier naturel j adéquat.

1.3.1 • RÉSULTATS IMPORTANTS SUR LES FORMES NORMIQUES

Nous introduisons ici les formes normiques, qui se révèleront déterminantes dans la démonstration du théorème de Tsen.

Définition 3. Soient n et d des entiers strictement positifs. Soit K un corps et ϕ une forme de dégré d en n variables à coefficients dans K. Si le seul zéro de ϕ dans K est le zéro trivial et si $n = d^i$, alors ϕ est appelée forme normique d'ordre i. Quand $i = 1$ on dit simplement que ϕ est normique.

Soit k un corps C_i admettant au moins une forme normique d'ordre i. On voit que par définition de la propriété C_i, un tel corps ne peut posséder de forme normique d'ordre strictement supérieur à i. De plus si un corps possède une forme normique d'ordre i il ne peut être C_j pour un entier naturel $j < i$, ceci permettra de justifier que l'entier i tel qu'un corps est C_i est optimal.

Exhiber des formes normiques peut donc se révéler utile pour montrer qu'un résultat est le meilleur que l'on puisse trouver. En outre, elles sont aussi cruciales pour la démonstration du théorème de Lang-Nagata : une forme normique peut en effet servir à établir l'existence d'un zéro non trivial pour une autre forme !
Avant d'y arriver on va s'intéresser à deux résultats. Le premier donne un exemple de forme normique et le second permet, à partir d'une forme normique, d'en générer d'autres de degré arbitrairement grand, ce qui servira dans la démonstration du théorème de Lang-Nagata.

Lemme 3. Si K possède une extension finie de degré $e > 1$, alors la norme de E vers K est une forme normique de degré e.

Démonstration. Pour un élément x de E, sa norme $N(x)$ est le determinant de la transformation linéaire $y \to xy$. Pour une base de E (E est vu comme un K espace vectoriel) choisie, $N(x)$ est un polynôme homogène de degré e en les coordonnées de x. De plus $N(x) \neq 0$ pour $x \neq 0$, la transformation linéaire considérée étant inversible pour $x \neq 0$. Donc $N(x)$ est une forme normique. □

Lemme 4. Si K n'est pas algébriquement clos, alors K admet des formes normiques de degré arbitrairement grand.

Démonstration. Soit ϕ une forme normique de degré e. On pose

$$\phi^{(1)} = \phi(\phi|\phi|\dots|\phi)$$
$$\phi^{(2)} = \phi^{(1)}(\phi|\phi|\dots|\phi)$$

etc., entre deux barres (|) on change la variable correspondante par une évaluation de ϕ en de nouvelles variables. On a la relation de récurrence pour $m \geqslant 1$:

$$\phi^{(m)} = \phi^{(m-1)}(\phi|\phi|\dots|\phi)$$

Plus explicitement, pour les premières itérations :

$$\phi(x_1|\dots|x_e)$$
$$\phi^{(1)} = \phi(\phi(x_1^1|\dots|x_e^1)|\dots|\phi(x_1^e|\dots|x_e^e))$$

Définie de la sorte, $\phi^{(m)}$ est une forme normique de degré e^{m+1}. □

Théorème 2. [LANG-NAGATA]
Soit K un corps C_i. Soit r un entier naturel non nul et $f_1, f_2, \dots, f_r$ des polynômes homogènes en n variables communes, et chacun de dégré d. Alors si $n > rd^i$ ces polynômes ont un zéro non trivial en commun dans K.

Notons qu'on ne travaille qu'avec des polynômes homogènes, ou formes. En effet, on ne sait que sur de rares corps, traiter les polynômes qui contiennent des monômes de degrés différents. L'hypothèse d'homogénéité est essentielle à la démonstration des théorèmes de Lang-Nagata et de Tsen.
Démonstration. On peut supposer que K n'est pas algébriquement clos, autrement la preuve est classique. Soit ϕ une forme normique de dégré $e \geqslant r$, dont l'existence est garantie par le lemme précédent. On considère la suite de formes normiques definie comme suit :

$$\phi^{(1)} = \phi^{(1)}(f) = \phi(f_1, \dots, f_r|f_1, \dots, f_r|\dots|f_1, \dots, f_r|0, \dots, 0)$$

$$\phi^{(2)} = \phi^{(2)}(f) = \phi^{(1)}(f_1, \ldots, f_r | f_1, \ldots, f_r | \ldots | f_1, \ldots, f_r | 0, \ldots, 0)$$

etc ... où on insère autant d'ensembles complets de $f_1, \ldots, f_r$ que possible, et à chaque insertion on utilise différents noms de variables. En procédant ainsi on sait que $\phi^{(1)}$ a $n\left[\frac{e}{r}\right]$ variables et est de dégré $de \leqslant dr\left(\left[\frac{e}{r}\right]+1\right)$. Si K est C_1, on veut :

$$n\left[\frac{e}{r}\right] > dr\left(\left[\frac{e}{r}\right]+1\right), \text{ i.e} \quad (n-dr)\left[\frac{e}{r}\right] > dr$$

Puisque $n - dr > 0$, on peut avoir cette condition en choisissant e assez grand. Dans ce cas $\phi^{(1)}$ possèdera un zéro non trivial, qui est un zéro commun à tous les f puisque ϕ est une forme normique. Si K est C_i pour $i > 1$, on doit choisir le plus grand $\phi^{(m)}$. On sait que $\phi^{(m)}$ est de degré $D_m = d^m e$, et si on dénote par N_m le nombre de variables de $\phi^{(m)}$, on a l'égalité suivante :

$$N_{m+1} = \left[\frac{N_m}{r}\right]$$

On veut choisir m assez grand pour que $N_m > D_m^i$ de sorte à pouvoir utiliser la propriété C_i de K. En notant $\left[\frac{N_m}{r}\right] = \left[\frac{N_m}{r}\right] - \left[\frac{t_m}{r}\right]$, avec $0 \leqslant t_m < r$ on a :

$$\left[\frac{N_{m+1}}{D_{m+1}^i}\right] = \left[\frac{n\left[\frac{N_m}{r}\right]}{d^i D_m^i}\right] = \left[\left[\frac{n}{rd^i}\right]\frac{N_m}{D_m^i}\right] - \left[\frac{n}{rd^i}\frac{t_m}{e^i(d^i)^m}\right] \geqslant \left[\frac{n}{rd^i}\frac{N_m}{D_m^i}\right] - \left[\frac{n}{rd^i}\frac{r}{e^i(d^i)^m}\right]$$

En utilisant la meme inégalité pour $m, m-1, \ldots 2$, on obtient :

$$\begin{aligned}
\left[\frac{N_{m+1}}{D_{m+1}^i}\right] &\geqslant \left(\left[\frac{n}{rd^i}\right]\right)^2\left(\left[\frac{N_{m-1}}{(D_{m-1})^i}\right] - \left[\frac{r}{e^i(d^i)^{m-1}}\right]\right) - \left[\frac{n}{rd^i}\right]\left[\frac{r}{e^i(d^i)^m}\right] \\
&\geqslant \ldots \\
&\geqslant \left(\left[\frac{n}{rd^i}\right]\right)^m\left[\frac{N_1}{D_1^i}\right] - \left[\tfrac{r}{e^i}\right]\left[\frac{n}{r}\right]\left[\frac{1}{(d^i)^{m+1}}\right]\left(\left(\left[\frac{n}{r}\right]\right)^{m-1} + \left(\left[\frac{n}{r}\right]\right)^{m-2} + \ldots + 1\right) \\
&\geqslant \left(\left[\frac{n}{rd^i}\right]\right)^m\left[\frac{N_1}{D_1^i}\right] - \left[\frac{r}{e^i}\right]\left[\frac{n}{r}\right]\left[\frac{1}{(d^i)^{m+1}}\right]\left[\frac{\left(\left[\frac{n}{r}\right]\right)^m - 1}{\left[\frac{n}{r}\right] - 1}\right]
\end{aligned}$$

On substitue $D_1 = de$, $N_1 = n[\frac{e}{r}] = n(\frac{e}{r} - \frac{t}{r})$ avec $0 \leqslant t < r$ et on obtient :

$$\begin{aligned}
\left[\frac{N_{m+1}}{D_{m+1}^i}\right] &\geqslant \left(\left[\frac{n}{rd^i}\right]\right)^{m+1}\left[\frac{e-t}{e^i}\right] - \left[\frac{r}{e^i}\right]\left[\frac{n}{r}\right]\left[\frac{1}{(d^i)^{m+1}}\right]\left[\frac{r(n^m - r^m)}{r^m(n-r)}\right] \\
&= \left(\left[\frac{n}{rd^i}\right]\right)^{m+1}\left[\frac{e-t}{e^i}\right] - \left[\frac{r}{e^i}\right]\left[\frac{n}{rd^i}\right]\left[\frac{r}{n-r}\right]\left(\left(\left[\frac{n}{rd^i}\right]\right)^m - \left[\frac{1}{(d^i)^m}\right]\right) \\
&= \left(\left[\frac{n}{rd^i}\right]\right)^{m+1}\left(\left[\frac{e-t}{e^i}\right] - \left[\frac{r^2}{e^i(n-r)}\right]\right) + \left[\frac{1}{(d^i)^m}\right]\left(\left[\frac{rn}{e^i d^i(n-r)}\right]\right) \\
&= \left(\left[\frac{n}{rd^i}\right]\right)^{m+1}\left(\left[\frac{(n-r)(e-t) - r^2}{e^i(n-r)}\right]\right) + \left[\tfrac{1}{(d^i)^m}\right]\left(\left[\frac{rn}{e^i d^i(n-r)}\right]\right)
\end{aligned}$$

puisque e peut être choisi assez grand de sorte que $(n-r)(e-t) - r^2 > 0$ et $\frac{n}{rd^i} > 1$, le premier terme tend vers ∞ lorsque m tend vers ∞. Le second terme tend vers 0 puisque $d > 1$. On aboutit alors au fait que $\frac{N_m}{(D_m)^i} \to \infty$ pour $m \to \infty$, ce qui achève la démonstration.

□

Ce résultat est déjà fort en lui-même, puisqu'il permet d'établir l'existence d'un zéro non trivial commun à plusieurs formes sous les conditions énoncées. Il va de plus être décisif dans la démonstration du théorème de Tsen, que nous allons maintenant établir.

1.3.2 • LE THÉORÈME DE TSEN

Voyons maintenant en quoi le théorème de Lang-Nagata permet de démontrer le théorème de Tsen, qui va justifier l'étude de la propriété C_i des corps. Nous allons déjà nous en servir pour établir un résultat de Lang sur les extensions algébriques des corps C_i. Il s'énonce comme suit :

Théorème 3. [LANG]
Soit K un corps C_i, alors toute extension algébrique A de K est elle aussi C_i.

Démonstration. Supposons que K soit un corps C_i pour i entier. Soit A une extension algébrique de K, et soit f une forme à coefficients dans A, à n variables, et de degré d tel que $n > d^i$.
Les coefficients de f sont tous dans une même extension finie E de K, on resteindra ainsi $f(X_1, \ldots, X_n)$ à E. On peut alors décomposer chacune des variables de f sur une base de E comme K-espace vectoriel, de cardinal entier e et notée $w_1, \ldots, w_e$. On pose pour i compris entre 1 et n :

$$X_i = X_{i,1} \cdot w_1 + \ldots + X_{i,e} \cdot w_e$$

Les $X_{i,j}$ étant des variables dans K. On peut alors réécrire :

$$f(X_1, \ldots, X_n) = f_1(X_{1,1}, \ldots, X_{1,e}, X_{2,1}, \ldots, X_{n,e}) \cdot w_1 + \ldots + f_e(X_{1,1}, \ldots, X_{1,e}, X_{2,1}, \ldots, X_{n,e}) \cdot w_e$$

où $f_1, \ldots, f_e$ sont des formes sur K, de degré d en $e \cdot n$ variables. Trouver un zéro non trivial de f dans E est donc équivalent à trouver un zéro commun à ces e formes. Or, $en > ed^i$ et K est C_i, on en déduit d'après le théorème de Lang-Nagata l'existence d'un zéro commun à ces formes, donc f possède un zéro dans E (qui est aussi un zéro inclus dans A). Ainsi, f vue comme forme sur A possède un zéro non trivial, il en résulte que A est C_i. □

Nous venons donc de prouver que toute extension algébrique d'un corps C_i est aussi C_i. Le théorème de Tsen permet quant à lui de traiter le cas des extensions de corps transcendantes, de degré de transcendance fini.
D'après ce qui a été établi dans le cadre de l'étude des formes normiques, intuitivement si un corps k est C_i et admet une forme normique d'ordre i, récursivement $k(X_1, \ldots, X_k)$ admet une forme normique d'ordre $i + k$. On déduit alors le lemme suivant :

Lemme 5. Soit k un corps C_i alors $k(t)$ est C_{i+1}.

Démonstration. Soit $P(x_1, \ldots, x_n)$ un polynôme homogène en n variables et de degré d sur $k(t)$ vérifiant $n > d^{i+1}$. Nous allons prouver que P admet un zéro non trivial. Soit

$$\begin{aligned} x_1 &= \zeta_{10} + \zeta_{11}t + \ldots + \zeta_{1s}t^s \\ x_2 &= \zeta_{20} + \zeta_{21}t + \ldots + \zeta_{2s}t^s \\ &\ldots \\ x_n &= \zeta_{n0} + \zeta_{n1}t + \ldots + \zeta_{ns}t^s \end{aligned}$$

Où les ζ_{ij} sont des éléments de k et s non déterminé pour l'instant mais pouvant être arbitrairement grand. Soit r le degré le plus élevé des coefficients de P, on peut alors réécrire P sous la forme :

$P(x_1, ..., x_n) = P_0(\zeta_{10}, \ldots, \zeta_{ns}) + P_1(\zeta_{10}, \ldots, \zeta_{ns})t + \ldots + P_{ds+r}(\zeta_{10}, \ldots, \zeta_{ns})t^{ds+r}$ où les P_i sont tous des polynômes homogènes de degré d en $n(s+1)$ variables. Pour les avoir tous nuls en même temps, on utilise le théorème 2 en satisfaisant l'inéquation

$n(s+1) > d^i(ds+r+1) \iff n - d^{i+1} > \dfrac{(r+1)d^i - n}{s}$ qui est satisfaite pour s assez grand. □

Nous allons énoncer maintenant le théorème de Tsen.

Théorème 4. [TSEN]
Si K est un corps C_i et E une extension de K de dégré de transcendence j, alors E est C_{i+j}.

Exemple 1. Soit j un entier naturel non nul. On déduit du théorème précédent que le corps $\mathbb{C}(T_1, \ldots, T_j)$ des fractions rationnelles à coefficients dans $\mathbb{C}$ est C_j, car $\mathbb{C}$ est C_0.
En outre, soit q une puissance d'un nombre premier p, et $\mathbb{F}_q$ un corps fini d'ordre q. Il vient que $\mathbb{F}_q(T_1, \ldots, T_j)$ est C_{j+1}, puisque d'après le théorème de Chevalley-Warning, $\mathbb{F}_q$ est C_1.
Notons que ces résultats sont optimaux, puisque nous avons remarqué l'existence de formes normiques du bon ordre pour les corps de fractions rationnelles.

Par conséquent, partant d'un corps K qui est C_i, il est possible d'en construire d'autres possédant cette même propriété, que ce soit par extension algébrique, transcendante de degré fini, ou en considérant le corps des fractions rationnelles à coefficients dans K. Or on avait déjà prouvé que les corps finis sont C_1, ou encore que $\mathbb{C}$ est C_0 : on en déduit en itérant que de nombreux corps sont C_i pour un certain i, et c'est cela qui donne de la robustesse à cette théorie. Toutefois, nous allons aussi étudier des corps dont le comportement échappe à ce cadre.

2
DES CORPS N'ÉTANT PAS C_i : LES CORPS $\mathbb{Q}_p$

Dans cette partie, nous allons prouver les résultats importants relatifs aux corps p-adiques, notés $\mathbb{Q}_p$. Nous allons d'abord procéder à leur construction.

2.1 CONSTRUCTION

2.1.1 • LES ANNEAUX DE VALUATION DISCRÈTE

On introduit les anneaux de valuation discrète, qui seront essentiels pour l'étude des corps $\mathbb{Q}_p$ puisque ces derniers seront construits à partir de tels anneaux. Nous allons aussi démontrer des résultats généraux sur ces anneaux, qui s'appliqueront dans le cas particulier de l'anneau de valuation discrète $\mathbb{Z}_p$ et de son corps des fractions $\mathbb{Q}_p$.

Définition 4. Soit R un anneau principal, R est dit de valuation discrète s'il possède un unique idéal premier non nul, noté $\mathfrak{m}(R)$ ou simplement $\mathfrak{m}$.

On peut prouver que $R/\mathfrak{m}(R)$ est un corps (par le fait que $\mathfrak{m}(R)$ est en fait maximal), on l'appelle le corps résiduel de l'anneau R. Par définition, les idéaux non nuls d'un anneau principal R sont de la forme πR avec π un élement de R.

Proposition 1. Soit R un anneau principal de valuation discrète et π un élément irréductible de R. Les idéaux non nuls de R sont de la forme $\pi^n R$ pour $n \geqslant 0$.

Démonstration. Puisque R est un anneau principal, les idéaux non nuls de R sont de la forme xR, où x est non nul. Or, on peut écrire x en produit de facteurs irréductibles soit $x = \pi^n u$ avec u inversible, car π est le seul élément irréductible de R à un facteur inversible près. On a bien $xR = \pi^n R$. □

Remarque 2. L'entier n ainsi défini s'appelle la valuation de x et est noté $\nu(x)$. Plus généralement , on pose $\nu(x) = \sup\{n \in \mathbb{N}; x \in \pi^n R\}$. On a $\nu(0) = +\infty$.

On étudie maintenant le corps K des fractions de R. Tout élément de K peut s'écrire $\frac{a}{b}$ avec $b \neq 0$ et on peut étendre la valuation à tout K en posant $\nu\left(\frac{a}{b}\right) = \nu(a) - \nu(b)$.

Proposition 2. L'application $\nu : \left| \begin{array}{ccc} K^* & \longrightarrow & \mathbb{Z} \\ x & \longmapsto & \nu(x) \end{array} \right.$ définit un morphisme surjectif et vérifie la propriété $\nu(x+y) \geqslant \inf(\nu(x), \nu(y))$.

Proposition 3. (Réciproque) Soit K un corps muni d'une application ν de K^* dans $\mathbb{Z}$ vérifiant les propriétés :
(i) $\nu(x+y) \geqslant \inf(\nu(x), \nu(y))$
(ii) $\nu(xy) = \nu(x) + \nu(y)$
Alors $R = \{a \in K, \nu(a) \geqslant 0\}$ est un anneau de valuation discrète de K tel que $\mathfrak{m}(R) = \{a \in K^*, \nu(a) > 0\}$.

Démonstration. On pose, pour tout entier n, $I_n = \{x \in R \mid \nu(x) \geqslant n\}$. On vérifie aisément que $I_0 = R$ est bien un anneau comme annoncé, mais aussi que tous les I_n sont des idéaux : la propriété (ii) garantit en effet la stabilité par multiplication par un élément de R, et la propriété (i) permet de vérifier le fait que I_n est bien un sous-groupe additif de R.
La propriété (ii) de la valuation induit que l'image de K (privé de 0) par ν est un sous-groupe additif de $\mathbb{Z}$ et est donc de la forme $n\mathbb{Z}$ où n est un entier naturel non nul. Quitte à diviser ν par n ce qui ne viole pas les propriétés d'une valuation, on peut dire que tous les entiers sont images d'un élément de K par ν.
Soit I un idéal de R : s'il existe $x \in R$ de valuation nulle, alors soit $y \in R$. On a $\nu\left(\frac{y}{x}\right) \geqslant 0$, donc $\frac{y}{x} \in R$ et $y = x \cdot \frac{y}{x} \in R$. On en conclut que $I = R$. Soit I un idéal distinct de R et 0, on veut montrer qu'il est de la forme I_n pour un certain $n > 0$. Soit x de valuation minimale dans I, par ce qui précède $n = \nu(x) \geqslant 1$, on a $I \in I_n$. En suivant le même raisonnement on montre que $I_n \subset I$, ce qui prouve que $I = I_n$. Tous les idéaux non restreints à 0 sont donc de la forme I_n pour un certain entier n.
Enfin, posons π un élément de valuation 1, qui jouera le rôle d'uniformisante. Soit $n \geqslant 1$, on a $\pi^n \in I_n$, on montre facilement que pour $x \in I_n$, on a $x = \pi^n \cdot \frac{x}{\pi^n}$ avec $\nu\left(\frac{x}{\pi^n}\right) \geqslant 0$ dans R, donc x est dans l'idéal engendré par π^n. Il vient : $I_n = \pi^n R$, tous les idéaux de R étant de cette forme et principaux, R est principal. De plus, le seul idéal premier parmi ceux construits est $I_1 = \mathfrak{m}(R)$ ce qui prouve que R est de valuation discrète. □

On va maintenant construire la complétion d'un anneau de valuation discrète en utilisant une uniformisante π (qui est un élément de valuation égale à 1). Considérons pour tout entier naturel n, l'anneau-quotient $R_n = R/\pi^{n+1}$, et notons $k = R_0$ le corps résiduel. A chaque classe d'équivalence α de ce corps résiduel, on associe un représentant $\{\alpha\}$ dans R. Soit $a \in R$, notons $\{\alpha_0\}$ son représentant modulo π, $a - \{\alpha_0\}$ est divisible par π et peut s'écrire sous la forme : $a_1 \cdot \pi$. On poursuit de la sorte en décomposant a_1 en $\{\alpha_1\} + a_2\pi$ avec a_2 dans R, etc. On aboutit au fait que les éléments de R_n peuvent s'écrire de manière unique sous la forme : $\xi_n = \{\alpha_0\} + \{\alpha_1\} \cdot \pi + \ldots + \{\alpha_n\} \cdot \pi^n$.

On considère alors un sous-anneau de l'anneau-produit des R_n, qu'on appelle $\hat{R}$ ou complétion de R, défini par les suites : $(\xi_0, \ldots, \xi_n, \ldots)$ qui sont les suites "compatibles" dans R, c'est-à-dire que $\xi_{n-1} \equiv \xi_n \pmod{\pi^n}$. On construit de fait le morphisme canonique : $\tau : R \longrightarrow \hat{R}$ qui associe à un élément x la suite de ses projections dans R_n telles que définies plus haut. Le seul élément de R divisible par toutes les puissances de π est de valuation infinie et il s'agit donc de 0, ce qui prouve donc l'injectivité du morphisme. S'il s'avérait que ce dernier était surjectif, on noterait abusivement par isomorphisme que $R = \hat{R}$, et on dirait que R est complet. Sachant qu'on a l'égalité $\hat{R}/\pi^n = R/\pi^n$, on en déduit la complétude de $\hat{R}$. On peut aussi étendre la valuation dans $\hat{R}$ en considérant qu'il s'agit de l'indice du premier élément non nul de la suite, ce qui conserve les propriétés attendues d'une valuation. On verra notament dans la section consacrée au théorème d'Hensel que cette notion algébrique de complétude coïncide avec celle de complétude pour une métrique bien choisie.

2.1.2 • CONSTRUCTION DE $\mathbb{Q}_p$ ET PREMIÈRES PROPRIÉTÉS

On fixe, dans cette section, p un nombre premier. On va munir l'anneau $\mathbb{Z}$ d'une valuation discrète à partir de la valuation de p dans la décomposition en produit de facteurs premiers des entiers. On pose ainsi : $\nu(x) = \sup\{n \in \mathbb{N};\ p^n | x\}$. L'entier p est de valuation 1. On constate immédiatement que ν vérifie bien les deux premières propriétés attendues pour une valuation discrète, mais pas la troisième car des éléments non divisibles par p, donc de valuation 0, ne sont pas inversibles dans $\mathbb{Z}$:

on peut prendre $p+1$ à titre d'exemple.
Pour contourner cela, on étend l'anneau $\mathbb{Z}$ en y ajoutant certaines fractions, celles de la forme $\frac{a}{b}$ avec b non divisible par p, et on note généralement $\mathbb{Z}_p$ l'anneau ainsi créé. Les propriétés d'une valuation sont toujours respectées par cette modification, et cela permet par la même occasion de rendre les éléments de valuation nulle inversibles, de sorte qu'on a bien un anneau de valuation discrète.
L'anneau $\mathbb{Z}_p$ est alors la complétion de cet anneau comme on l'a établi en 1.3.1, et $\mathbb{Q}_p$ en est le corps des fractions. L'anneau construit a la propriété d'être complet, et le corps résiduel est $k = \mathbb{Z}/p\mathbb{Z}$. Par la construction de la complétion, on pourrait penser que $\mathbb{Q}_p$ est isomorphe aux séries de Laurent formelles à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, et se comporte donc de la même façon vis-à-vis de la propriété C_i, mais ce n'est en fait pas le cas.

Proposition 4. Le corps $\mathbb{Z}/p\mathbb{Z}(T)$ est C_2.

Démonstration. Il suffit d'appliquer le théorème de Tsen à $\mathbb{Z}/p\mathbb{Z}$, qui est C_1 d'après le théorème de Chevalley-Warning. □

Nous démontrerons dans la partie suivante que $\mathbb{Z}/p\mathbb{Z}((T))$ est lui aussi C_2. On pourrait s'attendre à ce que le corps $\mathbb{Q}_p$ vérifie cette même propriété, mais il n'en est rien, bien qu'il soit tout de même en relation étroite avec elle, ce que nous aborderons plus tard avec le théorème d'Ax-Kochen. Remarquons en premier abord :

Proposition 5. Le corps $\mathbb{Q}_p$ n'est pas isomorphe à $\mathbb{Z}/p\mathbb{Z}((T))$.

Démonstration. Le corps $\mathbb{Q}_p$ contient $\mathbb{Z}$ et est donc de caractéristique 0, tandis que $\mathbb{Z}/p\mathbb{Z}((T))$ est lui de caractéristique p. □

Cela signifie aussi que l'addition et la multiplication ont un comportement différent dans ces deux corps, et que ces opérations sont plus difficiles à effectuer dans $\mathbb{Q}_p$ puisqu'elles ne se font pas de la manière "naturelle" propre aux séries formelles $\mathbb{Z}/p\mathbb{Z}((T))$.
En fait, nous pouvons remarquer que la caractéristique joue un rôle essentiel quand il s'agit de confronter de tels corps. En effet, si le fait d'avoir la même caractéristique est une condition nécessaire pour que deux corps soient isomorphes, elle est aussi suffisante lorsque ceux-ci sont à valuation discrète, complets et de même corps résiduel.

Proposition 6. (Admis) Si R est un anneau de valuation discrète complet et qu'il a la même caractéristique que son corps résiduel k, alors R est isomorphe à l'anneau des séries formelles $k[[T]]$, et son corps des fractions K est isomorphe à $k((T))$.

2.2 DES RÉSULTATS INTÉRESSANTS

2.2.1 • CONSTRUIRE DES RACINES DE POLYNÔMES DANS $\mathbb{Q}_p$

Dans cette section, nous réutiliserons les notations propres aux anneaux de valuation discrète introduits en 1.3.1. Nous nous intéresserons uniquement à ceux qui sont complets.
Considérons r polynômes homogènes en n variables à coefficients dans R, qu'on note $f_1, \dots, f_r$. Comme dans la démonstration des théorèmes de Lang-Nagata et de Tsen, il serait intéressant de

trouver un vecteur x non nul qui soit simultanément racine de tous ces polynômes. Une condition nécessaire pour vérifier cela est :

$$\forall m \in \mathbb{N}, \forall j \in [1; r], f_j(x) \equiv 0[\pi^{1+m}]$$

où π est l'uniformisante, de valuation 1, qui nous a permis d'écrire les éléments du complété de R en section 2.1.
De surcroît, cette condition est en fait suffisante lorsque R, anneau de valuation discrète, est complet !

Théorème 5. Soit R un anneau de valuation discrète complet. Soient r un entier strictement positif et f_j pour j compris entre 1 et r des polynômes homogènes à coefficients dans R et en n variables. Supposons de plus que R_m est un anneau fini pour tout m. Alors les f_j ont un zéro non trivial commun dans R si et seulement si ils en ont un, non divisible par π, dans $R_m = R/\pi^{m+1}$ pour tout entier naturel m.

Démonstration. Considérons pour tout entier m strictement positif, l'homomorphisme canonique $\phi_m : R_m \longrightarrow R_{m-1}$ qui correspond à la congruence modulo π^m. En d'autres termes, il permet de passer d'un terme au précédent dans une suite d'éléments compatibles de R, correspondant à un élément de $\hat{R}$. On notera abusivement de la même façon l'application qui agit identiquement sur des n-uplets de R_m, et c'est celle-ci que nous utiliserons au cours de cette démonstration.
Pour chaque m, on note S_m l'ensemble des solutions non triviales dans R_m aux équations $f_j(x) = 0$. Par hypothèse, cet ensemble est non vide pour tout entier m. On restreint même S_m aux zéros primitifs, c'est-à-dire ceux dont une des coordonnées n'est pas divisible par π. Notons de plus pour $j > m$, $S_{j,m}$ l'image de S_m par l'application $\phi_{m+1} \dots \phi_{j-1}\phi_j$, c'est-à-dire la projection des zéros de R_j dans R_m. On obtient de cette façon une suite décroissante d'ensembles :
$S_m \supset S_{m+1,m} \supset \dots \supset S_{j-1,m} \supset S_{j,m} \supset \dots$
Introduisons alors T_m l'intersection des $S_{m,j}$ pour $j \geqslant m$. Elle est non vide car c'est l'intersection d'une suite décroissante d'ensembles non vides par hypothèse, et si elle était vide alors les ensembles $S_{m,j}$ le seraient à partir d'un certain rang j, ce qui n'est pas le cas. L'ensemble T_m correspond à l'ensemble des solutions modulo π^{m+1} qu'on peut relever en des solutions modulo π^{j+1}, pour tout $j \geqslant m$.
On remarque directement que $\phi_m(T_m) \subset T_{m-1}$, et l'inclusion réciproque est aussi vraie : soit en effet $x_{m-1} \in T_{m-1}$, on considère son image réciproque $\phi_m^{-1}(x_{m-1})$ par ϕ_m. Elle rencontre par définition $S_{m,j}$ fini pour tout $j \geqslant m$ et rencontre donc T_m, d'où $x_{m-1} \in \phi_m(T_m)$.
De ce fait, prenons $\xi_0 \in T_0$. On peut alors trouver par ce qui précède, $\xi_1 \in T_1$ vérifiant $\phi_1(\xi_1) = \xi_0$. En itérant, on construit une suite $(\xi_0, \dots, \xi_n, \dots)$ compatible, elle correspond bien à un élément de R par complétude. Cet élément est par conséquent un zéro non trivial (les éléments de la suite étant primitifs) commun aux f_j. □

Remarque 3. Cette propriété peut aussi se démontrer en se passant de l'hypothèse de finitude des anneaux R_m, en utilisant le lemme d'Hensel (2.2.2). Nous ne démontrerons pas ici ce résultat difficile établi par Greenberg. Le théorème ci-dessus suffit toutefois à montrer l'équivalence pour $\mathbb{Q}_p$, car ces R_m sont finis, et correspondent à $\mathbb{Z}/p^{m+1}\mathbb{Z}$.

Théorème 6. [GREENBERG]
Si k est un corps C_i, alors $k((T))$ est C_{i+1}. En particulier, si k est un corps fini alors $k((T))$ est C_2, c'est le cas notamment de $\mathbb{Z}/p\mathbb{Z}((T))$.

Démonstration. Considérons f un polynôme homogène à coefficients dans $k((T))$, à n variables, de degré d avec $n > d^{i+1}$. On multiplie par le dénominateur commun des coefficients pour se ramener dans $k[[T]]$.
Par le théorème précédent, et sachant que $k[[T]]$ est un anneau de valuation discrète complet, il suffit de trouver un zéro primitif dans l'anneau quotient $k[[T]]/T^{m+1}$ pour tout m. Ceci nous permet de supprimer aussi les monômes de degré strictement plus grand que m des coefficients, et on se ramène donc à une équation polynômiale dans $k[T]$ pour tout m. Or, le théorème de Tsen garantit que $k[T]$ est C_{i+1} et donc le polynôme considéré y possède bien une racine modulo T^m pour tout m.
Par le théorème précédent et la remarque, ceci assure l'existence d'un zéro dans $k((T))$, qui est par conséquent C_{i+1}. □

On a donc prouvé qu'il suffit de trouver un zéro modulo p^n pour tout n, pour garantir qu'il en existe une dans $\mathbb{Z}_p$ commune à un système d'équations polynômiales. Pour autant, ceci ne suffit pas à ce que ce corps soit C_2...
Remarquons de plus que le résultat montré est optimal pour les séries formelles $k((T))$, étant donné qu'on dispose dans certains cas d'une forme normique d'ordre $i+1$ par le théorème suivant :

Proposition 7. Soit R un corps muni d'une valuation discrète, de corps résiduel κ. Si κ possède une forme normique N^* d'ordre i, alors R possède une forme normique N d'ordre $i+1$.

Démonstration. En effet, N^* est un polynôme homogène sur κ, en n variables et de degré d ($d^i = n$). On étend alors cette forme en relevant les coefficients de ce polynôme (qui sont dans κ) dans K, et on obtient alors un polynôme homogène $P \in K[X]$. Soit alors $\pi \in K$ un élément de valuation 1, on pose $N(x_1, \dots, x_{nd}) = P(x_1, \dots, x_n) + \pi P(x_{n+1}, \dots, x_{2n}) + \dots + \pi^{d-1} P(x_{n(d-1)+1}, ..., x_{nd})$ et cette application convient. Elle est en effet de degré d, en $nd = d^{i+1}$ variables et si on suppose que $(x_1, \dots, x_{nd})$ est un zéro de N alors on peut montrer qu'il est trivial.
On le suppose en effet non trivial et on procède par récurrence sur le maximum des valuations des x_i non nuls. Comme N^* est un polynôme homogène, on peut supposer que toutes les valuations sont positives, sinon, si par exemple x_1 est de valuation strictement négative, on va utiliser le fait que $x_1^{-d} N(x_1, \dots, x_n d) = N(1, x_1^{-1} x_2, \dots, x_1^{-1} x_{nd})$ comme N est un polynôme homogène de degré d et en faisant la même opération pour tous les éléments de valuation strictement négative, on obtient un zéro dont toutes les projections sont dans A l'anneau de valuation discrète associé à K.
Notons ϕ la projection sur κ, le corps résiduel de A. On a alors : $N^*(\phi(x_1), \dots, \phi(x_n)) = 0$. Donc comme N^* est une forme normique, on a $\phi(x_1) = \dots = \phi(x_n) = 0$.
On peut donc écrire $x_1 = \pi x_1', \dots, x_n = \pi x_n'$ où les x_i' sont de valuations positives, et inférieure à 1 de celle de x_i quand $x_i \neq 0$. En conséquence, on a $\pi^d P(x_1, \dots, x_n) + \pi^d P(x_{n+1}, ..., x_{2n}) + \dots + \pi^{d-1} P(x_{n(d-1)+1}, \dots, x_{nd}) = 0$ soit en simplifiant par π qui est non nul, on obtient un nouveau zéro $(x_{n+1}, \dots, x_{nd}, x_1', \dots, x_n')$ avec les derniers éléments qui ont perdu 1 en valuation (sauf s'ils sont déjà nuls). On peut recommencer avec $(x_{n+1}, \dots, x_{2n})$ et ainsi de suite jusqu'à avoir diminué le maximum de valuation des x_i non nuls de 1. Par conséquent et d'après ce qui précède, tous les x_i sont de valuation infinie donc nuls, donc la forme est bien normique. □

On peut déduire de ce qui précède que si κ est C_0 alors K admet une forme normique d'ordre 1 et que dans le cas contraire K possède une forme normique d'ordre 2.

2.2.2 • THEORÈME DE HENSEL

Dans le cadre des anneaux de valuation discrète, et se limitant au cadre des équations polynomiales il existe un critère qui garantit l'existence d'une solution pour une équation de la forme :

$$f(x) = 0$$

Dans un ensemble plus facile à manipuler comme $\mathbb{R}$, on sait résoudre une telle équation moyennant quelques conditions. Il s'agit d'utiliser la méthode de Newton qui est une méthode algorithmique qui permet de converger vers la solution de l'équation en construisant une suite numérique. Le théoreme du point fixe de Banach permet de prouver la convergence de la suite construite. Le lemme de Hensel s'inscrit dans la continuité de ce résultat et s'applique à des anneaux de valuation discrète complets. On considère donc R un tel anneau, muni d'une valuation v, de paramètre uniformisant π, de corps résiduel k et dont l'ensemble des fractions est noté K. En choissant un réel strictement positif γ et en posant pour tout x dans K :

$$|x| = \gamma^{-v(x)}$$

on définit une norme sur K et c'est elle qui sera utilisée pour le théorème (on vérifie aisement qu'elle possede les propriétés d'une norme). L'ensemble K muni de la distance induite par cette norme devient un espace metrique, et la complétude se transmet grace au lemme suivant :

Lemme 6. L'anneau de valuation discrète R est complet si et seulement si K est un espace métrique complet.

Le lemme de Hensel s'énonce alors comme suit :

Théorème 7. [HENSEL]
Soit a un élément de R tel que $f'(a) \neq 0$ et $\left|\dfrac{f(a)}{f'(a)^2}\right| < 1$. Alors la suite de Newton :

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)} \qquad n = 0, 1, \dots$$

initialisée à $a_0 = a$ converge vers un zéro ξ de f. Ce zéro satisfait : $|\xi - a| < |f'(a)|$ et il est le seul zéro de f à satisfaire cette inégalité.

Démonstration. On pose $\delta = v(f'(a))$, par hypothèse $\left|\dfrac{f(a)}{f'(a)^2}\right| < 1$. Donc $v\left(\dfrac{f(a)}{f'(a)^2}\right) > 0$, i.e $v(f(a)) - 2\delta > 0$. On en déduit que $v(f(a)) \geqslant 2\delta + 1 \iff f(a) \equiv 0[\pi^{2\delta+1}]$. En divisant par $f'(a)^2$ on obtient :

$$\frac{f(a)}{f'(a)^2} \equiv 0[\pi]$$

Etant donné que $a_1 - a_0 = a_1 - a = -\dfrac{f(a)}{f'(a)} = -f'(a)\dfrac{f(a)}{f'(a)^2}$, on en conclut que :

$$a_1 \equiv a[\pi^{1+\delta}]$$

On va montrer par récurrence que les deux propriétés suivantes sont vérifiées :

$$f(a_n) \equiv 0[\pi^{2\delta+n+1}] \qquad (*)$$

$$a_n \equiv a_{n-1}[\pi^{\delta+n}] \qquad (**)$$

Ce qui prouvera que la suite $(a_n)_{n\in\mathbb{N}}$ converge vers un zéro ξ de f tel que :

$$\xi \equiv a[\pi^{\delta+1}]$$

On a montré en début de preuve que les propositions $(*)$ et $(**)$ sont vraies pour $n = 0$. Pour conclure la preuve par récurrence il suffit de prouver leur hérédité. On suppose donc que $(*)$ et $(**)$ sont vraies pour une valeur $n \in \mathbb{N}$ et on veut montrer que c'est toujours le cas pour $n + 1$. $(**)$ implique :

$$a_n \equiv a_0[\pi^{\delta+1}]$$

Ce qui implique $f'(a_n) \equiv f'(a)[\pi^{1+\delta}]$, de sorte que $v(f'(a_n)) = v(f'(a)) = \delta$. Sachant $(*)$: $f(a_n) \equiv 0[\pi^{1+n+2\delta}]$, on en déduit que :

$$\frac{f(a_n)}{f'(a_n)} \equiv 0[\pi^{\delta+n+1}]$$

d'où finalement $a_{n+1} \equiv a_n[\pi^{1+n+\delta}]$, ce qui achève l'hérédité de $(**)$. Mais f étant polynomiale, elle est égale a son développement de Taylor, donc on peut écrire :

$$f(a_{n+1}) = f(a_n)+(a_{n+1}-a_n)f'(a_n)+c_n(a_{n+1}-a_n)^2 = f(a_n)-f'(a_n)\frac{f(a_n)}{f'(a_n)}+c_n(\frac{f(a_n)}{f'(a_n)})^2 = c_n(\frac{f(a_n)}{f'(a_n)})^2$$

D'ou $f(a_{n+1}) \equiv 0[\pi^{2n+2+2\delta}]$. Cette congruence est plus forte que ce qui est demandé, et permet donc de conclure sur l'hérédité de $(*)$.
Il ne reste plus qu'à prouver l'unicité de ξ. On prend donc η tel que $f(\eta) = 0$ avec $\eta \equiv a[\pi^{1+\delta}]$. Pour montrer l'unicité on va prouver que :

$$\eta \equiv a_n[\pi^{\delta+n+1}] \quad \forall n \in \mathbb{N}$$

par récurrence, ce qui prouvera que $\eta = \xi$. La proposition est vraie pour $n = 0$. Pour $n \in \mathbb{N}$ un développement de Taylor nous donne $0 = f(\eta) = f(a_n) + f'(a_n)(\eta - a_n) + (\eta - a_n)^2 d_n$, $d_n \in R$. En divisant par $f'(a_n)$ ($v(f'(a_n)) = \delta$) et en faisant passer a_n de l'autre côté de la congruence on obtient :

$$\eta \equiv a_n - \frac{f(a_n)}{f'(a_n)}[\pi^{\delta+2n+2}]$$

ce qui implique $\eta = a_{n+1}[\pi^{\delta+n+2}]$. □

Ce résultat se généralise en plus grande dimension pour n polynômes $f_1, \dots f_n$ en n variables X_1, $\dots$, X_n. Par commodité on pose $\underline{f} = (f_1, \dots, f_n)$ un vecteur de composantes polynomiales telles que $\forall x = (x_1, \dots, x_n) \in R^n$, $\underline{f}(x) = (f_1(x), \dots, f_n(x))$. On définit la matrice jacobienne :

$$M_{\underline{f}} = \left(\frac{\partial f_i}{\partial x_j}\right)$$

et son déterminant :

$$J_{\underline{f}} = det(\partial f_i/\partial x_j).$$

La généralisation requiert de considérer des vecteurs $\underline{f}$ dont les composantes sont des séries formelles en n variables sur R. Dans ce cas, $\underline{f}(x)$ pour x dans $\mathbb{R}^n$ n'a de sens que si toutes les séries composantes $f_i(x)$ convergent. De la même manière on peut définir l'opération de composition de deux éléments de ce type par composition de leurs séries composantes. Le théorème se généralise alors comme suit :

Théorème 8. Soit $\underline{f} = (f_{r+1}, \dots, f_n)$ un système de $n-r$ polynômes en n variables sur un anneau de valuation discrète complet R. On suppose qu'il existe un élément $a \in R^n$ et un entier δ tel que :

$$\underline{f}(a) \equiv 0[\pi^{2\delta+1}]$$

et tel que la matrice jacobienne $M_{\underline{f}}(a)$ réduite modulo $\pi^{\delta+1}$ soit de rang maximal. Alors il existe $b \in \mathbb{R}^n$ qui est un zéro de $\underline{f}$ et qui vérifie :

$$b \equiv a[\pi^{\delta+1}]$$

Un des intérêts du lemme d'Hensel est de permettre de relever une solution d'une équation dans $\mathbb{Z}/p\mathbb{Z}$, en une solution dans $\mathbb{Z}_p$. En effet, la condition $\left|\frac{f(a)}{f'(a)^2}\right| < 1$ implique en particulier que $\nu(f(a)) > 0$ et donc que p divise $f(a)$. Partant de a divisible par p, on construit algorithmiquement notre solution dans $\mathbb{Z}_p$ en établissant étape par étape ses coefficients pour chaque puissance de p. Ce théorème permet donc non seulement de mettre en évidence l'existence d'une racine à un polynôme dans un anneau de valuation discrète complet, mais aussi de la construire.

Exemple 2. On pose pour $p = 5$ le polynôme : $P(X) = X^2 + 1$
On en cherche une racine dans $\mathbb{Z}_p$. Pour cela, on remarque d'abord que dans $\mathbb{Z}/5\mathbb{Z}$:

$$P(2) \equiv 0[5]$$

Et de plus $P'(2) \equiv 4[5]$ d'où $\nu(P'(2)) = 0$ ce qui permet de satisfaire l'hypothèse du lemme d'Hensel. Ainsi partant de 2, on peut construire une racine carrée de -1 dans $\mathbb{Z}_p$.

Plus généralement, de tels procédés peuvent être appliqués pour passer d'un corps résiduel au complété, pourvu qu'il soit muni de la bonne métrique, d'une géométrie adéquate. Par exemple, sur $\mathbb{R}$, la méthode des tangentes de Newton est très similaire à celle employée par le lemme d'Hensel. Dans le cadre des corps $\mathbb{Q}_p$, il n'est pas toujours possible de relever les zéros d'une forme, du corps résiduel vers le complété. Pourtant, nous allons voir dans la section suivante un cas particulier pour lequel le lemme d'Hensel se révèle être d'une importance capitale.

2.3 ETUDE DES FORMES QUADRATIQUES : $\mathbb{Q}_p$ EST $C_2(2)$

On avait déjà une intuition du lien entre les corps $\mathbb{Q}_p$ et la propriété C_2, et celle-ci va gagner en consistance grâce à l'étude des formes quadratiques.
En effet, on est en mesure de prouver que le corps $\mathbb{Q}_p$ est, pour n'importe quel p premier, C_2 en degré 2, c'est-à-dire que les formes quadratiques en 5 variables ou plus possèdent nécessairement un zéro non trivial.
Comme évoqué précédemment, le lemme d'Hensel nous est ici fort utile pour relever des zéros partant du corps résiduel $\mathbb{Z}/p\mathbb{Z}$, qui est C_1 par le théorème de Chevalley-Warning.

Proposition 8. Le corps $\mathbb{Q}_p$ est $C_2(2)$ pour tout nombre premier p.

Démonstration. Soit f une forme quadratique à coefficients dans $\mathbb{Q}_p$. Quitte à faire un changement de variables, les résultats classiques d'algèbre bilinéaire nous permettent d'écrire la forme quadratique f dans une base orthonormée, soit sous la forme $f = a_1X_1^2 + \ldots + a_nX_n^2$. Quitte à multiplier tous les coefficients, on peut supposer que tous les a_i sont des entiers $p-$adiques non nuls. Ensuite, quitte à remplacer X_i par p^kX_i, on peut supposer que tous les a_i sont de valuation au plus 1. Cela permet de réécrire f sous la forme $f = f_0 + pf_1$, où $f_0 = e_1X_1^2 + \ldots e_rX_r^2$ et $f_1 = e_{r+1}X_{r+1}^2 + \ldots + e_nX_n^2$, les e_i étant des entiers $p-$adiques unitaires. Enfin, quitte à remplacer f par pf, on peut supposer que $r \geqslant n - r$.
Il s'agit désormais de considérer deux cas : le cas où $p = 2$ est plus technique, et sera traité après le cas où p est impair. Supposons donc que p soit impair. Montrons que si $r \geqslant 3$, f_0 a un zéro non trivial dans $\mathbb{Z}_p$. L'hypothèse $r \geqslant 3$ est bien vérifiée, car on a supposé $n \geqslant 5$ et $r \geqslant n - r$, soit $2r \geqslant n \geqslant 5$. D'après le théorème de Chevalley-Warning, comme $r \geqslant 3 > 2 = d$ et f_0 n'a pas de terme constant, on dispose d'un vecteur $x \in \mathbb{Z}_p^r$ tel que $f_0(x) \equiv 0[p]$. Pour toutes les composantes x_i pour lesquelles p ne divise pas x_i, on constate alors que $\dfrac{\partial f_0}{\partial x_i} = 2e_ix_i \not\equiv 0[p]$, puisque p est impair. Le lemme de Hensel affirme alors l'existence d'un certain $y = (y_1, \ldots, y_r)$, zéro de f_0 dans $\mathbb{Z}_p^r$ et tel que $y \equiv x[p]$, ce qui garantit que y est non nul, et on trouve $(y_1, \ldots, y_r, 0, \ldots, 0)$ comme zéro non trivial de f.

On suppose désormais que $p = 2$. On ne peut plus appliquer directement le lemme de Hensel dans sa forme la plus simple avec $\delta = 0$ à cause de l'apparition du 2 dans la dérivée, on doit donc l'appliquer avec $\delta = 1$. En effet, si x est un zéro de f modulo 8 et x_i une composante qui n'est pas divisible par 2, alors on sait que $\dfrac{\partial f_0}{\partial x_i} = 2e_ix_i \not\equiv 0[4]$, donc le lemme de Hensel donne un zéro de f dans $\mathbb{Z}_2$, congru à x modulo 4. Il s'agit donc de prouver l'existence d'un zéro non-trivial de f modulo 8.
On considère deux sous-cas, selon que $r < n$ ou $r = n$. Pour le premier sous-cas on suppose que $r < n$. On rappelle que $n \geqslant 5$ et on considère $g = e_1X_1^2 + e_2X_2^2 + e_3X_3^2 + 2e_nX_n^2$. Il est clair que si on trouve un zéro non-trivial de g modulo 8, alors on en aura un pour f en choisissant toutes les autres variables nulles. D'après les hypothèses sur les e_i, on sait qu'il existe $\alpha \in \mathbb{Z}_2$ tel que $e_1 + e_2 = 2\alpha$. Ainsi $e_1 + e_2 + 2e_n\alpha^2 \equiv 2\alpha + 2\alpha^2 \equiv 2\alpha(1+\alpha) \equiv 0[4]$, donc il existe $\beta \in \mathbb{Z}_2$ tel que $e_1 + e_2 + 2e_n\alpha^2 = 4\beta$. En choisissant $x_1 = x_2 = 1$, $x_3 = 2\beta$ et $x_n = \alpha$, on trouve :

$$g(x) = e_1 + e_2 + e_3(2\beta)^2 + 2e_n\alpha^2 = 4\beta + e_3 \cdot 4\beta^2 \equiv 4\beta + 4\beta^2 \equiv 0[8]$$

Ainsi, nous avons explicité un zéro non-trivial de g modulo 8, qui donne un zéro non-trivial de f modulo 8 comme attendu.
Pour le deuxième sous-cas, on suppose que $r = n$, et on pose $g = e_1X_1^2 + \ldots + e_5X_5^2$. De même que précédemment, si on trouve un zéro non-trivial de g modulo 8, il sera aisé d'en trouver un pour f. On pose $e_1 + e_2 = 2\alpha$ et $e_3 + e_4 = 2\beta$. Si ni α ni β n'est divisible par 2, on choisit $x_1 = x_2 = x_3 = x_4 = 1$, sinon, si par exemple $\alpha \equiv 0[2]$, on choisit $x_1 = x_2 = 0$. Dans tous les cas, on a $e_1X_1^2 + e_2X_2^2 + e_3X_3^2 + e_4X_4^2 = 4\gamma$, donc en posant $x_5 = 2\gamma$ on trouve bien $g(x) = 4\gamma + 4\gamma^2 \equiv 0[8]$. On a bien trouvé un zéro non-trivial de g modulo 8, ce qui conclut la preuve. □

Enfin, pour être complets, nous pouvons mentionner le résultat suivant, que nous ne démontrons pas, mais dont la preuve est dans le livre de Greenberg ([1], p.108) :

Théorème 9. [DEMJANOV, LEWIS]
Le corps $\mathbb{Q}_p$ est $C_2(3)$ pour tout nombre premier p.

Notons que pour $p \geqslant 3$, les raisonnements effectués pour le cas $p = 2$ ne sont plus valables. En effet, le résultat d'algèbre bilinéaire qui permet de "diagonaliser" la forme f n'a pas d'équivalent lorsqu'on travaille sur des monômes de degré plus élevé. La démarche adoptée permet de prouver l'existence de racines uniquement dans le cas de formes dites diagonales, qui sont somme de monômes en une variable chacun, mais pour $p \geqslant 3$ toutes les formes ne sont pas diagonalisables.
Tous les résultats démontrés jusqu'ici dans la partie 2, ont donné aux mathématiciens des années 1950, de bonnes raisons de penser que les corps $\mathbb{Q}_p$ sont C_2. Aussi, Artin avait émis cette conjecture, et nous allons voir comment Guy Terjanian a réussi quelques années plus tard à la nier, en introduisant des formes pertinentes dont le seul zéro est le zéro trivial. Bien que les corps $\mathbb{Q}_p$ soient $C_2(2)$ et $C_2(3)$, ils ne sont pas C_2, car certains degrés plus élevés résistent à la propriété C_2. C'est l'objet de la section suivante.

2.4 LE CORPS $\mathbb{Q}_p$ N'EST PAS $C_{3-\epsilon}$

Malgré des résultats encourageants qui permettent de construire des racines à des équations polynômiales particulières dans $\mathbb{Q}_p$, que ce soit via le lemme d'Hensel ou en construisant une suite compatible de solutions modulo p^n, on n'arrive pas à systématiser l'existence de racines pourvu que le nombre de variables soit suffisamment grand par rapport au degré. Les corps $\mathbb{Q}_p$ ne sont en effet C_2 pour aucun nombre premier p, contrairement à un autre corps de valuation discrète complet de corps résiduel $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}((T))$.
En fait, on peut même montrer que les corps $\mathbb{Q}_p$ ne sont $C_{3-\epsilon}$ pour aucun $\epsilon > 0$, ce qui est vrai en se permettant d'étendre la définition de la propriété C_i à des réels strictement positifs. Ils ne sont en particulier pas C_2. Nous ne savons en revanche pas s'ils sont C_3 ou non, faute de contre-exemple.
On se propose par la suite de prouver ce résultat. Pour y arriver, on utilisera la démarche adoptée par Browkin et Terjanian en introduisant les formes "valant 1 modulo une puissance de p".

Définition 5. Soit $r \in \mathbb{N}^*$. Soit a un élément de $\mathbb{Z}_p$, on dit qu'une forme $f \in \mathbb{Z}_p[X_1, \ldots, X_n]$ vaut a modulo p^r si et seulement si pour tout $x \in \mathbb{Z}_p^n$ non divisible par p, on a :

$$f(x) \equiv a[p^r]$$

On s'intéressera exclusivement à celles valant 1 modulo p^r. Si on s'intéresse à un monôme de la forme X^d, on remarque d'abord que pour que X^d vérifie cette propriété, il faut nécessairement que le polynôme $X^d - 1$ possède $p^r - p^{r-1} = (p-1)p^{r-1}$ racines dans $\mathbb{Z}/p^r\mathbb{Z}$ (excluant les p^{r-1} multiples de p), et celles-ci sont en fait tous les éléments du groupe multiplicatif G constitué des éléments de $\mathbb{Z}/p^r\mathbb{Z}$ non divisibles par p, d'ordre $(p-1)p^{r-1}$. Il vient que si $(p-1)p^{r-1}$ divise d, alors X^d vaut 1 modulo p^r, et la réciproque est vraie car on peut prouver que le groupe G est cyclique.
On constate qu'à une variable, il est facile de construire de telles formes, mais c'est plus compliqué en augmentant le nombre de variables. Ce qui vient d'être établi prouve toutefois que si une telle forme existe, son degré doit être divisible par $(p-1)p^{r-1}$ (on peut le démontrer par récurrence en le nombre de variables).
En fait, on peut construire des formes valant 1 modulo p^r avec un nombre de variables suffisamment grand devant le degré. Pour cela,fixons r et considérons la solution du système :

$$\begin{cases} a_1 + \ldots + a_{r+1} = 1 \\ (r+1) \cdot a_1 + \ldots + (2r+1) \cdot a_{r+1} = 0 \\ \ldots \\ (r+1)^r \cdot a_1 + \ldots + (2r+1)^r \cdot a_{r+1} = 0 \end{cases}$$

Introduisant une matrice de Vandermonde V, il peut se réécrire sous la forme :

$$V(r+1, r+2, \ldots, 2r+1) \cdot (a_1, \ldots, a_{r+1})^T = (1, 0, \ldots, 0)^T$$

La solution de ce système est évidemment un vecteur à coefficients dans $\mathbb{Q}$. On se rend toutefois compte, en inversant la matrice de Vandermonde, que les $a_0, \ldots, a_r$ solutions sont en fait les éléments de la première ligne de l'inverse de $V(r+1, r+2, \ldots, 2r+1)$, or ceux-ci peuvent s'écrire en fonction de $\binom{2r+1}{r}$ et se révèlent être entiers par cette méthode. De là, la solution de notre système est à coefficients dans $\mathbb{Z}$, ce qui va donc nous permettre de poser un polynôme à coefficients dans $\mathbb{Z}_p$ et de raisonner en termes de congruences.

Notons n la partie entière de $\dfrac{p^r}{2r+1}$. On pose successivement des formes à coefficients dans $\mathbb{Z}_p$ jusqu'à en obtenir une valant un modulo p^r. Tout d'abord, pour k variant entre 1 et n :

$$\psi_k(X_1, \ldots, X_k) = \sum_{i=1}^{r+1} (a_i \cdot X_1^{p^r-(r+i)(k-1)} (X_2, \ldots, X_k)^{r+i})$$

Puis :

$$\phi_k(X_1, \ldots, X_n) = \sum_{1 \geqslant i_1 \geqslant \ldots \geqslant i_k \geqslant n} \psi_k(X_{i_1}, \ldots, X_{i_k})$$

On définit alors :

$$f(X_1, \ldots, X_n) = \sum_{i=1}^{n} (-1)^{k+1} \phi_k(X_1, \ldots, X_n)$$

$$g(X_1, \ldots, X_n) = f(X_1^{p-1}, \ldots, X_n^{p-1})$$

On vérifie laborieusement à l'aide des propriétés des coefficients $a_1, \ldots, a_{r+1}$ que g vaut 1 modulo p^{r+1}. Il s'agit bien d'un polynôme homogène en n variables, et de degré : $d = (p-1)p^r$, qui est bien un degré plausible (le plus petit) pour une telle forme.

Nous allons maintenant comprendre l'intérêt d'avoir construit une forme g valant un modulo p^r quant à l'étude du caractère $C_{3-\epsilon}$ de $\mathbb{Q}_p$. En effet, maintenant établie, elle va servir à trouver des formes dont le seul zéro est le zéro trivial. On pose $q+1$ la partie entière de $\dfrac{d}{r}$ de sorte que $(q+1)r \geqslant d$ et :

$$G = (g + \ldots + g) + p^r \cdot (g + \ldots + g) + \ldots + p^{qr} \cdot (g + \ldots + g)$$

Dans chaque parenthèse, on somme $p^r - 1$ fois g, qu'on applique à chaque fois à de nouvelles variables. Le nombre de variables de G est alors $N = (q+1) \cdot (p^r - 1) \cdot n$, et son degré est toujours $d = (p-1)p^{r-1}$.

Proposition 9. Le seul zéro de G est le zéro trivial.

Démonstration. Soit x une racine de G. Par l'absurde, supposons qu'elle est non nulle, et par homogénéité du polynôme on peut la supposer primitive, c'est-à-dire non divisible par p, en divisant x par la plus grande puissance de p possible.

Comme $G(x) = 0$, on a en particulier $G(x) \equiv 0[p^r]$, ce qui veut dire que la somme des $p^r - 1$ premiers G est divisible par p^r. Or, chaque "g" vaut soit 0 soit 1 modulo p^r, et vaut 0 si et seulement si les coefficients de x auxquels il s'applique sont divisibles par p. Il vient que chacun de ces "g" s'annule

nécessairement impliquant ainsi que toutes les composantes de x associées sont divisibles par p.
Par récurrence finie pour k allant de 1 à q, on considère de même la congruence modulo p^{kr}. Ceci annule à chaque fois les "g" associées aux puissances inférieures de p puisque le fait que les composantes de x associées soient divisibles par p implique que $g(x)$ est divisible par p^d, avec $d > qr$ par hypothèse. On montre ainsi que les "g" suivants s'annulent eux aussi modulo p^r et donc que les composantes de x associées sont elles aussi divisibles par p.
Finalement, toutes les composantes de x sont divisibles par p et x l'est aussi. Or, cela contredit notre hypothèse, donc $x = 0$ et c'est la seule racine de la forme G. □

On déduit de cet exemple le théorème attendu :

Théorème 10. Soit $\epsilon > 0$, $\mathbb{Q}_p$ n'est pas $C_{3-\epsilon}$.

Démonstration. On utilise comme contre-exemple la forme G. On a : $d^3 = (p-1)^3 \cdot p^{3r-3}$. Prenant $\epsilon > 0$ on a aussi : $d^{3-\epsilon} = (p-1)^{3-\epsilon} \cdot p^{3(r-1)\epsilon}$. De plus, $q+1$ équivaut en l'infini à $\left[\frac{d}{r}\right] = \left[\frac{(p-1)p^{r-1}}{r}\right]$., et n à $\left[\frac{p^{r-1}}{2r}\right]$, d'où $N \sim \left[\frac{p^{3r-3}}{2r^2}\right] \cdot \left[\frac{p}{p-1}\right]$. On vérifie toujours que $N < d^3$; par ailleurs pour r tendant vers l'infini, on a : $\left[\frac{N}{d^{3-\epsilon}}\right] \sim \left[\frac{p \cdot p^{\epsilon r}}{(p-1)2r^2}\right]$ ce qui tend vers l'infini. On a donc pour r suffisamment grand, $N > d^{3-\epsilon}$, or G de degré d à N variables ne s'annule pas ; d'où $\mathbb{Q}_p$ n'est pas $C_{3-\epsilon}$. □

Ce résultat est de plus le meilleur que l'on puisse trouver par cette méthode, en effet :

Lemme 7. Soit $g \in \mathbb{Z}_p[X_1, \ldots, X_n]$ homogène telle que $n > (1 + p + \ldots + p^r)d$, alors il existe un x non divisible par p vérifiant : $f(x) \equiv 0[p^{r+1}]$.
Cela signifie donc qu'on ne peut pas trouver de forme valant 1 modulo p^{r+1} d'un si grand nombre de variables.

On admettra ce lemme puisqu'il découle de la construction par vecteurs de Witt de $\mathbb{Q}_p$, qui permet entre autres d'y calculer des additions et des multiplications, mais que nous avons choisi de ne pas étudier car elle est fastidieuse et peu utile ici.
Nous n'avons certes pas réussi à construire une forme valant 1 modulo p^r à nombre de variables maximal, mais pourtant cela suffit à établir notre théorème, et l'optimum n'est de toute façon pas suffisant pour s'attaquer à la propriété C_3.
Nous avons ainsi fait mentir l'intuition qui ferait penser que les corps $\mathbb{Q}_p$ sont C_2. On peut même prouver, ce qui sort du cadre de notre étude, que ces corps ne satisfont la propriété C_i pour aucun i. Ce résultat a été établi par les mathématiciens Alemu, Arkhipov et Karatsuba [13].

Théorème 11. [ALEMU, ARKHIPOV, KARATSUBA] (Admis)
Soit p premier et i un entier naturel. Le corps $\mathbb{Q}_p$ n'est pas C_i.

En outre, ceci finit d'appuyer que le raisonnement mené dans le cadre des formes quadratiques ne pourra pas être déroulé pour n'importe quel degré ! L'étude des formes quadratiques est très spécifique. Toutefois, le lien entre les corps $\mathbb{Q}_p$ et la propriété C_2 ne s'arrête absolument pas au degré 2.
En effet, un résultat important dont nous chercherons à comprendre la démonstration dans la prochaine section est le théorème d'Ax-Kochen qui, à défaut de pouvoir établir la propriété C_2, se contente d'énoncer que, fixant un degré d, seul un nombre fini de corps $\mathbb{Q}_p$ ne sont pas $C_2(d)$. Ce résultat permet de fixer l'idée que même les corps qui ne sont C_i pour aucun i gardent un lien étroit avec la théorie d'Artin et Lang. Il reste donc fructueux de les étudier par ce prisme !

Théorème 12. [AX-KOCHEN]
Soit $d \in \mathbb{N}^*$. Seul un nombre fini de corps $\mathbb{Q}_p$ ne sont pas $C_2(d)$.

3
LES CORPS $\mathbb{Q}_p$ ET LA PROPRIÉTÉ C_2 : LE THÉORÈME D'AX-KOCHEN

Intuitivement, on aurait pu penser, à tort, que pour p premier fixé, le corps $\mathbb{Q}_p$ vérifie la propriété C_2. En effet, ce corps possède beaucoup de similarités avec le corps des séries de Laurent formelles à coefficients dans $\mathbb{Z}/p\mathbb{Z}$: les deux sont des corps de valuation discrète complets, et ils partagent le même corps résiduel $\mathbb{Z}/p\mathbb{Z}$.
Ils ne sont pour autant pas isomorphes, et ne vérifient pas toutes les mêmes propriétés comme nous l'avons vu précédemment. Néanmoins, nous allons montrer via le principe d'Ax-Kochen, que les corps $\mathbb{Q}_p$ et $\mathbb{Z}/p\mathbb{Z}((T))$ sont en fait très proches du point de vue de la logique du premier ordre. Nous appliquerons ce principe très général au cas particulier de la propriété faiblement C_2 en degré d.
Pour ce faire, on peut d'abord se rappeler de la propriété 6 admise. On se rend compte que pour que $\mathbb{Q}_p$ soit isomorphe à $\mathbb{Z}/p\mathbb{Z}((T))$, il aurait juste manqué que ces deux corps soient de même caractéristique. Or, on va pouvoir "forcer le passage à la caractéristique 0" des $\mathbb{Z}/p\mathbb{Z}((T))$ en considérant le produit infini de ces corps, pris sur l'ensemble des nombres premiers. De la sorte, le produit des Q_p et celui des $\mathbb{Z}/p\mathbb{Z}((T))$ seront de même caractéristique, mais ce seront de simples anneaux et non plus des corps ! Une construction à partir de la notion d'ultrafiltre va permettre de contourner cette difficulté, puis d'établir une propriété d'équivalence au sens de la logique du premier ordre.

3.1 LOGIQUE DU PREMIER ORDRE ET THÉORIE DES CORPS VALUÉS HENSÉLIENS

Pour parvenir à prouver l'équivalence au sens de la logique du premier ordre, il nous faut d'abord définir cette logique, et introduire quelques notions et théorèmes en lien qui en découlent. L'objectif n'est pas ici de démontrer tout ce que nous allons énoncer, mais de rappeler les résultats qui nous seront utiles, et de les rendre accessibles à quelqu'un n'ayant pas étudié formellement cette branche des mathématiques.
Nous verrons aussi de quelle manière les corps valués henséliens (c'est-à-dire qui vérifient le lemme d'Hensel) peuvent être étudiés du point de vue de la logique du premier ordre.

3.1.1 • FORMALISME ÉLÉMENTAIRE DE LA LOGIQUE DU PREMIER ORDRE

Définition 6. Un langage $\mathscr{L}$ est la donnée de trois ensembles, à savoir :
(i) : un ensemble $\mathscr{C}$ de symboles représentant les constantes ;
(ii) : un ensemble $\mathscr{F}$ de symboles de fonctions, où chaque élément $f \in \mathscr{F}$ est associé à un entier n_f qui est son arité ;
(iii) : un ensemble $\mathscr{R}$ de symboles de relations, où chaque élément $R \in \mathscr{R}$ est associé à un entier n_R qui est son arité.

Définition 7. Soit un langage $\mathscr{L} = \mathscr{C} \cup \mathscr{F} \cup \mathscr{R}$. Une $\mathscr{L}$-structure $\mathscr{M}$ est la donnée de :
(i) : un ensemble M non vide, appelé domaine de la structure ;
(ii) : un élément $c^{\mathscr{M}}$ pour tout $c \in \mathscr{C}$;

(iii) : une fonction $f^{\mathscr{M}}$, de M^{n_f} dans M, pour tout $f \in \mathscr{F}$;
(iv) : une relation $R^{\mathscr{M}}$ sur M^{n_R} pour tout $R \in \mathscr{R}$.
Ces trois derniers éléments de la définition correspondent aux interprétations des symboles de constantes, de fonctions et de relations.

Exemple 3. Pour assimiler tout ce formalisme, on se propose l'exemple du langage $\mathscr{L} = \{0, 1\} \cup \{+, \cdot\} \cup \{=, <\}$. Le 0 et le 1 pourront s'interpréter par la suite dans des modèles, comme le neutre de l'addition et de la multiplication respectivement, et il est nécessaire de les introduire pour définir leurs propriétés.
A partir de ce langage, on peut définir une structure ayant pour domaine l'ensemble des entiers naturels $\mathbb{N}$. On y interprète les symboles 0 et 1 par les entiers qui nous sont familiers, et les fonctions binaires $+$ et $\cdot$, d'arité 2, ainsi que les relations de comparaison et d'égalité, par leur définition habituelle.

On a donc défini proprement ce que sont un langage et une structure. Il nous faut donc voir comment écrire proprement les formules logiques sur un langage, et comment les interpréter dans une structure. Pour cela, on se donne un ensemble $\mathscr{V}$ de symboles de variables qui prendront leurs valeurs dans le domaine ainsi que les symboles permis en logique du premier ordre : $\{\forall, \exists, =, \neg, \wedge, \vee, (,)\}$.
En fait, toutes les propositions que l'on pourra écrire en logique du premier ordre seront celles qui ne font pas appel à la notion d'ensembles. Autrement dit, on ne définit pas les ensembles en logique du premier ordre, et donc pas l'appartenance ni la relation d'inclusion. On pourra écrire toutes les formules logiques habituelles ne faisant pas appel au formalisme ensembliste. Lorsqu'on écrira $\forall v$ ou $\exists v$, où v est un symbole de variable, les v parcourus seront en fait ceux du domaine de la structure, ce qui évite d'avoir recours au symbole d'appartenance. On appelle toutes ces propositions des "formules" au premier ordre.
On appelle termes les éléments qu'on peut calculer dans le domaine de la structure : par exemple, sur $\mathbb{Z}$, il s'agit des sommes et produits de constantes (0 et 1 en général) et de variables.
Nous nous garderons de définir proprement la construction des formules et des termes, ainsi que leur interprétation, qui se font de manière inductive selon les règles logiques qui sont familières au lecteur.
Dans les formules, on peut distinguer deux types de variables : les variables liées, qui sont précédées d'un quantificateur "pour tout" ou "il existe", et les autres variables, dites libres. La variable liée est en fait ce qu'on appelle plus communément une variable muette, dont on peut remplacer le nom par n'importe quel autre nom de variable. Une formule définie uniquement à partir de variables liées est dite close, on s'intéressera essentiellement à de telles formules. La valeur de vérité des autres formules dépend de la valeur qu'on assigne aux variables libres.

Exemple 4. La formule $(\forall x \exists y, y = x) \wedge (\exists x \exists y R(x, y))$ est une formule close du premier ordre. Les variables x et y sont en effet liées.
La formule $x = y$ est bien une formule du premier ordre, mais elle n'est pas close car x et y sont libres. La valeur de vérité dépend de la valeur qu'on donne à ces deux variables : sur le domaine $\mathbb{Z}$, si on prend $x = y = 2$, la formule est vraie, mais pour $x = 2$ et $y = 3$ elle est fausse.
En revanche, $\forall x \in \mathbb{N}, \exists y \in \mathbb{N}, y > x$ ne relève pas de la logique du premier ordre, puisqu'elle fait appel à la construction des ensembles.

Définition 8. Soit ϕ une formule close. On dit que la formule ϕ est satisfaite dans la $\mathscr{L}$-structure $\mathscr{M}$ si elle s'interprète par "vrai". On note dans ce cas $\mathscr{M} \vDash \phi$.
De plus, on note $\phi(v_1, \ldots, v_n)$ une formule dépendant des variables libres $v_1, \ldots, v_n$. Soient $a_1, \ldots, a_n$

des éléments du domaine M, qui sont les interprétations des variables $v_1, \dots, v_n$. On dit que $\mathscr{M} \vDash \phi(a_1, \dots, a_n)$ si ϕ est vraie en les éléments $a_1, \dots, a_n$.
L'interprétation rigoureuse des formules se définit par induction sur les formules, suivant les règles logiques usuelles. Pour mener une telle induction structurelle, prenant des formules ϕ et ψ, on peut définir inductivement les formules $\phi \wedge \psi$, $\phi \vee \psi$ et $\neg\phi$. En outre pour une formule $\phi(v)$ en une variable, on peut construire $\forall x, \phi(x)$ et $\exists x, \phi(x)$. Tous ces cas définissent les règles d'induction de l'ensemble des formules.

Exemple 5. La formule $\forall x \exists y, y > x$, sera bien satisfaite si on travaille sur le domaine $\mathbb{N}$ dans le langage défini plus tôt.

Voyons maintenant comment on peut établir un ensemble d'axiomes, ou une théorie, ce qui permettra de définir ce qu'est un corps du point de vue de la logique du premier ordre.

Définition 9. Soit un langage $\mathscr{L}$. Une $\mathscr{L}$-théorie, notée $\mathscr{T}$, est un ensemble de formules closes. Une $\mathscr{L}$-structure $\mathscr{M}$ est un modèle de cette théorie si et seulement si pour toute formule ϕ de $\mathscr{T}$, on a $\mathscr{M} \vDash \phi$.
On appelle généralement les formules closes constituant une théorie, les axiomes de cette théorie.

Ce formalisme nous permet de définir ce qu'est un corps au sens de la logique du premier ordre. Ainsi, cette théorie nous permettra d'étudier les corps $\mathbb{Q}_p$.
Pour cela, introduisons le langage $\mathscr{L}_F$ ("F" pour "fields"), qui nous sert à définir les axiomes des corps : $\mathscr{L}_F = \{+, \cdot, 0, 1, =\}$.

Définition 10. Un corps est un modèle de la $\mathscr{L}_F$-théorie constituée des axiomes suivants :
(1) $\forall x \forall y \forall z, x + (y + z) = (x + y) + z$
(2)$\forall x \forall y, x + y = y + x$
(3) $\forall x, x + 0 = x$
(4) $\forall x \exists y, x + y = 0$
(5) $\forall x \forall y \forall z, x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
(6) $\forall x \forall y \forall z, x \cdot (y \cdot z) = (x \cdot y) \cdot z$
(7) $\forall x \forall y, x \cdot y = y \cdot x$
(8) $\forall x, x \cdot 1 = x$
(9) $\forall x \exists y, (x = 0 \vee x \cdot y = 1)$
(10) $\neg(1 = 0)$
En particulier, tous les corps vus précédemment dans ce rapport vérifient ces axiomes.

En outre, la caractéristique, dont nous avons déjà évoqué le rôle primordial pour la preuve du théorème d'Ax-Kochen, peut elle aussi être définie à partir de la logique du premier ordre. On pourra donc bien la manipuler dans nos prochains raisonnements.

Définition 11. Soit p un nombre premier. On définit la formule associée à la propriété de caractéristique p, que l'on note $Char(p)$:

$$Char(p) : 1 + ... + 1 = 0$$

où il y a p fois le terme 1 dans l'addition.
Un corps est de caractéristique p si et seulement si il satisfait cette propriété.
De plus, on peut définir la caractéristique 0 par une quantité dénombrable de formules, en considérant pour chaque p premier, la formule $\neg Char(p)$.

3.1.2 • LA CLASSE DES CORPS VALUÉS HENSÉLIENS

En revanche, on est plus en peine pour écrire sous forme de formules au premier ordre, les propriétés d'une valuation sur un corps. En effet, la valuation est à valeur dans $\mathbb{Z}$, or, le seul corps de travail dont nous disposons est celui fourni par le domaine. Ainsi, si on travaille sur le domaine $\mathbb{Q}_p$, on ne peut pas définir directement les axiomes propres à la valuation puisque cela nécessiterait d'introduire $\mathbb{Z}$ et donc de faire appel à la logique ensembliste. Une astuce va pourtant nous permettre de nous sortir de cette ornière.
L'idée principale est d'associer, à chaque entier n dans l'image de la valuation, un élément du corps étudié étant de valuation n. De cette façon, on aura pas besoin d'introduire l'ensemble des entiers relatifs puisque la valuation pourra être décrite à partir de notre domaine même.
On travaillera ici avec des corps valués dont la valuation n'est pas nécessairement discrète, donc pas forcément à valeur dans $\mathbb{Z}$. Ce cadre général nous sera utile ultérieurement pour construire les ultraproduits.

Définition 12. On dit qu'un corps valué F, de valuation ν, est un corps valué avec cross section, si et seulement si il existe une application injective $i : \nu(F) \to F$, telle que i est un morphisme de groupes de $\nu(F^*)$ dans F^* et vérifiant : $\forall x \in \nu(F), \nu(i(x)) = x$.

On se rend compte facilement que tous les corps de valuation discrète, et en particulier $\mathbb{Q}_p$ et $\mathbb{Z}/p\mathbb{Z}((T))$, vérifient cette propriété. En effet, reprenant la notation antérieure de π pour désigner une uniformisante, on peut poser i telle que :

$$\forall n \in \mathbb{Z}, i(n) = \pi^n; i(\infty) = 0$$

Cette application est bien un morphisme de groupes de $(\mathbb{Z}, +)$ dans $(F, \cdot)$ où F est le corps d'étude.
A partir de maintenant, on se permettra de noter abusivement :

$$\nu(x) = i(\nu(x))$$

Pour un corps valué F, la valuation est dorénavant une application de F dans F, et elle est donc à valeur dans notre domaine, ce qui permet de l'étudier du point de vue de la logique du premier ordre. Dans toute la suite de la construction du principe d'Ax-Kochen, la valuation renverra à cette redéfinition à valeur dans le corps valué.
De plus, l'image de la valuation ainsi formé $\nu(F^*)$ est bien un groupe car i est un morphisme de groupes ; ce faisant, on va pouvoir ordonner ce groupe selon le même ordre que l'ancien groupe de valuation qui lui est isomorphe. Toutes les propriétés d'une valuation seront conservées.
Pour ajouter ces axiomes à la théorie définissant les corps, il nous faut étendre notre langage : on construit une fois pour toutes $(L)_{VF} = (L)_F \cup \{\leq, \nu, V\}$ le langage des corps valués. V est une relation unaire, qui s'interprète par vrai en l'élément x si et seulement x est un élément du groupe de valuation.

Définition 13. Un corps valué avec cross section est le modèle de la $\mathscr{L}_{VF}$-théorie constituée des axiomes suivants :
(1) les axiomes des corps introduits en définition 10
(2) les axiomes définissant les propriétés de la valuation :
(i) $\forall v_1 (v_1 = 0 \leftrightarrow \nu(v_1) = 0)$
(ii) $\forall v_1 \forall v_2, \nu(v_1 \cdot v_2) = \nu(v_1) \cdot \nu(v_2)$
(iii) $\forall v_1 \forall v_2, \nu(v_1) \leqslant \nu(v_2) \to \nu(v_1) \leqslant \nu(v_1 + v_2)$

(3) le groupe de valuation est un groupe multiplicatif :
(i) $\forall v_1 \forall v_2, V(v_1) \wedge V(v_2) \to V(v_1 \cdot v_2)$
(ii) $\forall v_1, V(v_1) \to (\exists v_2, V(v_2) \wedge v_1 \cdot v_2 = 1)$
(4) les quatre axiomes définissant la relation d'ordre totale sur le groupe de valuation :
(i) $\forall v_1 \forall v_2, (V(v_1) \wedge V(v_2)) \to ((v_1 \leqslant v_2) \vee (v_2 \leqslant v_1))$
(ii) $\forall v_1 \forall v_2, (V(v_1) \wedge V(v_2) \wedge (v_1 \leqslant v_2) \wedge (v_2 \leqslant v_1)) \to v_1 = v_2$
(iii) $\forall v_1 \forall v_2 \forall v_3, (V(v_1) \wedge V(v_2) \wedge V(v_3) \wedge (v_1 \leqslant v_2) \wedge (v_2 \leqslant v_3)) \to (v_1 \leqslant v_3)$
(iv) $\forall v_1 \forall v_2 \forall v_3, (V(v_1) \wedge V(v_2) \wedge V(v_3) \wedge (v_1 \leqslant v_2)) \to (v_1 \cdot v_3 \leqslant v_2 \cdot v_3)$
(5) les axiomes de cross section :
(i) $\forall v_1, V(\nu(v_1))$
(ii) $\forall v_1, V(v_1) \to (\nu(v_1) = v_1)$

Maintenant qu'on a défini ce qu'est un corps valué, il faut ajouter le caractère hensélien. Celui-ci permet en fait de rendre compte d'une conséquence de la complétude, d'une manière compatible avec la logique du premier ordre.
On considèrera ici la version suivante du lemme d'Hensel, qui correspond à celle vue en section 2.2, mais cette fois sans spécifier de la suite convergeant vers le zéro :

Proposition 10. Soit F un corps valué avec cross section. On introduit son anneau d'entiers $R = \{x \in F / \nu(x) \geqslant 1\}$ (cela désigne, pour $\mathbb{Q}_p$, l'anneau d'entiers $\mathbb{Z}_p$). Le corps F est dit hensélien si et seulement si il satisfait la propriété suivante :
Pour tout polynôme f à coefficients dans R tel qu'il existe a dans R vérifiant $f'(a) \neq 0$ et, du point de vue du groupe valué :

$$\nu(\frac{f(a)}{f'(a)^2}) > 1$$

Alors il existe $b \in R$ tel que $f(b) = 0$ et $\nu(b) = \nu(a)$.

Cette propriété peut se formaliser en termes de formules au premier ordre, notamment car les polynômes peuvent être considérés uniquement à partir de leurs coefficients, et parce qu'on peut calculer des valeurs de ces polynômes sans mal. Tout le travail nécessaire a aussi été abattu vis-à-vis de la valuation.

Proposition 11. On peut retranscrire le lemme d'Hensel sur un corps valué avec cross section F en termes d'axiomes de la logique du premier ordre.

Démonstration. Fixons n un entier naturel, et considérons les polynômes sur R de degré n. Un polynôme f correspond bijectivement au $(n+1)$-uplet $(a_0, \cdots, a_n)$ de ses coefficients, avec a_n non nul.
On cherche à écrire un axiome H_n correspondant au lemme d'Hensel restreint aux polynômes de degré n. De la sorte, on pourra introduire exactement le bon nombre, fini, de coefficients espérés.
On peut dorénavant écrire le lemme d'Hensel en degré n :

$$H_n : \forall a_0 \cdots \forall a_n \forall d, [(\nu(a_0)) \geqslant 1 \wedge \cdots \wedge (\nu(a_n) \geqslant 1) \wedge \neg(a_n = 0) \wedge \neg(f'(a) = 0) \wedge (d \cdot f'(a) = 1) \wedge (\nu(a \cdot d \cdot d) > 1)]$$

$$\to [\exists b, (f(b) = 0 \wedge \nu(b) = \nu(a))]$$

Cette formule est bien une formule close au premier ordre, et traduit la propriété que l'on veut exprimer. En effet, l'introduction des variables muettes $a_0, \cdots, a_n$ peut bien s'écrire formellement pour

le n donné, en se passant des points de suspension, car elle est de longueur finie. La notation "d" introduite permet de désigner l'inverse de $f'(a)$, ce qu'on vérifie en exigeant que le produit des deux vale 1.
Les inégalités de valuation correspondent aux conditions pour que les coefficients du polynôme soient bien dans l'anneau d'entiers R : il est donc bien possible de se restreindre aux polynômes à coefficients dans R.
Il reste une subtilité à éluder : le calcul des valeurs de f et f', qui n'est pas explicité par souci de concision dans la formule H_n, peut se faire par calclul de termes du premier ordre. En effet, on a :

$$f(a) = a_0 + a_1 \cdot a + ... + a_n \cdot a \cdot ... \cdot a$$

Où "a" est multiplié k fois par lui-même dans le monôme de degré k. On peut analoguement écrire $f'(a)$ car on connaît l'expression sous forme de polynôme de f', en fonction des coefficients introduits.
Un corps valué avec cross section est alors hensélien si et seulement si il satisfait H_n pour tout entier naturel n. Ce faisant, il suffit de rajouter tous les axiomes H_n à la $\mathscr{L}_{VF}$-théorie des corps valués avec cross section construite précédemment. Ceci conclut la démonstration. □

On va rajouter un élément de vocabulaire précis pour désigner des structures "axiomatisables".

Définition 14. Une classe $\mathscr{K}$ de $\mathscr{L}$-structures est dite élémentaire, si et seulement si il existe une $\mathscr{L}$-théorie $\mathscr{T}$ dont les modèles sont exactement les structures contenues dans $\mathscr{K}$. Dans ce cas, $\mathscr{T}$ est appelé l'ensemble des axiomes de $\mathscr{K}$.

Ainsi, on a prouvé que la classe des $\mathscr{L}_{VF}$-structures ayant pour domaines les corps valués henséliens avec cross section, est élémentaire, et l'ensemble de ses axiomes correspond à ceux définis pour les corps valués avec cross section ainsi que ceux construits pour vérifier le lemme d'Hensel.

3.1.3 • QUELQUES THÉORÈMES DE LA LOGIQUE DU PREMIER ORDRE

On va maintenant énoncer, principalement sans démonstration, les théorèmes découlant de la logique du premier ordre, qui nous seront utiles pour la suite de la démonstration.

En premier lieu, nous avons évoqué le fait que nous voulions établir une équivalence entre deux structures au sens de la logique du premier ordre. Il nous faut formaliser ce que cela signifie.

Définition 15. Soit une $\mathscr{L}$-structure $\mathscr{M}$. On appelle $\mathscr{M}$-théorie complète, et on note $Th(\mathscr{M})$, l'ensemble des formules satisfaites dans $\mathscr{M}$. Formellement, on peut écrire $Th(\mathscr{M}) = \{\phi | \mathscr{M} \vDash \phi\}$. On dit que cette théorie est complète car pour toute formule logique ϕ, ϕ ou $\neg\phi$ est satisfaite, et donc l'une ou l'autre est dans $Th(\mathscr{M})$.
Soient maintenant deux $\mathscr{L}$-structures, $\mathscr{M}$ et $\mathscr{N}$. On dit que $\mathscr{M}$ et $\mathscr{N}$ sont équivalents au sens de la logique du première ordre, et on note $\mathscr{M} \equiv \mathscr{N}$, si et seulement si $Th(\mathscr{M}) = Th(\mathscr{N})$. Cette équivalence signifie que dans ces deux structures, les exacts mêmes énoncés au premier ordre sont vérifiés.

Pour démontrer l'équivalence logique entre deux structures, nous bénéficions d'un outil assez puissant : en effet, l'existence d'un isomorphisme entre deux structures garantit cette propriété. Définissons d'abord ce qu'est un isomorphisme entre des structures.

Définition 16. Soient $\mathscr{M}$ et $\mathscr{N}$ deux $\mathscr{L}$-structures de domaines respectifs M et N. On dit que le morphisme $j : M \to N$ est un $\mathscr{L}$-morphisme élémentaire si et seulement si pour tous symboles

de variables $v_1, \ldots, v_n$ et toute formule $\phi(v_1, \ldots, v_n)$, on a $\mathscr{M} \vDash \phi(a_1, \ldots, a_n)$ si et seulement si $\mathscr{N} \vDash \phi(j(a_1), \ldots, j(a_n))$.
Si un tel morphisme est bijectif, on pourra naturellement le qualifier d'isomorphisme élémentaire. On note dans ce cas $\mathscr{M} \cong \mathscr{N}$

Ce faisant, on a l'intuition par cette définition que, si un isomorphisme élémentaire entre $\mathscr{M}$ et $\mathscr{N}$ existe, on peut associer à chaque élément de M un unique élément de N qui se comporte de la même façon que lui.
Pour les formules closes notamment, les mêmes formules logiques au premier ordre devraient être satisfaites grâce à cette bijection. Et c'est effectivement ce qu'il se passe.
Pour pouvoir démontrer très rigoureusement le théorème suivant, on notera qu'il est utile d'adjoindre au langage $\mathscr{L}$ de la structure $\mathscr{M}$, un symbole de constante pour chaque élément du domaine M, qui s'interprète naturellement par l'élément du domaine associé. Le nouveau langage $\mathscr{L}_M$ a pour avantage de permettre de traiter les formules contenant des variables libres, comme des formules closes en chaques n-uplet de constantes du domaine possible, et donc de les inclure dans la théorie complète de $\mathscr{M}$. De la sorte, si on considère $\mathscr{N}$ isomorphe à $\mathscr{M}$ par le morphisme j, on peut prendre le même symbole de constante pour désigner $c \in M$ et $j(c)$ son élément dans N associé, de sorte que les mêmes formules seront satisfaites sous le même langage $\mathscr{L}_M$.

Proposition 12. Soient $\mathscr{M}$ et $\mathscr{N}$ deux $\mathscr{L}$-structures. Si $\mathscr{M} \cong \mathscr{N}$, alors $\mathscr{M} \equiv \mathscr{N}$

Démonstration. Cela se démontre par induction sur les formules au premier ordre. Nous nous proposons de montrer brièvement, et en sautant quelques détails techniques, pourquoi la propriété s'itère bien grâce au bon choix de définition pour un isomorphisme élémentaire (le cas de base est laborieux et nous avons choisi d'omettre de le définir proprement par souci de concision).
Soient deux formules closes ϕ, ψ ayant la même valeur de vérité dans les deux structures. Il en est de même pour les formules induites $\psi \wedge \phi$, $\neg\phi$ et $\psi \vee \phi$ de manière évidente.
Supposons que c'est vrai aussi pour On peut aussi considérer les formules de la forme $\exists x, \phi(x)$ et $\forall x, \phi(x)$, pour un ϕ dépendant d'une variable. On a : $\mathscr{M} \vDash \exists x, \phi(x)$
Si et seulement si il existe a_1 dans $\mathscr{M}$ tel que $\mathscr{M} \vDash \phi(a_1)$
Si et seulement si $\mathscr{N} \vDash \phi(j(a_1))$, par définition du morphisme élémentaire
Si et seulement si il existe b_1 dans $\mathscr{M}$ tel que $\mathscr{M} \vDash \phi(b_1)$, la réciproque étant vraie car j est bijectif
Si et seulement si $\mathscr{N} \vDash \exists x, \phi(x)$.

Pour la propriété $\forall x, \phi(x)$, le schéma de démonstration est le même. La propriété est vraie par induction, toutes les formules au premier ordre ont la même valeur de vérité sur les deux structures. Ainsi, $Th(\mathscr{M}) = Th(\mathscr{N})$, et on a l'équivalence logique. □

Ce résultat nous sera très utile pour démontrer l'équivalence logique escomptée.
Il nous manque maintenant quelques résultats à énoncer sur ce qu'on appelle des modèles saturés. Ceux-ci vont nous permettre de mettre en oeuvre, dans la démonstration finale de l'équivalence logique au premier ordre, un raisonnement dit de "va-et-vient". Commençons par introduire un nouvel objet, les types.

Définition 17. Soit $A \subseteq M$, où M est le domaine de la $\mathscr{L}$-structure $\mathscr{M}$. Comme évoqué précédemment, on peut associer à chaque élément $a \in A$ un symbole de constante c_a. Posant le langage $\mathscr{L}_A = \mathscr{L} \cup \{c_a | a \in A\}$, on va considérer A les formules closes sur le langage $\mathscr{L}_A$. Autrement dit, ce sont toutes les formules sur $\mathscr{L}$ de la forme $\phi(a_1, \ldots, a_n)$, avec $a_1, \ldots, a_n$ des éléments de A.

On note alors $Th_A(\mathscr{M})$ la théorie complète sur ce nouveau langage. Autrement dit, cet ensemble contient les formules satisfaites faisant uniquement référence à des éléments de A explicitement.

Ce procédé généralise ce que nous évoquions plus tôt quant à l'adjonction de nouveaux symboles de constantes pour chaque élément du domaine. Partant de ces formules closes sur le nouveau langage $\mathscr{L}_A$, il nous reste à définir ce qu'est un type.

Définition 18. Un ensemble S de $\mathscr{L}$-formules est dit satisfiable s'il existe une structure $\mathscr{M}$ et des éléments $a_1, \dots, a_n$ de son domaine M tels que pour tout $\phi \in S$, $\mathscr{M} \vDash \phi(a_1, ..., a_n)$. Cela signifie qu'on peut avoir toutes ces formules conjointement vraies pour un modèle et pour une même interprétation des symboles de variables.
Soit alors $A \subseteq M$ et $\mathscr{L}_A$ le langage associé, construit à la définition précédente. Un n-type sur A est un ensemble P de formules sur $\mathscr{L}_A$ en les variables $v_1, \dots, v_n$ tel que $Th_A(\mathscr{M}) \cup P$ est satisfiable. Autrement dit, il existe une interprétation des variables $v_1, \dots, v_n$ telle que les formules de P sont satisfaites dans un certain modèle $\mathscr{N}$ vérifiant les propriétés de $\mathscr{M}$ à variables dans A, $Th_A(\mathscr{M})$.
L'ensemble P est dit complet si pour toute formule ϕ sur $\mathscr{L}_A$ à variables libres $v_1, \dots, v_n$, ϕ est dans P ou $\neg\phi$ est dans P.

Les types correspondent en fait à toutes les relations que l'on peut faire avec les éléments de A. Si la seule relation dont on dispose dans notre ensemble est la relation d'ordre notée $>$, alors les types sont les relations avec les termes construits sur les éléments de A.
Profitons d'avoir introduit la notion de satisfiabilité des formules logiques pour faire un détour par un théorème fondamental de la logique du premier ordre, dont nous aurons besoin plus tard : le théorème de compacité.

Théorème 13. [THÉORÈME DE COMPACITÉ]
Un ensemble S de $\mathscr{L}$-formules si et seulement si tout sous-ensemble fini de formules de S est satisfiable.

La puissance de ce théorème réside en ce qu'il suffit, pour prouver qu'une théorie possède un modèle, que tout sous-ensemble fini de ses formules en possède un : c'est pourtant loin d'être évident au premier abord. Cela permet, par exemple, d'affirmer qu'il existe un modèle de $Th(\mathbb{R})$ dont le domaine possède un majorant, en utilisant que tout ensemble fini de réels en admet un. Il n'est même pas nécessaire d'exhiber un tel modèle pour s'en assurer !

Nous avons maintenant besoin d'introduire un peu de théorie de la cardinalité pour comprendre ce qui suit. Rappelons qu'un ensemble A est dit de cardinal $\aleph_0$ si et seulement si il est dénombrable, c'est-à-dire en bijection avec l'ensemble des entiers naturels $\mathbb{N}$ par une application f : cela signifie que A est "de la même taille" que $\mathbb{N}$ et qu'on peut indexer ses éléments par les entiers. En outre, $\aleph_1$ est le cardinal des ensembles en bijection avec $\mathbb{R}$. Par l'hypothèse du continu, l'infini immédiatement plus grand que $\mathbb{N}$ est celui de $\mathbb{R}$, soit $\aleph_1$.

Définition 19. Soit $\mathscr{T}$ une théorie complète et $\mathscr{M}$ une $\mathscr{L}$-structure. Soit κ un cardinal éventuellement infini. On dit que $\mathscr{M}$ est κ-saturé si pour tout $A \subseteq M$ de cardinal strictement plus petit que κ, $|A| < \kappa$, tout type sur A est réalisé dans $\mathscr{M}$.
De plus, si $\mathscr{M}$ est $|M|$-saturé (on peut montrer que faire plus grand est impossible), alors on dit simplement que $\mathscr{M}$ est saturé.

Cette définition peut paraître obscure, mais prenons un exemple. Plaçons-nous sur $\mathbb{Q}$, qui est de cardinal $\aleph_0$ car dénombrable, et munissons-nous de la relation de comparaison usuelle $<$.

Considérons un ensemble d'éléments de $\mathbb{Q}$ $a_1, \ldots, a_n$ de cardinal $n < \aleph_0$, alors intuitivement, on sait qu'on peut toujours intercaler un rationnel où on le souhaite parmi ces éléments. Ainsi pourvu de prendre un type, c'est-à-dire des formules satisfiables, ce type sera réalisé par un élément de $\mathbb{Q}$: par exemple, $v_1 < a_1, \ldots, v_1 < a_n$ est un 1-type qui est ici bien réalisé en prenant $v_1 = min(a_1, \ldots, a_n) - 1$. On peut donc dire que $\mathbb{Q}$ muni de $<$ est saturé : de tels objets existent.
Prenant un ensemble de cardinal $\aleph_0$ dans $\mathbb{Q}$, par exemple $\mathbb{N}$ lui-même, le 1-type : pour tout entier n, $(n < v_1)$, n'est pas réalisé, car $\mathbb{N}$ ne possède pas de majorant. Ceci corrobore ce qui a été précisé dans la définition : il faut que le cardinal de l'ensemble considéré soit strictement plus petit que celui du domaine. Pour autant, on peut trouver un domaine plus grand pour lequel ce type est satisfait : c'est le théorème de compacité qui permettrait facilement de s'en assurer (le lecteur curieux pourra se reporter à des cours de logique du premier ordre pour le comprendre). Généralement, il est possible de rendre les types réalisables dans un certain modèle, en construisant un autre modèle plus grand. Cela permet d'aboutir à un modèle saturé.
Les modèles saturés ont un intérêt énorme pour la construction d'isomorphismes. Voici les théorèmes principaux de logique du premier ordre sur de tels objets.

Théorème 14. [ISOMORPHISME ENTRE MODÈLES SATURÉS]
Soient $\mathscr{M}$ et $\mathscr{N}$ deux modèles saturés d'une théorie complète $\mathscr{T}$, dont les domaines sont de même cardinal κ. Alors $\mathscr{M} \cong \mathscr{N}$.

C'est là la première mise en évidence d'isomorphisme entre deux structures. On peut essayer de comprendre l'idée sous-jacente à la preuve de ce théorème en étudiant le modèle saturé de cardinal dénombrable, $\mathbb{Q}$, pour la théorie définissant les axiomes usuels de la relation d'ordre totale $<$.
On considère un autre modèle saturé dénombrable $\mathscr{M}$ possédant lui aussi une relation d'ordre totale. M étant dénombrable, on peut indexer ses éléments par les entiers : $a_1, \ldots, a_n, \ldots$. On prend dans son domaine, une suite croissante de sous-ensembles, $A_1 \subset \ldots \subset A_n \subset \ldots$ tel que chaque A_i contient les éléments $a_1, \ldots, a_i$.
On associe à a_1 n'importe quel rationnel, par exemple 1, par la fonction f_1 : c'est notre initialisation.. De plus récursivement, on peut construire un morphisme f_n de A_n dans $\mathbb{Q}$ injectif, conservant la relation d'ordre et donc étant bien un isomorphisme au sens des structures. On veut de plus que f_n restreint à A_{n-1} vaille f_{n-1}, c'est une suite d'applications "compatible". Pour montrer cela, procédons par récurrence, soit n un entier et supposons que f_n soit construite. a_{n+1} peut être placé quelque part entre les $a_1, \ldots, a_n$, par la relation d'ordre. Ceci donne par exemple deux comparaisons à vérifier, $a_i < a_{n+1}$ et $a_j > a_{n+1}$ pour deux i et j. De plus, le fait que $\mathbb{Q}$ est saturé implique que le 1-type $(f(a_i) < v, f(a_j) > v)$ sur la variable v, est saturé. Par conséquent, on peut trouver un rationnel $b = f(a_{n+1})$ intercalé entre $f(a_i)$ et $f(a_j)$. La même chose serait faisable si a_{n+1} constituait un majorant ou minorant de A_n. C'est ici qu'interviendrait l'hypothèse de saturation dans la preuve générale du théorème.
On construit donc $f = \cup_{n \in \mathbb{N}} f_n$, qui est bien définie à valeur dans M par l'énumération de M. C'est par construction une injection. L'égalité des cardinaux implique que c'est une bijection. Ceci finit de prouver le théorème dans un cas simplifié, sur des domaines dénombrables.

En outre, comme il est possible de prendre un modèle et de le "saturer", on va pouvoir établir des isomorphismes partant de modèles non saturés. Nous nous contenterons d'énoncer le résultat suivant qui est un corollaire du théorème célèbre de logique du premier ordre établi par Löwenheim et Skolem.

Théorème 15. [LÖWENHEIM-SKOLEM POUR LES MODÈLES SATURÉS]

Soit $\mathscr{L}$ un langage dénombrable, $\mathscr{M}$ une $\mathscr{L}$-structure infinie de domaine M. Alors il existe un modèle saturé de $Th(\mathscr{M})$ de cardinal $\aleph_1$ (considérant que l'hypothèse du continu est vérifiée).

En particulier, l'hypothèse de langage dénombrable s'applique bien sûr au langage $\mathscr{L}_{VF}$ des corps valués henséliens avec cross section, construit plut tôt. Ce théorème va nous permettre de construire des modèles saturés de cardinalité contrôlée et donc isomorphes par le théorème d'isomorphisme sur les modèles saturés. C'est là la clé du raisonnement par va-et-vient.
Il reste à savoir sur quels objets nous pouvons appliquer ces théorèmes : c'est l'objet de la prochaine section.

3.2 ULTRAFILTRES ET PRODUIT INFINI DE CORPS VALUÉS HENSÉLIENS

Dans cette partie, nous allons voir en quelle mesure quotienter par une relation d'équivalence un produit dénombrable de corps valués henséliens, permet de conserver une structure de corps pour l'anneau-produit. Les ultrafiltres constituent l'objet approprié pour établir la relation d'équivalence espérée.

3.2.1 • FILTRES ET ULTRAFILTRES

Définition 20. [FILTRES] Soit I un ensemble non vide. Un filtre $\mathscr{D} \subseteq P(P(I))$ est un ensemble de parties de I tel que, pour toutes parties A et B de I :
(1) $\emptyset \notin D$ et $I \in D$
(2) Stabilité par intersection finie : si $A \in \mathscr{D}$ et $B \in \mathscr{D}$, alors $A \cap B \in \mathscr{D}$
(3) Si $A \in \mathscr{D}$ et $A \subseteq B \subseteq I$, alors $B \in \mathscr{D}$

Exemple 6. (1) On appellera filtre trivial le filtre $\mathscr{D}_T = \{I\}$.
(2) Soit $j \in I$, $\mathscr{D}_j = \{X \subseteq I / j \in X\}$ est un filtre, dit filtre principal engendré par j. En effet, il contient I car j est dans I, mais pas l'ensemble vide. De plus, une intersection de deux ensembles contenant j, contient toujours j, ce qui donne la stabilité par intersection. Enfin, si $A \in \mathscr{X}$, il contient j, donc toute partie plus grande que A au sens de l'inclusion contient aussi j, ce qui conclut la démonstration. (3) On appelle filtre de Frechet, $\mathscr{D}_F = \{X \subseteq I /$ le complémentaire de X dans I est fini$\}$. Il s'agit d'un filtre uniquement lorsque I est infini.

Intuitivement, un filtre contiendra essentiellement les parties constituées de beaucoup d'éléments de I : le filtre de Frechet fait d'ailleurs apparaître, lorsque I est infini, la notion de "tout, sauf une partie finie" intrinsèque au théorème d'Ax-Kochen.
Nous avons besoin maintenant de filtres particuliers, appelés ultrafiltres.

Définition 21. Soit $\mathscr{D}$ un filtre sur I, $\mathscr{D}$ est un ultrafiltre si et seulement si, pour tout $X \subseteq I$, soit X est un élément du filtre, soit son complémentaire dans I est un élément du filtre.
En particulier, les filtres principaux (engendrés par un élément $j \in I$) sont des ultrafiltres.

Le filtre de Frechet sera en effet crucial pour aboutir au principe d'Ax-Kochen. Il nous faut d'abord démontrer deux lemmes avant d'exhiber son lien avec les ultrafiltres.

Lemme 8. Soit $\mathscr{D}$ un filtre sur I, et $X \subseteq I$ non vide qui n'est pas dans $\mathscr{D}$. Alors il existe un filtre $\mathscr{D}_X$ tel que $\mathscr{D} \subseteq \mathscr{D}_X$ et $I \backslash X \in \mathscr{D}_X$

Démonstration. Posons $\mathscr{D}_X = \{Y \subseteq I / \exists Z \in \mathscr{D}, Z\backslash X \subseteq Y\}$.
Remarquons déjà qu'il contient $I\backslash X$, il suffit en effet de prendre $Z = I$ qui est bien dans $\mathscr{D}$. On a en outre $\mathscr{D} \subseteq \mathscr{D}_X$, puisque soit Y un élément de $\mathscr{D}$, pour $Z = Y$ on a bien $Z\backslash X = Y\backslash Y \subseteq X$
Montrons maintenant qu'il s'agit d'un filtre :
(1) $\emptyset \notin \mathscr{D}_X$. Par l'absurde, s'il en faisait partie, on aurait $Z \in \mathscr{D}$ tel que $Z\backslash X \subseteq \emptyset$, donc $Z \subseteq X$ et $Z \cap (I\backslash X) = \emptyset \in \mathscr{D}$ par stabilité par l'intersection de $\mathscr{D}$; or c'est impossible car $\mathscr{D}$ est un filtre. En outre, $I \in \mathscr{D}$ en testant pour $Z = I$. (2) Soit A et B deux éléments de $\mathscr{D}_X$. Il existe Z_A et Z_B dans $\mathscr{D}$ tels que $Z_A\backslash X \subseteq A$ et $Z_B\backslash X \subseteq B$. Posons $Z = Z_A \cap Z_B \in \mathscr{D}$ (par intersection), alors $Z\backslash X = (Z_A\backslash X) \cap (Z_B\backslash X) \subseteq A \cap B$. Donc $A \cap B$ est dans $\mathscr{D}_X$, d'où la stabilité par intersection.
(3) Soit $A \in \mathscr{D}_{\mathscr{X}}$ et B tel que $A \subseteq B \subseteq I$. Il existe $Z_A \in \mathscr{D}$ tel que $Z_A\backslash X \subseteq A$, par conséquent $Z_A\backslash X \subseteq B$ d'où $B \in \mathscr{D}_X$.
Ceci prouve que $\mathscr{D}_X$ est un filtre ayant les propriétés voulues. □

Lemme 9. Pour tout filtre $\mathscr{D}$ sur I, il existe un ultrafiltre $\mathscr{U}$ tel que $\mathscr{D} \subseteq \mathscr{U}$.

Démonstration. On considère $\mathscr{F}$ l'ensemble des filtres contenant $\mathscr{D}$, et on l'ordonne par inclusion. On veut montrer que $\mathscr{F}$ est inductif, c'est-à-dire que toute chaîne totalement ordonnée pour l'inclusion possède un majorant dans $\mathscr{F}$. Soit une chaîne non vide totalement ordonnée $(\mathscr{C}_\alpha)$ indexée par α croissants dans un ensemble totalement ordonné de même cardinalité que la chaîne. Montrons que $\mathscr{C}$, la réunion des filtres de la chaîne, est un filtre :
(1) $\mathscr{C}$ contient I car il est présent au moins dans chaque élément de la chaîne. $\emptyset \notin \mathscr{C}$ car l'ensemble vide n'est contenu dans aucun des filtres de la chaîne.
(2) Soient A et B dans $\mathscr{C}$, alors $A \in \mathscr{C}_\alpha$ et $B \in \mathscr{C}_\beta$, alors la relation d'ordre totale sur la chaîne implique que pour $\gamma = max(\alpha, \beta)$, A et B sont des éléments de $\mathscr{C}_\gamma$, qui est un filtre et contient donc $A \cap B$. D'où $A \cap B \in \mathscr{C}$.
(3) Soit $A \in \mathscr{C}$ et $A \subseteq B \subseteq I$, il existe un α tel que $A \in \mathscr{C}_\alpha$. Or $\mathscr{C}_\alpha$ est un filtre, et par la troisième propriété des filtres, il contient B. Donc $B \in \mathscr{C}$.
$\mathscr{C}$ est un filtre qui contient $\mathscr{D}$, il est bien dans $\mathscr{F}$ et c'est un majorant de la chaîne considéré. Donc $\mathscr{F}$ est inductif.
Par le lemme de Zorn (équivalent à l'axiome du choix), $\mathscr{F}$ possède un élément maximal au sens de l'inclusion, notons le $\mathscr{U}$. Montrons qu'il s'agit d'un ultrafiltre :
Soit $X \subseteq I$, supposons par l'absurde que ni X, ni $I\backslash X$ ne sont dans $\mathscr{U}$. Alors par le lemme précédent, on peut l'étendre en un filtre $\mathscr{V}$ contenant X. Ceci induit $\mathscr{U} \subsetneq \mathscr{V}$, et $\mathscr{V}$ est dans $\mathscr{F}$; ceci contredit le caractère maximal de $\mathscr{U}$. Donc $\mathscr{U}$ contient soit X, soit $I\backslash X$, c'est un ultrafiltre comme attendu. □

On peut maintenant écrire le théorème faisant le lien entre filtre de Frechet et ultrafiltres.

Théorème 16. L'intersection de tous les ultrafiltres non principaux sur un ensemble infini I est le filtre de Frechet $\mathscr{D}_F$.

Démonstration. Posons $\mathscr{D}$ l'intersection de tous les ultrafiltres non principaux. On peut vérifier sans difficulté que c'est un filtre.
Soit $j \in I$, et soit $\mathscr{U}$ un ultrafiltre contenant $\{j\}$. Nécessairement par la propriété (3) des filtres, $\mathscr{D}_j \subseteq \mathscr{U}$, puis on a égalité, car s'il existait un élément de $\mathscr{U}$ ne contenant pas j, son intersection avec $\{j\}$ serait vide. L'ultrafiltre $\mathscr{U}$ est donc principal.
Par contraposée, un ultrafiltre non principal ne contient $\{j\}$ pour aucun $j \in I$, et contient donc toujours $I\backslash\{j\}$. De plus, soit une partie finie $\{j_1 \cdots, j_n\}$, $I\backslash\{j_1 \cdots, j_n\}$ est dans tout ultrafiltre non principal comme intersection des $I\backslash\{j_k\}$ pour k entre 1 et n, et est donc dans $\mathscr{D}$. Il vient $\mathscr{D}_F \subseteq \mathscr{D}$.

Réciproquement, soit A une partie infinie de I telle que $I\backslash A$ est infinie. Considérons le filtre de Frechet, il ne contient ni A, ni $I\backslash A$ par définition, donc on peut l'étendre en un filtre contenant $I\backslash A$ par le premier lemme, qu'on peut ensuite étendre en un ultrafiltre par le deuxième lemme. Cet ultrafiltre ne peut pas être principal, car il contient $\mathscr{D}_F$ qui pour tout j, possède $I\backslash\{j\}$. On peut faire de même pour construire un ultrafiltre non principal contenant A ; ainsi ni A ni $I\backslash A$ n'est dans $\mathscr{D}$. Il vient nécessairement : $\mathscr{D} = \mathscr{D}_F$. □

3.2.2 • CONSTRUCTION DES ULTRAPRODUITS ET PREMIÈRES PROPRIÉTÉS

Nous venons de définir les propriétés importantes relatives aux ultrafiltres. Ces objets vont nous servir à définir une relation d'équivalence par laquelle on va quotienter le produit infini $\sum_{p\in\mathbb{P}} \mathbb{Q}_p$, de sorte que l'on puisse travailler sur un corps. Ecrivons proprement la relation d'équivalence à partir de laquelle on va travailler.

Proposition 13. Soit $\mathscr{M}_i$ des $\mathscr{L}$-structures indexées sur l'ensemble infini I, et soit $\mathscr{D}$ un ultrafiltre. On assimile le produit cartésien des domaines de ces structures, $\prod M_i$, à l'ensemble des fonctions $\{f \,:\, I \to \cup M_i \mid \forall i, f(i) \in M_i\}$. On pose $f \sim_{\mathscr{D}} g$ si et seulement si $\{i \in I | f(i) = g(i)\} \in \mathscr{D}$. La relation $\sim_{\mathscr{D}}$ est une relation d'équivalence.

Démonstration. Soient f, g, h dans $\prod M_i$:
(1) $f \sim_{\mathscr{D}} f$ car $\{i \in I | f(i) = f(i)\} = I \in \mathscr{D}$, d'où la réflexivité.
(2) La symétrie est immédiate.
(3) Si $f \sim_{\mathscr{D}} g$ et $g \sim_{\mathscr{D}} h$, alors notons $A = \{i \in I | f(i) = g(i)\}$ et $B = \{i \in I | h(i) = g(i)\}$, qui sont dans l'ultrafiltre. Par stabilité des filtres, $A \cap B \in \mathscr{D}$. Or, $A \cap B \subseteq \{i \in I | f(i) = h(i)\}$ donc $\{i \in I | f(i) = h(i)\} \in \mathscr{D}$ et $f \sim_{\mathscr{D}} h$, la relation est transitive.
Par conséquent, $\sim_{\mathscr{D}}$ est bien une relation d'équivalence. □

On peut par suite raisonner sur les classes d'équivalence par la relation induite par un ultrafiltre, $\prod M_i/\mathscr{D}$, dans la structure que l'on note $\prod \mathscr{M}_i/\mathscr{D}$. Une telle structure est appelée ultraproduit. On représentera chaque élément de l'ultraproduit par la notation $[f]$ où f est un représentant de la classe d'équivalence.
L'interprétation des fonctions, constantes et relations se fait de manière assez naturelle dans ce domaine. Par exemple, pour les fonctions, prenant un élément $[f]$ et une fonction g d'arité 1, on pose par exemple $g([f]) = [g(f(i)) | i \in I]$. On dit de plus pour la relation unaire R que $[f] \in R$ si et seulement si $[i \in I | f(i) \in R] \in \mathscr{D}$. On peut montrer qu'une telle interprétation est bien définie, c'est-à-dire que le résultat est le même pour deux représentants différents de la même classe d'équivalence.
On a dorénavant tous les éléments pour prouver le théorème fondamental des ultraproduits, qui stipule exactement quelles sont les formules satisfaites par un ultraproduit. Cela va permettre de justifier toute la construction effectuée jusqu'à présent.

Théorème 17. [THÉORÈME FONDAMENTAL DES ULTRAPRODUITS]
Soit $\mathscr{M}$ l'ultraproduit des $\mathscr{M}_i$ pour l'ultrafiltre $\mathscr{D}$. Soit $\phi(v_1, \ldots, v_n)$ une formule définie sur les variables libres $v_1, \ldots, v_n$, et soit $([g_1], \ldots, [g_n]) \in (\prod M_i/\mathscr{D})^n$. Alors $\prod \mathscr{M}_i/\mathscr{D} \vDash \phi([g_1], \ldots, [g_n])$ si et seulement si $\{i \in I | \mathscr{M}_i \vDash \phi(g_1(i), \ldots, g_n(i))\} \in \mathscr{D}$.

Démonstration. La démonstration se fait par induction sur les formules. N'ayant pas défini proprement comment se fait cette induction, on va proposer une ébauche intuitive de démonstration, qui

capture les idées majeures de la preuve.
On se permettra de noter de manière abusive, le symbole de fonction f à la place de l'interprétation de la fonction dans le domaine $f^{\mathscr{M}}$, ce qui ne nuit pas à la compréhension. De plus, on se passera de préciser que toutes les formules peuvent utiliser les variables libres introduites dans l'énoncé, on notera simplement ϕ pour une telle formule.

Le cas de base de l'induction est en fait les formules dites atomiques, qui consistent en la relation entre plusieurs termes, $\phi = R([t_1], \dots, [t_n])$. Or, on a :
$\prod \mathscr{M}_i/\mathscr{D} \vDash \phi$
Si et seulement si $R([t_1], \dots, [t_n])$
Si et seulement si $\{i \in I | R(t_1(i), \dots, t_n(i))\} \in \mathscr{D}$
Si et seulement si $\{i \in I | R(t_1(i), \dots, t_n(i))\} \in \mathscr{D}$
Si et seulement si $\{i \in I | \mathscr{M}_i \vDash \phi(g_1(i), \dots, g_n(i))\} \in \mathscr{D}$.
C'est formellement un jeu d'écriture sur la définition qu'on a choisie pour les relations.

Pour l'hérédité, soient deux formules ϕ et ψ qui vérifient la propriété voulue. Les manières de construire inductivement de nouvelles formules sont de considérer : $\phi \wedge \psi$, $\phi \vee \psi$, $\neg\phi$, $\exists[x]\phi([x])$ et $\forall[x]\phi([x])$. On va prouver que l'induction fonctionne bien pour trois cas : $\phi \cup \psi$ et $\exists[x]\phi([x])$ et $\neg\phi$. Les deux autres cas (le "et" logique et le connecteur "pour tout") peuvent se construire à partir des trois précédents, si bien qu'il n'est pas nécessaire de les explorer.

Pour la formule $\phi \vee \psi$:
$\prod \mathscr{M}_i/\mathscr{D} \vDash \phi \vee \psi$
Si et seulement si $\prod \mathscr{M}_i/\mathscr{D} \vDash \phi$ ou $\prod \mathscr{M}_i/\mathscr{D} \vDash \psi$
Si et seulement si $\{i \in I | \mathscr{M}_i \vDash \phi\} \in \mathscr{D}$ ou $\{i \in I | \mathscr{M}_i \vDash \psi\} \in \mathscr{D}$
Si et seulement si $\{i \in I | \mathscr{M}_i \vDash \phi \vee \psi\} \in \mathscr{D}$: en effet, le sens direct provient de l'inclusion $\{i \in I | \mathscr{M}_i \vDash \phi\} \subseteq \{i \in I | \mathscr{M}_i \vDash \phi \vee \psi\}$. Remarquons réciproquement que si ni $\{i \in I | \mathscr{M}_i \vDash \phi\} \in \mathscr{D}$, ni $\{i \in I | \mathscr{M}_i \vDash \psi\} \in \mathscr{D}$, alors $I \backslash (\{i \in I | \mathscr{M}_i \vDash \phi\} \cup \{i \in I | \mathscr{M}_i \vDash \psi\}) \in \mathscr{D}$ par intersection, ce qui se réécrit $I \backslash \{i \in I | \mathscr{M}_i \vDash \phi \vee \psi\} \in \mathscr{D}$; il vient $\{i \in I | \mathscr{M}_i \vDash \phi \vee \psi\} \notin \mathscr{D}$ ce qui prouve le sens réciproque de l'équivalence.
On obtient l'équivalence espérée.

Pour la formule $\exists[x]\phi([x])$:
On veut montrer que $\exists[x]\phi([x])$ est vrai si et seulement si $\{i \in I | \mathscr{M}_i \vDash \exists x, \phi(x))\} \in \mathscr{D}$. Supposons qu'il existe $[y] \in \prod M_i/\mathscr{D}$ tel que $\phi([y])$ est satisfaite. Alors par la propriété d'hérédité, $\{i \in I | \mathscr{M}_i \vDash \phi(y(i))\} \in \mathscr{D}$. donc $\{i \in I | \mathscr{M}_i \vDash \exists x, \phi(x))\} \in \mathscr{D}$ en considérant $x = y(i)$ dans M_i.
Réciproquement, supposons que $A = \{i \in I | \mathscr{M}_i \vDash \exists x, \phi(x))\} \in \mathscr{D}$, l'objectif est de construire un élément y vérifiant : $\{i \in I | \mathscr{M}_i \vDash \phi(y(i))\} \in \mathscr{D}$. Pour cela, soit $i \in A$, notant x_i l'élément tel que $\mathscr{M}_i \vDash \phi(x_i)$ on pose $y(i) = x_i$ et pour $i \in I \backslash A$, on peut prendre $y(i) = 0$. Il vient que $B = \{i \in I | \mathscr{M}_i \vDash \phi(y(i))$ est plus grand que A pour l'inclusion donc est dans $\mathscr{D}$. Finalement, on a bien montré que $\exists[z] \in \prod M_i/\mathscr{D}$ tel que $\phi([z])$, pour $z = y$.

La propriété voulue pour la négation logique se démontre elle aisément en utilisant que le complémentaire d'un élément de l'ultraproduit $\mathscr{D}$ n'est pas dans $\mathscr{D}$.

Ceci permet de se convaincre que l'induction sur les formules du premier ordre fonctionne, et donc

que $\prod \mathscr{M}_i/\mathscr{D} \vDash \phi([g_1], \ldots, [g_n])$ si et seulement si $\{i \in I | \mathscr{M}_i \vDash \phi(g_1(i), \ldots, g_n(i))\} \in \mathscr{D}$. □

3.2.3 • RETOUR AUX CORPS VALUÉS HENSÉLIENS : VERS LE PRINCIPE D'AX-KOCHEN

La propriété générale qu'on vient de démontrer sur la structure d'ultraproduit est en réalité très puissante, car on sait exactement quelles formules sont satisfaites au premier ordre sur la structure. En particulier, cela permet d'étudier les axiomes de la théories des corps valués henséliens avec cross section sans plus de démonstrations.

Proposition 14. Soit $\mathscr{K}$ une classe élémentaire de $\mathscr{L}$-structures. Soit I un ensemble infini, $\mathscr{M}_i$ une famille de modèles de la classe $\mathscr{K}$ et $\mathscr{D}$ un ultrafiltre. Alors $\prod \mathscr{M}_i/\mathscr{D}$ est dans $\mathscr{K}$.
En particulier, un ultraproduit sur la classe élémentaire des corps valués henséliens avec cross section est toujours un corps valué hensélien avec cross section. C'est notamment le cas de $\prod_{p\in\mathbb{P}} \mathbb{Q}_p/\mathscr{D}$ et de $\prod_{p\in\mathbb{P}} \mathbb{Z}/p\mathbb{Z}((T))/\mathscr{D}$.

Démonstration. Soit ϕ un axiome de la classe $\mathscr{K}$, et une collection $\mathscr{M}_i$ de structures de la classe indexées sur l'ensemble infini I. Soit $\mathscr{D}$ un ultrafiltre. On sait que $\{i \in I | \mathscr{M}_i \vDash \phi\} = I \in \mathscr{D}$. Donc d'après le théorème fondamental des ultraproduits, $\prod \mathscr{M}_i/\mathscr{D} \vDash \phi$. Par conséquent, $\prod \mathscr{M}_i/\mathscr{D}$ satisfait tous les axiomes de la théorie associée à $\mathscr{K}$, il est bien dans $\mathscr{K}$. □

Nous avions aussi évoqué précédemment l'intérêt de passer à la caractéristique 0 pour les ultraproduits $\prod_{p\in\mathbb{P}} \mathbb{Q}_p/\mathscr{D}$ et $\prod_{p\in\mathbb{P}} \mathbb{Z}/p\mathbb{Z}((T))/\mathscr{D}$. Or, on a déjà construit ce qu'il nous faut pour prouver que ces deux corps vérifient la propriété escomptée.

Proposition 15. Soit $\mathscr{D}$ un ultrafiltre sur l'ensemble infini $\mathbb{P}$ des nombres premiers. Les corps $\prod \mathbb{Q}_p/\mathscr{D}$ et $\prod \mathbb{Z}/p\mathbb{Z}((T))/\mathscr{D}$ sont de caractéristique nulle.

Démonstration. Il s'agit encore d'invoquer le théorème fondamental des ultraproduits.
Soit n un entier premier. Tous les corps $\mathbb{Q}_p$ étant de caractéristique nulle, $\{p \in \mathbb{P} | \mathbb{Q}_p \vDash \neg Char(n)\} = \mathbb{P} \in \mathscr{D}$. Ainsi par le théorème fondamental des ultraproduits : $\prod \mathbb{Q}_p/\mathscr{D} \vDash \neg Char(n)$. Ceci valant pour tout n premier, $\prod \mathbb{Q}_p/\mathscr{D}$ est de caractéristique 0.
Pour l'ultraproduit $\prod \mathbb{Z}/p\mathbb{Z}((T))/\mathscr{D}$, la démonstration est sensiblement identique, en remarquant que pour n premier fixé, $\{p \in \mathbb{P} | \mathbb{Z}/p\mathbb{Z}((T)) \vDash \neg Char(n)\} = \mathbb{P}\backslash\{n\} \in \mathscr{D}_F \subseteq \mathscr{D}$ où $\mathscr{D}_F$ est le filtre de Frechet.
□

En outre, il faut spécifier quelle est la valuation (avec cross section) qu'on vient de construire sur l'ultraproduit. On peut penser intuitivement que comme le groupe de valuation d'un corps $\mathbb{Q}_p$ est isomorphe à $\mathbb{Z}$, alors le groupe de valuation sur l'ultraproduit serait isomorphe à $\prod \mathbb{Z}/\mathscr{D}$. C'est en réalité bien le cas.
De même, on peut étudier le corps résiduel est se rendre compte qu'il est isomorphe à $\prod(\mathbb{Z}/p\mathbb{Z})/\mathscr{D}$.

Proposition 16. Soit $\mathscr{D}$ un ultrafiltre non principal. Les corps résiduels et groupes de valuation de $\prod \mathbb{Q}_p/\mathscr{D}$ et de $\prod \mathbb{Z}/p\mathbb{Z}((T))/\mathscr{D}$ sont isomorphes avec :
(1) $\nu((\prod \mathbb{Q}_p/\mathscr{D})^*) \cong \prod \mathbb{Z}/\mathscr{D} \cong \nu((\prod(\mathbb{Z}/p\mathbb{Z})/\mathscr{D})^*)$.
(2) $\overline{\prod \mathbb{Q}_p/\mathscr{D}} \cong \prod(\mathbb{Z}/p\mathbb{Z})/\mathscr{D} \cong \overline{\prod \mathbb{Z}/p\mathbb{Z}((T))/\mathscr{D}}$, cette notation ayant été adoptée pour désigner le corps résiduel.
(3) Les corps résiduels sont de caractéristique 0.

La démonstration se fait assez naturellement en faisant simplement attention à la manipulation des classes d'équivalence vis-à-vis de l'ultrafiltre. Il faut se rappeler que le groupe de valuation de

$\mathbb{Q}_p$ est, par la cross section, isomorphe à $\mathbb{Z}$ en tant que groupe, puis construire autour du morphisme associé.
Pour la caractéristique nulle des corps résiduels, il suffit de calculer la caractéristique de $\prod(\mathbb{Z}/p\mathbb{Z})/\mathscr{D}$ en utilisant le théorème fondamental des ultrafiltres, puis invoquer l'isomorphisme établi au point (2).
On sait que les résultats établis ci-dessus sont vrais pour tous les ultrafiltres non principaux. Or, connaissant leur intersection, le filtre de Frechet, on va pouvoir faire finalement intervenir la notion de "tout, sauf un nombre fini" propre au principe d'Ax-Kochen.

Théorème 18. Soient $\mathscr{M}_i$ et $\mathscr{N}_i$ deux collections de $\mathscr{L}$ structures indexées sur le même ensemble infini I. Supposons que pour tout ultrafiltre non principal $\mathscr{D}$, $\prod \mathscr{M}_i/\mathscr{D} \equiv \prod \mathscr{N}_i/\mathscr{D}$.
Soit ϕ une formule logique au premier ordre sur le langage $\mathscr{L}$. Alors $\mathscr{M}_i \vDash \phi$ pour tous les i sauf un nombre fini, si et seulement si $\mathscr{N}_i \vDash \phi$ pour tous les i sauf un nombre fini.

Démonstration. Supposons que $\mathscr{M}_i \vDash \phi$ pour tous les i sauf un nombre fini. L'ensemble $A = \{i \in I | \mathscr{M}_i \vDash \phi\}$ est donc dans le filtre de Frechet $\mathscr{D}_F$.
Soit alors $\mathscr{D}$ un ultrafiltre non principal. $\mathscr{D}_F \subset \mathscr{D}$ donc $A \in \mathscr{D}$. Par le théorème fondamental des ultraproduits, $\prod \mathscr{M}_i/\mathscr{D} \vDash \phi$, ce faisant par l'équivalence logique au premier ordre, $\prod \mathscr{N}_i/\mathscr{D} \vDash \phi$. Ainsi, $B = \{i \in I | \mathscr{N}_i \vDash \phi\} \in \mathscr{D}$.
Ceci valant pour tout ultrafiltre non principal, B est dans l'intersection des ultrafiltres non principaux, donc dans le filtre de Frechet. Par conséquent, $I \backslash B$ est fini, et $\mathscr{N}_i \vDash \phi$ pour tous les i sauf un nombre fini.
Le sens réciproque fonctionne de manière identique en échangeant le rôle de $\mathscr{M}_i$ et de $\mathscr{N}_i$, ce qui prouve l'équivalence. □

La construction des ultraproduits permet donc d'effectuer la moitié du travail dans l'objectif de démontrer le principe d'Ax-Kochen. La deuxième moitié va consister en la démonstration de l'équivalence logique au premier ordre, hypothèse indispensable du théorème précédent, pour les corps valués henséliens $\prod \mathbb{Q}_p/\mathscr{D}$ et $\prod \mathbb{Z}/p\mathbb{Z}((T))/\mathscr{D}$. On va en fait démontrer quelque chose de plus fort, à savoir l'existence d'un isomorphisme entre ces deux structures.

3.3 L'ÉQUIVALENCE LOGIQUE AU PREMIER ORDRE

Nous allons maintenant démontrer qu'il existe un isomorphisme élémentaire entre les corps valués henséliens avec cross section $\prod \mathbb{Q}_p/\mathscr{D}$ et $\prod \mathbb{Z}/p\mathbb{Z}((T))/\mathscr{D}$, ce qui implique l'équivalence logique espérée. Le caractère hensélien de ces deux objets est loin d'être anodin dans notre démarche, et il nous faut ajouter quelques propriétés relatives aux corps vérifiant le lemme d'Hensel, qui nous permettront de construire un isomorphisme.

3.3.1 • QUELQUES CONSÉQUENCES DU LEMME D'HENSEL

Dans cette partie, on va noter $\overline{F}$ le corps résiduel d'un corps valué hensélien F. On rappelle de plus que la valuation utilsée est celle construite en section 3.1.2 pour les corps valués avec cross section, à valeurs dans le groupe de valuation de F.
Les résultats que nous allons présenter ici font appel à des notions très poussées de la théorie des corps valués, aussi nous nous proposons de les énoncer sans démonstration. Ils sont fondamentaux pour le raisonnement dit de "va-et-vient" évoqué en section 3.1.3.

Il nous faut d'abord définir ce qu'est un morphisme de corps valués. On attend d'un tel morphisme qu'il soit d'abord un morphisme de corps, mais aussi qu'il préserve la valuation, dans un sens que nous allons préciser.

Définition 22. Soient F et F' deux corps valués avec cross section, et leurs valuations notées respectivement $\nu_F : F \to F$ et $\nu_{F'} : F' \to F'$. On dit que $f : F \to F'$ est un morphisme de corps valués si et seulement si c'est un morphisme de corps, et s'il préserve la valuation, ce qui s'écrit : $f \circ \nu_F = \nu_{F'} \circ f$.

On peut interpréter la propriété de préservation de la valuation de la façon suivante : le morphisme de corps f envoie le groupe de valuation sur F dans le groupe de valuation de F'. Ainsi, en se restreignant au groupe de valuation sur F, f induit un morphisme de groupe injectif de $\nu(F)$ dans $\nu_{F'}$. En outre, soient deux éléments de F, notés a et b. Alors si a et b sont de même valuation dans F, $f(a)$ et $f(b)$ le sont aussi puisque $\nu_{F'}(f(a)) = f(\nu_F(a)) = f(\nu_F(b)) = \nu_{F'}(f(b))$. C'est cela qui fait dire que la valuation est préservée.
Ayant défini ce qu'est un morphisme sur les corps valués, on peut maintenant introduire la notion d'hensélisation. Prenant un corps valué, on se demande si on peut en prendre une extension, toujours valuée, qui soit hensélienne. C'est en fait toujours possible, et l'hensélisation d'un corps valué correspond à sa plus petite extension vérifiant cette propriété.

Définition 23. Soit G un corps valué. Un corps valué hensélien K est une hensélisation de G si et seulement si : (1) Le corps G est une extension de K.
(2) Si F est un corps valué hensélien et $\mu : G \to F$ est un morphisme de corps valués injectif, alors μ s'étend de manière unique à un morphisme de corps valués injectif $\lambda : K \to F$. Autrement dit, tout corps valué hensélien étendant F est une extension de K, et K est donc "le plus petit corps possible" qui vérifie (1).
Par cette définition, si elle existe, une hensélisation est unique à isomorphisme de corps valués près.

Proposition 17. (Admis) Tout corps valué F possède une hensélisation, K, unique à isomorphisme près. De plus, les groupes de valuations et corps résiduels de F et K sont isomorphes, respectivement en tant que groupes et en tant que corps.

On étudie maintenant les extensions algébriques des corps valués henséliens ; celles-ci seront utiles pour l'argument de va-et-vient. On admet encore les propositions suivantes, issues de la théorie des corps valués, que nous invoquerons librement dans la démonstration du principe d'Ax-Kochen.

Proposition 18. [UNICITÉ DU PROLONGEMENT DE LA VALUATION]
Soit F_0 un corps valué hensélien et F une extension algébrique de F_0. Alors la valutation ν_{F_0} s'étend de manière unique à F. Autrement dit, deux entensions algébriques de F_0, F et G, isomorphes comme corps, sont isomorphes comme corps valués, le groupe de valuation est unique à isomorphisme de groupes près.

La proposition suivante donne une manière de trouver l'hensélisation d'un corps valué F_0, pourvu qu'on en connaisse une extension F elle-même hensélienne.

Proposition 19. [CONDITION SUFFISANTE D'HENSÉLISATION]
Soit F un corps valué de valuation ν, soit F_0 un sous-corps de F valué. On note $\widetilde{F_0}$ la clotûre algébrique relative de F_0 dans F, c'est-à-dire l'ensemble des éléments de F algébriques sur F_0.
Alors $\nu\left(\widetilde{F_0}^*\right) = \{x \in \nu(F^*) \,|\exists n \in \mathbb{Z}, x^n \in \nu(F_0^*)\}$, que l'on appelle la clotûre sous les racines de

$\nu(F^*)$: c'est le plus petit groupe engendré par les racines des éléments de $\nu(F_0^*)$.
Supposons en outre que F est hensélien, qu'on a l'égalité des corps résiduel $\overline{F} = \overline{F_0}$, que $Char(\overline{F}) = 0$ et que $\nu\left(\widetilde{F_0}^*\right) = \nu(F_0^*)$ (cela signifie que $\nu(F_0^*)$ est déjà clos sous les racines). Alors $\widetilde{F_0}$ est une hensélisation de F_0.

Voyons maintenant un résultat intéressant sur les extensions transcendantes d'un corps valué hensélien : il nous permet d'étendre un isomorphisme de corps valués henséliens, à un isomorphisme entre deux extensions de degré de transcendance 1 de ces corps.

Proposition 20. [ISOMORPHISME SUR LES EXTENSIONS TRANSCENDANTES]
Soient F et G deux corps valués henséliens, et deux sous-corps valués henséliens respectifs, F_0 et G_0, élémentairement isomorphes par un isomorphisme f. Soient $x \in F$ et $y \in G$, respectivement transcendants sur F_0 et G_0.
Supposons que $\nu(F_0(x)^*) = \nu(F_0)$, que $\overline{F_0(x)} = \overline{F_0}$ et que pour tout a dans F_0, $f(\nu_F(x-a)) = \nu_G(y - f(a))$. Alors on peut étendre l'isomorphisme f en un isomorphisme élémentaire f_x de telle sorte que $F_0(x) \cong G_0(y)$.

L'hypothèse sur les valuations revient en fait à la condition d'isomorphisme de corps valués, $f \circ \nu_F = \nu_G \circ f$, en prenant $y = f(x)$. Ceci nous donne l'intuition que f, étendu à $F_0(x)$, envoie x sur y, ou envoie du moins un élément de même valuation que x sur y. C'est ce qui se passera en pratique lorsqu'on emploiera cette proposition dans la démonstration du principe d'Ax-Kochen.
Voici enfin une dernière proposition, portant sur la cardinalité du groupe de valuation.

Proposition 21. [CARDINALITÉ DU GROUPE DE VALUATION]
Soit F valué hensélien et F_0 un sous-corps valué hensélien de F, soit x dans F transcendant sur F_0. Si $\overline{F_0(x)} \cong \overline{F_0}$, et si $\nu(F_0)$ est non réduit à $\{1\}$, alors l'adjonction de x n'augmente pas le cardinal du groupe de valuation, c'est-à-dire : $|\nu(F_0(x)^*)| = |\nu(F_0^*)|$.

L'hypothèse de non trivialité du groupe de valuation, permet d'assurer que $\nu(F_0)$ contient au moins un élément y de valuation différente de 1, et contient donc le groupe engendré par y isomorphe à $\mathbb{Z}$. Ainsi, par cette hypothèse, le groupe de valuation est infini, et on travaille sur des cardinaux infinis. La proposition signifie par conséquent qu'on reste dans le "même infini" $\aleph_(\alpha)$ par adjonction d'un élément moyennant certaines hypothèses, ce qui se révèle important du point de vue des modèles de théories du premier ordre.

3.3.2 • DÉMONSTRATION DU PRINCIPE D'AX-KOCHEN

Tout est maintenant en place pour mettre en place l'argument de va-et-vient de la démonstration du principe d'Ax-Kochen. On va découper la preuve en plusieurs étapes par souci de clarté, et expliquer chacune d'entre elles en mettant bout à bout les arguments évoqués dans les sections 3.1 et 3.3.1.

Théorème 19. [PRINCIPE D'AX-KOCHEN GÉNÉRAL]
Soient F et G deux corps valués henséliens avec cross section. Supposons que leurs groupes de valuation respectifs sont des $\mathscr{L}_G$-structures équivalentes au premier ordre, $\nu_F(F^*) \cong \nu_G(G^*)$, que $Char(\overline{F}) = Char(\overline{G}) = 0$ et que $\overline{F} \cong \overline{G}$ comme $\mathscr{L}_F$-structures. Alors $F \cong G$.

Commençons par la première étape du théorème : il s'agit de prouver qu'on peut se restreindre à des modèles saturés de cardinal $\aleph_1$.

Démonstration. [ÉTAPE 1]
On travaille sur le langage $\mathscr{L}_{VF}$ des corps valués avec cross section. Ce langage est fini donc dénombrable. D'après le théorème de Löwenheim-Skolem pour les modèles saturés, il existe deux modèles saturés de cardinal $\aleph_1$, qu'on note F_{sat} et G_{sat}, tels que $F_{sat} \vDash Th(F)$ et $G_{sat} \vDash Th(G)$.
En particulier, la théorie $\mathscr{T}$ des corps valués henséliens est comprise dans $Th(F)$ et $Th(G)$. Ceci implique que F_{sat} et G_{sat} sont des corps valués henséliens avec cross section.
Il reste à vérifier que F_{sat} et G_{sat} vérifient les hypothèses du principe d'Ax-Kochen général portant sur les corps résiduels et les groupes de valuation. Or, soit une formule ϕ du langage des corps $\mathscr{L}_F$ vérifiée par $\overline{F}$ et $\overline{G}$. On peut la réécrire en une formule ϕ' sur le langage $\mathscr{L}_{VF}$ des corps valués, en rajoutant à chaque occurence de variable libre ou liée a, qu'on veut : $\nu(a) = 1$ de sorte qu'on est bien dans le corps résiduel. Ainsi, $F \vDash \phi'$ si et seulement si $\overline{F} \vDash \phi$. En particulier, toutes les formules portant sur les corps résiduels de F et G sont comprises dans $Th(F)$ et $Th(G)$ sous cette nouvelle forme, et elles traduisent bien le fait qu'on parle des éléments du corps résiduel. Ce faisant, elles sont satisfaites aussi bien par F_{sat} que par G_{sat}, ce qui prouve que $Char(\overline{F_{sat}}) = Char(\overline{G_{sat}}) = 0$ et $\overline{F_{sat}} \cong \overline{G_{sat}}$
Finalement, on a, de la même façon, $\nu_{F_{sat}}(F_{sat}^*) \cong \nu_{G_{sat}}(G_{sat}^*)$. En effet, les formules sur le langage des groupes $\mathscr{L}_G$ peuvent elles aussi être transcrites sur $\mathscr{L}_{VF}$, puisque l'appartenance au groupe de valuation se traduit par la relation unaire notée V sur $\mathscr{L}_{VF}$. Les corps F_{sat} et G_{sat} satisfont les hypothèses du théorème. De plus, par construction, $F \equiv F_{sat}$ (puisque $Th(F)$ est une théorie complète) et $G \equiv G_{sat}$. Ceci implique que $F \equiv G$ si et seulement si $F_{sat} \equiv G_{sat}$. On peut donc se contenter de prouver le théorème pour F_{sat} et G_{sat} qui sont saturés et de cardinal $\aleph_1$. □

On suppose dorénavant, ce que cette étape 1 rend légitime, que F et G sont saturés de cardinal $\aleph_1$.
On est tenté d'utiliser, pour construire un isomorphisme entre F et G, le théorème d'isomorphisme sur les modèles saturés ; mais celui-ci nécessite déjà que $F \cong G$ ce qui est précisément ce qu'on est en mal de prouver... Néanmoins, on va pouvoir l'appliquer à leurs corps résiduels $\overline{F}$ et $\overline{G}$.
L'objectif de la deuxième étape est de montrer que $\overline{F} \cong \overline{G}$ et que $\overline{F}$ et $\overline{G}$ sont relativement algébriquement clos dans F et G respectivement, en les considérant par isomorphisme comme des sous-corps de F et G.

Démonstration. [ÉTAPE 2]
De manière générale, les corps $\overline{F}$ et $\overline{G}$ sont isomorphes à des sous-corps de F et G respectivement (comme quotients de F et G, par la construction effectuée en section 2.1). Ils sont donc de cardinal plus petit que celui de F et G, $\aleph_1$. Les groupes de valuation sont eux des sous-groupes multiplicatifs de F et G donc sont aussi de cardinal plus petit que $\aleph_1$.
En outre, les types sur les structures $\overline{F}$ et $\overline{G}$ de cardinal strictement plus petit que $|\overline{F}|$ sont réalisés, puisqu'on peut, par la même manipulation que dans l'étape 1, les relever en types sur F et G. Ainsi, $\overline{F}$ et $\overline{G}$ sont des modèles saturés. Or, par hypothèse, $\overline{F} \equiv \overline{G}$, donc par le théorème d'isomorphisme sur les modèles saturés, $\overline{F} \cong \overline{G}$. Notons f_0 l'isomorphisme élémentaire entre ces deux structures.

Montrons maintenant que $\overline{F}$ est relativement algébriquement clos dans F. Soit P un polynôme non constant à coefficients dans $\overline{F}$, de degré $p \geqslant 1$. Considérons, comme nous l'avons fait en section 2.1, R_F l'anneau d'entiers de F, c'est-à-dire les éléments $t \in F$ vérifiant $\nu_F(t) \geqslant 1$ dans le cadre de la cross section. Soit x un élément de F qui n'est pas dans R_F, c'est-à-dire $\nu_F(x) < 1$. Alors les monômes présents dans $P(x)$, l'évaluation de P en x, sont de la forme $a_n \cdot x^n$ où n est entier, et où le coefficient a_n est un élément de $\overline{F}$ qui vérifie $\nu_F(a_n) = 1$. Ce faisant, $\nu_F(a_n \cdot x^n) = (\nu_F(x))^n$, ces valuations sont

distinctes deux à deux (car $\nu_F(x) < 1$), la plus petite étant atteinte par le monôme de plus haut degré, elle vaut $(\nu_F(x))^p$. Or par propriété de la valuation, la valuation de la somme est le minimum des valuations lorsqu'elles sont distinctes : ainsi $\nu(P(x)) = (\nu_F(x))^p \neq \nu(0)$. Donc x n'annule pas P.
Par suite, toute racine de P dans F est dans l'anneau d'entier R_F. Soit a une telle racine si elle existe. On est autorisé à prendre sa classe $\overline{a}$ dans $\overline{F}$. Alors $P(a) = 0$ donc $P(\overline{a}) = \overline{P(a)} = \overline{0} = 0$. Par conséquent, on peut factoriser : $P(X) = (X - \overline{a}) \cdot Q(X)$ où Q est un polynôme de degré décrémenté de 1. Supposons par l'absurde que $a \neq \overline{a}$, alors a annule toujours Q donc $\overline{a}$ aussi, et ainsi de suite. Dès lors, faisant décroître le degré, on finit par factoriser complètement P sous la forme $P(X) = (X - \overline{a})^p$. Or, a est racine de P donc $a = \overline{a}$ ce qui contredit l'hypothèse. D'où $a = \overline{a}$ et $a \in \overline{F}$. $\overline{F}$ est relativement algébriquement clos dans F. Identiquement, $\overline{G}$ est relativement algébriquement clos dans G. □

Pour passer à la suite de la démonstration, on se débarasse d'un cas assez simple, celui pour lequel $\nu_F(F^*) = \nu_F(F^*) = 1$. En effet, dans ce cas, $F = \overline{F}$ et $G = \overline{G}$, et comme $\overline{F} \equiv \overline{G}$, il vient immédiatement $F \equiv G$.
Le principe d'Ax-Kochen étant donc déjà vrai pour de tels corps, on traite l'autre cas et on suppose dorénavant que les groupes de valuation sont non triviaux. Ceci nous place en position d'appliquer les théorèmes vus précédemment sur l'adjonction d'élément, et donc d'étendre notre isomorphisme f_0 à des structures plus grandes que les corps résiduels.
L'objectif de l'étape suivante est donc d'étendre l'isomorphisme pour aller vers les corps F et G. C'est là la base de l'argument évoqué de "va-et-vient" : on part d'une sous-structure plus petite, le corps résiduel, pour grandir jusqu'au corps valué de base.
Plus précisément, ce qu'on veut démontrer étant un peu plus compliqué, on va l'énoncer explicitement.

Proposition 22. [ÉTAPE 3]
Soient F_1 et G_1 deus sous-corps valués relativement algébriquement clos dans F et G, et contenant les corps résiduels : $\overline{F} \subseteq F_1$, $\overline{G} \subset G_1$,. Supposons en outre que $\nu_F(F_1^*)$ et $\nu_G(G_1^*)$ sont dénombrables, et qu'il existe un isomorphisme élémentaire f_1 entre F_1 et G_1.
Soit alors $x \in F$. Il existe deux extensions de F_2 et G_2 de F_1 et G_1 toujours incluses dans F et relativement algébriquement closes, de groupes de valuation dénombrables, avec $x \in F_2$ et telles qu'il existe un isomorphisme élémentaire f_2 entre F_2 et G_2, qui étend f_1. Par cet isomorphisme, on peut écrire $F_2 \cong G_2$.
Les corps F_2 et G_2 possèdent les mêmes propriétés que F_1 et G_1, de sorte qu'on pourra itérer ce raisonnement avec eux, en y ajoutant d'autres éléments de F.

Démonstration. Si x est déjà contenu dans F_1, il suffit de prendre $F_2 = F_1$, $G_2 = G_1$ et $f_2 = f_1$. Supposons maintenant que $x \notin F_1$. Pour arriver à nos fins, nous allons devoir invoquer à bon escient les théorèmes vus en section 3.3.1.
Comme F_1 est relativement algébriquement clos dans F, x est transcendant sur F_1, ce qui nous invite naturellement à considérer l'extension transcendante $F_1(x)$ sur laquelle on désire appliquer le théorème d'isomorphisme sur les extensions transcendantes. La suite de la preuve consiste à vérifier les hypothèses de ce théorème. Il convient de distinguer deux sous-cas pour y parvenir. Nous pourrons ensuite prouver le cas général, pour n'importe quel élément x.

Premier cas : x n'agrandit pas le groupe de valuation, $\nu(F_1^*) = \nu(F_1^*(x))$:

Comme $\overline{F} \subseteq F_1 \subset F_1(x)$, on a $\overline{F} = \overline{F_1} = \overline{F_1(x)}$. De plus, par hypothèse la caractéristique des corps résiduels est 0, et F_1 étant relativement algébriquement clos, donc son groupe de valuation est

directement clos sous les racines. Par condition suffisante d'hensélisation, $\widetilde{F_1} = F_1$ est l'hensélisation de F_1 et F_1 est hensélien. Il en va de même pour G_1.
Il nous manque maintenant une seule hypothèse pour appliquer le théorème d'isomorphisme sur les extensions transcendantes, l'existence du y dans G_1 ayant la bonne priorité vis-à-vis des valuations. Montrons que le y recherché existe.

Pour cela, on va utiliser le fait que F est saturé, et prouver que les propriétés que doivent satisfaire y correspondent exactement à la satisfaction d'un 1-type sur G.
L'image de la valuation de $\nu(F_1(x))$ est dénombrable par hypothèse, ainsi l'ensemble $\{\nu_F(x-b)|b \in F_1\}$ est lui aussi dénombrable. Ce faisant, on peut prendre un sous-ensemble $A_1 \subset F_1$ dénombrable, tel que $\{\nu_F(x-a)|a \in A_1\} = \{\nu_F(x-b)|b \in F_1\}$. Ceci permet de s'assurer que l'ensemble A_1 sur lequel on veut définir un type est bien pertinent. En effet, $|A_1| = \aleph_0 < \aleph_1$, et F est $\aleph_1$-saturé par hypothèse, donc il réalise les types portant sur A_1.
En fait, c'est plutôt dans G que l'on cherche y, et c'est par conséquent sur un autre ensemble que A_1 qu'on va raisonner, qui sera lui dans G_1. Posons $S = f_1(A_1) \cup \nu_G(G_1^*) \in G_1$, qui est dénombrable. Formellement, il s'agit des éléments de G_1 associés aux éléments de A_1 par l'isomorphisme élémentaire avec F_1. On se munit du langage $\mathscr{L}_S = \mathscr{L}_{VF} \cup c_s|s \in S$, pour lequel on a introduit un symbole de constante pour chaque élément de S. On veut trouver un y tel que pour chaque élément a de A_1, $f_1(\nu_F(x-a)) = \nu_G(\nu_G(y-f(a)))$. Au premier ordre, cela revient à chercher un élément du domaine F vérifiant pour tout $a \in A_1$ la formule en une variable libre : $\phi_a(v) \ : \ c_{f_1(\nu(x-a))} = \nu(v - c_{f_1(a)})$. Les symboles de constantes correspondent bien par la construction de A_1 et S, à des éléments de S, et sont donc dans $\mathscr{L}_S$.

On pose alors $P = \{\phi_a|a \in A_1\}$. On veut montrer que c'est un 1-type sur S, autrement dit que $T = P \cup Th_S(G)$ est satisfiable. Pour ce faire, on va appliquer le théorème de compacité. Soit un sous-ensemble fini T' de T, il contient un sous-ensemble P' de formules de P, associé à un sous-ensemble fini A_1' de A_1. La finitude de cet ensemble implique qu'on peut y prendre b tel que $w = \nu_F(x-b)$ y est maximal. Pour tout entier naturel non nul n, on a $\nu_F(nw) = w$, ce faisant, prenant $a \in A_1'$:

$$\nu_F(a-nw-b) \geqslant min\{\nu_F(x-a), \nu_F(x-b), \nu_F(nw)\} = min\{w, w, \nu_F(x-a)\}$$

.
D'où : $\nu_F(a-nw-b) \geqslant \nu_F(x-a)$,
et on est dans le cas d'égalité lorsque $\nu_F(x-a) < w$.

En outre, cette égalité est vraie pour tout n sauf au plus 1. En effet, soit $m < n$, supposons par l'absurde qu'on a conjointement $\nu_F(a-nw-b) > \nu_F(x-a)$ et $\nu_F(a-mw-b) > \nu_F(x-a)$, alors :

$$w \ = \ \nu_F((n-m)w) \ \geqslant \ min\{\nu_F(a-nw-b), \nu_F(a-mw-b)\} \ > \ \nu_F(x-a)$$

.
Par conséquent, on est dans le cas d'égalité, ce qui contredit $\nu_F(a-nw-b) > \nu_F(x-a)$. L'ensemble A_1' étant fini, on peut par conséquent trouver un entier n tel que pour tout a dans A_1', $\nu_F(a-nw-b) = \nu_F(x-a)$. Par conséquent, on pose $y = f_1(b-nw)$, de telle sorte que :
$f_1(\nu_F(x-a)) \ = \ f_1(\nu_F(b-nw-a)) \ = \ \nu_G(f_1(b-nw-a)) \ = \ \nu_G(y-f(a))$
En ayant appliqué l'identité $f_1 \circ \nu_F = \nu_F \circ f_1$.
Le y ainsi choisi satisfait les formules de P' et donc le modèle G satisfaisant $Th_S(G)$ et les formules

de P' pour la valeur $v = y$: T' est satisfiable.
Par théorème de compacité, T est satisfiable, ce qui signifie que P est bien un 1-type sur S. Par saturation de G, ce type est réalisé.

On a donc bien un élément de G, noté y, tel que la propriété voulue sur les valuations est satisfaite pour $a \in A_1$. La construction de A_1 nous permet par ailleurs ensuite de prouver que cette propriété est aussi vraie pour b dans F_1 quelconque : en comparant ce b avec $a \in A_1$ tel que $\nu_F(x-a) = \nu_F(x-b)$, on obtient bien $f_1(\nu_F(x-b)) = \nu_G(y - f(b))$. On omet les quelques lignes, purement techniques, de calcul sur les valuations qui aboutissent à ce résultat.
Les hypothèses sont maintenant toutes vérifiées, ce qui nous permet d'appliquer le théorème d'isomorphisme sur les extensions transcendantes : il existe un isomorphisme élémentaire g_1 entre $F_1(x)$ et $G_1(y)$, ce qui signifie que $F_1(x) \cong G_1(y)$.
Ceci n'est pas suffisant car on souhaiterait de plus que $F_1(x)$ et $G_1(y)$ soient relativement algébriquement clos sur F et G. En fait, ce n'est pas tout à fait le cas, mais on peut encore décider de les étendre en passant à l'hensélisation, qui dans ce cas précis est une clôture algébrique. En effet, comme $\nu(F_1(x)^*) = \nu(F_1^*)$ dans ce premier cas, $\nu(F_1(x)^*)$ est clos sous les racines, ce qui nous permet de dire que l'hensélisation de $F_1(x)$ est $F_2 = \widetilde{F_1(x)}$. Le même argument s'applique pour $G_1(y)$, on note G_2 son hensélisation.
Le théorème d'unicité du prolongement de la valuation permet de plus de dire qu'on a toujours isomorphisme de corps valués entre F_2 et G_2, on prolonge donc g_1 en un isomorphisme élémentaire f_2 entre F_2 et G_2. Le théorème d'existence de l'hensélisation dit en outre que le passage de $F_1(x)$ à F_2 ne modifie pas le groupe de valuation, qui reste donc dénombrable.
F_2 et G_2 vérifient toutes les propriétés désirées, ainsi ce premier cas est prouvé.

2ème cas : x est un élément de $\nu(F^*)$:

On se rend déjà compte par le théorème de cardinalité du groupe de valuation, que $\nu_F(F_1(x)^*)$ est toujours dénombrable. Ainsi, l'argument de construction du y, passant par un 1-type, est toujours valable.
L'autre subtilité est qu'ici, le groupe de valuation est étendu et n'est plus clos sous les racines. Par conséquent, l'hensélisation de $F_1(x)$ n'est plus sa clôture algébrique relative, et on n'arrive pas directement à la conclusion.
Pour surmonter cette nouvelle contrainte, on raisonne comme suit (on se propose ici de n'expliquer que brièvement les étapes de la construction). Posant V et W les groupes de valuations de $F_1(x)$ et $G_2(y)$, on prend leur clôture sous les racines respectives, qu'on note $\widetilde{V}$ et $\widetilde{W}$. A chaque élément de V, on ajoute au plus un élément par entier relatif, ce faisant on a une injection de $\widetilde{V}$ dans $\cup_{v \in V} \mathbb{Z}$ qui est dénombrable comme réunion dénombrable : $\widetilde{V}$ reste dénombrable. La saturation du groupe de valuation couplée au théorème d'isomorphisme sur les modèles saturés (les groupes de valuation de F et G entier étant supposés équivalents) implique par ailleurs l'existence d'un isomorphisme entre $\widetilde{V}$ et $\widetilde{W}$.
On prend alors l'extension de corps de $F_1(x)$ engendrée par $\widetilde{V}$, ce sur quoi on passe ensuite comme dans le premier cas à l'hensélisation pour construire deux extensions F_2 et G_2 vérifiant les hypothèses escomptées. D'où le résultat dans ce deuxième cas.

Dans le cas général, x est toujours transcendant sur F_1, mais il est possible que $\nu_F(F_1(x)^*)$ soit

strictement plus grand pour l'inclusion que $\nu_F(F_1^*)$, sans forcément qu'on ait comme dans le cas 2, $x \in \nu_F(F^*)$. Malgré cela, on est en capacité de ruser pour faire appel à ces deux cas.
Le groupe de valuation $\nu_F(F_1(x)*)$ est toujours dénombrable par le théorème de cardinalité. On peut donc énumérer les éléments qui y ont été ajoutés à $\nu_F(F_1^*)$, en les notant $\{x_i | i \in \mathbb{N}\}$.
On peut alors construire des extensions de F_1 successives, en ajoutant successivement l'élément x_i à l'étape i par le second cas, pour construire F_{x_i} isomorphe élémentairement à G_{x_i} par f_{x_i}.
Ces morphismes sont compatibles les uns avec les autres, de sorte qu'on peut construire l'isomorphisme élémentaire $f_2 = \cup_{i\in\mathbb{N}} f_{x_i}$, entre $F_2 = \cup_{i\in\mathbb{N}} F_{x_i}$ et $G_2 = \cup_{i\in\mathbb{N}} G_{x_i}$. Par cette opération, F_2 vérifie bien les propriétés voulues. On vérifie que son groupe de valuation est dénombrable comme réunion dénombrable. On vérifie également qu'il est relativement algébriquement clos, car tout polynôme sur F_2 a pour coefficients $a_0 \in F_{x_{i(a0)}}, \dots, a_p \in F_{x_{i(ap)}}$, et prenant n le maximum de $(i(a_0), \dots, i(a_n))$, les coefficients sont tous dans F_{x_n} qui est relativement algébriquement clos.
En revanche, rien ne dit qu'on a ajouté x dans F_2 par cette construction. Ainsi, on va étendre, encore une fois en ajoutant les nouveaux éléments du groupe de valuation de $F_2(x)$ à F_2, F_2 à F_3, etc, F_i à F_{i+1}, et en étendant l'isomorphisme f_2 à f_i pour i entier. Considérons $F_x = \cup_{i\in\mathbb{N}^*} F_i$, $G_x = \cup_{i\in\mathbb{N}^*} G_i$, et $f_x = \cup_{i\in\mathbb{N}^*} f_i$. Pour les mêmes raisons que dans la constructions de F_2, l'isomorphisme élémentaire f_x est bien défini, les groupes de valuation restent dénombrables et la clôture algébrique relative est vérifiée. De plus, soit cette fois $y \in \nu(F_x(x))$, alors il existe i tel que $y \in \nu(F_i(x))$ car y est dans le groupe de valuation de F et est généré à partir de x à l'aide d'un nombre fini d'éléments vivant dans les corps F_k, et on prend i le "k" le plus grand. Donc y est ajouté en construisant F_{i+1} ce qui implique que $y \in F_{i+1}$ et donc $y \in F_x(x)$. Par conséquent, ajouter x à F_x n'ajoute aucun élément au groupe de valuation pour $F_x(x)$. On en revient donc au premier cas, ce qui permet d'étendre nos deux corps et notre isomorphisme pour construire $F_{final} \cong G_{final}$, ce qu'il fallait démontrer.
On note que par symétrie, il est possible d'inverser les rôles de F et de G, et donc de choisir d'ajouter des éléments de G bien précis. □

Le plus dur est démontré, il nous suffit maintenant d'invoquer à nouveau un argument dit de va-et-vient, en considérant une réunion infinie de morphismes continus. L'idée est d'adjoindre un par un les éléments de F, en partant du cas de base qui est notre isomorphisme élémentaire entre les corps résiduels $\overline{F}$ et $\overline{G}$. Démontrons formellement la dernière étape du principe d'Ax-Kochen général.
Démonstration. [ÉTAPE 4]
On part de f_0 l'isomorphisme élémentaire entre $\overline{F}$ et $\overline{G}$. Ces deux corps vérifient bien les propriétés nécessaires pour appliquer l'étape 3 inductive.
Prenons deux chaînes inductives énumérant F et G, notées $(a_\alpha : \alpha < \aleph_1)$ et $(b_\alpha : \beta < \aleph_1)$. On construit inductivement les isomorphismes f_α, où pour passer de α à $\alpha + 1$, on ajoute les éléments a_α à F puis b_α à G. On peut considérer alors $f = \cup f_\alpha$, bien défini car les morphismes s'étendent successivement. C'est un isomorphisme élémentaire entre F et G d'où $F \cong G$. Le principe d'Ax-Kochen général est établi. □

Ceci conclut cette partie, on a bien l'équivalence élémentaire qu'on espérait.

3.4 LE THÉORÈME D'AX-KOCHEN

On peut mettre les éléments bout à bout et démontrer le théorème qui nous intéresse pour les propriétés faiblement C_2 sur les corps $\mathbb{Q}_p$. C'est en fait une application tout à fait directe du principe

d'Ax-Kochen.

Théorème 20. [PRINCIPE D'AX-KOCHEN]
Pour tout ultrafiltre non principal, on a l'équivalence logique au premier ordre $\prod \mathbb{Z}/p\mathbb{Z}((T))/\mathscr{D} \equiv \prod \mathbb{Q}_p/\mathscr{D}$.
Une propriété au premier ordre satisfaite par tous les $\prod \mathbb{Z}/p\mathbb{Z}((T))$ sauf un nombre fini d'entre eux, l'est par tous les $\mathbb{Q}_p$ sauf un nombre fini d'entre eux.

Démonstration. Soit $\mathscr{D}$ un ultrafiltre non principal. Il suffit de vérifier les hypothèses du principe d'Ax-Kochen général, prenant $F = \prod \mathbb{Z}/p\mathbb{Z}((T))/\mathscr{D}$ et $G = \prod \mathbb{Q}_p/\mathscr{D}$. Or, nous avons déjà montré précisément tout ce dont nous avons besoin en section 3.2.3. □

En particulier, on peut appliquer ce principe puissant au cas des propriétés $C_2(d)$, pour d entier. Cette application est connue sous le nom de théorème d'Ax-Kochen, et c'est le résultat que nous souhaitions démontrer.

Théorème 21. [THÉORÈME D'AX-KOCHEN]
Soit $d \in \mathbb{N}^*$. Seul un nombre fini de corps $\mathbb{Q}_p$ ne sont pas $C_2(d)$.

Démonstration. Soit $d \in \mathbb{N}^*$. Notons $N = d^2 + 1$, et $c(d)$ le nombre de N-uplets d'entiers naturels de somme d. On peut sans difficulté exprimer la propriété C_2 en degré d par une formule logique au premier ordre de la façon suivante :
$K_d \ : \ \forall a_1 \dots \forall a_{c(d)}, (\neg(a_1 = 0) \vee \dots \vee \neg(a_{c(d)} = 0)) \to \exists x, \neg(x = 0) \wedge f(x) = 0$
Où, indexant tous les monômes à N variables de degré d entre 1 et $c(d)$, f correspond à la forme dont les coefficients sont $a_1, \dots, a_{c(d)}$, et $f(x)$ peut donc s'écrire au premier ordre comme somme et produit.
On a démontré en section 2, que tous les corps $\mathbb{Z}/p\mathbb{Z}((T))$ sont C_2, et en particulier $C_2(d)$. Ils satisfont par conséquent tous la formule du premier ordre K_d. Par le principe d'Ax-Kochen, tous les corps $\mathbb{Q}_p$ sauf un nombre fini sont $C_2(d)$. □

Remarque 4. Le principe d'Ax-Kochen ne permet en revanche pas de prouver que les corps $\mathbb{Q}_p$ sauf un nombre fini, sont C_2 (et tant mieux, car nous avons démontré qu'aucun ne l'est). En effet, tous les corps $\mathbb{Z}/p\mathbb{Z}((T))$ sont C_2, mais on ne peut pas appliquer le principe d'Ax-Kochen à la propriété C_2. Une telle propriété ne peut pas s'écrire sous la forme d'une unique formule au premier ordre, pour s'en persuader, essayons de le faire pour comprendre ce qui bloque.
La propriété C_2 implique de travailler avec des polynômes de tout degré. Pour cela, il faudrait pouvoir introduire une quantité infinie de coefficients, ce que l'on ne peut pas faire à la main en une seule formule. Une autre piste à explorer est d'introduire explicitement le degré, en commençant par "$\forall d \in \mathbb{N}^*$", mais on voit qu'il faut introduire l'ensemble $\mathbb{N}^*$, ce que le premier ordre ne permet pas. Toutes nos tentatives sont heureusement vaines.

L'approche de démonstration pour laquelle nous avons optée correspond à la preuve historique portée par James Ax et Simon Kochen. D'autres méthodes ont pu être mises en oeuvre pour aboutir à la même conclusion, certaines empruntant à la géométrie (qu'on doit entre autres à Denef et Colliot-Thélène).
En outre, Brown a réussi, en approfondissant la démarche d'Ax et Kochen et en y ajoutant quelques notions algébriques, à exhiber une constante $m(d)$, pour d entier strictement positif, à partir de laquelle tous les corps $\mathbb{Q}_p$ pour $p > m(d)$ sont $C_2(d)$. Enonçons sans démonstration ce joli résultat, prouvé en 1978.

Théorème 22. [BROWN]
Soit $d \in \mathbb{N}^*$. On pose :

$$m(d) = 2^{2^{2^{2^{11^{d^{4d}}}}}}$$

Alors pour tout nombre premier $p \geqslant m(d)$, $\mathbb{Q}_p$ est $C_2(d)$.

Pratiquement, cette constante ne revêt aucun intérêt. Elle est parfois loin d'être optimale, par exemple on a vu que la propriété est toujours vraie pour les degrés 2 et 3. Nous invitons tout de même le lecteur à prendre un instant pour s'émerveiller devant ce que l'abstraction pure est capable de mettre en lumière.

Le principe d'Ax-Kochen est très spécifique au cas des corps $\mathbb{Q}_p$ et $\mathbb{Z}/p\mathbb{Z}((T))$. Notons tout de même qu'on peut l'appliquer à des extensions algébriques ou transcendantes de $\mathbb{Q}_p$. En effet, pour chaque p premier, on prend un élément x_p algébrique sur $\mathbb{Q}_p$ de degré d'algébricité n_p. On peut voir $\mathbb{Q}_p(x_p)$ comme une $\mathbb{Q}_p$ algèbre de dimension n_p, comme dans les raisonnements de la section 1.3. On peut munir $\mathbb{Q}_p(x_p)$ d'une unique valuation, comme nous le garantit la proposition 18 de prolongement de valuation. Prenant y_p un élément algébrique de degré n_p sur chaque corps $\mathbb{Z}/p\mathbb{Z}((T))$, on peut montrer que $\mathbb{Z}/p\mathbb{Z}((T))(y_p)$ a même groupe de valuation que $\mathbb{Q}_p(x_p)$ à isomorphisme près.
Par le théorème de Lang, les $\mathbb{Z}/p\mathbb{Z}((T))(y_p)$ sont tous C_2. Remarquons que toutes les hypothèses du principe d'Ax-Kochen général s'appliquent pour l'ultraproduit des corps $\mathbb{Q}_p(x_p)$.

Corollaire 1. Soit pour chaque p premier, x_p un élément algébrique sur $\mathbb{Q}_p$. Soit d un entier naturel non nul. Alors tous les corps $\mathbb{Q}_p(x_p)$ sauf un nombre fini sont $C_2(d)$.

On a un résultat plus parlant pour une extension transcendante de degré 1 : par le théorème de Tsen, les corps $\mathbb{Z}/p\mathbb{Z}((U))(T)$sont C_3, et on peut les comparer aux corps de fractions rationnelles $\mathbb{Q}_p(T)$, qu'on peut valuer. On peut faire la même chose avec les corps de séries de Laurent formelles, en utilisant le théorème de Greenberg. Il vient :

Corollaire 2. Tous les corps $\mathbb{Q}_p(T)$ sauf un nombre fini sont $C_3(d)$.
Tous les corps $\mathbb{Q}_p((T))$ sauf un nombre fini sont $C_3(d)$.

On ne pourra guère étudier plus de corps par cette méthode.
Le lien viscéral unissant $\mathbb{Q}_p$ à la propriété C_2 a donc été explicité. Si parmi cette famille de corps, aucun n'est C_2, beaucoup sont faiblement C_2 en beaucoup de degrés. Ainsi, la théorie C_i reste très éclairante malgré tout.
La relation paradoxale que les corps $\mathbb{Q}_p$ entretiennent avec cette théorie, peut d'ailleurs être vue sous un autre angle, en étudiant un outil plus moderne issu de la topologie algébrique, la dimension cohomologique. Cette grandeur se révèle elle aussi être fortement corrélée au caractère C_i d'un corps. Nous allons voir dans la prochaine partie ce qu'elle peut apporter à notre étude.

4
LA PROPRIÉTÉ C_i ET LA DIMENSION COHOMOLOGIQUE

Dans cette partie on va définir les groupes de cohomologie d'un groupe fini (ou profini). Soit k un corps, et k^{sep} sa clôture séparable. On va voir qu'il y a des connexions entre la dimension cohomologique du groupe de Galois $Gal(k^{sep}/k)$ et les propriétés C_i de k. Brièvement, Serre a conjecturé que pour tout $r \geqslant 0$, la propriété C_r implique que la dimension cohomologique est inférieure à r.
Ici, on s'intéresse aux cas où $r \leqslant 2$, et plus longuement au cas $r = 1$, qui donne de très bons critères pour comprendre les corps C_1. Nous ferons par ailleurs le lien avec ce qui a été vu dans les parties précédentes.

4.1 LA COHOMOLOGIE DE GROUPE

Dans cette partie on donne d'abord la définition, pour un groupe fini G donné, de la cohomologie de groupe fini $H^i(G, A)$, où A est un G-module. On généralise ensuite la définition pour les cas où G est un groupe profini, et pour les cas où A n'est plus commutatif.
On va essayer, de manière succincte et sans tout démontrer, de donner au lecteur une bonne idée de ce qu'est la cohomologie de groupe. Ceci permettra alors dans les sections suivantes, d'établir les liens entre dimension cohomologique et propriété C_r.

4.1.1 • LA COHOMOLOGIE D'UN GROUPE FINI

Définition 24. Soit G un groupe, A un groupe abélien muni de l'addition, on dit que A est un G-module si A est muni d'une action : $G \times A \to A$, $(g, a) \mapsto ga$ de G, qui satisfait les conditions suivantes : pour tous $g_1, g_2 \in G$ et pour tous $a, b \in A$, on a
(1) $1a = a$;
(2) $g_1(a + b) = g_1a + g_1b$;
(3) $(g_1g_2)a = g_1(g_2a)$.

Définition 25. Soient A, B deux G-modules et $f : A \to B$ un homomorphisme. On appelle f un G-homomorphisme si pour tout $g \in G$ et tout $a \in A$, on a $f(ga) = gf(a)$. On note $Hom_G(A, B)$ l'ensemble des tous les G-homomorphismes de A à B.

On rappelle quelques notions sur les modules libres.

Définition 26. Soit M un module. On dit qu'un sous-ensemble B de M est une base, si et seulement si,

1. tout élément de M est combinaison linéaire d'éléments de B ;
2. pour toutes familles finies $(e_i)_{1\leq i\leq n}$ d'éléments de B deux à deux distincts et $(a_i)_{1\leq i\leq n}$ d'éléments de l'anneau sous-jacent telles que $a_1e_1 + \cdots + a_ne_n = 0$, on a $a_1 = \cdots = a_n = 0$.

Définition 27. Un module libre est un module qui possède une base.

Définition 28. Pour un module M sur un anneau R, une résolution libre à droite de M est une suite exacte de R-modules (probablement infinie)

$$0 \leftarrow M \xleftarrow{d_0} E_0 \xleftarrow{d_1} E_2 \leftarrow \cdots$$

telle que chaque E_i est un R-module libre.

On va définir les groupes de cohomologie d'un groupe fini G. Les G-modules sont naturellement les modules sur l'anneau $\mathbb{Z}[G]$. On commence par introduire une résolution libre à droite du G-module $\mathbb{Z}$ muni de l'action triviale.

Un q-uplet $(g_1, g_2, \cdots, g_q) \in G^q$ est appelé une q-cellule. Soit X_q le G- module libre généré par toutes les q-cellules, c'est-à-dire,

$$X_q = \bigoplus \mathbb{Z}[G](g_1, g_2, \cdots, g_q)$$

et pour $q = 0$ on prend $X_0 = \mathbb{Z}[G]$.

Puis on va définir les morphismes ϵ et d_i comme ci-dessous :

$$\begin{array}{rccc} \epsilon : & X_0 & \to & \mathbb{Z} \\ & \sum_{g\in G} C_g g & \mapsto & \sum_{g\in G} C_g. \\ d_1 : & X_1 & \to & X_0 \\ & (g) & \mapsto & g-1. \end{array}$$

$$\begin{array}{rccl} d_q : & X_q & \longrightarrow & X_{q-1} \\ & d_q(g_1, \cdots, g_q) & = & g_1(g_2, \cdots, g_q) \\ & & & +\sum_{i=1}^{q-1}(-1)^i(g_1, \cdots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \cdots, g_q) \\ & & & +(-1)^q(g_1, \cdots, g_{q-1}). \end{array}$$

On peut vérifier qu'on a obtenu de la sorte une suite exacte de G-modules :

$$0 \leftarrow \mathbb{Z} \xleftarrow{\epsilon} X_0 \xleftarrow{d_1} X_1 \xleftarrow{d_2} X_2 \xleftarrow{d_3} \cdots$$

Maintenant, pour un G-module A, par la suite exacte ci-dessus, on a un complexe (qui n'est plus exact en général) :

$$Hom_G(X_0, A) \xrightarrow{\partial_1} Hom_G(X_1, A) \xrightarrow{\partial_2} Hom_G(X_2, A) \to \cdots$$

Avec $\operatorname{Im} \partial_q \subseteq \ker \partial_{q+1}$. Alors les groupes de cohomologie sont définis par

$$H^q(G, A) = \ker \partial_{q+1} / \operatorname{Im} \partial_q$$

Remarque 5. La résolution libre que l'on prend ici est appelée la résolution standard. En fait on peut calculer la cohomologie de groupe G avec les coefficients dans A à partir de n'importe quelle résolution libre de $\mathbb{Z}$ en suivant les étapes ci-dessus. Les résultats sont indépendants du choix de la résolution libre.

On se propose d'étayer les cas correspondant à de petites dimensions. On appelle les éléments de $\ker \partial_{q+1}$ "q-cocycles" et les éléments de $\operatorname{Im} \partial_q$ "q-cobords". On peut écrire formellement ces ensembles pour les petites dimensions :

$\ker \partial_1 = \{x \in A : \forall g \in G, (\partial_1 x)(g) = gx - x = 0\}$, et on note $\ker \partial_1 = A^G$. Alors $H^0(G, A) = A^G$.

$\ker \partial_2 = \{x \in Hom_G(X_1, A) : \forall g_1, g_2 \in G, x(g_1 g_2) = g_1 x(g_2) + x(g_1)\}$.

$\operatorname{Im} \partial_1 = \{x \in Hom_G(X_1, A) : \forall g \in G, x(g) = gx - x\}$.

On remarque que

$$Hom_G(X_0, A) = Hom_G(\mathbb{Z}[G], A) = A$$

Et pour $q \geqslant 1$, on peut identifier $Hom_G(X_q, A)$ avec l'ensemble des applications $G^q \to A$.

Pour le cas $q = 1$, on a l'expression suivante :

$$\begin{array}{rl} \partial_1 : & A \to Hom_G(X_1, A) \\ & (\partial_1 x)(g) = gx - x, \ \ \forall g \in G \text{ et } x \in A \end{array}$$

et dans le cas général :

$$\begin{array}{rlll} \partial_q : & Hom_G(X_{q-1}, A) & \longrightarrow & Hom_G(X_q, A) \\ & (\partial_q x)(g_1, \cdots, g_q) & = & g_1 x(g_2, \cdots, g_q) \\ & & & + \sum_{i=1}^{q-1} (-1)^i x(g_1, \cdots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \cdots, g_q) \\ & & & + (-1)^q x(g_1, \cdots, g_{q-1}) \end{array}$$

où x est une application $G^q \to A$.

Exemple 7. Si l'action d'un groupe G sur un G-module A est triviale, alors $\ker \partial_2 = Hom(G, A)$ et $\operatorname{Im} \partial_1 = 0$. D'où

$$H^1(G, A) = Hom(G, A).$$

En particulier, si $A = \mathbb{Q}/\mathbb{Z}$, on a le groupe dual

$$H^1(G, \mathbb{Q}/\mathbb{Z}) = Hom(G, \mathbb{Q}/\mathbb{Z}) = \chi(G).$$

Définition 29. Soit G un groupe fini. Un G-module A est dit G-induit s'il peut être répresenté comme

$$A = \bigoplus_{g \in G} gD$$

où $D \subset A$ est un sous-groupe.

Par exemple, $\mathbb{Z}[G] = \bigoplus_{g \in G} g(\mathbb{Z}.1)$ est G-induit. Soit D un groupe abélien, alors

$$\mathbb{Z}[G] \otimes D \simeq \bigoplus_{g \in G} g(\mathbb{Z} \otimes D)$$

est encore G-induit.

Proposition 23. La cohomologie d'un module induit est nulle en degré supérieur ou égal à 1.

Démonstration. Soient G un groupe fini et A un G-module induit. Soit $A = \bigoplus_{g \in G} gD$, alors on a une bijection entre $Hom_G(X_q, A)$ et $Hom_{\mathbb{Z}}(X_q, D)$. Les X_q sont des modules libres sur $\mathbb{Z}$, donc le complexe de cochaînes

$$Hom_{\mathbb{Z}}(X_0, D) \to Hom_{\mathbb{Z}}(X_1, D) \to Hom_{\mathbb{Z}}(X_2, D) \to \cdots$$

est exact, c'est-à-dire que le complexe

$$Hom_G(X_0, A) \to Hom_G(X_1, A) \to Hom_G(X_2, A) \to \cdots$$

est exact, alors $H^q(G, A) = 0$ pour tout $q \geq 1$.

□

Exemple 8. En guise d'exemple, on calcule les groupes de cohomologie d'un groupe cyclique $C_n = \mathbb{Z}/n\mathbb{Z}$ avec des coefficients dans $\mathbb{Z}$ (avec l'action triviale). Soit σ un générateur de C_n. On a une résolution libre de $\mathbb{Z}$ comme un $\mathbb{Z}[C_n]$-module :

$$0 \leftarrow \mathbb{Z} \leftarrow \mathbb{Z}[C_n] \xleftarrow{\sigma-1} \mathbb{Z}[C_n] \xleftarrow{N} \mathbb{Z}[C_n] \xleftarrow{\sigma-1} \mathbb{Z}[C_n] \xleftarrow{N} \mathbb{Z}[C_n] \leftarrow \cdots$$

où $N = 1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1}$. On peut utiliser cette résolution pour calculer la cohomologie. Soit σ le générateur de C_n, alors

$$\mathbb{Z}[C_n] = \bigoplus_{i=0}^{n-1} \mathbb{Z}.\sigma^i$$

Pour tout $c_0 + c_1\sigma + \cdots + c_{n-1}\sigma^{n-1} \in \mathbb{Z}[C_n]$, si $f \in Hom_{C_n}(\mathbb{Z}[C_n], \mathbb{Z})$, on a alors

$$\begin{aligned} f(c_0 + c_1\sigma + \cdots + c_{n-1}\sigma^{n-1}) &= f(c_0) + f(c_1\sigma) + \cdots + f(c_{n-1}\sigma^{n-1}) \\ &= f(c_0) + \sigma.f(c_1) + \cdots + \sigma^{n-1}.f(c_{n-1}) \\ &= f(c_0) + f(c_1) + \cdots + f(c_{n-1}) \\ &= (c_0 + c_1 + \cdots c_{n-1})f(1) \end{aligned}$$

Ainsi, un C_n-homomorphisme f de $\mathbb{Z}[C_n]$ dans $\mathbb{Z}$ ne dépend que de valeur de $f(1)$,

$$Hom_{C_n}(\mathbb{Z}[C_n], \mathbb{Z}) = \mathbb{Z},$$

Le complexe de cochaînes s'écrit alors

$$\mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{n} \mathbb{Z} \to \cdots .$$

Par conséquent,

$$H^n(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = \begin{cases} \mathbb{Z} & n = 0; \\ 0 & n = 1, 3, 5, \cdots \\ \mathbb{Z}/n\mathbb{Z} & n = 2, 4, 6, \cdots \end{cases}$$

Similairement, si A est un groupe abélien muni d'action triviale de C_n, alors

$$H^n(\mathbb{Z}/n\mathbb{Z}, A) = \begin{cases} A & n = 0; \\ A[n] & n = 1, 3, 5, \cdots \\ A/nA & n = 2, 4, 6, \cdots \end{cases}$$

où $A[n] = \{a \in A : na = 0\}$.

4.1.2 • LA COHOMOLOGIE DE GROUPE PROFINI

Pour considérer la cohomologie du groupe de Galois absolu $Gal(k^{sep}/k)$, on a besoin de généraliser la définition de la cohomologie pour les groupes profinis (les limites projectives des groupes finis). Tout d'abord on a besoin des groupes munis de structure topologique.

Définition 30. Un groupe topologique est un groupe $(G, \cdot)$ muni d'une topologie pour laquelle les applications

$$G \times G \to G, \quad (g_1, g_2) \mapsto g_1 \cdot g_2$$

et

$$G \to G, \quad g \mapsto g^{-1}$$

sont continues ($G \times G$ étant muni de la topologie produit).

Par exemple, si on a un groupe G, supposons que G soit muni de la topologie discrète. Alors G est un groupe topologique parce que toutes les applications sont continues sous la topologie discrète.

Définition 31. Un homomorphisme entre deux groupes topologiques est un homomorphisme de groupe continu.

Un isomorphisme entre deux groupes topologiques est un isomorphisme de groupes et un homéomorphisme d'espaces topologiques en même temps.

Les groupes topologiques et les homomorphismes constituent une catégorie. On s'intéresse aux limites projectives dans cette catégorie : en fait, on a déjà manipulé une limite projective sans le dire lorsqu'on a parlé des corps $\mathbb{Q}_p$. On va voir que $\mathbb{Z}_p$ pour p premier peut être vu comme la limite projective des $\mathbb{Z}/p^n\mathbb{Z}$. On définit d'abord ce qu'est un système projectif :

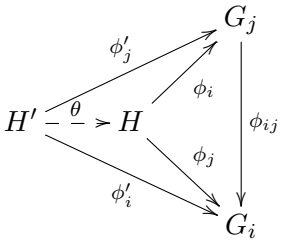
Définition 32. Soit $(I, \leq)$ un ensemble ordonné. On considère une famille de groupes topologiques $(G_i)_{i\in I}$ et pour tout couple $(i, j) \in I^2$ tel que $i \leqslant j$ un homomorphisme $\phi_{ij} : G_j \longrightarrow G_i$. On dit que le système $((G_i)_{i\in I}, (\phi_{ij}))$ est projectif si :

— $\forall i \in I, \phi_{ii} = \mathrm{Id}_{G_i}$

— $\forall i, j, k \in I, i \leqslant j \leqslant k \implies \phi_{ik} = \phi_{ij} \circ \phi_{jk}$

Lorsque ces conditions sont vérifiées, on peut montrer que la limite projective existe, au sens suivant :

Proposition 24. Soit $((G_i)_{i\in I}, (\phi_{ij}))$ un système projectif de groupe topologique. Il existe un groupe topologique H, qui est unique à isomorphisme près, et une famille d'homomorphismes $\phi_i : H \to G_i$ vérifiant la propriété suivante : $\forall i, j, i \leqslant j \implies \phi_i = \phi_{ij} \circ \phi_j$. et vérifiant une propriété universelle : Si H' est un groupe topologique et pour $i \in S'$, $\phi'_i : S' \to E_i$ est une famille d'applications vérifiant la propriété $\forall i, j\ , i \leqslant j \implies \phi'_i = \phi_{ij} \circ \phi'_j$, alors il existe un unique homomorphisme $\theta : H' \to H$ tel que $\phi'_i = \phi_i \circ \theta$.



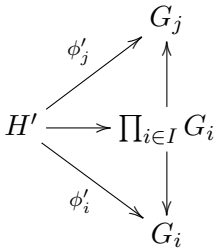
Démonstration.

Existence : Soit $\prod_{i\in I} G_i$ le produit de tous les groupes, muni de la topologie de produit. Soit H l'ensemble de toutes les applications

$$f : I \to \bigcup_{i\in I} G_i$$

telles que $\phi_{ij}(f(j)) = f(i)$ pour tout $i \leqslant j$. Si $f_1, f_2 \in H$, alors $\phi_{ij}((f_1 f_2)(j)) = f_1(i) f_2(i)$ pour tout $i \leqslant j$, ce qui implique $f_1 f_2 \in H$. Alors H est un sous-groupe de $\prod_{i\in I} G_i$, muni de la topologie comme un sous-espace de $\prod_{i\in I} G_i$. Alors H est un groupe topologique.

On va vérifier la propriété universelle pour H. D'abord, $\prod_{i\in I} G_i$ est l'objet de produit dans la catégorie de groupes topologiques. Alors il existe un homomorphisme $H' \to \prod_{i\in I} G_i$, tel que le diagramme suivant est commutatif,



Soit $h' \in H'$ et h son image dans $\prod_{i\in I} G_i$. Puisque $\phi'_i = \phi_{ij} \circ \phi'_j$, $h(j) = \phi'_j(h')$, $h(i) = \phi'_i(h')$, alors

$$h(i) = \phi'_i(h') = \phi_{ij}(\phi'_j(h')) = \phi_{ij}(h(j)).$$

D'après notre définition de H, l'image de H' dans $\prod_{i\in I} G_i$ est contenue dans $H \subset \prod_{i\in I} G_i$. Ainsi, il existe un homomorphisme $\theta : H' \to H$ tel que $\phi'_i = \phi_i \circ \theta$ pour tout $i \in I$.

Unicité : Soient H, H' sont deux groupes topologiques qui satisfont la propriété universelle. Alors il existe un unique homomorphimse $\theta : H' \to H$ et un unique $\theta' : H \to H'$ tels $\phi'_i = \phi_i \circ \theta$ et $\phi_i = \phi'_i \circ \theta'$. Alors $\theta \circ \theta'$ est un homomorphisme $H \to H$ qui satisfait que $\phi_i = \phi_i \circ \theta \circ \theta'$. Mais id_H est aussi l'homomorphisme qui satisfait cette condition et doit être en plus unique. Donc $\theta \circ \theta' = id_H$. On a aussi $\theta' \circ \theta = id_{H'}$ par le même moyen. Alors H et H' sont isomorphes.

□

Définition 33. Le groupe topologique H défini précedemment est appelé limite projective du système $((G_i)_{i\in I}, (\phi_{ij}))$ et on le note $\varprojlim G_i$. Cette limite est unique à isomorphisme près.

Définition 34. Un groupe G est dit profini s'il est limite projective d'un système projectif de groupes finis et d'homomorphismes de groupes, où les groupes finis sont munis de topologie discrète.

Exemple 9. Les groupes finis sont profinis.

Exemple 10. On arrive bien à montrer que $\mathbb{Z}_p$ est une limite projective. En effet, dans la partie 2.1, on avait introduit des morphismes que l'on qualifiait de compatibles, entre $\mathbb{Z}/p^{n+1}\mathbb{Z}$ et $\mathbb{Z}/p^n\mathbb{Z}$. Cela correspond en fait aux applications constituant un système projectif. Soit $G_n = \mathbb{Z}/p^{n+1}\mathbb{Z}$ muni d'une topologie discrète pour tout $n \geqslant 0$. Soit

$$f_{mn} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$$

l'homomorphisme canonique pour tout $m \geqslant n$. Ainsi on peut vérifier que $((G_n), (f_{mn}))$ est un système projectif. Donc l'anneau d'entiers p-adiques $\mathbb{Z}_p$ s'écrit

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

Pour avoir une intuition de $\mathbb{Z}_p$, à partir de la construction de la limite projective, les éléments de $\mathbb{Z}_p$ peuvent être vus comme les suites $(a_n)_{n\geqslant 0}$ telles que

$$a_n \in \mathbb{Z}/p^n\mathbb{Z} \quad \text{et} \quad a_n \equiv a_{n+1} \mod p^n.$$

Exemple 11. Le groupe de Galois absolu $Gal(k^{sep}/k)$ d'un corps k est profini. En effet, par définition de la limite projective, il est limite projective des $Gal(L/k)$ quand L parcourt les extensions galoisiennes finies de k.

Par exemple, soit $\mathbb{F}_q$ un corps fini constitué de q éléments. On note $\mathbb{F}_{q^n}$ le corps de décomposition du polynôme $X^{q^n-1}-1$ sur $\mathbb{F}_q$. On peut montrer que la clôture séparable de $\mathbb{F}_q$ est exactement

$$\bar{\mathbb{F}_q} = \bigcup_{n\geqslant 1} \mathbb{F}_{q^n},$$

qui est aussi la clôture algébrique.De plus $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \mathbb{Z}/n\mathbb{Z}$. Si $n|m$, alors l'inclusion $\mathbb{F}_{q^n} \subset \mathbb{F}_{q^m}$ implique un homomorphisme de groupes $Gal(\mathbb{F}_{q^m}/\mathbb{F}_q) \to Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Par conséquent, les groupes de Galois $(Gal(\mathbb{F}_{q^n}/))_{n\geqslant 1}$ et ces homomorphismes constituent un système projectif de groupes finis. En notant $\hat{\mathbb{Z}}$ la limite projective du système composé de tous les $\mathbb{Z}/n\mathbb{Z}$:

$$Gal(\mathbb{F}_q^{sep}/\mathbb{F}_q) = \varprojlim Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$$

est un groupe profini.

Exemple 12. Tout sous groupe fermé d'un groupe profini est profini.

Pour un groupe profini, on peut définir l'indice d'un sous-groupe fermé même si celui-ci n'est pas toujours d'indice fini. Cela se fait grâce à la notion de nombre surnaturel. Par définition, un nombre surnaturel est le produit formel $\prod_p p^{n_p}$, où p parcourt l'ensemble des nombres premiers et $n_p \in \mathbb{N} \cup \{\infty\}$. On définit, de manière analogue aux définitions dans $\mathbb{N}$, le ppcm,le pgcd et le produit d'une famille quelconque de nombres surnaturels.

Définition 35. Soit G un groupe profini. Soit H un sous-groupe fermé de G.

L'indice de H dans G noté $[G : H]$ est le nombre surnaturel défini comme le ppcm des $[G/U : H/(H \cap U)]$ (qui sont des entiers naturels) quand U parcourt l'ensemble des sous-groupes ouverts distingués de G. L'ordre d'un groupe profini est le nombre surnaturel $[G : \{1\}]$.

Il est important de noter que "d'indice fini" au sens usuel veut dire la même chose que d'indice fini au sens de la définition précédente. Pour s'en convaincre, on peut prouver le lemme suivant :

Lemme 10. Soit H un sous-groupe fermé d'un groupe profini G . Alors H est d'indice fini (au sens usuel) si et seulement si $[G : H]$ (défini comme dans la définition) est un entier naturel. De plus dans ce cas $[G : H]$ est l'indice de H au sens usuel. En particulier H est ouvert si et seulement si le nombre surnaturel $[G : H]$ est un entier naturel.

La dernière proposition du lemme 10 est très intéressante car elle permet de caractériser une propriété topologique d'un sous-groupe fermé d'un groupe profini, par une propriété arithmétique souvent aisée à manipuler.

Maintenant on retourne à la cohomologie. On suppose que le G-module A est muni d'une action continue de G.

Définition 36. Soit G un groupe profini et A un G-module muni de la topologie discrète, on dit que A est un G-module discret si l'action de $G : G \times A \to A$ est une application continue.

En fait, pour un groupe profini G et un $G-$module discret A, on peut remplacer dans la construction de la cohomologie, $Hom_G(X_q, A) = \{\text{les applications } x : G^q \to A\}$ par $C^q(G, A)$, qui est l'ensemble des applications continues de G^q dans A. En se restreignant aux applications continues, on peut finalement définir la cohomologie d'un groupe profini.

Définition 37. Soient G un groupe profini et A un G-module discret, $C^q(G,A)$ l'ensemble de toutes les applications continues de G^q dans A. Introduisons l'application $\partial_q : C^{q-1}(G,A) \to C^q(G,A)$:

$$\begin{aligned}(\partial_q x)(g_1,\cdots,g_q) =& g_1 x(g_2,\cdots,g_q)\\ &+\sum_{i=1}^{q-1}(-1)^i x(g_1,\cdots,g_{i-1},g_ig_{i+1},g_{i+2},\cdots,g_q)\\ &+(-1)^q x(g_1,\cdots,g_{q-1})\end{aligned}$$

On a alors un complexe de cochaînes $C^*(G,A) = ((C^q(G,A),(\partial_q))$. On appelle

$$H^q(G,A) = \ker \partial_{q+1}/\operatorname{Im}\partial_q$$

les groupes de cohomologie de G à coefficients dans A.

4.1.3 • LA FONCTORIALITÉ ET LA SUITE EXACTE DE COHOMOLOGIE

Étant donnée la définition de $H^q(G,A)$, on se demande ce qui change lorsqu'on remplace A par un autre G-module B. Si $f : A \to B$ est un homomorphisme de G-modules, alors il induit un homomorphisme de complexes de cochaînes $f_* : C^*(G,A) \to C^*(G,B)$, c'est-à-dire, on a des homomorphismes

$$f_* : C^n(G,A) \to C^n(G,B), \quad x(g_1,\cdots,g_n) \mapsto fx(g_1,\cdots,g_n)$$

tels que le diagramme

$$\begin{array}{ccccccc}\cdots & \longrightarrow & C^n(G,A) & \xrightarrow{\partial_n} & C^{n+1}(G,A) & \longrightarrow & \cdots\\ & & \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle f_*} & & \\ \cdots & \longrightarrow & C^n(G,B) & \xrightarrow{\partial_n} & C^{n+1}(G,B) & \longrightarrow & \cdots\end{array}$$

est commutatif. On peut ensuite montrer que cet homomorphisme de complexes de cochaînes induit des homomorphismes de groupes de cohomologie

$$H^n(G,A) \to H^n(G,B).$$

On peut obtenir quelques résultats en utilisant l'algèbre homologique. Voici un théorème dont la démonstration ne sera pas donnée ici, qui permet d'établir l'existence d'une suite exacte longue de cohomologie.

Théorème 23. Etant donnée une suite exacte de G-modules

$$0 \to A \to B \to C \to 0,$$

il existe des homomorphismes

$$\delta : H^n(G,C) \to H^{n+1}(G,A)$$

tels que l'on a une suite exacte

$$0 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G,A) \to \cdots$$

$$\cdots \to H^n(G,A) \to H^n(G,B) \to H^n(G,C) \xrightarrow{\delta} H^{n+1}(G,A) \to \cdots.$$

On appelle les δ les homomorphismes de transition.
Maintenant on regarde les cas où G, A sont tous changés au profit de G', A'.

Définition 38. Soient G, G' deux groupes profinis et $\phi : G' \to G$ un homomorphisme. Soient A un G-module discret et A' un G'-module discret, $f : A \to A'$ un homomorphisme tel que pour tout $a \in A$, $g' \in G'$, $f(\phi(g')a) = g'f(a)$. Alors on appelle un tel couple $(\phi, f) : (G, A) \to (G', A')$ un morphisme de paires (G, A).

Un tel homomorphisme de paires induit des homomorphismes

$$(\phi, f)_* : C^n(G, A) \to C^n(G', A'), \quad x \mapsto f \circ x \circ \phi.$$

Ils commutent avec ∂, ils induisent donc des homomorphismes

$$H^n(G, A) \to H^n(G', A')$$

Lorsque H est un sous-groupe fermé de G et $A = A'$ est un G-module discret, le couple compatible de $H \hookrightarrow G$ et $A \xrightarrow{id} A$ induit un homomorphisme de restriction

$$Res : H^n(G, A) \to H^n(H, A).$$

Lorsque H est un ouvert d'indice fini n dans G, fixant un élément g dans chaque classe à droite de $H\backslash G$, on définit un homomorphisme

$$cor : C^n(H, A) \to C^n(G, A)$$

par

$$(corx)(g_1, \cdots, g_n) = \sum_{g \in H\backslash G} \bar{g}^{-1} x(\bar{g}g_1 g\bar{g_1}^{-1}, \cdots, \bar{g}g_n g\bar{g_n}^{-1})$$

On peut vérifier que les cor sont bien définits et commutent avec ∂. Alors on a un homomorphisme de corestriction

$$Cor : H^n(H, A) \to H^n(G, A).$$

Par exemple en degré 0, $Cor : A^H \to A^G$ s'écrit explicitement

$$Cor(a) = \sum_{g \in H\backslash G} ga.$$

Proposition 25. Soit H un sous-groupe ouvert de G, alors

$$Cor \circ Res = [G : H].$$

Remarque 6. En degré 0,

$$A^G \xrightarrow{Res} A^H \xrightarrow{Cor} A^G,$$

pour un $a \in A^G$,

$$Cor \circ Res(a) = \sum_{g \in H\backslash G} ga = |H\backslash G|a = [G : H]a.$$

Par la proposition suivante, on va voir que l'on peut faire l'échange librement entre le foncteur H^q et la limite inductive de paires (G, A).

Proposition 26. Soit $(G_i)_i$ un système projectif de groupes profinis et $(A_i)_i$ un système inductif de G_i-modules discrets (où les morphismes $A_i \to A_j$ sont compatibles avec les morphismes $G_j \to G_i$). Alors pour tout $q \geqslant 0$,

$$H^q(\varprojlim G_i, \varinjlim A_i) = \varinjlim H^q(G_i, A_i)$$

Cette proposition permet de ramener des problèmes de cohomologie sur des groupes profinis, à de la cohomologie sur des groupes finis. On en verra un exemple au corollaire 3, qui nécessite d'abord d'introduire les groupes de torsion.

Définition 39. Un groupe est appelé un groupe de torsion si tous ses éléments sont d'ordre fini.

Proposition 27. Un groupe abélien A est un groupe de torsion si et seulement si $A \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.

Corollaire 3. Soient G un groupe profini et A un G-module discret. Pour tout $q \geqslant 1$, les groupes $H^q(G, A)$ sont des groupes de torsion.

Pour le montrer, voyons d'abord le cas où G est un groupe fini.

Lemme 11. Soit G un groupe fini, $|G| = m$. Alors pour tout $n \geqslant 1$ et tout G-module A, on a

$$mH^n(G, A) = 0, \quad n \geqslant 1$$

Démonstration. D'après la proposition 25, on prend $H = \{1\}$. Alors $Cor \circ Res = [G : H] = m$. Mais $H^n(\{1\}, A) = 0$ pour tout $n \geqslant 1$. Alors $H^n(G, A)$ est annulé par m pour tout $n \geqslant 1$. □

Démonstration. [Démonstration du Corollaire 3] D'après le lemme précédent, pour tout $n \geqslant 1$, $H^n(G, A)$ sont des groupes de torsion lorsque G est fini. En utilisant la proposition 26,

$$H^n(G, A) = \varinjlim H^n(G/U, A^U)$$

où U parcourt tous les sous-groupes ouverts de G. On en déduit que $H^n(G, A)$ est une limite des groupes de torsion, ainsi $H^n(G, A)$ est un groupe de torsion ($H^n(G, A) \otimes_{\mathbb{Z}} \mathbb{Q} = \varinjlim H^n(G/U, A^U) \otimes_{\mathbb{Z}} \mathbb{Q} = 0$).

□

Exemple 13. Soit G un groupe profini, $\mathbb{Q}$ est muni d'action triviale de G. D'après le corollaire 11, pour tout $n \geqslant 1$, $H^n(G, \mathbb{Q})$ est un groupe de torsion. Mais $H^n(G, \mathbb{Q})$ est aussi un $\mathbb{Q}$-espace vectoriel. Alors pour tout $n \geqslant 1$, $H^n(G, \mathbb{Q}) = 0$.

Par ailleurs, la suite exacte

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

induit une suite exacte

$$H^1(G, \mathbb{Q}) \to H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z}) \to H^2(G, \mathbb{Q})$$

Donc on a un isomorphisme

$$H^2(G, \mathbb{Z}) \simeq H^1(G, \mathbb{Q}/\mathbb{Z}) = Hom(G, \mathbb{Q}/\mathbb{Z}) = \chi(G).$$

4.1.4 • LA DIMENSION COHOMOLOGIQUE

Maintenant on va définir la dimension cohomologique d'un groupe. Soit p un nombre premier. On note

$$A[n] = \{a \in A : na = 0\},$$
$$A[p^\infty] = \bigcup_{n \geqslant 1} A[p^n].$$

Rappelons qu'un groupe abélien de torsion A est dit p-primaire si tout élément de A est d'ordre une puissance de p. Tout groupe abélien de torsion A est somme directe (pour p premier) de ses composantes p-primaires $A[p^\infty]$. Un G-module discret est simple s'il est non nul et n'admet pas de sous G-module autre que 0 et lui-même.

Définition 40. Pour un groupe profini G et un nombre premier p, on note $cd_p(G)$ le plus petit nombre $n \in \mathbb{N} \cup \{\infty\}$ tel que pour tout G-module discret de torsion A et pour tout $q > n$, la composante p-primaire de $H^q(G, A)$ est nulle. On appelle $cd_p(G)$ la p-dimension cohomologique et la dimension cohomologique est définie par $cd(G) = \sup_p cd_p(G)$.

Proposition 28. Soient G un groupe profini et A un G-module discret simple annulé par p, on a $cd_p(G) \leqslant n$ si et seulement si $H^{n+1}(G, A) = 0$.

Il est important de noter que la notion de p-dimension cohomologique est importante pour les groupes profinis. Elle est surtout intéressante pour les groupes infinis.

En effet, on peut montrer que la p-dimension cohomologique d'un groupe fini est soit nulle (si p ne divise pas son cardinal) ou infinie dans le cas contraire.

Exemple 14. On a l'égalité $cd_p(\hat{\mathbb{Z}}) = 1$ pour tout nombre premier p. On va le montrer dans l'exemple 22.

4.1.5 • LA COHOMOLOGIE DE PRO-p-GROUPE

Nous allons maintenant définir ce qu'est un p-Sylow d'un groupe profini, et en énoncer quelques propriétés. Il est vital d'introduire cette notion, puisqu'elle servira à démontrer le résultat souhaité sur la dimension cohomologique pour les corps C_1, plus particulièrement dans l'équivalence fondamentale de la proposition 38, en section 4.3.2.

Définition 41. On dit que G est un pro-p-groupe si son ordre est une puissance de p.

Un p-groupe de Sylow (ou p-Sylow) d'un groupe profini G est un sous groupe fermé H de G qui est un p-pro-groupe et tel que l'indice $[G : H]$ est premier avec p.

Proposition 29. Soit G_p un p-Sylow de G un groupe profini. Alors $cd_p(G) = cd_p(G_p) = cd(G_p)$.

Exemple 15. Le groupe additif $\mathbb{Z}_p$ est un p-groupe de Sylow de $\hat{\mathbb{Z}}$. Ceci vient notamment du lemme chinois, qui implique que $\hat{\mathbb{Z}}$ est le produit des $\mathbb{Z}_p$ pour p premier. Alors

$$cd(\mathbb{Z}_p) = cd_p(\mathbb{Z}_p) = cd_p(\hat{\mathbb{Z}}) = 1.$$

Le théorème suivant nous donne un critère important permettant de majorer la p-dimension cohomologique d'un pro-p-groupe :

Théorème 24. Soit G un pro-p-groupe et $n \in \mathbb{N}$. Alors $cd_p(G) \leqslant n$ si et seulement si $H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0$.

Démonstration. Ce résultat découle en fait de la proposition 29 et du lemme 12, qui sont admis. Si $cd_p(G) \leqslant n$, alors $H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0$ d'après la définition. Réciproquement, supposons que $H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0$. D'après la propostion 28, il suffit de démontrer les cas où A est un G-module discret simple annulé par p. On peut montrer que A est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ grâce au lemme suivant. □

Lemme 12. Soit G un pro-p-groupe. Alors tout G-module discret annulé par p est simple est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

4.1.6 • LA COHOMOLOGIE NON-ABÉLIENNE

On se propose finalement d'élargir les définitions de H^0 et H^1 à un cadre plus large, dans lequel le G-module A n'est pas nécessairement commutatif. On peut alors parler de cohomologie non-abélienne.

Définition 42. Soient G un groupe profini et A un groupe. On dit que A est un G-groupe s'il est muni d'une action de G qui satisfait les conditions suivantes :

1. L'action $(g, a) \mapsto {}^g a$ est une application continue de $G \times A$ dans A ;
2. ${}^1 a = a$ pour tout $a \in A$;
3. ${}^{gh}a = {}^g({}^h a)$ pour tout $g, h \in G$ et $a \in A$;
4. ${}^g(a_1 a_2) = {}^g a_1 \, {}^g a_2$ pour tous $g \in G$ et $a_1, a_2 \in A$.

Définition 43. Soit A un G-groupe. On définit $H^0(G, A) = A^G$. On appelle une application $G \to A$, $g \mapsto x(g)$ un 1-cocycle, si pour tous $g, h \in G$, on a $x(gh) = x(g)^g x(h)$. On note $Z^1(G, A)$ l'ensemble de tous les 1-cocycles. Deux 1-cocycles x, y sont dits cohomologues, s'il existe un $a \in A$ tel que pour tout $g \in G$, on a $y(g) = a^{-1} x(g)^g a$. C'est une relation d'équivalence sur $Z^1(G, A)$ et on note l'ensemble quotient $H^1(G, A)$.

On peut voir que les définitions de H^1 et H^2 coïncident avec les groupes de cohomologie de degrés 0 et 1 lorsque A est commutatif.

Théorème 25. Soient G un groupe et

$$1 \to A \to B \to C \to 1$$

une suite exacte de G-groupes. Alors il y a une suite exacte d'ensembles pointés

$$1 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(B, G) \to H^1(G, C).$$

Remarque 7. Un ensemble pointé est un ensemble X avec un élément distingué $x_0 \in X$, qui est appelé le point de base. On dit qu'une application $f : X \to Y$ est un morphisme de l'ensemble pointé (X, x_0) dans (Y, y_0) si $f(x_0) = y_0$. Dans ce théorème, supposons que les éléments d'identité de A^G, B^G, C^G sont leur points de base. Dans $H^1(G, A), H^1(G, B), H^1(G, C)$, les points de base sont leurs classes du cocycle unité. On parle de suite d'ensembles pointés

$$\cdots \to (X, x_0) \xrightarrow{f} (Y, y_0) \xrightarrow{g} (Z, z_0) \to \cdots$$

dans le terme (Y, y_0), lorsque $f(X) = g^{-1}(z_0)$.

4.2 LA COHOMOLOGIE GALOISIENNE

Dans cette partie on abordera la méthode de la descente galoisienne, qu'on appliquera aux espaces vectoriels munis d'une action semi-linéaire du groupe de Galois.
Ensuite, ce travail préparatoire nous donnera assez d'outils pour nous intéresser à la cohomologie du groupe de Galois absolu d'un corps. C'est cette notion qu'on reliera, dans les sections suivantes, à la propriété C_i. En particulier, on énoncera le théorème de Hilbert 90.

4.2.1 • LA DESCENTE GALOISIENNE POUR LES ESPACES VECTORIELS

Soit K/k une extension galoisienne finie dont le groupe de Galois est $G = Gal(K/k)$. On note $G_k = Gal(k^{sep}/k)$

Définition 44. Soient K/k une extension galoisienne finie dont le groupe de Galois est $G = Gal(K/k)$, et V un espace vectoriel sur K. On dit d'une action de G sur K est semi-linéaire , si pour tout $g \in G$, $a \in K$ et $v \in V$, on a

$$g(av) = (ga)(gv).$$

On note $V^G := \{v \in V : gv = v \quad \forall g \in G\}$ le sous-espace de V fixé par G. Il est évidemment un espace vectoriel sur k.

Lemme 13. Soit W un espace vectoriel sur k. Alors on a un k-isomorphisme

$$\begin{array}{ccc} W & \to & (W \otimes_k K)^G \\ w & \mapsto & w \otimes 1 \end{array}$$

où G agit sur $W \otimes_k K$ via le deuxième facteur.

Démonstration. On écrit W comme une somme directe d'espaces de dimension 1 sur une base de vecteurs dans k : $(e_1, \ldots, e_n)$

$$W = \bigoplus_{i=1}^{n} ke_i$$

D'après la théorie de Galois, on sait que $K^G = k$. Alors

$$(ke_i \otimes_k K)^G \simeq ke_i$$

Donc :

$$(W \otimes_k K)^G = \bigoplus_{i=1}^{n} (ke_i \otimes_k K)^G \simeq \bigoplus_{i=1}^{n} ke_i = W.$$

□

Lemme 14 (Speiser)**.** Soit V un k-espace vectoriel muni d'une action semi-linéaire de G. Alors on a un K-isomorphisme

$$\begin{array}{rccc} \lambda : & V^G \otimes_k K & \to & V \\ & v \otimes a & \mapsto & av \end{array}$$

Démonstration. On considère l'application naturelle

$$\lambda_K : (V \otimes_k K)^G \to V \otimes_k K,$$

où l'action de G sur K est triviale, et sur V comme dans le lemme. Par définition, $(V \otimes_k K)^G \simeq V^G \otimes_k K$, donc λ_K peut être identifiée avec l'application $(V^G \otimes_k K) \otimes_k K \to V \otimes_k K$ obtenue par produit tensoriel avec K qui est muni de l'action de G. λ est un isomorphisme si et seulement si λ_K est un isomorphisme. En regardant le produit tensoriel $K \otimes_k K$ où G agit trivialement sur le premier facteur et naturellement sur le second, on voit que

$$K \otimes_k K \simeq \bigoplus_{g \in G} K e_g,$$

où G agit sur la droite en permutant les éléments de base. Cette décomposition induit une décomposition du $K \otimes_k K$-module $V \otimes_k K$ comme une somme directe des K-espaces vectoriels $e_g(V \otimes_k K)$. En identifiant $e_1(V \otimes_k K)$ avec un K-espace vectoriel W muni d'une action triviale de G, on obtient un isomorphisme de $K[G]$-module $V \otimes_k K \simeq W^n$, où n est l'ordre de G et G agit sur la droite en permutant les facteurs. Alors les éléments de $(V \otimes_k K)^G$ correspondent à des éléments diagonaux de W^n, et la multiplication par e_g dans $V \otimes_k K$ correspond à mettre les composantes d'un vecteur dans W^n à 0 sauf celui indexé par g. De sorte que le $K \otimes_k K$-sous-module de $V \otimes_k K$ généré par $(V \otimes_k K)^G$ contient tous les éléments correspondant aux vecteurs de la forme $(0, 0, \cdots, w, 0, \cdots, 0)$ dans W^n. Ceci montre la surjectivité de λ_K, et son injectivité est une conséquence évidente de l'injectivité de l'application diagonale $W \to W^n$.

□

On a donc le corollaire suivant :

Corollaire 4. La catégorie des espaces vectoriels sur k et la catégorie des espaces vectoriels sur K munis d'action semi-linéaire de G sont équivalentes.

Ensuite on va voir que le groupe de cohomologie $H^1(Gal(K/k), Aut_K(K^n))$ classifie les actions semi-linéaires de G sur un K-espace vectoriel de dimension n. Étant donné une 1-cochaîne $x : G \to GL_n(K)$, on peut définir une action de G sur K^n comme

$$G \times K^n \to K^n, \quad (g, v) \to x(g)(gv).$$

Alors c'est une action semi-linéaire si et seulement si,

$$x(g_1g_2)(g_1g_2v) = x(g_1)(g_1x(g_2)(g_2v)), \quad \forall v \in K^n, g_1, g_2 \in G,$$

si et seulement si

$$x(g_1g_2)(v) = x(g_1)^{g_1}x(g_2)(v), \quad \forall v \in K^n, g_1, g_2 \in G,$$

si et seulement si

$$x_{g_1g_2} = {x_{g_1}}^{g_1}x_{g_2}, \quad \forall g_1, g_2 \in G,$$

si et seulement si x est un 1-cocycle.

Soient x, y deux 1-cocycles $G \to GL_n(K)$, V_x et V_y deux K-espaces vectoriels de dimension n munis des actions semi-linéaires de G définis respectivement par x et y. Soit $\phi : V_x \to V_y$ un isomorphisme de k-espaces vectoriels. Alors ϕ est un G-semi-linéaire isomorphisme si et seulement si

$$\phi(x(g)(gv)) = y(g)(g\phi(v)), \quad \forall v \in K^n, g \in G,$$

si et seulement si

$$y(g)(v) = \phi(x(g)(g\phi^{-1}(g^{-1}v))), \quad \forall v \in K^n, g \in G,$$

si et seulement si

$$y_g = \phi \circ x_g \circ {}^g\phi^{-1}, \quad \forall g \in G,$$

si et seulement si x, y sont cohomologues.

En conclusion, le groupe de cohomologie $H^1(Gal(K/k), GL_n(K))$ classifie les actions semi-linéaires de G sur un K-espace vectoriel de dimension n.

En même temps, on sait qu'à un K-espace vectoriel muni d'une action semi-linéaire de G de dimension n correspond exactement un k-espace vectoriel, qui est unique à isomorphisme près. Alors on a montré la proposition suivante.

Proposition 30 (Hilbert 90)**.** Pour une extension galoisienne K/k, on a, pour tout $n \geqslant 1$

$$H^1(Gal(K/k), GL_n(K)) \simeq 0$$

Corollaire 5.

$$H^1(Gal(K/k), K^\times) \simeq 0$$

Remarque 8. La proposition 30 est la version moderne de Hilbert 90. La version originale avait comme hypothèse : K/k est une extension cyclique.

Corollaire 6. Soit K/k une extension cyclique finie et soit σ un générateur du groupe de Galois $Gal(K/k)$. Alors pour tout $\alpha \in K$, si $N_{K/k}(\alpha) = 1$ alors $\alpha = \beta/\sigma(\beta)$ pour un certain $\beta \in K$ où $N_{K/k}$ est une norme de K vers k.

Citons maintenant trois applications intéressantes du théorème de Hilbert 90 qui découlent du corollaire 6.

L'utilisation du théorème de Hilbert 90, nous permet de trouver tous les triplets pythagoriciens c'est a dire tous les rationnels sur le cercle unité.

Application 1 : Soient a, b deux nombres rationnels tels que $a^2 + b^2 = 1$ alors il existe $c, d \in \mathbb{Z}$ tels que :

$$(a, b) = \left(\frac{c^2 - d^2}{c^2 + d^2}, \frac{2cd}{c^2 + d^2}\right)$$

Démonstration. La démonstration se fait en utilisant le théorème de Hilbert 90 à l'extension $\mathbb{Q}(i)/\mathbb{Q}$. En effet si $a^2 + b^2 = 1$ alors $\alpha = a + ib$ a pour norme 1 et d'après le corrolaire ci-dessus il existe $c + id \in \mathbb{Q}(i)$ tel que :

$$\alpha = a + ib = \frac{c + id}{\sigma(c + id)} = \frac{c + id}{c - id} = \frac{c^2 - d^2}{c^2 + d^2} + \frac{2icd}{c^2 + d^2}$$

□

Plus géneralement, en considérant l'extension $\mathbb{Q}(\sqrt{-D})/\mathbb{Q}$ pour $D > 0$ on peut montrer le corollaire suivant :

Corollaire 7. Soient a, b deux nombres rationnels tels que $a^2 + Db^2 = 1$ alors il existe $c, d \in \mathbb{Z}$ tels que :

$$(a, b) = \left(\frac{c^2 - Dd^2}{c^2 + Dd^2}, \frac{2cd}{c^2 + Dd^2}\right)$$

En utilisant encore le théorème de Hilbert 90, on peut prouver que toute extension cyclique de degré n peut être obtenue en adjoignant la racine n-ième d'un certain élement, si le corps de base contient une racine primitive de l'unité.
Application 2 : Soit k un corps et soit $n \geqslant 1$ un entier tel que $(char(k) \wedge n) = 1$. Supposons que k contienne une racine primitive n-ième de l'unité, ζ_n. Si K/k est une extension cyclique de degré n alors il existe $a \in F$ tel que $k = K(a^{1/n})$.
Cette extension est connue sous le nom d'extension de Kummer et la théorie de Kummer étudie ce genre d'extensions.
Une autre utilisation du théorème de Hilbert 90 nous permet d'obtenir le résultat suivant sur les fonctions rationnelles :
Application 3 : Soit $f \in \mathbb{C}(x)$ une fonction rationnelle satisfaisant

$$f(x)f(\zeta x)f(\zeta^2 x)...f(\zeta^{n-1}x) = 1$$

pour $\zeta = \zeta_n = \exp\left(\frac{2i\pi}{n}\right)$. Alors il existe $g(x) \in \mathbb{C}(x)$ tel que

$$f(x) = \frac{g(x)}{g(\zeta x)}.$$

Exemple 16. Si $f(x) = \zeta$ alors f satisfait clairement la condition précédente et on a $\zeta = \frac{g(x)}{g(\zeta x)}$ pour $g(x) = \frac{1}{x}$.

Dans la partie 4.3.2 nous verrons que H^1 peut être encore utilisé pour classifer les algèbres centrales simples.

4.2.2 • LA COHOMOLOGIE GALOISIENNE ET LA DIMENSION COHOMOLOGIQUE DES CORPS

Dans cette section on verra quelques exemples de la cohomologie de la forme $H^n(Gal(K/k), A(K))$, où k est un corps, K est une extension galoisienne de k, A est un foncteur de la catégorie des extensions séparables algébriques de k dans la catégorie des $Gal(K/k)$-groupes qui satisfont les axiomes suivants :

1. $A(K) = \varinjlim A(K_i)$ où K_i parcourt toutes les sous-extensions de type fini de K sur k ;
2. Si $K \to K'$ est une injection, le morphisme correspondant $A(K) \to A(K')$ est aussi une injection.
3. Si K'/K est une extension galoisienne, alors $A(K) = H^0(Gal(K'/K), A(K'))$.

On note $H^n(K'|K, A)$ au lieu de $H^n(Gal(K'/K), A(K'))$, et note $H^n(k, A)$ au lieu de $H^n(k^{sep}|k, A(k^{sep}))$.

Proposition 31. Soit n un entier supérieur ou égal à 1, premier à la caractéristique de k. On a :

$$H^1(k, \mu_n) = k^\times/(k^\times)^n.$$

Démonstration. La suite exacte courte

$$0 \to \mu_n \to (k^{sep})^\times \xrightarrow{n} (k^{sep})^\times \to 0$$

induit une suite exacte longue

$$0 \to \mu_n \cap k \to k^\times \xrightarrow{n} k^\times \to H^1(k, \mu_n) \to H^1(Gal(k^{sep}/k, (k^{sep})^\times).$$

Et selon Hilbert 90, $H^1(Gal(k^{sep}/k, (k^{sep})^\times) = 0$. Alors

$$H^1(k, \mu_n) = k^\times/(k^\times)^n.$$

□

Proposition 32. Soit K/k une extension galoisienne. Alors $H^n(Gal(K/k), K^+) = 0$ pour tout $n \geqslant 1$.

Démonstration. Supposons que K/k soit une extension finie. D'après le théorème de la base normale, il existe un $x \in K$ tel que $Gal(K/k)x$ est une base de K comme un k-espace vectoriel, c'est-à-dire,

$$K^+ = \bigoplus_{g \in Gal(K/k)} g(kx).$$

Ainsi K^+ est un $Gal(K/k)$-module induit. On en déduit : $H^n(Gal(K/k), K^+) = 0$ pour tout $n \geqslant 1$.

Pour les extensions galoisiennes en général, on peut montrer le même résultat en prenant une limite inductive, d'aprèes la proposition 26. □

Proposition 33 (Artin-Schreier)**.** Soit k un corps de caractérisitique p. Soit $\Phi : k^{sep} \to k^{sep}, x \to x^p - x$. Alors

$$H^1(k, \mathbb{Z}/p\mathbb{Z}) \simeq k/\Phi(k)$$

et

$$H^n(k, \mathbb{Z}/p\mathbb{Z}) = 0$$

pour tout $n \geqslant 2$.

Démonstration. On peut vérifier que

$$0 \to \mathbb{Z}/p\mathbb{Z} \to k^{sep} \xrightarrow{\Phi} k^{sep} \to 0$$

est une suite exacte de G_k-modules, où $\mathbb{Z}/p\mathbb{Z}$ est muni de l'action triviale. Alors elle induit une suite exacte longue :

$$0 \to \mathbb{Z}/p\mathbb{Z} \to k^+ \xrightarrow{\Phi} k^+ \xrightarrow{\delta} H^1(k, \mathbb{Z}/p\mathbb{Z}) \to H^1(k, k^+) \to \cdots$$

$$\cdots \to H^n(k, \mathbb{Z}/p\mathbb{Z}) \to H^n(k, k^+) \to H^n(k, k^+) \xrightarrow{\delta} H^{n+1}(k, \mathbb{Z}/p\mathbb{Z}) \to \cdots .$$

En utilisant la propostion précedente, $H^n(k, k^+) = 0$ pour tout $n \geqslant 1$. Alors on a

$$H^1(k, \mathbb{Z}/p\mathbb{Z}) \simeq k/\Phi(k)$$

$$H^n(k, \mathbb{Z}/p\mathbb{Z}) = 0$$

pour tout $n \geqslant 2$.

□

Maintenant on s'intéresse à la dimension cohomologique d'un groupe de Galois absolu G_k de k.

Proposition 34. Si k est un corps de caractéristique p, alors $cd_p(G_k) \leqslant 1$.

Démonstration. D'après la proposition 33, on a $H^n(G_k, \mathbb{Z}/p\mathbb{Z}) = 0$ pour tout $n \geqslant 2$. Soit H le p-groupe de Sylow de G_k, on a aussi $H^2(H, \mathbb{Z}/p\mathbb{Z}) = 0$. On applique le théorèeme 24, alors $cd_p(H) \leq 1$. Selon la proposition 29, $cd_p(G_k) = cd_p(H) \leqslant 1$. □

Proposition 35 (Transition d'une extension algébrique)**.** Soit K une extension algébrique d'un corps k, et soit p un nombre premier. On a $cd_p(G_K) \leqslant cd_p(G_k)$, et il y a égalité dans chacun des deux cas suivants :

1. $[K : k]_s$ est premier à p ;
2. $cd_p(G_k) < \infty$ et $[K : k]_s < \infty$.

Proposition 36. Soit K un corps complet pour une valuation discrète de corps résiduel k. Pour tout nombre premier p, on a

$$cd_p(G_K) \leqslant 1 + cd_p(G_k).$$

Il y a égalité lorsque $cd_p(G_k) < \infty$ et que p est distinct de la caractéristique de K.

De ces résultats, on déduit un lien fondamental entre dimension cohomologique et propriété C_i. En effet, on en déduit que la dimension cohomologique se transmet de la même façon aux extensions algébriques et transcendantes de dimension finie, que la propriété C_i. Rappelons que la dimension cohomologique est la borne supérieure des p-dimensions.
Si K est est une extension algébrique de de dimension finie de k, le cas d'égalité 2 de la proposition 36 donne que $cd(G_k) = cd(G_K)$ lorsque $cd(G_k)$ est fini. De la même façon lorsque k est C_i pour un entier i donné, K l'est aussi pour le même entier i.
Pour le corps des séries de Laurent formelles $K = k((T))$ d'un corps k tel que $cd(G_k)$ est fini, on remarque que le cas d'égalité de la proposition 37 est nécessairement atteint en tous les p sauf la caractéristique de k, et que K vérifie bien les hypothèses. Combinant cela avec la proposition 35 pour $p = char(k)$, on en déduit que $cd(G_K) = 1 + cd(G_k)$. Or, le théorème 6, de Greenberg, assure que si k est C_i alors $k((T))$ est C_{i+1}. On peut montrer qu'il en est de même pour le corps des fractions rationnelles sur k.
L'entier de la propriété C_i suit les mêmes lois de transition que la dimension cohomologique, ce qui confirme le parallèle qu'on peut établir entre les deux notions.

Théorème 26. Soit k un corps vérifiant $cd(G_k)$ finie, alors :
(1) Si K en est une extension algébrique, $cd(G_K) = cd(G_k)$.
(2) Si $K = k(T)$ ou $K = k((T))$ alors $cd(G_K) = cd(G_k) + 1$.

Enonçons quelques exemples de calcul de dimension cohomologique pour le groupe de Galois absolu d'un corps k.

Exemple 17. Si $k = \mathbb{R}$, alors $G_{\mathbb{R}} = Gal(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$. Pour $p \neq 2$, on sait que d'après le lemme 11, pour tout $n \geqslant 1$ et tout $G_{\mathbb{R}}$-module A, $H^n(G_{\mathbb{R}}, A)$ est de 2-torsion. Alors $cd_p(G_{\mathbb{R}}) = 0$ pour tout $p \neq 2$. Et $cd_2(G_{\mathbb{R}}) = \infty$ (en utilisant la propriété de la cohomologie de groupe cyclique, l'exemple 8).

Exemple 18. On verra dans l'exemple 22 que si k est un corps fini, $cd_p(G_k) = cd_p(\hat{\mathbb{Z}}) = 1$ pour tout p premier.

Exemple 19. Si K est un corps local non-Archimédien (par exemple une extension finie de $\mathbb{Q}_p$), il vérifie la condition de la propostion 36, et le corps résiduel k est un corps fini. Alors on a vu que $cd_p(G_k) = 1$ pour tout p premier. Il vient $cd_p(G_K) = cd_p(G_k) + 1 = 2$.

4.3 LA PROPRIÉTÉ C_1 ET LA DIMENSION COHOMOLOGIQUE

On va d'abord définir les algèbres centrales simples puis le groupe de Brauer et enfin parler du lien entre ce groupe et la propriété C_1. Ceci va justement permettre de donner une propriété fondamentale portant sur la dimension cohomologique des corps C_1.

4.3.1 • LES ALGÈBRES CENTRALES SIMPLES (CSA) ET LE THÉORÈME DE WEDDERBURN

Définition 45. Une algèbre à division est une algèbre sur un corps k donné avec la possibilité de diviser par tout élément non nul (à droite et à gauche). Notons que la multiplication n'est pas nécessairement associative ou commutative.

Une k-algèbre A est dite centrale si son centre est réduit à k. Elle est dite simple si ses seuls idéaux bilatères sont 0 et A. Par exemple une algèbre à division est centrale sur son centre $Z(D)$, et est bien évidemment simple.
Donnons maintenant un autre exemple d'algèbre centrale simple classique.

Exemple 20. Notons D une algèbre à division sur un corps k, et $n \geqslant 1$. L'anneau des matrices $M_n(D)$ est simple et on peut vérifier que son centre est constitué des homothéties de rapport appartenant à $Z(D)$. Il en découle que $M_n(D)$ est simple centrale sur le corps $Z(D)$.

Étant donné un module M sur un anneau unitaire A, l'ensemble $End_A(M)$ de ses endomorphismes de modules est un anneau par rapport à l'addition définie comme suit, $(f+g)(x) = f(x) + g(x)$, pour tout x dans M, et le produit donné par la composition, $(fg)(x) = f \circ g(x) = f(g(x))$, pour tout x dans M.

Théorème 27. (Wedderburn) Soit A, une algèbre simple de dimension finie sur un corps k. Alors il existe un entier $n \geqslant 1$ et une algèbre à division $D \supset k$ tels que A soit isomorphe à l'anneau matriciel $M_n(D)$. De plus, l'algèbre à division D est unique à isomorphisme près.

La preuve de ce théorème découle des deux lemmes suivants :

Lemme 15. (Schur) Soit M un module simple sur une k-algèbre A. Alors $End_A(M)$ est une algèbre à division.

Lemme 16. (Rieffel) Soit L un idéal gauche non nul dans une k-algèbre simple A, et posons $D = End_A(L)$. Alors l'application $\lambda_L : A \to End_D(L)$ qui à tout $a \in A$ associe l'endomorphisme $x \mapsto ax$ est un isomorphisme. Notons que dans un anneau A, un idéal gauche n'est rien d'autre qu'un sous-module du A-module gauche A.

Preuve du théorème de Wedderburn : Comme A est de dimension finie, une chaîne descendante d'idéaux gauches doit se stabiliser. Soit donc L un idéal gauche minimal ; il s'agit alors d'un A-module simple. Par le lemme de Schur, $D = End_A(L)$ est une algèbre à division, et par le lemme de Rieffel, nous avons un isomorphisme $A \cong End_D(L)$. Le lemme de Schur donne alors un isomorphisme $End_D(L) \cong M_n(D)$, où n est la dimension de L sur D (elle est finie puisque L est déjà de dimension finie sur k). Pour l'énoncé d'unicité, supposons que D et D' sont des algèbres de division pour lesquelles $A \cong M_n(D) \cong M_m(D')$ avec des entiers appropriés n, m. L'idéal minimal gauche L satisfait alors $D^n \cong L \cong D'^m$, d'où une chaîne d'isomorphismes $D \cong End_A(D^n) \cong End_A(L) \cong End_A(D'^m) \cong D'$.

Corollaire 8. Soit k un corps algébriquement clos. Alors toute k-algèbre centrale simple est isomorphe à $M_n(k)$ pour un certain entier $n \geqslant 1$.

Démonstration. D'après le théorème de Wedderburn, il suffit de voir que la seule algèbre à division $D \supset k$ de dimension finie sur k est k.
En effet , soit d un élement non nul de D. La famille $(d^i)_{i \in N}$ est liée, et donc il existe un polynome annulateur de d , et puisque D est une algèbre à division , il n'admet donc pas de diviseur de 0 donc on peut le supposer irréductible.
Alors $k[d]$ est un corps de dimension finie sur k, et comme k est algébriquement clos, $k[d]$ est k. Ainsi $d \in k$, et $D = k$. □

Le théorème de Wedderburn nous permet d'affirmer que si A est une algèbre simple de dimension finie sur k, alors il existe une algèbre à division $D \supset k$ et un entier $n \geqslant 0$, tel que $A \simeq M_n(D)$, où D est unique. Alors on peut "classifier" les CSA sur k par les algèbres à division D.

En plus on verra une propriété importante, qui dit qu'une CSA est une algèbre simple de dimension finie qui peut être identifiée avec l'algèbre de matrices d'un corps, en changeant le corps de base.

Lemme 17. Soient A une k-algèbre de dimension finie, et K/k une extension finie. A est une algèbre centrale simple sur k si et seulement si $A \otimes_k K$ est une algèbre centrale simple sur K.

Théorème 28. Une k-algèbre de dimension finie est une algèbre centrale simple si et seulement s'il existe un nombre $n > 0$ et une extension finie K/k tel que $A \otimes_k K \simeq M_n(K)$.

Démonstration. Soit A une CSA, on note $\bar{k}$ la clôture algébrique de k. $A \otimes_k \bar{k}$ est une CSA sur $\bar{k}$, alors d'après le corollaire 8, il existe un nombre $n > 0$ tel que $A \otimes_{\bar{k}} \bar{k} \simeq M_n(\bar{k})$. On peut voir toute extension finie de k comme une sous-extension de $\bar{k}$, et cela induit l'inclusion $A \otimes_k K \hookrightarrow A \otimes_k \bar{k}$ et $A \otimes_k \bar{k}$ est exactement $\bigcup_K A \otimes_k K$, où K parcourt toutes les extensions finies de k. En outre, il existe une extension finie K/k, telle que $A \otimes_k K$ contient tous les éléments qui correspondent aux éléments de base venant de l'isomorphisme $A \otimes_k \bar{k} \simeq M_n(\bar{k})$. On a alors $A \otimes_k K \simeq M_n(K)$.

En revanche s'il existe une extension finie K/k telle que $A \otimes_k K \simeq M_n(K)$, on sait que $M_n(K)$ est une CSA sur K, alors d'aprèes le lemme précédent A est une CSA. □

Définition 46. Pour une algèebre centrale simple sur k, on dit qu'une extension K de k est un corps de décomposition, s'il existe un nombre $n > 0$ tel que $A \otimes_k K \simeq M_n(K)$. On appelle $\sqrt{\dim_k A}$ le degré de A.

On note $CSA_K(n)$ l'ensemble des classes d'isomorphismes des CSAs sur k de degré n et décomposées par K.

On peut en plus considérer que l'extension choisie est galoisienne par le théorème suivant.

Théorème 29. Une k-algèbre de dimension finie est une algèbre centrale simple si et seulement si il existe un nombre $n > 0$ et une extension galoisienne finie K/k tel que $A \otimes_k K \simeq M_n(K)$.

Remarque 9. Pour montrer ce théorème, on sait que pour toute extension separable finie K/k, la plus petite extension normale de k contenant K est une extension galoisienne finie de k. D'où en appliquant le théorème 28 le résultat escompté.

4.3.2 • LE GROUPE DE BRAUER

On supposera dans toute cette section que k est un corps parfait.

Théorème 30. On a une bijection entre $CSA_K(n)$ et $H^1(Gal(K/k), PGL_n(K))$.

Démonstration. Soit A une CSA dans $CSA_K(n)$. D'abord on va construire un 1-cocycle via A. On sait que tous les automorphismes d'une algèbre de matrices (ou d'une CSA en général par le théorème de Skolem-Noether) sont intérieurs. Alors $Aut_K(M_n(K)) \simeq PGL_n(K)$. On note $\phi : M_n(K) \to A \otimes_k K$ l'isomorphisme. On définit

$$\begin{array}{rccc} x: & Gal(K/k) & \to & Aut_K(M_n(K)) \simeq PGL_n(K) \\ & g & \mapsto & \phi^{-1}({}^g\phi) \end{array}$$

c'est-à-dire pour $m \in M_n(K)$, $x(g)(m) = \phi^{-1}(g\phi(g^{-1}m))$. Alors

$$x(gh)(m) = \phi^{-1}(gh\phi(h^{-1}g^{-1}m)) = \phi^{-1}(gx(h)(g^{-1}m)) = x(g) \circ ({}^g x(h))(m)$$

Et dans la forme matricielle, $x(gh) = x(g) \cdot {}^g x(h)$. Donc x est bien un 1-cocycle. On a donc une application $CSA_K(n) \to H^1(Gal(K/k), PGL_n(K))$. On peut vérifier l'injectivité en vérifiant que deux CSAs isomorphes donnent une même classe dans H^1.

En revanche, à partir d'un cocycle $x : Gal(K/k) \to Aut_K(M_n(K))$ on peut obtenir une action tordue sur $M_n(K)$ de $Gal(K/k)$ par

$$Gal(K/k) \times M_n(K), (g, m) \mapsto x(g)(gm)$$

et c'est une $Gal(K/k)$-action. On prend $A = M_n(K)^{Gal(K/k)}$ ou l'action par $Gal(K/k)$ est définie par le morphisme ci-dessus associé à x. D'après le lemme 14 (Speiser), on a l'isomorphisme suivant :

$$A \otimes_k K = M_n(K)^{Gal(K/k)} \otimes_k K \simeq M_n(K)$$

Et on utilise le lemme 17, on a une CSA A dans $CSA_n(K)$ provenant d'un 1-cocycle dans $H^1(Gal(K/k), PGL_n(K)$ On peut vérifier que les deux applications sont bijectives.

□

De plus, soient A, B deux CSAs, $A \in CSA_K(m)$ et $B \in CSA_K(n)$, on a $(A \otimes_k B) \otimes_k K \simeq (A \otimes_k K) \otimes_K (B \otimes_k K) \simeq M_m(K) \otimes_K M_n(K) \simeq M_{mn}(K)$. On en déduit que $A \otimes_k B$ est une CSA décomposée par K de degré mn d'après le lemme 17. Il en découle une application

$$CSA_m(K) \times CSA_n(K) \to CSA_{mn}(K), \quad ([A], [B]) \mapsto [A \otimes_k B]$$

(on note $[A]$ la classe d'isomorphisme de A) et donc d'après la proposition ci-dessus, on a une application

$$H^1(Gal(K/k), PGL_m(K)) \times H^1(Gal(K/k), PGL_n(K)) \to H^1(Gal(K/k), PGL_{mn}(K)).$$

C'est explicitement induit par l'application

$$End_K(K^m) \otimes End_K(K^n) \to End_K(K^m \otimes K^n), \quad (\phi, \psi) \mapsto \phi \otimes \psi$$

ce qui donne une application

$$GL_m(K) \times GL_n(K) \to GL_{mn}(K),$$

et finalement

$$PGL_m(K) \times PGL_n(K) \to PGL_{mn}(K).$$

On définit un système inductif d'ensembles $(CSA_K(n))_{n\in\mathbb{N}}$ dans lequel si $n|m$ on a une application

$$CSA_K(n) \to CSA_m(K), \quad [A] \mapsto [A \otimes_k M_{m/n}(k)]$$

On note $Br(K|k) := \varinjlim_n CSA_K(n) \simeq \varinjlim_n H^1(Gal(K/k), PGL_n(K))$. C'est l'ensemble de toutes les classes de CSA sur k décomposées par K.

Soient A, B deux CSAs dans $Br(K|k)$. On note A^{op} l'anneau opposé de A, c'est-à-dire un anneau qui possède le même groupe additif sous-jacent que A, et tel que sa multiplication est effectuée dans l'ordre opposé. On sait que $A \otimes_k B \simeq B \otimes_k A$ et $A \otimes_k A^{op} \simeq End_k(A) = M_n(k)$ où n est la dimension de A sur k, on a

Lemme 18. On appelle $Br(K|k)$ muni de l'unité $[M_n(K)]$, ou groupe de Brauer de k relatif à K, la multiplication $([A], [B]) \mapsto [A \otimes_k B]$ et l'inverse $[A] \mapsto [A^{op}]$. Il vient que $Br(K|k)$ est un groupe abélien.

Définition 47. Le groupe de Brauer est la réunion de tous les $Br(K|k)$ pour toutes les extensions finies galoisiennes K sur k. C'est-à-dire,

$$Br(k) := \varinjlim_K Br(K|k)$$

où K décrit le système projectif de toutes les extensions finies galoisiennes sur k.

Par cette définition, si deux CSAs A, B représentent un même élément dans $Br(k)$, alors il existe m, n tels que $A \otimes_k M_m(k) \simeq B \otimes_k M_n(k)$. On dit que A et B sont Brauer-équivalentes. D'après le théorème de Wedderburn, c'est la même chose que de dire qu'il existe une algèbre à division D telle que $A \simeq M_n(D)$ et $B \simeq M_m(D)$.

Proposition 37.

$$Br(k) \simeq H^2(Gal(k^{sep}/k), (k^{sep})^\times).$$

Démonstration. Ici on va seulement présenter une ébauche de démonstration. Pour une extension galoisienne finie K/k, soit $Gal(K/k) = G$. On a une suite exacte de G-groupes :

$$1 \to K^\times \to GL_m(K) \to PGL_m(K) \to 1$$

Cela induit une suite exacte de cohomologie :

$$H^1(G, GL_m(K)) \to H^1(G, PGL_m(K)) \xrightarrow{\delta} H^2(G, K^\times)$$

On note $H^1(G, PGL_\infty(K)) := \varinjlim_n H^1(G, PGL_n(K)) \simeq Br(K|k)$. En prenant la limite projective sur m on a donc une application

$$H^1(G, PGL_\infty(K)) \xrightarrow{\delta} H^2(G, K^\times)$$

D'abord on vérifie que δ est un morphisme de groupes, dans le sens où $H^1(G, PGL_\infty)$ est muni du produit que l'on a défini ci-dessus. On a de plus montré dans la partie 4.2 que $H^1(G, GL_m) = 1$, de sorte que δ est une injection.

Pour montrer que δ est surjectif, soit $n = |Gal(K/k)|$, on a $K \bigotimes_k K$ comme un K-espace vectoriel en dimension n, par conséquent la multiplication par un élément inversible dans $K \bigotimes_k K$ donne un K-automorphisme. On a alors un diagramme commutatif compatible avec l'action de G, dans lequel toutes les lignes sont exactes.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^\times & \longrightarrow & (K \bigotimes_k K)^\times & \longrightarrow & (K \bigotimes_k K)^\times / K^\times & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & K^\times & \longrightarrow & GL_n(K) & \longrightarrow & PGL_n(K) & \longrightarrow & 1 \end{array}$$

Il en découle un un diagramme commutatif :

$$\begin{array}{ccccc} H^1(G, (K \bigotimes_k K)^\times / K^\times) & \longrightarrow & H^2(G, K^\times) & \longrightarrow & H^2(G, (K \bigotimes_k K)^\times) \\ \downarrow & & \downarrow{\scriptstyle id} & & \\ H^1(G, PGL_n(K)) & \xrightarrow{\delta} & H^2(G, K^\times) & & \end{array}$$

Il suffit donc de montrer que $H^2(G, (K \bigotimes_k K)^\times) = 0$. Comme $(K \bigotimes_k K)^\times \simeq K^\times \bigotimes \mathbb{Z}[G]$ est un module induit par G, on sait d'après la proposition 23 que $H^2(G, (K \bigotimes_k K)^\times) = 0$.

Donc

$$Br(K|k) \simeq H^2(Gal(K/k), K^\times)$$

et en passant à la limite sur K

$$Br(k) \simeq H^2(Gal(k^{sep}/k), (k^{sep})^\times)$$

□

On note $G_k = Gal(k^{sep}/k)$.

Proposition 38. Soit k un corps parfait . Les propriétés suivantes sont équivalentes :

1. On a $cd(G_k) \leqslant 1$;
2. On a $Br(K) = 0$ pour toute extension algébrique K sur k ;

Remarque 10. On s'est limité à k parfait dans cette partie car la définition de la p-dimension cohomologique donnée ici n'est pas la bonne pour un corps imparfait de caractéristique p. Le cas où k est un corps imparfait recquiert de définir la cohomologie par la notion de dérivation formelle, chose qui sera omise ici.

Démonstration. $1 \implies 2$: Soit K/k est une extension algébrique et $cd(G_k) \leqslant 1$; le groupe G_K est un sous-groupe fermé de G_k, on a donc $cd(G_K) \leqslant cd(G_k) \leqslant 1$. Pour tout p premier, on considère une suite exacte :

$$1 \to \mu_p \to K^\times \xrightarrow{x \mapsto x^p} K^\times \to 1$$

où μ_p est le groupe formé par toutes les racines p-ièmes de l'unité dans K. Cela induit une suite exacte de cohomologie :

$$H^2(G_K, \mu_p) \to H^2(G_K, K^\times) \to H^2(G_K, K^\times) \to H^3(G_K, \mu_p)$$

et $H^2(G_K, \mu_p) = 0$ et $H^3(G_K, \mu_p) = 0$ par le fait que $cd(G_K) \leqslant 1$, alors $x \mapsto x^p$ induit une bijection sur $H^2(G_K, K^\times)$. Alors $Br(K)[p^\infty] = H^2(G_K, K^\times)[p^\infty] = 0$. D'après le corollaire 3, $H^2(G_K, K^\times)$ est un groupe de torsion,

$$H^2(G_K, K^\times) = \bigoplus_p H^2(G_K, K^\times)[p^\infty],$$

D'où $Br(K) = 0$ pour toutes les extensions algébriques K/k.

$1 \iff 2$: Soit H un p-groupe de Sylow de G_k et soit K/k l'extension correspondante. Par la même suite exacte que ci-dessus, $Br(K)[p^\infty] = H^2(G_K, K^\times)[p^\infty] = 0$ implique que $H^2(G_K, \mu_p) = 0$. Le groupe H est un pro-p-groupe, son action sur μ_p est triviale, alors on peut identifier μ_p et $\mathbb{Z}/p\mathbb{Z}$. D'après le théorème 24, on a $cd(H) \leqslant 1$, c'est-à-dire $cd_p(G_k) \leqslant 1$. □

Proposition 39. Si k est un corps C_1, alors $Br(k) = 0$.

Démonstration. Soit A une algèbre à division de degré n décomposée par une extension galoisienne finie K/k. On note $G = Gal(K/k)$. Alors $A \otimes_k K \simeq M_n(K)$. On a une application

$$A \otimes_k K \simeq M_n(K) \xrightarrow{det} K$$

et puisque $(A \otimes_k K)^G \simeq A$, on a l'application appelée la norme réduite :

$$nr : A \to k$$

Pour tout $a \in A\backslash\{0\}$, a est inversible, alors la matrice correspondante est inversible, $nr(a) \neq 0$. D'où nr ne s'annule qu'en 0. En plus il est un polynôme en n^2 inconnues et de degré n. Cela entre en contradiction avec la propriété C_1 de k lorsque $n > 1$, donc $n = 1$, d'où $Br(k) = 0$. □

Voyons un autre résultat dû à Wedderburn.

Théorème 31. [PETIT THÉORÈME DE WEDDERBURN]
Les algèbres à divisions finies sont des corps

Démonstration. Soit k une algèbre à division finie, alors k est centrale sur son centre $Z(k)$ qui est un corps fini , donc C_1 par le théorème de Chevalley Warning. Par la proposition précédente, $k \simeq Z(k)$ qui est un corps. □

En combinant les deux propositions ci-dessus, si k est C_1, alors toutes les extensions algébriques sur k sont C_1, et le groupe de Brauer de toute extension algébrique de k est nul, on a donc tout de suite :

Corollaire 9. Si k est C_1, alors $cd(G_k) \leqslant 1$.

Remarque 11. Afin de montrer que $cd(G_k) \leqslant 1$, on peut trouver une autre méthode utilisant la cohomologie modifiée $\hat{H}^i(G, A), i \in \mathbb{Z}$. Soient K une extension algébrique de k et L/K une extension galoisienne finie, G=$Gal(L/K)$, N une norme de L vers K.Le théorème de Hilbert 90 nous donne le fait que $\hat{H}^1(G, L^\times) = H^1(G, L^\times) = 0$. Si $Br(K) = 0$, alors $\hat{H}^2(G, L^\times) = H^2(G, L^\times) = 0$; si N est surjective, alors $\hat{H}^0(G, L^\times) = K^\times/N_{L|K}(L^\times) = 0$. D'après le théorème de la trivialité cohomologique, si pour deux valeurs consécutives de q et pour tout sous-groupe g de G, $\hat{H}^q(g, A) = 0$, alors A est cohomologiquement trivial. Ainsi les conditions de la proposition 24 sont aussi équivalentes aux deux propositons suivantes :

1. Pour toute extension algébrique K de k et toute extension galoisienne finie L/K, le $Gal(L/K)$-module $L^\times$ est cohomologiquement trivial.
2. Pour toute extension algébrique K de k et toute extension galoisienne finie L/K, la norme $N_{L/K} : L^\times \to K^\times$ est surjective.

Comme K est C_1 (D'après le théorème de Lang), l'équation :

$$N(x) = ax_0^d$$

pour $x_0 \in L$ et $x \in K$ possède une solution non triviale (x_0, x) puisqu'il s'agit d'une équation de dégré d en $d+1$ variables sur K . Si $x_0 = 0$, on aurait $N(x) = 0$ donc $x = 0$ ce qui est impossible puisque la solution (x_0, x) est non triviale. Ce qui entraine que $N(x/x_0) = a$. Alors $N : L^\times \to K^\times$ est surjective.

Notons que la réciproque de cette proposition est fausse ! En effet, on peut construire des corps de dimension cohomologique 1 mais non C_1. En général ces constructions sont parfois complexes et techniques.

Exemple 21. On note $\mathbb{H}$ l'algèbre associative unifère sur $\mathbb{R}$ engendrée par trois éléments i, j, k satisfaisant les relations quaternioniques :

$$i^2 = j^2 = k^2 = ijk = -1.$$

$\mathbb{H}$ et $\mathbb{R}$ sont toutes les deux algèbres à division sur $\mathbb{R}$ avec centre $\mathbb{R}$. Comme $\mathbb{H} \otimes \mathbb{H} \simeq M_4(\mathbb{R})$ alors

$$Br(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\} \simeq \mathbb{Z}/2\mathbb{Z}$$

Exemple 22. D'après le théorème de Chevalley-Warning, un corps fini F est C_1, alors $Br(F) = 0$.

On rapelle l'exemple 11, $G_F = \hat{\mathbb{Z}}$. Comme F est C_1, alors $cd(G_F) = cd(\hat{\mathbb{Z}}) \leqslant 1$. En même temps, pour tout p premier,

$$H^1(\hat{\mathbb{Z}}, \mathbb{Z}/p\mathbb{Z}) = Hom(\hat{\mathbb{Z}}, \mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z},$$

On en déduit que $cd_p(\hat{\mathbb{Z}}) \geqslant 1$ pour tout p premier. On a donc $cd(G_F) = cd(\hat{\mathbb{Z}}) = 1$.

Exemple 23. Soit K un corps complet de valuation discrète dont le corps résiduel est un corps fini (par exemple $\mathbb{Q}_p$). On note K_n l'unique extension non-ramifiée de degré n de K. Remarquons l'égalité $Br(K) = \bigcup_n Br(K_n|K)$, que l'on ne cherche pas à démontrer ici. Alors K_n/K est une extension cyclique et $Br(K_n|K) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. On a donc un isomorphisme

$$inv_K : Br(K) = \bigcup_n Br(K_n|K) \simeq \bigcup_n \frac{1}{n}\mathbb{Z}/\mathbb{Z} = \mathbb{Q}/\mathbb{Z}.$$

Exemple 24. Le groupe de Brauer d'un corps global K peut être déterminé par le théorème de Brauer-Hasse-Noether, qui est un théorème difficile issu de la théorie du corps de classe global :
(i) soit $a \in Br(K)$, pour toutes les places v sauf un nombre fini des places, l'image de a par l'application $Br(K) \to Br(K_v)$ est nulle ;
(2) on a une suite exacte :

$$0 \to Br(K) \to \bigoplus_v Br(K_v) \xrightarrow{\sum_v inv_{K_v}} \mathbb{Q}/\mathbb{Z} \to 0.$$

4.4 LE CAS DES CORPS C_2 : LES RÉSULTATS DE MERKURJEV ET SUSLIN

Proposition 40. Soient k un corps commutatif ayant la propriété C_2 et D une algèbre à division de centre k et de dimension finie. La norme réduite $nr : D^\times \to k^\times$ est surjective.

Démonstration. Soit $[D : k] = n^2$ et $a \in k^\times$. Alors $nr(x) = at^n$ est une forme de degré n en $n^2 + 1$ inconnues, la propriété C_2 implique que cette équation a une solution non triviale. Donc a est dans l'image de nr. □

De plus, Merkurjev et Suslin ont montré le résultat suivant (compliqué) :

Théorème 32. Soit k un corps parfait. Les propriétés suivantes sont équivalentes :

1. $cd(G_k) \leqslant 2$;
2. Pour toutes les extensions finies K sur k et toutes les algèbres à division de centre K de dimension finie, la norme réduite est surjective.

Ainsi, lorsque k est parfait, la propriété C_2 implique $cd(G_k) \leqslant 2$. Pour un corps k vérifiant la propriété C_2, si *char* $k = 0$, il est déjà parfait. En revanche, si *char* $k = p > 0$ on prend sa clôture parfaite F, alors F/k est algébrique, F est aussi C_2 et $[F : k]_s = 1$. D'après un théorème de transition, $2 \geqslant cd_q(G_F) = cd_q(G_k)$ pour tous les nombres premiers q. Alors $cd(G_k) \leqslant 2$ pour un corps C_2 en général.

Ce n'est pas l'objet de ce travail que de le démontrer, mais on sait que les corps $\mathbb{Q}_p$ sont de dimension cohomologique 2. Or, ces corps ne sont pas C_2 comme nous l'avons démontré en section 2. Ils sont donc des contre-exemples simples à la réciproque, qui voudrait qu'un corps k tel que $cd(G_k) = 2$ soit C_2. On remarque qu'ici, on a un contre-exemple bien plus naturel que pour la dimension cohomologique 1, pour lequel les contre-exemples connus (dont celui construit historiquement par Ax) sont tous plus élaborés.
D'autre part, on a aussi vu via le théorème d'Ax-Kochen, que les corps $\mathbb{Q}_p$ ont un lien profond avec la propriété C_2. Ainsi, le fait qu'on ait $cd(G_{\mathbb{Q}_p}) = 2$ n'est pas si étonnant. C'est de nature à nous conforter quant à la corrélation relativement bonne entre dimension cohomologique et caractère C_i : ici, quand un corps k vérifie $cd(G_k) = 2$, il n'est pas certain que k soit C_2 mais pour autant, il risque d'être fortemement lié à la propriété C_2.

On a ainsi dans cette partie abordé le fait que pour $r \leqslant 2$, un corps C_r est de dimension cohomologique plus petite que r. Ces résultats s'inscrivent dans une conjecture plus grande, énoncée par Serre, qui n'est toujours pas démontrée à ce jour.

Conjecture 1. [SERRE]
Soit $r \in \mathbb{N}$, et k un corps. Si k est C_r, alors $cd(G_k) \leqslant r$.

5
CONCLUSION

La théorie d'Artin et Lang se révèle être un cadre très propice à l'étude de l'existence de zéros aux polynômes homogènes sur un corps donné. Dans beaucoup de corps, les formes ayant suffisamment de variables par rapport à leur degré possèdent nécessairement un zéro non trivial, plus exactement lorsque le nombre de variables excède une certaine puissance entière du degré.. C'est notamment le cas des corps finis qui sont C_1, ou plus trivialement des corps algébriquement clos qui sont C_0. En outre, le caractère C_i d'un corps possède la propriété remarquable de se transmettre à des extensions de ce corps. Ainsi, il est en quelque sorte héréditaire, ce qui a pour conséquence qu'une foultitude de corps, dont certains que nous avons exhibé ici, sont C_i pour un entier i donné.
Il existe pourtant des corps qui ne sont C_i pour aucun i, comme par exemple les corps p-adiques $\mathbb{Q}_p$. Toutefois, ces derniers restent étroitement liés à la propriété C_2, ainsi que nous l'avons prouvé via le théorème d'Ax-Kochen, en mettant en oeuvre des méthodes assez surprenantes tirées de la logique du premier ordre. Ainsi, dans beaucoup de cas, augmenter le nombre de variables par rapport au degré suffit à y faire apparaître un zéro non trivial. Une grande partie des corps que nous connaissons sont donc très sensibles à la propriété C_i. On peut espérer qu'il en soit de même pour d'autres corps. Pour comprendre ces questions de manière plus systématique, des outils algébriques adaptés ont été introduits. Une tentative relativement fructueuse a été d'utiliser la dimension cohomologique pour décrire le caractère C_i. Celle-ci s'avérait très prometteuse en ce que cette grandeur décrit très bien les corps C_0 et C_1, et se transmet de manière analogue à la propriété C_i, aux extensions d'un corps donné. Toutefois, un corps de dimension cohomologique i n'est pas forcément C_i, les corps $\mathbb{Q}_p$ en sont un bon contre-exemple pour $i = 2$. Les deux notions sont relativement bien corrélées, mais ne coïncident pas exactement pour autant. La dimension cohomologique est aujourd'hui bien comprise, mais caractériser plus précisément son lien avec la propriété C_i reste un sujet de recherche actif. Il subsiste en effet des conjectures fondamentales, comme celle de Serre, qui ne sont toujours pas tranchées.
D'autres manières d'aborder le problème de l'existence de zéros à un polynôme sont aujourd'hui explorées. On peut notamment citer le fait que des tentatives sont effectuées par des méthodes de géométrie algébrique : l'étude de variétés dites rationnellement connexes a par exemple permis de voir les corps C_1 d'une nouvelle manière. La théorie d'Artin est Lang est donc encore à ce jour un sujet de recherche actif, à la fois passionnant et complexe. A travers ce travail, nous espérons avoir bien mis en lumière certains des aspects principaux de ce domaine, et avoir attisé la curiosité du lecteur à explorer plus en profondeur l'état actuel de la recherche. C'est en tout cas un objectif que nous, auteurs, poursuivrons certainement à l'avenir, tant ces questions nous ont captivés.

Bibliographie

1. Marvin J. GREENBERG : "Lectures on forms in many variables", W. A. Benjamin, 1969, pp. 1-182.
2. Olivier WITTENBERG : "La connexité rationnelle en arithmétique", septembre 2008, p. 4-19.
3. Bjorn POONEN : "Rational Points on Varieties" American Mathematical Society, 2017, pp. 1-292.
4. T. Y. LAM : "Introduction to quadratic forms and over fields", American Mathematical Society, volume 67 de la collection Graduate Studies in Mathematics, 2005, pp. 1-530.
5. Alex KRUCKMAN : "The Ax-Kochen theorem : an application of model theory to algebra", 2013, pp. 1-66.
6. Lou VAN DEN DRIES : "Model theory of valued fields", extrait de "Model theory in Algebra, Analysis and Arithmetic", collection Lecture Notes in Mathematics, Automne 2004, pp. 1-29.
7. Guy TERJANIAN : "Progrès récents dans l'étude de la propriété C_i des corps", issu du volume 8, tome 2 de "Séminaire Delange-Pisot-Poitou. Théorie des nombres", 1966-1967, pp. 1-8.
8. David HARARI : "Cohomologie galoisienne et théorie des nombres", Magistère d'Orsay, 2011-2012, pp. 1-65.
9. Philippe GILLE et Tamás SZAMUELY : "Central simple algebras and Galois cohomology", Cambridge studies in advanced mathematics, 2006, pp. 17-150 et 223-258.
10. R. PARIMALA : "Some Aspects of the Algebric Theory of Quadratic Forms" in "Quadratic and Higher Degree Forms", Krishnaswami Alladi, 2013, pp. 181-206.
11. Seewoo LEE : "Hilbert's theorem 90", Math-Berkeley, 6 novembre 2006, pp. 1-5.
12. Jean-Pierre SERRE : "Cohomologie galoisienne", collection Lecture Notes in Mathematics, 1994, pp. 1-181.
13. G.I. ARKHIPOV AND A.A. KARATSUBA, "On the local representation of zero by a form", Izv. Akad. Nauk SSSR Ser. Mat. 45 (1981), 948-961 ; translated in Math USSR-Izv, 19 (1982), 23l-240