Magistère de Mathématiques Fondamentales et Appliquées à l'Informatique

Mémoire de magistère « Arithmétique et p-adique »

par
Xavier CARUSO

Sommaire

Soutenu le 7 octobre 2002, à l'ÉNS, Paris.

Introduction

Après deux ans d'écoles préparatoires, je décide d'intégrer l'École Normale Supérieure en 1999, en mathématiques. Je suis, pendant la première année, divers cours de licence et de maîtrise donnés à l'école. Les cours d'algèbre, bien que plus difficiles et moins accessibles à mon sens, m'emballent plus et c'est pour cette raison que je décide de travailler pour mon exposé de maîtrise, avec Erwan Biland sur un sujet étiqueté « algèbre » proposé par Yves Laszlo et qui s'intitule « $\mathbb{Z}$ est simplement connexe ». Je n'avais alors que peu d'idée (bien que je connaissais déjà l'expression « simplement connexe » pour la topologie, mais je ne voyais pas comment elle pouvait s'appliquer en algèbre, et encore moins à $\mathbb{Z}$) de ce que signifiait tout cela, mais les exposés sont là pour faire travailler les élèves et c'est ainsi que je découvris la théorie de la ramification algèbrique.

À côté de cela, je n'avais pas trop envie de passer l'agrégation, comme le font certains élèves en deuxième année, et comme il nous avait été dit que cela n'était pas nécessaire, je décidai de ne pas m'y présenter en deuxième année. Cette deuxième année fut donc consacrée à mon DEA : je décidai de suivre mes amours de l'an passé et commençais à suivre les cours du DEA de Mathématiques Pures à Orsay sans toutefois y être inscrit, ce que je verrais l'année suivante si tout se passait correctement comme le voulait plus ou moins la procédure classique.

Au second semestre, je choisis un sujet pour le stage que je décidai de fait avec Christophe Breuil. Ce sujet était en fait plus un sujet de thèse (je ne vais pas le détailler dans cette introduction, ce sera fait dans la suite du mémoire), mais le DEA servirait à comprendre les bases et à étudier des cas particuliers, particulièrement un seul en fait. Toutefois, pendant ce second semestre, comme il me restait encore du temps pour me consacrer à ce mémoire, je préférai continuer à suivre des cours d'algèbre à Orsay ou à Chevaleret, mais aussi de logique et d'informatique, deux domaines qui me plaisent également. En troisième année par contre, je me remis à l'algèbre et finis mon DEA.

D'autre part, en fin de terminale, j'avais été sélectionné pour les Olympiades de mathématiques et étais allé à Mar-Del-Plata pour faire les épreuves. C'est sans doute cela qui me donna l'envie de m'occuper de la relève les années suivantes. Depuis ma première année à l'ENS, donc, j'encadre, avec d'autres personnes et notamment Claude Deschamps, généralement quelques jours du stage de préparation de la délégation française à cette olympiade. Il s'agit d'une formation rapide pour les meilleurs élèves de terminale qui vont bientôt être confronté à des exercices d'un style tout à fait nouveau pour eux.

Mais il faut se rendre à l'évidence, deux semaines pour préparer ces gens c'est souvent trop court, et les résultats de la France étaient rarement à la hauteur de nos espérances. C'est pour cela que se créa une association répondant au nom d'Animath (`http://www.animath.fr`) dont le but est justement de recruter des élèves dès la seconde, et leur expliquer un peu plus de mathématiques, peut-être utiles pour les olympiades mais pas forcément. De mon côté, il arrive que de temps en temps je m'occupe de ces élèves ou que je passe une après-midi à leur corriger des copies.

Ce mémoire se divise en quatre parties :

La première partie très courte est juste un curriculum vitæ.

La seconde partie, intitulée « Arithmétique », est consacrée à mon parcours scolaire. Elle commence par une introduction au domaine de recherche qui commence par présenter le sujet qui m'intéresse à des non-spécialistes et finit par exposer clairement quel théorème va m'intéresser pendant les années à venir et quelles méthodes il est envisagé que j'emploie pour le résoudre. Cette introduction au domaine de recherche est suivi de mon exposé de maîtrise et de mon mémoire de DEA. Le premier, comme je l'ai déjà expliqué, présente la théorie de la ramification algébrique et donne un sens à l'expression « $\mathbb{Z}$ est simplement connexe ». Le second traite un cas particulier de mon projet de thèse démontré pour la première fois par Michel Raynaud en 1974.

La troisième partie, intitulée « Vulgarisation », regroupe certains textes que j'ai écrits, censés être compréhensibles avez assez peu de bagages mathématiques (un bac scientifique est souvent le bienvenu

toutefois). Il y a tout d'abord un texte sur l'axiome du choix qui fait de nombreux rappels en théorie des ensembles classique. Vient ensuite un cours d'arithmétique de base, où l'on présente principalement les congruences et les premiers théorèmes qui vont avec et où l'on explique comment on résout des équations dans $\mathbb{Z}/n\mathbb{Z}$ autant d'un point de vue théorique que pratique. Finalement, on trouve dans cette partie des introductions à des domaines de mathématiques parfois originaux, souvent méconnus, pas forcément simples mais demandant peu de prérequis. Ces introductions ont été rédigées pour de bons élèves de lycée et font travailler le lecteur par l'intermédiaire de questions assez importantes pour l'étude du sujet bien qu'en général non primordiales.

Finalement, la quatrième partie, intitulée « Informatique », présente deux librairies que j'ai écrites et qui peuvent être utiles de façon générale. La première appelée `mp3d` permet de faire relativement facilement des figures en trois dimensions avec Métapost qui peuvent ensuite être insérées dans n'importe document TEX ou LATEX ou n'importe quoi permettant d'introduire un fichier postscript. La seconde appelée `PrettyCurses` est un complément à la libraire `Curses` de perl. Elle implémente un certain nombre d'objets qu'il peut être utile d'avoir sous la main lorsque l'on veut faire un programme de saisie, ces objets étant principalement des zones de saisie, des menus, des formulaires.

Pour finir, je tiens à remercier tout d'abord mon directeur de DEA, Christophe Breuil, mais aussi certains de mes camarades comme Yann Ollivier qui m'a proposé de faire partie de Animath, David Madore qui m'a souvent fait découvrir des horizons nouveaux en mathématiques. Je remercie de façon plus générale tous les professeurs que j'ai eu depuis mon entrée à l'ENS et tous les gens qui m'ont été de bon conseil.

Je vous souhaite bonne lecture.

Première partie

Curriculum Vitæ

Xavier Caruso
né le 24 avril 1980 à Cannes

Adresse : 45, rue d'Ulm – 75005 Paris
Tél : 06.60.81.27.55
Mail : xavier.caruso@ens.fr
Célibataire

Études

1997 Baccalauréat scientifique (mention Bien).

1999 Reçu à Centrale, aux Mines, à Polytechnique et à l'Ecole Normale Supérieure. J'ai choisi d'intégrer l'Ecole Normale Supérieure.

1999/2000 Licence de mathématiques (mention Très Bien). J'ai suivi au sein de l'Ecole Normale Supérieure les cours suivants : Algèbre I (par A. Beauville), Analyse I (par I. Ekeland), Analyse complexe (par Faraud), Intégration et probabilités (par F. Comets), Logique (par A. Louveau).

Maîtrise de mathématiques (mention Très Bien). J'ai suivi au sein de l'Ecole Normale Supérieure les cours suivants : Algèbre II (par L. Illusie), Analyse II (par F. Béthuel), Topologie algébrique (par P. Vogel), Géométrie différentielle (par J.B. Bost), Théorie spectrale (par M. Duflo), Mouvement brownien (par J.F. Le Gall) – sans examen.

Exposé de maîtrise sous la direction de Y. Laszlo intitulé « $\mathbb{Z}$ est simplement connexe ».

Été 2000 Participation en tant qu'intervenant au stage de préparation de la délégation française à l'olympiade internationale de mathématiques.

2000/2001 Début de DEA. J'ai suivi les cours suivants à Orsay et à Chevaleret : Introduction à la géométrie algébrique (par J.B. Bost), Corps locaux, corps de nombres, schémas en groupes commutatifs finis et plats (par J.M. Fontaine), Groupes et algèbres de Lie (par B. Keller), Représentations p-adiques (par P. Colmez) – sans examen, Variétés abéliennes (par J.B. Bost, M. Raynaud et J.M. Fontaine) – sans examen, Théorie des modèles (par M. Dickmann) – sans examen.

Été 2001 Participation en tant qu'auditeur aux Journées Arithmétiques se déroulant cette année à Lille.

Participation en tant qu'intervenant au stage de préparation de la délégation française à l'olympiade internationale de mathématiques.

École d'été à Barcelone sous la direction de Bas Edixhoven et de Christophe Breuil.

2001/2002 Fin de DEA. J'ai suivi les cours suivants à Orsay, à Chevaleret et à Villletanneuse : Cohomologie galoisienne (par J.M. Fontaine), Méthodes pour les corps globaux (par D. Bernardi) – sans examen, Cohomologie étale (par F. Morel), Cohomologie p-adique (par F. Mokrane) – sans examen.

Participation en tant qu'auditeur au groupe de travail « Rappels sur la théorie de Hodge p-adique ; formes modulaires p-adiques et représentations localement analytiques » organisé par Laurent Lafforgue, Christophe Breuil et Amhed Abbes.

Mémoire de DEA sous la direction de Christophe Breuil intitulé « Représentations géométriques du groupe de Galois absolu d'un corps local ».

Été 2002 Participation en tant que professeur à un stage de mathématiques pour élèves de lycée à Vendôme.

Divers

1997 Premier accessit du concours général de Mathématiques.
Quatrième accessit du concours général de Physique.
Participation aux Olympiades Internationales de Mathémathématiques à Mar del Plata en Argentine.

Langages connus : LaTeX, `html`, `C`, `C++`, `perl`
Langues : français (langue maternelle), anglais, notions d'allemand.
Loisirs : promenades, jeux de réflexion.

Deuxième partie

Arithmétique

Chapitre 1

Introduction au domaine de recherche

Sommaire

L'arithmétique est principalement l'étude de l'anneau des entiers relatifs $\mathbb{Z}$, de son corps des fractions $\mathbb{Q}$ formé de ce que l'on appelle les nombres rationnels et des extensions finies ou algébriques de ce dernier. Ce texte se propose de décrire un des multiples aspects de cette étude, et d'énoncer un résultat encore conjectural permettant de voir quelle genre de choses on attend et en quoi elles sont intéressantes.

Ce texte commence donc par faire de très brefs rappels sur la géométrie algébrique et la localisation qui débouchent naturellement sur la présentation de $\mathbb{Q}_p$ et de ses extensions. Il nous faudra aussi consacrer quelques pages à l'étude des groupes de Galois de ces extensions car il s'agit vraiment de l'objet simple à manipuler qui détient énormément d'informations. On sera alors en mesure de conclure en énonçant le résultat dont on a déjà parlé et de donner quelque vague idée de la façon dont on peut l'attaquer.

1.1 Un peu de géométrie algébrique

1.1.1 Les idées de base de la géométrie algébrique

Comme son nom l'indique, la géométrique algébrique essaie de donner un sens géométrique à un objet purement algébrique, précisément aux anneaux. L'idée consiste plus ou moins, étant donné un anneau A, de voir A comme l'anneau des polynômes sur un certain « objet géométrique ». Bien entendu, pour l'instant cela n'a pas grand sens : il reste encore à définir « objet géométrique » et même « anneau des polynômes » parce que si l'on sait ce que sont les polynômes à coefficients dans $\mathbb{R}$, $\mathbb{C}$ ou même n'importe quel anneau, on ne sait pas *a priori* ce qu'est l'anneau des polynômes à coefficients dans un « objet géométrique », typiquement un espace topologique.

Nous n'allons pas ici détailler toutes les constructions permettant de concrétiser la chose précédente car elles ne rentrent pas dans le cadre de cet exposé. Nous allons plutôt présenter un exemple qui permet de se faire une idée intuitive de la situation, puis appliquer cet exemple à l'arithmétique, c'est-à-dire à l'anneau $\mathbb{Z}$.

Donc, pour commencer, on remplace $\mathbb{Z}$ par $\mathbb{C}[u]$, l'anneau des polynômes à une variable à coefficients complexes. D'après ce qui a été dit précédemment, il n'est pas surprenant d'apprendre que l'« objet géométrique » associé à cet anneau est la droite complexe, $\mathbb{C}$ donc. De la même façon, si on avait choisi de considérer $\mathbb{C}[u,v]$, l'anneau des polynômes en deux variables à coefficients complexes, l'« objet géométrique » associé aurait été le plan complexe, c'est-à-dire $\mathbb{C}^2$.

Mais restons avec la droite complexe et donc avec l'anneau $\mathbb{C}[u]$. Ce qu'il est important de remarquer, c'est que ce dictionnaire que nous n'avons que peu détaillé est compatible avec les extensions. Mais, déjà, extension de quoi ? On n'a toujours pas de corps pour l'instant. En fait, le corps que l'on va considérer est le corps des fractions de $\mathbb{C}[u]$, c'est-à-dire $\mathbb{C}(u)$, le corps des fractions rationnelles à coefficients complexes, et ce un peu de la même façon qu'en arithmétique $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$. Bien évidemment, cela ne se généralise pas directement à toutes les situations : il faut au moins supposer que l'anneau considéré est intègre, et même un peu plus pour que les choses se passent correctement, mais nous n'allons pas non plus entrer dans ces détails.

Considérons maintenant K une extension disons finie de $\mathbb{C}(u)$. À partir de cela, on peut en fait construire un nouvel anneau, qui sera inclus dans K, dont le corps des fractions sera K et qui correspondra moralement à l'extension $K/\mathbb{C}(u)$ mais vue simplement sur $\mathbb{C}[u]$. Plus précisément, on a la définition suivante :

Définition 1.1.1.1. *On reprend les notations de la situation précédente. Un élément $x \in K$ est dit* entier *sur $\mathbb{C}[u]$ s'il existe un polynôme P* unitaire *à coefficients dans $\mathbb{C}[u]$ vérifiant $P(x) = 0$. Cela revient en fait simplement à demander que le polynôme minimal de x sur $\mathbb{C}(u)$ soit à coefficient dans $\mathbb{C}[u]$.*

*On définit finalement l'*anneau des entiers *de l'extension $K/C(u)$ comme l'ensemble des éléments $x \in K$ entiers sur $\mathbb{C}[u]$ (dont il faut vérifier par ailleurs qu'il forme bien un anneau). On le note souvent $\mathcal{O}_K$.*

On peut résumer la situation par le diagramme suivant :

$$\begin{array}{ccc} \mathcal{O}_K & \longrightarrow & K \\ {\scriptstyle n}\downarrow & & \downarrow{\scriptstyle n} \\ \mathbb{C}[u] & \longrightarrow & \mathbb{C}(u) \end{array}$$

On a alors plusieurs propriétés intéressantes sur cet anneau des entiers $\mathcal{O}_K$, notamment le fait que si n désigne le dégré de l'extension $K/\mathbb{C}(u)$, $\mathcal{O}_K$ est en fait un $\mathbb{C}[u]$-module libre de dimension n également.

Mais prenons encore un exemple. Prenons tout d'abord $K = \mathbb{C}(u, v)$ qui certes n'est pas une extension finie de $\mathbb{C}(u)$ mais cela n'a pas pour l'instant d'importance. On ne peut pas dans ce cas définir l'anneau des entiers, mais il est ici tout à fait légitime de considérer qu'il s'identifie à $\mathbb{C}[u, v]$.

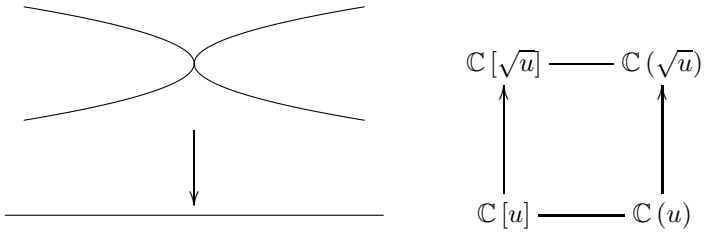
Essayons maintenant de comprendre la vision géométrique. L'« objet géométrique » associé à $\mathbb{C}[u]$ est, comme on l'a déjà dit, la droite complexe $\mathbb{C}$. Également, l'« objet géométrique » associé à $\mathbb{C}[u, v]$ est le plan complexe $\mathbb{C}^2$. L'extension, elle, est en outre donnée par une application $C(u) \to C(u, v)$. Bien entendu, il était sous-entendu précédemment que celle-ci était l'inclusion canonique. Ce qu'il est important de constater, c'est qu'à cette inclusion correspond une application entre les objets géométriques : ici, c'est précisément la première projection $\varphi : \mathbb{C}^2 \to \mathbb{C}$. Pourquoi cela ? Parce que si l'on prend $P \in \mathbb{C}[u]$ et qu'on le compose par φ, c'est-à-dire qu'on lui associe le polynôme $\tilde{P}(u, v) = P \circ \varphi(u, v) = P(u)$, on retrouve précisément l'inclusion canonique qui définissait l'extension dont on était parti.

Essayons maintenant de faire la même chose sur un exemple qui est une extension finie. Prenons par exemple $\mathbb{C}(\sqrt{u})$ qui est bien une extension de $\mathbb{C}(u)$, là encore en utilisant l'inclusion canonique. On peut encore déterminer l'anneau des entiers dans ce cas et voir qu'il s'identifie à $\mathbb{C}[\sqrt{u}]$. Pour comprendre quel « objet géométrique » on va associer à cet anneau, il est nécessaire de modifier un peu son écriture. Ajouter $\sqrt{u}$, c'est ajouter une nouvelle variable v et imposer que celle-ci vérifie $v^2 = u$. Autrement dit, $\mathbb{C}[\sqrt{u}]$ n'est autre que le quotient $\mathbb{C}[u, v] / (v^2 - u)$. Il s'agit donc de trouver une partie de $\mathbb{C}^2$ sur laquelle les polynômes sont définies à $(v^2 - u)$ près, c'est-à-dire sur laquelle ajouter ou enlever $(v^2 - u)$ ne modifie rien, c'est-à-dire sur laquelle $(v^2 - u)$ est nul. On prend donc la partie :

$$A = \left\{(u, v) \in \mathbb{C}^2 \;\middle|\; v^2 = u\right\}$$

Il s'agit d'une parabole et de la même façon que tout à l'heure l'application de A dans $\mathbb{C}$ qui correspond à notre extension est encore la première projection.

Récapitulons avec le dessin suivant :



1.1.2 De l'intérêt de la localisation et de la complétion

On aimerait dire au vu du dessin précédent que l'extension $\mathbb{C}(\sqrt{u})/\mathbb{C}(u)$ ne se comporte pas de la même façon en 0 qu'ailleurs. Mais dit comme ça, cette phrase n'a pas de sens. C'est ce que nous allons plus ou moins préciser dans ce paragraphe.

Notons que l'on aimerait une description locale certes, mais aussi purement algébrique puisque l'on aimerait l'appliquer ensuite à l'arithmétique, c'est-à-dire à $\mathbb{Z}$ et $\mathbb{Q}$. On n'a donc plus le choix maintenant, il va nous falloir préciser quelque peu comment on construit l'« objet géométrique » associé à un anneau donné. Citons pour cela le théorème suivant :

Théorème 1.1.2.1. *Les idéaux maximaux de* $\mathbb{C}[u]$ *sont exactement ceux engendrés par les éléments* $(u-x)$ *où* x *parcourt* $\mathbb{C}$.

Ce théorème dit si l'on peut regarder la droite complexe non pas comme un ensemble de complexes justement, mais plutôt comme un ensemble d'idéaux maximaux de l'anneau $\mathbb{C}(u)$. Plus précisément au lieu de parler du complexe x, il s'agit de parler de l'idéal engendré par $(u-x)$ (qui est maximal), mais cela ne modifie guère les choses finalement. Cette définition se généralise en fait plus ou moins, et dans de bonnes conditions, on peut considérer que l'« objet géométrique » associé à un anneau est en fait l'ensemble de ces idéaux maximaux[1]. Bien évidemment, il faut encore définir la géométrie sur cet objet mais nous n'allons pas le faire.

On aimerait maintenant faire la chose suivante. On considère un complexe x ou si l'on préfère un idéal maximal de $\mathbb{C}(u)$ et on aimerait construire à partir de cela, on nouvel anneau dont l'« objet géométrique » associé serait le seul point x. On aimerait en outre que si l'on part d'une extension de $\mathbb{C}(t)$, celle-ci fournisse une « extension » de ce nouveau anneau, dont l'« objet géométrique » associé soit exactement l'ensemble des points qui se projettent sur x.

Une solution pour arriver à ça est d'éliminer tous les idéaux maximaux de $\mathbb{C}[u]$ différents de $(u-x)$. Cela se fait en inversant formellement tous les éléments qui n'appartiennent pas à l'idéal engendré par $(u-x)$. On pose donc :

$$\mathbb{C}[u]_x = \left\{ \frac{P}{Q} \,\middle|\, (u-x) \text{ ne divise pas } Q \right\}$$

Ce nouvel anneau s'appelle naturellement le *localisé* de $\mathbb{C}[u]$ en l'idéal maximal engendré par $(u-x)$ et répond bien à la question que l'on se posait.

Mais cela ne nous suffit pas, principalement car l'étude des « extensions » de cet anneau repose en général principalement sur l'étude de l'extension correspondante du corps des fractions et on peut vérifier facilement que le corps des fractions n'a pas changé. Donc, après avoir *localisé*, il va falloir *compléter*. L'idée qui se cache derrière le procédé de complétion est en fait assez simple. Comme tout à l'heure on a rajouté formellement des inversibles, il s'agit maintenant de rajouter l'élément $\sqrt{u}$, mais seulement au « voisinage » de $x \in \mathbb{C}^\star$, de sorte qu'il n'apparaisse plus lorsque l'on regarde l'extension de notre nouveau corps, et ce pour la bonne raison qu'il y était déjà avant. Cela pour l'instant n'a pas grand sens mais voyons comment on procède.

Un bon moyen de s'en sortir dans ce cas est de considérer non plus l'anneau des polynômes à une variable à coefficients dans $\mathbb{C}$, mais celui des séries formelles. On remarquera qu'ainsi on a en outre rajouter les inverses qui nous manquaient tout à l'heure. On constatera d'ailleurs que cela revient exactement à rajouter la fonction $\frac{1}{u}$ au « voisinage » de $x \neq 0$.

La situation est donc maintenant devenue la suivante. On part de $\mathbb{C}[\![u]\!]$, l'anneau des séries formelles à coefficients dans $\mathbb{C}$, on considère son corps des fractions $\mathbb{C}((u))$. L'extension qui correspond à $\mathbb{C}(\sqrt{u})$ est $\mathbb{C}((\sqrt{u}))$ ou encore $\mathbb{C}((u,v)) / (v^2 - u)$. On ne voit peut-être pas encore très bien l'intérêt de considérer ces objets plus gros, ni pourquoi d'ailleurs ce corps ne contient vraiment qu'une information locale mais cela va devenir clair avec le théorème suivant :

[1] La définition générale consiste non pas à prendre l'ensemble des idéaux maximaux, mais plutôt l'ensemble des idéaux premiers pour former ce que l'on appelle le *spectre* de l'anneau.

Théorème 1.1.2.2 (Puiseux). *Toute extension finie de $\mathbb{C}((u))$ est de la forme $\mathbb{C}((\sqrt[n]{u}))$ où n est tout simplement de l'extension considérée.*

Sur notre exemple, si l'on regarde au-dessus de 0, l'extension est comme on vient de le voir $\mathbb{C}((\sqrt{u}))$, ce qui signifie qu'au dessus de 0 deux courbes se croisent. Ailleurs, l'extension n'aurait pas été un corps, elle aurait été $\mathbb{C}((u)) \times \mathbb{C}((u))$, ce qui signifie bien qu'il y a deux courbes mais qu'elles ne se croisent pas. Plus généralement, si au-dessus d'un point l'extension est $\mathbb{C}((\sqrt[n_1]{u})) \times \ldots \times \mathbb{C}((\sqrt[n_k]{u}))$, cela voudra dire qu'on aura un paquet de n_1 courbes qui se croisent en un point, puis un paquet de n_2 courbes qui se croisent en un autre point et ainsi de suite.

Noter finalement que ceci n'aurait pas marché aussi bien si l'on avait remplacé $\mathbb{C}$ par $\mathbb{R}$ par exemple. En effet, $\mathbb{C}((t))$ est aussi une extension finie de $\mathbb{R}((t))$ et pourtant n'entre pas dans le cadre précédent. Là, l'erreur n'est pas difficile à corriger puisqu'il suffit d'autoriser $\mathbb{R}$ et $\mathbb{C}$. Plus généralement si on remplace $\mathbb{C}$ par un corps k de caractéristique nulle, l'erreur se corrige encore de la même façon en disant que les extensions finies de $k((u))$ sont de la forme $K((\sqrt[n]{u}))$ où n est un entier et K une extension finie de k. Cette extension finie toutefois ne va pas se voir directement sur le dessin.

1.2 Un peu d'arithmétique

À partir de maintenant, on remplace l'anneau $\mathbb{C}[u]$ par $\mathbb{Z}$, l'anneau des nombres entiers relatifs. On remplace donc évidemment $\mathbb{C}(u)$ par $\mathbb{Q}$, le corps des nombres rationnels et on va essayer de généraliser la vision géométrique donnée précédemment à cet exemple.

1.2.1 L'identité géométrique des entiers

L'« objet géométrique » associé à l'anneau $\mathbb{Z}$ va être comme on l'a déjà plus ou moins expliqué l'ensemble des nombres premiers, que l'on va noter $\mathcal{P}$.

Prenons maintenant K ce que l'on appelle un *corps de nombres*, c'est-à-dire une extension finie de $\mathbb{Q}$. Comme tout à l'heure, on peut considérer l'anneau des entiers et l'une des questions que l'on peut se poser est de décrire $\mathcal{O}_K$ et en particulier de décrire l'« objet géométrique » qui lui est associé.

De fait, les méthodes précédentes s'adaptent pour la description de cet objet géométrique. On commence par choisir un nombre premier p, on localise, on complète, on obtient ainsi un corps appelé $\mathbb{Q}_p$ dont la construction sera expliquée au paragraphe suivant. L'extension K va fournir une algèbre au-dessus de $\mathbb{Q}_p$, précisément l'algèbre $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$ et celle-ci va se décomposer en produits d'extensions finies de $\mathbb{Q}_p$ et comme précédemment il y a un moyen relativement simple étant donné une extension finie de $\mathbb{Q}_p$ de déterminer à combien d'intersections elle correspond.

1.2.2 Présentation de $\mathbb{Q}_p$

Tout à l'heure, on a un peu sorti magiquement l'anneau $\mathbb{C}[\![u]\!]$, mais en fait ceci n'a rien d'anecdotique et peut même se généraliser relativement simplement. Pour cela, il faut avoir le bon point de vue sur les séries formelles : une série formelle est en fait la donnée pour tout entier n d'un polynôme de degré n et ce de façon compatible, cela voulant dire que les coefficients de bas degré coïncident quand ils le peuvent. Dans un langage que certains trouvent châtié, cela s'écrit :

$$\mathbb{C}[\![u]\!] = \varprojlim_{n \in \mathbb{N}} \mathbb{C}[u]/u^n$$

Bien entendu si l'on avait voulu regarder au voisinage de 1, il aurait fallu considérer :

$$\varprojlim_{n \in \mathbb{N}} \mathbb{C}[u]/(u-1)^n$$

Pour $\mathbb{Z}$, on fait la même chose en posant :

$$\mathbb{Z}_p = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$$

Un élément de $\mathbb{Z}_p$ est ainsi une sorte de série formelle en p, mais il faut faire attention qu'il ne faut ni les additionner, ni les multiplier comme on le fait avec des séries formelles classiques. Cela est dû au fait que $\mathbb{Z}/p^n\mathbb{Z}$ n'est pas isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$ ni en tant qu'anneau, ni même en temps que groupe. Il est même possible de dire *via* ces analogies où on devrait prendre les coefficients pour former une telle série formelle : il s'agit simplement du premier quotient de la limite projective, c'est-à-dire ici $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

On a en fait un énoncé précis qui dit tout ça :

Théorème 1.2.2.1 (Développement de Hensel). *Soit S un système de représentants dans $\mathbb{Z}$ des classes de $\mathbb{Z}/p\mathbb{Z}$ (par exemple on peut prendre $S = \{0, 1, \ldots, p-1\}$). Alors tout élément $x \in \mathbb{Z}_p$ s'écrit de façon unique sous la forme :*

$$x = \sum_{n=0}^{\infty} a_n p^n$$

où tous les a_n sont des éléments de S.

On remarque tout d'abord que l'addition ce coup-ci est vraiment celle de $\mathbb{Z}_p$ mais qu'il n'y a pas de formules simples pour exprimer les coefficients qui apparaissent dans la décomposition de $x + y$ en fonction de ceux qui apparaissent dans celle de x et celle de y. Il n'y a pas non plus de formule simple pour le produit.

On remarque en outre qu'il aurait été possible de choisir les éléments de S non pas dans $\mathbb{Z}$ mais dans $\mathbb{Z}_p$, ceci principalement car pour tout entier n, les anneaux $\mathbb{Z}/p^n\mathbb{Z}$ et $\mathbb{Z}_p/p^n\mathbb{Z}_p$ sont isomorphes et donc $\mathbb{Z}_p$ s'écrit également comme la limite projective suivante :

$$\mathbb{Z}_p = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p/p^n\mathbb{Z}_p$$

Il s'agit finalement de définir $\mathbb{Q}_p$ qui est bien entendu le corps des fractions de $\mathbb{Z}_p$. De la même façon que pour les séries formelles, il suffisait d'inverser u pour passer de $\mathbb{C}[\![u]\!]$ à $\mathbb{C}((u))$, ici, il suffit d'inverser p pour passer de $\mathbb{Z}_p$ à $\mathbb{Q}_p$. De plus, le développement de Hensel s'adapte aussi pour décrire les éléments de $\mathbb{Q}_p$:

Théorème 1.2.2.2 (Développement de Hensel). *Soit S un système de représentants dans $\mathbb{Z}$ des classes de $\mathbb{Z}/p\mathbb{Z}$ (par exemple on peut prendre $S = \{0, 1, \ldots, p-1\}$). Alors tout élément $x \in \mathbb{Q}_p$ s'écrit de façon unique sous la forme :*

$$x = \sum_{n=-\infty}^{\infty} a_n p^n$$

où tous les a_n sont des éléments de S et les a_n sont nuls pour n suffisamment petit.

1.2.3 Description de $\mathbb{Q}_p$

Il est possible d'améliorer quelque peu le développement de Hensel. En fait, il existe une unique application $T : \mathbb{F}_p \to \mathbb{Z}_p$ qui soit multiplicative et une section de la projection canonique.

Si $a \in \mathbb{F}_p$, on note traditionnellement $[a]$ l'image de a par l'application T définie précédemment, c'est ce que l'on appelle le *représentant de Teichmüller* de a. Il n'est pas forcément difficile de la construire mais nous n'allons pas le faire ici.

On peut maintenant utiliser ces représentants particuliers dans le développement de Hensel, les opérations pouvant alors s'exprimer par des formules certes compliquées mais qui existent. Elles sont de la forme, si a_n et b_n sont des éléments de $\mathbb{F}_p$:

$$\begin{aligned}\left(\sum_{n\in\mathbb{N}}[a_n]\,p^n\right)+\left(\sum_{n\in\mathbb{N}}[b_n]\,p^n\right) &= \sum_{n\in\mathbb{N}}[S_n]\,p^n\\ \left(\sum_{n\in\mathbb{N}}[a_n]\,p^n\right)\times\left(\sum_{n\in\mathbb{N}}[b_n]\,p^n\right) &= \sum_{n\in\mathbb{N}}[P_n]\,p^n\end{aligned}$$

où S_n et P_n s'expriment comme des polynômes à coefficients entiers en $a_0,\ldots,a_n,b_0,\ldots,b_n$, polynômes très laborieux à écrire au demeurant.

On remarquera que cette description aurait aussi permis de définir directement $\mathbb{Z}_p$ par un autre procédé. Il aurait fallu considérer les suites d'éléments de $\mathbb{F}_p$ et mettre sur cet ensemble les lois définies par les polynômes mentionnés précédemment. Cela n'est en fait pas sans intérêt car l'on peut remplacer $\mathbb{F}_p$ par n'importe quel anneau et l'on construit ainsi à chaque fois un anneau. L'anneau construit à partir de A s'appelle l'*anneau des vecteurs de Witt* de A et se note traditionnellement $W(A)$.

On peut de façon analogue construire le développement « décimal » d'un élément de $\mathbb{Q}_p$, c'est-à-dire un élément du quotient de $\mathbb{Q}_p/\mathbb{Z}_p$ en invoquant les *covecteurs de Witt*. Finalement, on peut aussi construire les éléments de $\mathbb{Q}_p$ ce coup-ci avec les *bi-vecteurs de Witt*.

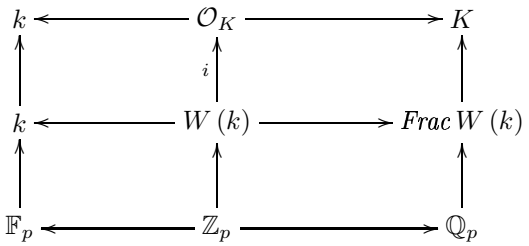
1.2.4 Les extensions finies de $\mathbb{Q}_p$

On aimerait avoir un théorème analogue à l'énoncé 1.1.2.2, mais ceci ne se passe aussi bien dans ce contexte et ce parce que $\mathbb{F}_p$ n'est ni algébriquement clos, ni de caractéristique nulle.

Commençons par voir ce que l'on peut faire pour le premier écueil. On avait vu dans les remarques suivant ledit théorème que si $\mathbb{C}[u]$ était remplacé par $k[u]$, il fallait faire attention à ne pas oublier les extensions de la forme $K[u]$ où K était une extension finie de k. Ici, c'est pareil à quelques transpositions près : si k est une extension finie de $\mathbb{Q}_p$, il ne faut pas oublier les extensions du type $\mathrm{Frac}\,W(k)$, où W désigne toujours l'anneau des vecteurs de Witt.

Un résultat précis est le théorème suivant :

Théorème 1.2.4.1. *Soit K une extension finie de $\mathbb{Q}_p$. On note $\mathcal{O}_K$ l'anneau des entiers de K et k le quotient $K/\mathcal{O}_K$ appelé généralement le corps résiduel. Dans ces conditions, il existe une unique application $i : W(k) \to \mathcal{O}_K$ faisant commuter le diagramme suivant :*



l'application $W(k) \to k$ étant celle qui à la suite $(a_0,\ldots,a_n,\ldots)$ associe a_0.

Ce théorème dit donc que l'on peut intercaler au milieu d'une extension finie K de $\mathbb{Q}_p$ une extension ayant le même corps résiduel que K et qui plus est peut se construire à partir des vecteurs de Witt. Ce que l'on aimerait désormais, c'est que K s'obtienne à partir de $W(k)$ simplement en ajoutant une racine

n-ième de $p = (0, 1, 0, \ldots, 0, \ldots)$ pour un certain n. Mais cela n'est pas vrai et c'est là qu'intervient le deuxième écueil.

Toutefois la situation n'est pas aussi désespérée qu'on pourrait le croire car cela est vrai si le degré de l'extension n'est pas un multiple du nombre premier p. Récipatulons tout cela en énonçant un nouveau théorème :

Théorème 1.2.4.2. *Soit k une extension finie de $\mathbb{F}_p$ et K une extension finie du corps Frac$W(k)$ dont le degré n est premier à p. Alors l'extension $K/\text{Frac}W(k)$ est isomorphe à l'extension Frac$W(k)\left[\sqrt[n]{p}\right]/\text{Frac}W(k)$.*

Attention, cela n'est plus vrai si p divise e.

1.2.5 La clôture algébrique de $\mathbb{Q}_p$

Ce que l'on a dit précédemment s'applique plus ou moins également à la clôture algébrique $\bar{\mathbb{Q}}_p$ de $\mathbb{Q}_p$. Donnons tout de suite le diagramme qui résume les résultats que l'on va commenter par la suite.

$$\begin{array}{ccc}
\bar{\mathbb{F}}_p & & \bar{\mathbb{Q}}_p \\
\Big| & & \Big| I_s \\
\bar{\mathbb{F}}_p & & \mathbb{Q}_p^{\text{mr}} \\
\Big| & & \Big| I_m = \varprojlim_{p\nmid n} \mathbb{Z}/n\mathbb{Z} = \prod_{\ell\neq p} \mathbb{Z}_\ell \\
\bar{\mathbb{F}}_p & & \mathbb{Q}_p^{\text{nr}} \\
\Big| & & \Big| \text{Gal}\left(\bar{\mathbb{F}}_p/\mathbb{F}_p\right) = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}} \\
\mathbb{F}_p & & \mathbb{Q}_p
\end{array}$$

Tout d'abord, on regarde l'extension que l'on obtient en rajoutant des éléments dans le corps résiduels : c'est $\mathbb{Q}_p^{\text{nr}}$, l'*extension maximale non ramifiée* comme on l'appelle généralement[2]. $\mathbb{Q}_p^{\text{nr}}/\mathbb{Q}_p$ est une extension galoisienne et le groupe de Galois s'identifie au groupe de Galois absolu de $\mathbb{F}_p$.

Vient ensuite l'extension maximale modérément ramifiée. Elle s'obtient précisément en rajoutant à $\mathbb{Q}_p^{\text{nr}}$ toutes les racines n-ième de p où n parcourt l'ensemble des entiers qui ne divisent pas p. Le théorème 1.2.4.2 s'applique également à cette situation et dit donc que si K est une extension finie de $\mathbb{Q}_p^{\text{nr}}$ de degré premier à p, alors elle est incluse dans $\mathbb{Q}_p^{\text{mr}}$.

Déterminer le groupe de Galois est quelque chose de relativement simple. Il suffit pour cela de choisir un entier n qui ne divise pas p et de se convaincre que l'extension $\mathbb{Q}_p^{\text{nr}}\left[\sqrt[n]{p}\right]/\mathbb{Q}_p$ est galoisienne de groupe de Galois $\mathbb{Z}/n\mathbb{Z}$.

Ce groupe de Galois est noté I_m et s'appelle le *groupe d'inertie modérée*. C'est lui qui va nous intéresser par la suite.

La dernière extension, elle, est plus compliquée à étudier. Elle est galoisienne évidemment et son groupe de Galois, noté I_s, est le *groupe d'inertie sauvage*. Décrire ce groupe n'est pas quelque chose d'immédiat, il est encore nécessaire pour cela d'introduire des extensions intermédiaires et même *a priori* en nombre infini. Nous n'allons pas plus détailler les choses vu que par la suite on ne s'intéressera systématiquement pas à ce groupe.

Finalement disons que le groupe de Galois de l'extension $\bar{\mathbb{Q}}_p/\mathbb{Q}_p^{\text{nr}}$ est appelé le *groupe d'inertie*.

[2]Le terme *non ramifié* vient du fait que si l'on regarde l'« objet géométrique » associé à cette extension, il n'y a qu'un trait, pas plusieurs qui se croisent.

1.3 Énoncé du résultat conjectural principal

Ce résultat commence par construire par des moyens géométriques des représentations dans un $\mathbb{F}_p$-espace vectoriel du groupe de Galois absolu de $\mathbb{Q}_p$, plus ou moins décrit précédemment donc. L'objet du théorème est de décrire ces représentations. Mais ces descriptions sont difficiles à faire principalement parce que la structure complète du groupe de Galois est difficile à décrire ; on va donc se débrouiller par la suite pour n'obtenir des représentations que du groupe d'inertie modérée que lui, on connaît quand même mieux.

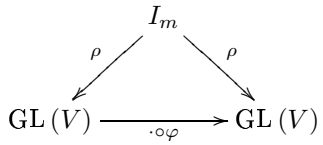
On commence cette partie en expliquant comment l'on peut classifier quelques unes des représentations de ce groupe d'inertie modérée.

1.3.1 Représentations simples du groupe d'inertie modérée

On se donne ρ une représentation *continue* de groupe d'inertie modérée de dimension finie, disons r, dans un $\mathbb{F}_p$-espace vectoriel. On rappelle que cela signifie que ρ est un morphisme de groupes de I_m dans $\mathrm{GL}(V)$ où V est un $\mathbb{F}_p$-espace vectoriel de dimension r. On peut aussi également voir ρ comme une action du groupe I_m sur l'espace vectoriel V, action respectant la linéarité.

La continuité de la représentation est simplement la continuité de ρ lorsque I_m est munie de la topologie profinie d'un groupe de Galois et lorsque V est muni de la topologie discrète. Si vous ne savez pas ce qu'est la topologie profinie d'un groupe de Galois, la continuité revient simplement à supposer que le noyau de ρ est d'indice finie dans I_m.

On va supposer pour l'instant que la représentation ρ est simple, c'est-à-dire qu'il n'existe pas de sous-espace vectoriel strict et non nul de V stable par tous les endomorphimes de l'image de ρ. On peut alors considérer l'ensemble des endomorphismes de ρ, souvent noté $\mathrm{End}(\rho)$. Il s'agit de l'ensemble des applications linéaires $\varphi : V \to V$ faisant commuter le diagramme suivant :



Il est remarquable de voir que muni de l'addition et de la composition des applications, l'ensemble $\mathrm{End}(\rho)$ hérite d'une structure de corps. Pour cela, il suffit de voir que toute application linéaire $\varphi \in \mathrm{End}(\rho)$, $\varphi \neq 0$, est une bijection. Mais si φ est non nulle, son noyau ne peut être V tout entier, mais il s'agit d'un espace stable pour tous les éléments de l'image de φ comme on peut le constater facilement, et donc comme on a supposé que ρ était simple, φ est injective. De même, en considérant l'image on montre que φ est surjective.

Une autre chose de remarquable est que l'ensemble $\mathrm{End}(\rho)$ est fini, puisque par exemple inclus dans $\mathrm{M}_r(\mathbb{F}_p)$, et donc il s'agit d'un corps fini. Celui-ci est donc en particulier commutatif. En outre, il est facile de voir que ce corps est de caractéristique p. Il est donc finalement isomorphe (non canoniquement) à $\mathbb{F}_q$ où $q = p^{r'}$ est une certaine puissance de p. Introduire $\mathbb{F}_q$ de cette façon n'est sans doute pas très adroit ; il est probablement mieux de fixer au préalable une clôture algébrique de $\mathbb{F}_p$, disons $\overline{\mathbb{F}}_p$, et de définir $\mathbb{F}_q$ par :

$$\mathbb{F}_q = \left\{ x \in \overline{\mathbb{F}}_p \mid x^q = x \right\}$$

Maintenant, V hérite d'une structure de $\mathrm{End}(\rho)$-espace vectoriel simplement en faisant naturellement agir les applications de $\mathrm{End}(\rho)$ sur les éléments de V. Mais tout $\mathrm{End}(\rho)$-sous-espace vectoriel de V va

être directement stable par tous les éléments de l'image de ρ. Comme on rappelle que l'on a supposé que ρ était simple, cela implique que V est en fait de dimension 1 sur $\mathrm{End}(\rho)$. En comptant les éléments maintenant, on obtient en outre $r = r'$.

Fixons maintenant un isomorphisme de corps $\varphi : \mathrm{End}(\rho) \to \mathbb{F}_q$ où $q = p^r$. Une chose à remarquer alors est que l'image de ρ est consitité d'applications $\mathrm{End}(\rho)$-linéaires et pas simplement $\mathbb{F}_p$-linéaires. D'autre part, comme V est de dimension 1 sur $\mathrm{End}(\rho)$, les applications $\mathrm{End}(\rho)$-linéaires de V sont simplement les multiplications par des scalaires, et donc on peut dire :

$$\rho : I_m \to (\mathrm{End}(\rho))^\star$$

ou encore si on utilise l'identification *via* φ :

$$\rho : I_m \to \mathbb{F}_q^\star$$

En outre, comme ρ est supposée continue, rappelons-le, la description de I_m nous dit que ρ va se factoriser en une application :

$$\rho : \mathrm{Gal}\left(\mathbb{Q}_p^{\mathrm{nr}}\left[\sqrt[n]{p}\right]/\mathbb{Q}_p^{\mathrm{nr}}\right) \to \mathbb{F}_q^\star$$

où n est un entier non divisible par p, et on peut même choisir $n = q - 1$.

Mais le groupe de Galois $\mathrm{Gal}\left(\mathbb{Q}_p^{\mathrm{nr}}\left[\sqrt[q-1]{p}\right]/\mathbb{Q}_p^{\mathrm{nr}}\right)$ s'identifie à l'ensemble des racines $(q-1)$-ième de l'unité dans $\bar{\mathbb{Q}}_p$, tout simplement en regardant par quoi est multiplié π, une racine $(q-1)$-ième de p ajoutée et fixée à l'avance. Et on peut montrer que l'ensemble de ces racines s'identifie également après réduction modulo p à l'ensemble $\left\{x \in \bar{\mathbb{F}}_p \;\middle|\; x^{q-1} = 1\right\}$ qui est précisément $\mathbb{F}_q^\star$.

Finalement ρ peut être vue comme un endomorphisme de groupes de $\mathbb{F}_q^\star$. Le groupe $\mathbb{F}_q^\star$ est cyclique de cardinal $q-1$, cet endomorphisme est donc simplement la multiplication d'un élément de $\mathbb{Z}/(q-1)\mathbb{Z}$. Mais ce nombre n'est pas canonique, il dépend de l'isomorphisme φ choisi au début. En fait, il n'est pas dur de voir que si l'on change φ en un φ', ce nombre va être multiplié par une puissance de p. L'idée consiste donc à écrire ce nombre en base p et à regarder la suite des chiffres écrits qui elle ne dépend pas de φ (plus précisément, seul l'endroit où l'on commence à lire la suite en dépend).

Récapitulons brièvement ce que l'on vient de faire. On vient d'associer à toute représentation continue simple de I_m dans un $\mathbb{F}_p$-espace vectoriel de dimension r, une suite de r entiers compris entre 0 et $p-1$. Cette association dépend en fait du choix d'un isomorphisme entre $\mathrm{End}(V)$ et $\mathbb{F}_q^\star$ mais une fois ce choix fait, on obtient presque une bijection, le seul écueil étant que les deux suites $(0,\ldots,0)$ et $(p-1,\ldots,p-1)$ correspondent toutes deux à la représentation triviale qui d'ailleurs n'est pas simple si $r \geqslant 2$. En outre, lorsque l'on modifie le choix de l'isomorphisme φ, la suite se modifie simplement par translation des termes ; en particulier les valeurs prises sont exactement les mêmes.

1.3.2 Un cas particulier

On considère ici une variété abélienne sur $\mathbb{Q}_p$. Nous n'allons pas définir précisément ce qu'est une *variété abélienne*, il est en gros nécessaire de savoir qu'il s'agit d'une variété, c'est-à-dire quelque chose défini localement comme le domaine d'annulation dans $\mathbb{Q}_p^n$ de polynômes à n variables à coefficients dans $\mathbb{Q}_p$. Le terme supplémentaire « abélienne » dit que l'on suppose quelques conditions de régularité sur la variété correspondant moralement à la connexité, à la compacité et à la lissité et que l'on met en outre sur cette variété une structure de groupe commutatif dont les lois de multiplication et de passage à l'inverse sont données par des formules polynômiales à coefficients dans $\mathbb{Q}_p$.

On suppose maintenant que cette variété abélienne à un modèle sur $\mathbb{Z}_p$, c'est-à-dire en fait que les polynômes qui servent à la définir ainsi que ceux servant à définir les lois peuvent être choisis à coefficients dans $\mathbb{Z}_p$. On suppose en outre des conditions de régularité sur le modèle, c'est-à-dire sur la variété définie

sur $\mathbb{Z}_p$ par les polynômes précédents. Ces conditions de régularité sont encore moralement la compacité et la lissité.

On étend dans un premier temps les scalaires à $\bar{\mathbb{Q}}_p$, cela revient à dire que l'on regarde la variété définie sur $\bar{\mathbb{Q}}_p$ par les mêmes polynômes que précédemment. On regarde ensuite dans cette nouvelle variété les points de p-torsion, c'est-à-dire l'ensemble des points qui sont tués par p pour la structure de groupe donnée sur la variété. On peut montrer qu'il s'agit d'un groupe fini, dont bien évidemment tous les éléments sont tués par p, c'est-à-dire en fait d'un $\mathbb{F}_p$-espace vectoriel, disons V.

Sur cet espace vectoriel agit naturellement le groupe de Galois de $\bar{\mathbb{Q}}_p$ sur $\mathbb{Q}_p$, mais on a dit que celui-ci était trop compliqué et qu'on préférait se restreindre au groupe d'inertie modérée, il s'agit donc de récupérer une action du groupe d'inertie modérée.

Dans un premier temps, le groupe d'inertie est un sous-groupe du groupe de Galois absolu de $\mathbb{Q}_p$. On peut donc commencer par restreindre la réprésentation d'inertie. Maintenant, on aimerait pouvoir factoriser par le groupe d'inertie sauvage, mais pour cela il faudrait qu'il agisse trivialement ce qui n'est en général pas le cas.

Ce que l'on fait, c'est que l'on considère une suite de Jordan-Hölder de notre représentation. Le résultat est qu'il existe toujours une suite :

$$0 = V_0 \subset V_1 \subset \ldots \subset V_k = V$$

qui soit telle que tous les V_i sont stables par la représentation et que celle-ci déduite sur le quotient V_{i+1}/V_i est simple. On peut en même montrer que ces quotients sont uniquement déterminés à réordonnement près.

Cela permet donc de récupérer $\rho : I_m \to W$ une représentation en choisissant l'un des quotients précédents.

Un petit lemme prouve que cette nouvelle représentation, du fait de sa simplicité, est triviale sur le groupe d'inertie sauvage I_s. Démontrons-le. Le groupe I_s est un pro-p-groupe qui agit sur V. Si $x \in W$, l'orbite de x est naturellement en bijection avec un sous-groupe de I_s et donc est de cardinal une puissance de p. Ainsi si x n'est pas fixé par I_s, son orbite va être de cardinal un multiple de p et finalement l'ensemble des $x \in W$ fixés par I_s va aussi être de cardinal un multiple de p. Cet ensemble sera donc non trivial, mais il forme un sous-espace stable de V. Comme la représentation est supposée simple, il est égal à W, ce qui démontre la propriété.

On récupère ainsi une représentation encore simple $\rho : I_m \to W$ qui d'après le paragraphe précédent peut-être décrite pour une suite de r entiers compris entre 0 et $p-1$. Le résultat, dû à RAYNAUD dit que dans ce cas, tous les entiers qui apparaissent sont soit 0, soit 1.

1.3.3 L'énoncé général

L'énoncé précédent peut en fait se généraliser amplement. Nous allons juste donner l'énoncé et pas essayer d'expliquer rigoureusement tous les termes qui apparaissent parce que ce serait désespéremment trop long.

On commence donc par prendre K une extension finie de $\mathbb{Q}_p$. Si k est le corps résiduel de K, on a vu que K pouvait être vu comme une extension du corps $\mathrm{Frac}\, W(k)$. Le degré de cette extension est noté e et est appelé l'*indice de ramification absolu* de K. Par exemple, si $K = \mathbb{Q}_p$, ce nombre vaut 1.

On considère maintenant une variété X propre et lisse sur K et on suppose que X admet un modèle propre, à réduction semi-stable sur l'anneau des entiers $\mathcal{O}_K$. Il faut juste savoir ici que « propre » est moralement un équivalent de « compact », que « à réduction semi-stable » signifie que l'on autorise certains types de singularités mais relativement gentilles.

On remarquera que l'on ne prend pas, dans ce cas général, une structure de groupe sur la variété. Ce qui va remplacer les points de p-torsion va être le dual d'un groupe de cohomologie étale. Plus précisément pour tout entier i, on peut regarder le groupe :

$$H^{i\ \star}_{\text{ét}}(X_{\bar{K}}, \mathbb{Z}/p\mathbb{Z})$$

où $\bar{K}$ est une clôture algébrique de K et donc $X_{\bar{K}}$ l'extension de X à $\bar{K}$. Si vous ne savez pas ce qu'est la cohomologie étale, il est sans doute bien de voir ça comme une boîte noire, comme une façon de construire un groupe qui décrit en gros la forme de la variété.

On fait ensuite la même chose que précédemment. Sur ce groupe de cohomologie, agit naturellement le groupe de Galois absolu de K. On restreint son action au groupe d'inertie (que l'on définit de la même façon que dans le cas de $\mathbb{Q}_p$), on considère un quotient de Jordan-Hölder, la représentation obtenu est alors simple et se factorise par le groupe d'inertie modérée. Il apparaît comme précédemment des nombres *a priori* compris entre 0 et $p-1$. La conjecture générale dit que ces nombres sont toujours inférieurs ou égaux à ie.

1.3.4 Les cas connus, les méthodes d'attaque

Il y a principalement deux cas de la conjecture précédente qui sont connus. Il s'agit du cas $i = 1$, démontré pour la première fois par Raynaud et du cas $e = 1$, démontré pour la première fois par Fontaine-Laffaille Messing pour le cas de bonne réduction et par Breuil pour le cas général. Le cas $i = 1$ a plus ou moins fait l'objet de mon mémoire de DEA, la formulation était quelque peu différente mais on peut si ramener. La méthode consiste alors à associer à ces objets compliqués que sont les variétés des objets plus simples censées les classifier qui sont essentiellement des modules sur $\mathcal{O}_K$ ou sur un anneau un peu plus compliqué, munis de certains applications. Démontrer le théorème devient ensuite un exercice d'algèbre linéaire, pas forcément simple mais toute la géométrie a plus ou moins disparue du problème.

Pour le cas général, la méthode d'attaque est similaire. Il faudra dans un premier temps associer à ces représentations provenant de la géométrie des objets d'algèbre linéaire qui conservent l'information voulue. Ces objets ont pour la plupart déjà été construits, introduits par Fontaine et largement généralisés par Breuil, et se présentent sous la forme de modules munis de filtrations et d'endomorphismes.

Il faudra ensuite manipuler ces objets d'algèbre linéaire pour obtenir l'information que l'on souhaite et simplement constater que le théorème est vrai.

Bien évidemment, ceci n'est qu'un schéma très simplifié de ce qu'il va falloir faire et il est évident que de nombreuses surprises attendent et vont appraître au fur et à mesure.

Bibliographie

[Ber77] P. Berthelot. Systèmes de honda des schémas en $\mathbb{F}_q$-vectoriels. *Bull. Soc. math. France*, 105 :225–239, 1977.

[Bre97] C. Breuil. Construction de représentations p-adiques semi-stables. *Ann. Scient. ENS.*, 31 :281–327, 1997.

[Bre98] C. Breuil. Cohomologie étale de p-torsion et cohomologie cristalline en réduction semi-stable. *Duke mathematical journal*, 95 :523–620, 1998.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Number 52 in GTM. Springer, 1977.

[Ray74] M. Raynaud. Schémas en groupes de type $(p, \ldots, p)$. *Bull. Soc. math. France*, 102 :241–280, 1974.

[Ser68] Jean Pierre Serre. *Corps locaux*. Hermann, 1968.

[Ser72] J.P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones math.*, 15 :259–331, 1972.

Chapitre 2

Exposé de maîtrise

Mon exposé de maîtrise s'intitule « Z **est simplement connexe** ». Je l'ai fait avec Erwan Biland, élève de ma promotion sous la direction de Yves Laszlo. Il reste normalement accessible à tout élève ayant suivi un cours d'algèbre de niveau maîtrise.

Sommaire

La théorie de la ramification présente deux aspects, l'un algébrique et l'autre topologique. Dans la théorie topologique, on montre qu'une surface S est simplement connexe si et seulement si tout revêtement non trivial de S se ramifie en au moins un point. Dans la théorie algébrique, on montre que tout corps de nombres distinct de $\mathbb{Q}$ se ramifie en au moins un idéal premier. On relie les deux théories en étudiant les surfaces de Riemann et leurs corps de fonctions méromorphes. L'énoncé "$\mathbb{Z}$ est simplement connexe" provient de cette analogie.

La ramification

2.1 Ramification et revêtement des surfaces

Dans cette partie, on va définir deux théories de la ramification ; l'une est topologique et porte sur les revêtements de surfaces, l'autre est algébrique et concerne les extensions de corps.

2.1.1 Surfaces topologiques

Définition 2.1.1.1. *On appelle surface topologique une variété topologique complexe de dimension 1.*

Définition 2.1.1.2. *Soient B et X des surfaces topologiques ; on appelle revêtement étale fini de B par X une application $\pi : X \longrightarrow B$ telle que, pour tout $b \in B$, il existe un voisinage ouvert V de b et des ouverts $(U_i)_{1\leq i\leq n}$ en nombre fini, disjoints deux à deux, tels que :*

- $\pi^{-1}(V) = \bigsqcup_{i=1}^{n} U_i$
- *pour tout i, $1 \leq i \leq n$, π induit un homéomorphisme de U_i sur V.*

Définition 2.1.1.3. *Avec les notations précédentes, l'application $b \mapsto n$ est localement constante. Donc si B est connexe, n ne dépend pas du point b choisi. On l'appelle le degré du revêtement.*

On appelle D le disque unité ouvert de $\mathbb{C}$ et $D^\star = D - \{0\}$. On appelle carte centrée de X en x, une carte définie sur un voisinage de x à valeur dans D qui envoie x en 0.

Définition 2.1.1.4. *Soient B et X des surfaces topologiques ; on appelle revêtement ramifié fini de B par X une application $\pi : X \longrightarrow B$ telle que, pour tout $b \in B$, il existe un voisinage ouvert V de b et des ouverts $(U_i)_{1\leq i\leq n}$ en nombre fini, disjoints deux à deux, tels que :*

- $\pi^{-1}(V) = \bigsqcup_{i=1}^{n} U_i$
- *pour tout i, $1 \leq i \leq n$, il existe $x_i \in U_i$ tel que $\pi(x_i) = b$ et des cartes complexes, $U_i \to D$ et $V \to D$, centrées respectivement en x_i et en b telles que l'application π s'écrive dans ces cartes $z \mapsto z^{d_i}$ avec $d_i \in \mathbb{N}^\star$.*

Définition 2.1.1.5. *L'entier d_i défini précédemment ne dépend que de x_i. On l'appelle l'indice de ramification de π en x_i.*

Définition 2.1.1.6. *On dit que π se ramifie en $b \in B$ s'il existe un point x au dessus de b d'indice de ramification strictement supérieur à 1. L'ensemble des points où π se ramifie est appelé l'ensemble de ramification de π. C'est une partie fermée discrète de B.*

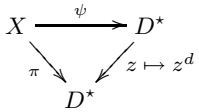
Définition 2.1.1.7. *L'application $b \mapsto \sum d_i$ est localement constante. Donc si on suppose que B est connexe, on définit de même que précédemment le degré d'un revêtement ramifié fini.*

La notion de revêtement ramifié fini découle naturellement de la notion de revêtement étale fini comme le montre le théorème suivant :

Théorème 2.1.1.8. *Soit B une surface topologique, Δ une partie fermée discrète dans B et $\pi : X \to B - \Delta$ un revêtement étale fini. Alors il existe une surface topologique $\widetilde{X} \supset X$ et un revêtement ramifié fini $\widetilde{\pi} : \widetilde{X} \to B$ prolongeant π. De plus $\widetilde{X} - X$ est une partie fermée discrète de $\widetilde{X}$.*

Démonstration. Faisons-le tout d'abord dans le cas où $B = D$ et $\Delta = \{0\}$. Quitte à raisonner séparément sur chaque composante connexe, on peut supposer que X est connexe. On prend $\pi : X \to D - \{0\}$ un revêtement fini de degré d et f l'application de $D^\star$ dans lui même qui à z associe z^d. Soient $b_0 \in D^\star$, x_0 un point au-dessus de b_0 et $\overline{x}_0 \in D^\star$, tel que $f(\overline{x}_0) = b_0$. L'application $\pi_\star : \pi_1(X, x_0) \to \pi_1(D^\star, b_0)$ est injective. En identifiant $\pi_1(D^\star, b_0)$ à $\mathbb{Z}$, l'image de $\pi_\star$ est $d\mathbb{Z}$. En effet, si $[\alpha]$ désigne un générateur de $\pi_1(D^\star, b_0)$, $[\alpha]$ agit sur la fibre au-dessus de b_0 par un cycle d'ordre d. De même $f_\star : \pi_1(D^\star, \overline{x}_0) \to \pi_1(D^\star, b_0)$ a pour image $d\mathbb{Z}$. Prenons alors u un lacet de X d'origine x_0. On considère $v = \pi \circ u$ qui est un lacet dans $D^\star$ d'origine b_0. On peut le relever en un chemin $\overline{u}$ d'origine $\overline{x}_0$ dans $D^\star$. Les propriétés de $\pi_\star$ et de $f_\star$ prouvent alors que $\overline{u}$ est un lacet.

On peut ainsi définir une application ψ de la façon suivante. Soit $x \in X$. Considérons u un chemin reliant x_0 à x. On considère $v = \pi \circ u$ et $\overline{u}$ le relèvement de v d'origine $\overline{x}_0$. En posant $\psi(x) = \overline{u}(1)$, on vient de voir que $\psi(x)$ ne dépend pas du choix du chemin u. L'application ψ ainsi définie est continue grâce à la continuité du relèvement. Comme on peut faire la même opération dans l'autre sens, on en déduit que ψ est un homéomorphisme. On a ainsi le diagramme commutatif suivant :



On pose alors $\widetilde{X} = X \sqcup \{\widetilde{x}\}$ et on prolonge la topologie de sorte que $\widetilde{\psi}$ prolongée en $\widetilde{x}$ par 0 reste un homéomorphisme. On prolonge également π en $\widetilde{\pi}$ en posant $\widetilde{\pi}(\widetilde{x}) = 0$. $\widetilde{\pi}$ est alors un revêtement ramifié fini de degré d de D.

Pour le cas général, on considère $(V_b)_{b \in \Delta}$ des ouverts disjoints de B tels que $b \in V_b$. On choisit des cartes centrées en b, $\psi_b : V_b \to D$ et on se ramène ainsi au cas précédent. $\surd$

2.1.2 Surfaces de Riemann

Définition 2.1.2.1. *On appelle surface de Riemann une variété analytique complexe de dimension 1.*

On dispose du théorème très important :

Théorème 2.1.2.2. *Soient B une surface de Riemann, X une surface topologiques et $\pi : X \to B$ un revêtement ramifié fini. Alors il existe une unique structure de surface de Riemann sur X telle que π soit holomorphe.*

Démonstration. Soit Δ l'ensemble de ramification de π. On se place tout d'abord dans le cas $B = D$, $\Delta = \{0\}$ et X connexe. On note d le degré de $pi : X \to D$. On retrouve la situation du théorème 2.1.1.8 pour $\pi : X - \pi^{-1}(0) \to D^\star$. On construit alors une carte $\psi : X \to D$ comme précédemment. ψ définit une structure analytique sur X. On remarque que ψ ainsi définie est unique modulo les rotations d'angle $\frac{2k\pi}{d}$.

On se ramène au cas général comme précédemment en découpant B en domaines de cartes centrées sur lesquels π ne se ramifie qu'au centre. On dispose alors d'un atlas sur X et la remarque que l'on vient de faire montre que les changements de cartes sont analytiques.

Si on choisit deux structures holomorphes σ et σ' sur X, alors on vérifie que l'application identité de (X, σ) dans (X, σ') est holomorphe et donc les deux structures sont équivalentes. $\surd$

2.2 Ramification et extensions de corps

2.2.1 Les anneaux de Dedekind

Définition 2.2.1.1 (Anneau nœthérien). *On dit qu'un anneau A est nœthérien s'il satisfait à l'une des trois conditions équivalentes suivantes :*

i) Tout idéal de A est engendré par un nombre fini d'éléments (ie tout idéal de A est un A-module de type fini).
ii) Toute suite croissante d'idéaux de A est stationnaire.
iii) Toute famille non vide d'idéaux de A admet un élément maximal.

Lemme 2.2.1.2. *Soit A un anneau nœthérien intègre. Alors tout idéal non nul de A contient un produit d'idéaux premiers non nuls.*

Démonstration. Notons Φ l'ensemble des idéaux non nuls de A ne vérifiant pas la propriété énoncée et supposons que $\Phi \neq \emptyset$.

Comme A est nœthérien, Φ possède un élément maximal. Notons-le $\mathfrak{a}$. Alors $\mathfrak{a}$ n'est pas un idéal premier donc il existe x et y n'appartenant pas à $\mathfrak{a}$ tels que $xy \in \mathfrak{a}$. On en déduit, par maximalité, que $\mathfrak{a} + Ax \notin \Phi$ et donc on peut écrire $\mathfrak{a} + Ax \supset \mathfrak{p}_1 \dots \mathfrak{p}_m$. De même on a $\mathfrak{a} + Ay \supset \mathfrak{q}_1 \dots \mathfrak{q}_n$.

On en déduit que $\mathfrak{a} \supset (\mathfrak{a} + Ax)(\mathfrak{a} + Ay) \supset \mathfrak{p}_1 \dots \mathfrak{p}_m \mathfrak{q}_1 \dots \mathfrak{q}_n$, ce qui contredit le fait que $\mathfrak{a} \in \Phi$. √

Lemme 2.2.1.3. *Soit A un anneau nœthérien. Alors tout idéal de A contient un produit d'idéaux premiers.*

Démonstration. Comme précédemment. √

Définition 2.2.1.4. *Soit A un anneau intègre. Soit K son corps des fractions. On dit que A est intégralement clos si les seuls éléments de K qui sont entiers sur A (ie qui sont racines d'un polynôme unitaire à coefficients dans A) sont les éléments de A.*

Définition 2.2.1.5 (Anneau de Dedekind). *Un anneau A est dit de Dedekind s'il est nœthérien, intégralement clos et si tout idéal premier non nul de A est maximal.*

Par exemple, tout anneau principal est un anneau de Dedekind.

Définition 2.2.1.6 (Idéal fractionnaire). *Soit A un anneau intègre. On note K son corps des fractions. On appelle idéal fractionnaire $\mathfrak{a}$ de A tout A-module inclus dans K tel qu'il existe $d \in A$ vérifiant $\mathfrak{a} \subset d^{-1}A$. Les idéaux de A sont des idéaux fractionnaires de A (en effet, on peut choisir $d = 1$). On les appelle parfois des idéaux entiers.*

Lemme 2.2.1.7. *Soit A un anneau de Dedekind. Soit $\mathfrak{p}$ un idéal premier non nul de A, alors il existe un unique idéal fractionnaire de A, $\mathfrak{p}'$ tel que $\mathfrak{p}\mathfrak{p}' = A$.*

Remarque 2.2.1.8. *$\mathfrak{p}'$ est noté $\mathfrak{p}^{-1}$*

Démonstration. Posons $\mathfrak{p}' = \{x \in K / x\mathfrak{p} \subset A\}$. C'est un idéal fractionnaire de A (en effet, tout élément x non nul de $\mathfrak{p}$ vérifie $x\mathfrak{p}' \subset A$).

Montrons tout d'abord que $\mathfrak{p}' \neq A$. En effet, soit $x \neq 0$ appartenant à $\mathfrak{p}$. D'après le lemme 2.2.1.2, on peut écrire $Ax \supset \mathfrak{p}_1 \dots \mathfrak{p}_n$. On peut choisir n minimal. On a alors $\mathfrak{p} \supset Ax \supset \mathfrak{p}_1 \dots \mathfrak{p}_n$ et donc il existe j tel que $\mathfrak{p} \supset \mathfrak{p}_j$. Par maximalité, on obtient $\mathfrak{p} = \mathfrak{p}_j$. On peut supposer $j = 1$. Posons maintenant $\mathfrak{b} = \mathfrak{p}_2 \dots \mathfrak{p}_n$ de sorte que l'on a $Ax \supset \mathfrak{p}\mathfrak{b}$ et $Ax \not\supset \mathfrak{b}$ (par minimalité de n). Considérons donc $y \in \mathfrak{b} - Ax$. On a alors $yx^{-1} \notin A$ et $\mathfrak{p}y \subset \mathfrak{p}\mathfrak{b} \subset Ax$ et donc, par définition de $\mathfrak{p}'$, $yx^{-1} \in \mathfrak{p}'$. On en déduit finalement que $\mathfrak{p}' \neq A$.

On vérifie que $\mathfrak{p}\mathfrak{p}' \subset A$. D'autre part, $A \subset \mathfrak{p}'$ et donc $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}'$ puis par maximalité $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}$ ou $\mathfrak{p}\mathfrak{p}' = A$.

Supposons que $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}$. Soit $x \in \mathfrak{p}'$, alors pour tout n, on a $x^n\mathfrak{p} \subset \mathfrak{p}$. On en déduit que $A[x]$ est un idéal fractionnaire. En effet, tout élément d non nul de $\mathfrak{p}$ vérifie alors $A[x] \subset d^{-1}A$. Mais $d^{-1}A$ est un A-module de type fini donc $A[x]$ est un A-module de type fini (car A est nœtherien), ce qui prouve que x est entier sur A puis est un élément de A (car A est intégralement clos). On en déduit que $\mathfrak{p}' = A$, ce qui est faux.

Finalement, on a bien $\mathfrak{p}\mathfrak{p}' = A$. √

Théorème 2.2.1.9. *Soit A un anneau de Dedekind, alors tout idéal fractionnaire non nul $\mathfrak{a}$ de A s'écrit, de façon unique, comme produit d'idéaux premiers de A. C'est-à-dire :*

$$\mathfrak{a} = \prod_{\mathfrak{p}\ premier} \mathfrak{p}^{n_\mathfrak{p}(\mathfrak{a})} \qquad \textit{(où les } n_\mathfrak{p}(\mathfrak{a}) \textit{ sont des entiers relatifs presque tous nuls)}$$

Démonstration. Remarquons tout d'abord que, via l'égalité $\mathfrak{a} = (d\mathfrak{a})(Ad)^{-1}$, on peut supposer que $\mathfrak{a}$ est un idéal entier (ie un idéal de A).

Notons Φ l'ensemble des idéaux entiers de A qui ne s'écrivent pas comme produit d'idéaux premiers et supposons que $\Phi \neq \emptyset$. Alors, comme A est nœthérien, Φ admet un élément maximal $\mathfrak{a}$. On a bien entendu $\mathfrak{a} \neq A$ donc d'après le théorème de Krull, il existe $\mathfrak{p}$ un idéal premier de A tel que $\mathfrak{a} \subset \mathfrak{p}$. On a alors $\mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} = A$ et $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1}$ (car $A \subset \mathfrak{p}^{-1}$ car $\mathfrak{p} \subset A$). On montre comme dans la preuve précédente que l'on ne peut pas avoir $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$ et donc on obtient $\mathfrak{a}\mathfrak{p}^{-1} \notin \Phi$ de sorte que l'on peut écrire $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_n$ puis $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \dots \mathfrak{p}_n$, ce qui est absurde. On en déduit que $\Phi = \emptyset$, ce qui prouve l'existence de la décomposition.

Pour montrer l'unicité, il suffit de voir que $\left(\prod_{\mathfrak{p} \text{ premier}} \mathfrak{p}^{n_\mathfrak{p}} = A \right)$ implique $n_\mathfrak{p} = 0$ pour tout $\mathfrak{p}$. Supposons que ce n'est pas le cas. Alors regroupant les puissances positives et les puissances négatives, on obtient l'égalité $\mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_m^{\alpha_m} = \mathfrak{q}_1^{\beta_1} \dots \mathfrak{q}_n^{\beta_n}$ où tous les exposants ainsi que m et n sont strictement positifs et tous les idéaux premiers qui apparaissent sont distincts. Mais alors on a $\mathfrak{p}_1 \supset \mathfrak{q}_1^{\beta_1} \dots \mathfrak{q}_n^{\beta_n}$ et donc il existe un entier j tel que $\mathfrak{p}_1 \supset \mathfrak{q}_j$ et puis par maximalité $\mathfrak{p}_1 = \mathfrak{q}_j$, ce qui est supposé faux. √

Ceci peut s'interpréter en disant que, de même que tout nombre d'un anneau principal peut se décomposer en produit de nombres premiers, tout idéal d'un anneau de Dedekind peut se décomposer en produit d'idéaux premiers.

Corollaire 2.2.1.10. *L'ensemble des idéaux fractionnaires non nuls d'un anneau de Dedekind forme un groupe.*

Proposition 2.2.1.11 (Formulaire). *Soit $\mathfrak{p}$ un idéal premier de A, un anneau de Dedekind. Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux fractionnaires de A. On a alors les formules suivantes :*

i) $n_\mathfrak{p}(\mathfrak{a}\mathfrak{b}) = n_\mathfrak{p}(\mathfrak{a}) + n_\mathfrak{p}(\mathfrak{b})$
ii) $\mathfrak{a} \subset A \quad \Rightarrow \quad n_\mathfrak{p}(\mathfrak{a}) \geq 0$
iii) $\mathfrak{a} \subset \mathfrak{b} \quad \Rightarrow \quad n_\mathfrak{p}(\mathfrak{a}) \geq n_\mathfrak{p}(\mathfrak{b})$
iv) $n_\mathfrak{p}(\mathfrak{a} + \mathfrak{b}) = \inf(n_\mathfrak{p}(\mathfrak{a}), n_\mathfrak{p}(\mathfrak{b}))$
v) $n_\mathfrak{p}(\mathfrak{a} \cap \mathfrak{b}) = \sup(n_\mathfrak{p}(\mathfrak{a}), n_\mathfrak{p}(\mathfrak{b}))$

Démonstration.
i) est essentiellement trivial.
ii) a été démontré dans le théorème précédent.
iii) vient du fait que $\mathfrak{a} \subset \mathfrak{b}$ équivaut à $\mathfrak{a}\mathfrak{b}^{-1} \subset A$.
iv) vient du fait que $\mathfrak{a} + \mathfrak{b}$ est la borne supérieure pour l'inclusion de $\{\mathfrak{a}, \mathfrak{b}\}$
v) vient du fait que $\mathfrak{a} \cap \mathfrak{b}$ est la borne inférieure pour l'inclusion de $\{\mathfrak{a}, \mathfrak{b}\}$

√

2.2.2 Ramification pour les anneaux principaux

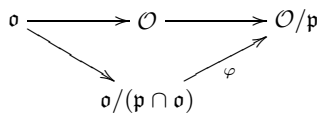
On considère ici un anneau principal $\mathfrak{o}$. On note k son corps des fractions. On considère alors K une extension finie séparable de degré n de k et $\mathcal{O}$ l'anneau des entiers de K sur $\mathfrak{o}$. On a alors le diagramme commutatif suivant :

$$\begin{array}{ccc} \mathcal{O} & \longrightarrow & K \\ \uparrow & \circlearrowleft & \uparrow n \\ \mathfrak{o} & \longrightarrow & k \end{array}$$

Définition 2.2.2.1. *On définit le spectre d'un anneau A comme l'ensemble des ses idéaux premiers non nuls. On le note $Spec(A)$.*

Lemme 2.2.2.2. *Soit $\mathfrak{p} \in Spec(\mathcal{O})$, alors $\mathfrak{p} \cap \mathfrak{o} \in Spec(\mathfrak{o})$ et $\mathcal{O}/\mathfrak{p}$ est une extension du corps $\mathfrak{o}/(\mathfrak{p} \cap \mathfrak{o})$.*

Démonstration. L'homomorphisme $\mathfrak{o} \longrightarrow \mathcal{O} \longrightarrow \mathcal{O}/\mathfrak{p}$ a pour noyau $\mathfrak{p} \cap \mathfrak{o}$ et donc se factorise de la façon suivante (où φ est injectif) :



On en déduit que $\mathfrak{o}/(\mathfrak{p} \cap \mathfrak{o})$ peut se voir comme un sous-anneau de l'anneau intègre $\mathcal{O}/\mathfrak{p}$. Il est donc intègre, ce qui prouve que $\mathfrak{p} \cap \mathfrak{o}$ est un idéal premier de $\mathfrak{o}$.

Soit $x \in \mathfrak{p}$, $x \neq 0$. On a alors une équation de dépendance intégrale $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$ où les $a_i \in \mathfrak{o}$. Quitte à diviser par x, on peut supposer $a_0 \neq 0$. Mais on a alors $a_0 \in \mathcal{O}x \cap \mathfrak{o} \subset \mathfrak{p} \cap \mathfrak{o}$ donc $\mathfrak{p} \cap \mathfrak{o}$ est un idéal premier non nul de $\mathfrak{o}$.

Il ne reste plus qu'à montrer que $\mathcal{O}/\mathfrak{p}$ est un corps. Soit donc $\overline{x} \in \mathcal{O}/\mathfrak{p}$, $\overline{x} \neq 0$. x est entier sur $\mathfrak{o}$ donc $\overline{x}$ est entier sur $\mathfrak{o}/(\mathfrak{p} \cap \mathfrak{o})$, on a ainsi une équation de dépendance intégrale (où on peut supposer $\overline{a_0} \neq 0$) :

$$\overline{x}^n + \overline{a_{n-1}}\,\overline{x}^{n-1} + \ldots + \overline{a_0} = 0 \qquad \text{avec} \quad \overline{a_i} \in \mathfrak{o}/(\mathfrak{p} \cap \mathfrak{o})$$

$$\overline{x}\left(-\frac{\overline{a_{n-1}}}{\overline{a_0}}\overline{x}^{n-1} - \ldots - \frac{\overline{a_1}}{\overline{a_0}}\right) = 1$$

ce qui prouve que $\overline{x}$ est inversible. √

Théorème 2.2.2.3. *$\mathcal{O}$ est un $\mathfrak{o}$-module libre de dimension n.*

Démonstration. Soit $x \in K$, alors il existe un polynôme à coefficients dans $\mathfrak{o}$ qui annule x ie $a_m x^m + \ldots + a_0 = 0$ puis $(a_m x)^m + a_{m-1}(a_m x)^{m-1} + \ldots + a_0 a_m^{m-1} = 0$, ce qui prouve que $a_m x \in \mathcal{O}$.

On peut donc trouver $(x_1, \ldots, x_n)$ une base de K sur k telle que tous les x_i appartiennent à $\mathcal{O}$. Comme l'extension est séparable, la trace est non dégénérée et on peut donc considérer la base duale $(y_1, \ldots, y_n)$.

Soit $z \in \mathcal{O}$. On peut alors écrire $z = \sum_{j=1}^{n} \alpha_j y_j$ avec $\alpha_j \in k$. Par dualité, on a $Tr(x_i z) = \alpha_i$. D'autre part, $x_i z \in \mathcal{O}$ donc $Tr(x_i z) \in k \cap \mathcal{O} = \mathfrak{o}$, ce qui prouve que $\alpha_i \in \mathfrak{o}$ et donc $\mathcal{O} \subset \bigoplus_{j=1}^{n} y_i \mathfrak{o}$. On en déduit que $\mathcal{O}$ est un $\mathfrak{o}$-module libre de dimension inférieure ou égale à n.

Mais on a vu que $(x_1, \ldots, x_n)$ est une famille libre sur k et donc sur $\mathfrak{o}$ d'éléments de $\mathcal{O}$. Donc finalement, $\mathcal{O}$ est de dimension n. √

Théorème 2.2.2.4. *$\mathcal{O}$ est un anneau de Dedekind.*

Démonstration. Soit $\mathfrak{a}$ un idéal de $\mathcal{O}$. $\mathfrak{a}$ est alors un $\mathfrak{o}$-module inclus dans $\mathcal{O}$. $\mathfrak{a}$ est donc de type fini sur $\mathfrak{o}$ et donc sur $\mathcal{O}$. Ceci prouve que $\mathcal{O}$ est nœthérien.

D'autre part $\mathcal{O}$ est intégralement clos.

Considérons $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}$. Alors comme nous l'avons vu dans la démonstration du lemme 2.2.2.2, $\mathcal{O}/\mathfrak{p}$ est un corps, ce qui prouve que $\mathfrak{p}$ est maximal. √

On a introduit tous les outils indispensables à la théorie algébrique de la ramification. Passons maintenant à l'exposé de cette théorie.

Soit p un nombre premier de $\mathfrak{o}$ (ie l'idéal $p\mathfrak{o}$ est premier). Alors $p\mathcal{O}$ est un idéal non nul de $\mathcal{O}$ (car il contient $p\mathfrak{o}$) et donc on a la décomposition (unique) :

$$p\mathcal{O} = \prod_{i=1}^{q} \mathfrak{p}_i^{e_i}$$

où les $\mathfrak{p}_i$ sont des idéaux premiers de $\mathcal{O}$ deux à deux distincts et les e_i sont des entiers strictement positifs.

Définition 2.2.2.5. *e_i s'appelle l'indice de ramification de $\mathfrak{p}_i$ sur $\mathfrak{o}$.*

Définition 2.2.2.6. *On dit que K se ramifie en p, s'il existe un i tel que $e_i > 1$.*

Proposition 2.2.2.7. *Les $\mathfrak{p}_i$ sont exactement les idéaux premiers $\mathfrak{p}$ de $\mathcal{O}$ tels que $\mathfrak{p} \cap \mathfrak{o} = p\mathfrak{o}$.*

Démonstration. Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}$.

Supposons que $\mathfrak{p} \supset p\mathcal{O}$, alors $\mathfrak{p} \cap \mathfrak{o}$ est un idéal premier de $\mathfrak{o}$ contenant p, donc $\mathfrak{p} \cap \mathfrak{o} = p\mathfrak{o}$. Réciproquement, si $\mathfrak{p} \cap \mathfrak{o} = p\mathfrak{o}$, alors $p \in \mathfrak{p}$ et donc $\mathfrak{p} \supset p\mathcal{O}$.

D'autre part, d'après les formules sur les anneaux de Dedekind, on a $\mathfrak{p} \supset p\mathcal{O}$, si et seulement si $n_{\mathfrak{p}}(p\mathcal{O}) \geq 1$.

On en déduit la proposition énoncée. √

Définition 2.2.2.8. *On en déduit que l'on a l'extension de corps $\mathfrak{o}/p\mathfrak{o} \to \mathcal{O}/\mathfrak{p}_i$. Son degré s'appelle le degré résiduel de $\mathfrak{p}_i$ sur $\mathfrak{o}$ et est noté f_i.*

Nous allons voir que la notion introduite correspond bien à la notion de revètements ramifiés finis.

Cette affirmation découle immédiatement du théorème suivant :

Théorème 2.2.2.9. *Avec les notations précédentes, on a* $\sum_{i=1}^{q} e_i f_i = n$

Démonstration. Montrons tout d'abord que si $\mathfrak{p}$ est un idéal premier non nul de $\mathcal{O}$ (en fait de n'importe quel anneau de Dedekind) et si $\mathfrak{a}$ est un idéal de $\mathcal{O}$, alors $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ est un espace vectoriel de dimension 1 sur $\mathcal{O}/\mathfrak{p}$. En effet, soit E un sous-espace vectoriel de $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$, alors E est de la forme $\mathfrak{b}/\mathfrak{a}\mathfrak{p}$ où $\mathfrak{a}\mathfrak{p} \subset \mathfrak{b} \subset \mathfrak{a}$. D'après les formules sur les anneaux de Dedekind, on obtient $\mathfrak{b} = \mathfrak{a}$ (soit $E = \mathfrak{a}/\mathfrak{a}\mathfrak{p}$) ou $\mathfrak{b} = \mathfrak{a}\mathfrak{p}$ (soit $E = 0$). On en déduit la propriété voulue.

Montrons alors que $\sum_{i=1}^{q} e_i f_i = \dim_{\mathfrak{o}/p\mathfrak{o}} \mathcal{O}/p\mathcal{O}$. Pour cela, on écrit la suite d'inclusion suivante :

$$\mathcal{O} \supset \mathfrak{p}_1 \supset \ldots \supset \mathfrak{p}_1^{e_1} \supset \mathfrak{p}_1^{e_1}\mathfrak{p}_2 \supset \ldots \supset \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \supset \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_q^{e_q} = p\mathcal{O}$$

Par la propriété précédente, on en déduit que le quotient de deux idéaux consécutifs qui apparait dans cette décomposition est de dimension 1 sur $\mathcal{O}/\mathfrak{p}_i$ et donc de dimension f_i sur $\mathfrak{o}/p\mathfrak{o}$, d'où le résultat annoncé.

Considérons pour finir $(x_1, \ldots, x_n)$ une base de $\mathcal{O}$ en tant que $\mathfrak{o}$-module. On obtient alors, en réduisant modulo $p\mathcal{O}$, une base de $\mathcal{O}/p\mathcal{O}$ comme $\mathfrak{o}/p\mathfrak{o}$-espace vectoriel ce qui prouve que $\dim_{\mathfrak{o}/p\mathfrak{o}} \mathcal{O}/p\mathcal{O} = n$ et achève la démonstration. √

Remarque 2.2.2.10. *Dans tout ce paragraphe, nous avons supposé que $\mathfrak{o}$ était un anneau principal pour simplifier les démonstrations. Cependant, tous les résultats énoncés précédemment restent vrais si on suppose seulement que $\mathfrak{o}$ est un anneau de Dedekind. Pour plus de détails, se reporter à [Sam71].*

Surfaces de Riemann et corps de fonctions méromorphes

2.3 Revêtements ramifiés et extensions étales

On s'intéresse désormais aux surfaces de Riemann connexes compactes. Etant donné X une telle surface de Riemann, on note $\mathcal{M}(X)$ son corps des fonctions méromorphes. Si $\pi : X \to B$, avec X et B deux surfaces de Riemann connexes compactes, est un revêtement ramifié fini analytique, on a un plongement $\pi^\star : \mathcal{M}(B) \to \mathcal{M}(X)$ qui fait de $\mathcal{M}(X)$ une extension du corps $\mathcal{M}(B)$. On montre que $\mathcal{M}$ constitue un foncteur de la catégorie des revêtements ramifiés finis de B dans la catégorie des extensions finies de $\mathcal{M}(B)$ et que ce foncteur est une équivalence de catégories. Nous nous contenterons de prouver partiellement ces propriétés.

2.3.1 Le foncteur $\mathcal{M}$

On admet le théorème suivant, dont la démonstration fait appel à l'analyse :

Théorème 2.3.1.1 (Théorème de séparation). *Soit X une surface de Riemann compacte, soient a et b des points distincts de X ; alors il existe une fonction méromorphe f sur X définie en a et b et telle que $f(a) \neq f(b)$.*

Corollaire 2.3.1.2. *Soit X une surface de Riemann compacte, soient $a_1 \dots a_d$ des points distincts de X ; alors il existe une fonction méromorphe f sur X définie en tous les a_i et telle que les valeurs $f(a_i)$ soient deux à deux distinctes.*

Démonstration. Pour tout couple $1 \leq i < j \leq d$, il existe une fonction f méromorphe sur X, définie en $a_1 \dots a_d$ et telle que $f(a_i) \neq f(a_j)$. En effet, le théorème de séparation nous fournit une fonction g méromorphe sur X définie en a_i et a_j avec $g(a_i) \neq g(a_j)$; quitte à ajouter une constante, on peut supposer que g ne s'annule pas sur $a_1 \dots a_d$, auquel cas $f = 1/g$ convient. Si maintenant on note A le sous-espace vectoriel (non nul) de $\mathcal{M}(X)$ constitué des fonctions méromorphes définies aux points $a_1 \dots a_d$, et A_{ij} le sous-espace des $f \in A$ tels que $f(a_i) = f(a_j)$, on vient de montrer $A_{ij} \neq A$, donc $\bigcup A_{ij} \neq A$. Toute fonction $f \in A - \bigcup A_{ij}$ répond à la question. $\surd$

Théorème 2.3.1.3. *Soient B et X deux surfaces de Riemann connexes compactes et $\pi : X \longrightarrow B$ un revêtement analytique de degré d de B par X. Alors $\mathcal{M}(X)$ est une extension finie de degré d de $\mathcal{M}(B)$.*

Démonstration. Soit $f \in \mathcal{M}(X)$. Montrons que f est algébrique sur $\mathcal{M}(B)$ de degré au plus d, en exhibant un polynôme annulateur de f de degré d. On note $\Delta \subset B$ l'image par π de l'ensemble des pôles de f. Pour $b \in B - \Delta$, on note $x_1 \dots x_d$ les antécédents de b par π (comptés avec leur indice de ramification) ; soient $a_i(b)$ les valeurs en $f(x_1) \dots f(x_d)$ des fonctions symétriques élémentaires :

$$a_0(b) = 1 \ , \ a_1(b) = \sum f(x_j) \ , \ \dots \ , \ a_n(b) = \prod f(x_j)$$

On a clairement, pour tout i, $a_i \in \mathcal{M}(B)$. Posons $P(Z) = \sum_i (-1)^i a_i Z^{d-i} \in \mathcal{M}(B)[Z]$ et montrons $P(f) = 0$. C'est clair car les $f(x_j)$ sont justement les racines de $P_b(Z) = \sum_i (-1)^i a_i(b) Z^{d-i}$.

Montrons que $\mathcal{M}(X)$ est étale de degré au plus d. $\mathcal{M}(X)$ est réunion filtrante des sous-extensions E de type fini de $\mathcal{M}(B)$. Comme les E sont de type fini et que leurs générateurs sont algébriques, ce sont des extensions finies donc étales (car $\mathcal{M}(B)$ est de caractéristique nulle), donc monogènes d'après le théorème de l'élément primitif, donc de degré au plus d. Par conséquent $\mathcal{M}(X)$ est de degré au plus d.

Montrons que le degré de $\mathcal{M}(X)$ est supérieur à d. Soit $b_0 \in B$ un point où le revêtement est non ramifié, et soient $x_1 \dots x_d$ les points de X au dessus de B (tous distincts donc). D'après le théorème de séparation, il existe $f \in \mathcal{M}(X)$ définie en les $x_1 \dots x_d$ et prenant en ces points des valeurs distinctes. Soit $P = \sum_{i=0}^{k} c_i Z^i$ un polynôme annulateur non nul de f, $c_i \in \mathcal{M}(B)$ pour tout i. L'ensemble des pôles des c_i est discret dans B, ainsi que l'ensemble de ramification du revêtement, donc il existe un voisinage V de b_0 tel que $V - \{b_0\}$ ne rencontre pas ces ensembles et tel que pour tout $b \in V - \{b_0\}$, la fonction f prend des valeurs distinctes en les points de $\pi^{-1}(b)$. Ces valeurs sont alors toutes racines de $P_b(Z)$, qui par conséquent est nul ou de degré supérieur à d. Mais si les c_i s'annulent en tout point de $V - \{b_0\}$, c'est qu'ils sont nuls partout, ce qui contredit $P \neq 0$, donc on a montré que le degré de P est au moins d. $\surd$

2.3.2 Une équivalence de catégories

Lemme 2.3.2.1. *Soient B un espace topologique et $b \mapsto P_b$ une application continue de B dans $\mathbb{C}_d[Z]$, l'espace des polynômes à coefficients dans $\mathbb{C}$ de degré inférieur ou égal à d. On suppose que pour tout $b \in B$, P_b admet d racines distinctes dans $\mathbb{C}$. On pose $X = \{(b,z) \in B \times \mathbb{C} \mid P_b(z) = 0\}$.*

Alors $\pi : \begin{pmatrix} X & \longrightarrow & B \\ (b,z) & \mapsto & b \end{pmatrix}$ est un revêtement de degré d de B.

Démonstration. C'est une application directe du théorème des fonctions implicites. $\surd$

Lemme 2.3.2.2. *Soit* $P(Z) = Z^d + a_1 Z^{d-1} + \ldots + a_d \in \mathbb{C}[Z]$ *et* z *une racine de* P, *alors* $|z| \leq \sup(1, |a_1| + \ldots + |a_d|)$.

Démonstration. Si $|z| > 1$, on écrit $z = -a_1 - \frac{a_2}{z} \ldots - \frac{a_d}{z^{d-1}}$ et on obtient $|z| \leq |a_1| + \ldots + |a_d|$. $\surd$

Théorème 2.3.2.3. *Soit* B *une surface de Riemann connexe. Soit* E *une extension finie de* $\mathcal{M}(B)$. *Alors il existe une surface de Riemann* X *et un revêtement ramifié* $\pi : X \to B$ *tels que le diagramme suivant commute :*

$$\begin{array}{ccc} \mathcal{M}(X) & \xleftarrow[\phi]{\sim} & E \\ & {\scriptstyle \pi^\star} \searrow \quad \swarrow & \\ & \mathcal{M}(B) & \end{array}$$

Démonstration. D'après le théorème de l'élément primitif, il existe $\zeta \in E$ tel que $E = \mathcal{M}(B)[\zeta]$. Soit $P(Z) = Z^d + a_1 Z^{d-1} + \ldots + a_d$ le polynôme minimal de ζ où les $a_i \in \mathcal{M}(B)$. On définit $P_b(Z) = Z^d + a_1(b) Z^{d-1} + \ldots + a_d(b)$. Considérons Δ l'ensemble des points $b \in B$ pour lesquels $a_i(b)$ n'est pas défini ou P_b n'est pas séparable.

Comme E est une extension étale, P est séparable et donc P et P' sont premiers entre eux ainsi leur résultant est non nul : On en déduit que l'ensemble des points d'annulation du résulant de P_b et P_b' est un fermé discret, ainsi l'ensemble des $b \in B$ pour lesquels P_b n'est pas séparable est également un fermé discret et donc Δ aussi.

Considérons donc $X = \{(b, z) \in (B - \Delta) \times \mathbb{C} \mid P_b(z) = 0\}$ et $\pi : \begin{pmatrix} X & \longrightarrow & B - \Delta \\ (b,z) & \mapsto & b \end{pmatrix}$. D'après le lemme 2.3.2.1, π est un revêtement. En appliquant alors le théorème 2.1.1.8, on voit que l'on peut le prolonger en $\widetilde{\pi} : \widetilde{X} \to B$ un revêtement ramifié topologique. Finalement le théorème 2.1.2.2 prouve qu'il existe une unique structure holomorphe sur $\widetilde{X}$ rendant $\widetilde{\pi}$ holomorphe.

Considérons Z l'application qui à $(b, z) \in X$ associe z. Comme π est localement un homéomorphisme biholomorphe, Z est holomorphe sur X. Soient $b \in \Delta$ et $x \in \pi^{-1}(b)$. Soient φ une carte de B centrée en b et ψ une carte de X centrée en x telles que π s'écrive dans ces cartes $z \mapsto z^r$. Si P désigne toujours le polynôme minimal de ζ, pour x' voisin de x et $b' = \pi(x')$, on a $P_{b'}(Z(x')) = 0$ d'où, d'après le lemme 2.3.2.1, $|Z(x')| \leq \sup(1, |a_1(b)|, \ldots, |a_d(b)|)$. En passant dans les cartes, on obtient $a_i(b') = \overline{a}_i(\varphi(b')) = \overline{a}_i\left(\psi(x')^r\right)$, et comme les a_i sont méromorphes, il existe $C_i > 0$ et $n_i \in \mathbb{Z}$ tels que $|a_i(b')| \leq C_i |\psi(x') - \psi(x)|^{n_i}$. Il existe donc $C > 0$ et $n \in \mathbb{Z}$ tels que $|Z(x')| \leq C |\psi(x') - \psi(x)|^n$ au voisinage de x et alors Z est méromorphe en x si bien que $Z \in \mathcal{M}(X)$.

Considérons alors le morphisme d'anneaux $\phi : E \to \mathcal{M}(X)$ défini par $\phi(\zeta) = Z$, qui est bien défini car $P(Z) = 0$. Il fait bien commuter le diagramme précédent, reste à montrer qu'il est bijectif. Pour l'injectivité, il suffit de montrer que P est le polynôme minimal de Z, et c'est clair car si $b \in B - \Delta$ et si $\pi^{-1}(b) = \{x_1, \ldots, x_d\}$, Z prend des valeurs toutes différentes en les x_i (voir démonstration du théorème 2.3.1.3. La surjectivité provient de l'égalité des degrés.

$\surd$

2.4 Lien avec la ramification

Soit $\mathbb{S}^2 = \mathbb{C} \cup \{\infty\}$.

On prend ici $\mathfrak{o} = \mathbb{C}\left[\mathbb{S}^2\right]$, l'anneau des fonctions méromorphes sur la sphère de Riemann et holomorphes sur $\mathbb{C}$. Il s'agit en fait de l'ensemble des polynômes à coefficients dans $\mathbb{C}$. C'est donc un anneau principal. Son corps des fractions est $k = \mathcal{M}\left(\mathbb{S}^2\right)$ qu'on note ici $\mathbb{C}\left(\mathbb{S}^2\right)$.

On a vu que se donner un revêtement ramifié fini de degré n de $\mathbb{S}^2$ par une surface de Riemann connexe compacte X équivaut à se donner une extension finie K de degré n de $\mathcal{M}\left(\mathbb{S}^2\right)$. On a alors :

$$\begin{array}{ccc} \mathcal{O}_X & \longrightarrow & \mathbb{C}(X) \\ \uparrow & & \uparrow n \\ \mathbb{C}\left[\mathbb{S}^2\right] & \longrightarrow & \mathbb{C}\left(\mathbb{S}^2\right) \end{array} \qquad \begin{array}{c} X \\ {\scriptstyle n}\downarrow{\scriptstyle \pi} \\ \mathbb{S}^2 \end{array}$$

Proposition 2.4.0.1. *L'anneau des entiers $\mathcal{O}_X$ est l'anneau des fonctions méromorphes sur X et holomorphes sur $X - \pi^{-1}(\infty)$. On le notera $\mathbb{C}[X]$.*

Démonstration. La démonstration effectuée dans le théorème 2.3.1.3 prouve que $\mathbb{C}[X]$ est entier sur $\mathbb{C}\left[\mathbb{S}^2\right]$. Réciproquement si $f \in \mathcal{M}(X)$ est entier sur $\mathbb{C}\left[\mathbb{S}^2\right]$, alors on peut écrire l'équation de dépendance intégrale $f^n + a_{n-1}(b) f^{n-1} + \ldots + a_0(b) = 0$ où les a_i sont holomorphes sur $\mathbb{C}$. Supposons que f admette un pôle d'ordre $\alpha > 0$ en $x \in X - \pi^{-1}(\infty)$, f^n admet alors en ce point un pôle d'ordre $n\alpha$ mais $a_{n-1}(b) f^{n-1} + \ldots + a_0(b)$ admet en ce point un pôle d'ordre inférieur à $(n-1)\alpha$, ce qui est absurde. √

Nous admettrons les résultats suivants :

Proposition 2.4.0.2. *Les idéaux premiers de $\mathbb{C}[X]$ sont exactement les idéaux de la forme $\mathfrak{p}_x = \{f \in \mathbb{C}[X] \mid f(x) = 0\}$ pour $x \in X - \pi^{-1}(\infty)$. En particulier les idéaux premiers de $\mathbb{C}\left[\mathbb{S}^2\right]$ sont exactement les idéaux de la forme $\mathfrak{p}_b$, $b \in \mathbb{C}$.*

Théorème 2.4.0.3. *Soit $x \in X - \pi^{-1}(\infty)$. Alors l'indice de ramification de $\mathcal{M}(X)$ en $\mathfrak{p}_x$ est égal à l'indice de ramification de π en x. En particulier pour $b \in \mathbb{C}$, $\mathcal{M}(X)$ se ramifie en $\mathfrak{p}_b$ si et seulement si π se ramifie en b.*

Le fait que $\mathbb{C}$ est simplement connexe assure que tout revêtement de degré supérieur ou égal à 2 se ramifie en au moins un point. Or d'après le théorème 2.1.1.8 se donner un revêtement de $\mathbb{C}$ c'est se donner un revêtement de $\mathbb{S}^2$. On peut donc dire que tout revêtement non trivial se ramifie en au moins un point autre que l'infini. Grâce au dictionnaire précédent, on peut énoncer ce résultat sous une forme plus algébrique : toute extension finie de $\mathcal{M}\left(\mathbb{S}^2\right)$ se ramifie sur $\mathbb{C}\left[\mathbb{S}^2\right]$ en au moins un idéal premier.

Mais ne pourrait-on pas trouver d'autres corps pour lesquels ce résultat reste vrai ?

Z est simplement connexe

A partir de maintenant et jusqu'à la fin, on se place dans la situation suivante : K est un corps de nombres (c'est-à-dire une extension finie de $\mathbb{Q}$) de degré $n \geq 2$. On note $\mathcal{O}_K$ l'anneau des entiers de K sur $\mathbb{Z}$. On a alors le diagramme suivant :

$$\begin{array}{ccc} \mathcal{O}_K & \longrightarrow & K \\ \uparrow & \circlearrowleft & \uparrow n \\ \mathbb{Z} & \longrightarrow & \mathbb{Q} \end{array}$$

Comme $\mathbb{Z}$ est un anneau principal, les résultats vus dans la première partie s'appliquent. En particulier, $\mathcal{O}_K$ est un anneau de Dedekind et un $\mathbb{Z}$-module libre de dimension n et l'on sait donner un sens au fait que K se ramifie en un nombre premier $p \in \mathbb{Z}$. On va prouver pour $\mathbb{Z}$ ce qu'on vient de prouver pour $\mathbb{C}\left[\mathbb{S}^2\right]$, à savoir que toute extension finie non triviale de $Frac(\mathbb{Z}) = \mathbb{Q}$ se ramifie en au moins un idéal premier non nul. Par analogie avec le précédent résultat qui signifiait que $\mathbb{C} = \mathrm{Spec}\left(\mathbb{C}\left[\mathbb{S}^2\right]\right)$ était simplement connexe, on énoncera alors « Spec $(\mathbb{Z})$ est simplement connexe » ou, pour employer une formule choc, « $\mathbb{Z}$ est simplement connexe ».

2.5 Préliminaires

2.5.1 Réseaux sur un espace euclidien

Dans toute la suite, E désignera un espace vectoriel euclidien. E est alors en bijection isométrique avec $\mathbb{R}^n$. On notera μ la mesure image de la mesure de Lebesgue sur $\mathbb{R}^n$ par cette application (qui ne dépend pas du choix de la bijection).

Théorème 2.5.1.1 (Caractérisation des sous-groupes discrets de E). *Soit E un espace euclidien de dimension d. Soit H un sous-groupe discret de E (pour la topologie induite par la norme de E). Alors H est de la forme $\mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_m$ où $(v_1, \ldots, v_m)$ est une famille libre de E sur $\mathbb{R}$.*

Démonstration. Soit $(e_1, \ldots, e_m)$ une famille libre sur $\mathbb{R}$ d'éléments de H avec m maximal pour cette proprieté. On définit alors :

$$K = \left\{ \sum_{i=1}^{m} \alpha_i e_i, \quad 0 \leq \alpha_i \leq 1 \right\}$$

K est alors un compact de E et donc $K \cap H$ est un ensemble compact et discret. Il est donc fini. Notons c son cardinal. Soit $x \in H$, alors grâce à la maximalité de m, on peut écrire $x = \sum_{i=1}^{m} \lambda_i e_i$ où les $\lambda_i \in \mathbb{R}$.

Pour $j \in \mathbb{N}^\star$, posons $x_j = \sum_{i=0}^{n} (j\lambda_i - [j\lambda_i])\, e_i \in K \cap H$. Ainsi il existe k et $l \leq c+1$ tels que $x_k = x_l$ et donc pour tout i, $\lambda_i = \dfrac{[k\lambda_i] - [l\lambda_i]}{k-l}$ si bien que $\lambda_i \in \dfrac{1}{k-l}\mathbb{Z} \subset \dfrac{1}{(c+1)!}\mathbb{Z}$. On en déduit que $H \subset \dfrac{e_1}{(c+1)!}\mathbb{Z} \oplus \ldots \oplus \dfrac{e_m}{(c+1)!}\mathbb{Z}$. Ainsi H est un $\mathbb{Z}$-module libre de dimension inférieur ou égale à m.

Or $(e_1, \ldots, e_m)$ est une famille libre d'éléments de H donc H est de dimension m.

Si $(v_1, \ldots, v_m)$ est une base de H sur $\mathbb{Z}$, alors l'espace qu'elle engendre sur $\mathbb{R}$ contient $e_1, \ldots, e_m$ et donc est de dimension m. Ceci prouve que $(v_1, \ldots, v_m)$ est une famille libre sur $\mathbb{R}$. √

Définition 2.5.1.2. *Un réseau de E est un sous-groupe discret de E de rang n.*

Définition 2.5.1.3. *Soit H un réseau de E et $\mathfrak{B} = (v_1, \ldots, v_n)$ une base de H (en tant que $\mathbb{Z}$-module). On appelle maille élémentaire relativement à la base $\mathfrak{B}$, l'ensemble suivant :*

$$P_{\mathfrak{B}} = \left\{ \sum_{i=1}^{n} \alpha_i v_i, \quad 0 \leq \alpha_i < 1 \right\}$$

Théorème 2.5.1.4 (Caractérisation des réseaux). *Soit H un sous-groupe discret de E, alors H est un réseau si et seulement s'il existe un sous-ensemble borné M de E tel que $M + H = E$.*

Démonstration. Soit H un réseau de E, soit $\mathfrak{B}$ une base de H, alors $M = P_{\mathfrak{B}}$ convient. Réciproquement, supposons qu'il existe M borné tel que $M + H = E$. Notons E_0 l'espace vectoriel engendré par H. Soit $x \in E$, alors pour tout $a \in \mathbb{N}$, on a une décomposition $ax = m_x + h_x$ où $m_x \in M$ et $h_x \in H$ et donc $x = \frac{1}{a}m_x + \frac{1}{a}h_x$. En faisant tendre a vers l'infini, on trouve $x \in E_0$. Finalement, on obtient $E = E_0$ et donc H est un réseau de E. √

Proposition 2.5.1.5. *$\mu(P_{\mathfrak{B}})$ ne dépend pas de la base $\mathfrak{B}$ choisie.*

Démonstration. Soient $\mathfrak{B} = (v_1, \ldots, v_n)$ et $\mathfrak{B}' = (v'_1, \ldots, v'_n)$ deux bases de H. Notons P la matrice de passage de $\mathfrak{B}$ à $\mathfrak{B}'$. On a alors $P \in GL_n(\mathbb{Z})$ et donc $|\det P| = 1$. D'autre part le théorème du changement de variable donne $\mu(P_{\mathfrak{B}'}) = |\det P|\, \mu(P_{\mathfrak{B}})$ d'où le résultat. √

Définition 2.5.1.6. *Le volume de l'un quelconque des $P_{\mathfrak{B}}$ est appelé le volume du réseau H et est noté $v(H)$.*

Proposition 2.5.1.7. *Si $(v_1, \ldots, v_n)$ est une base sur $\mathbb{Z}$ du reseau H, alors :*

$$v(H) = |\det(\langle v_i, v_j \rangle)|^{1/2}$$

Démonstration. Soit $(e_1, \ldots, e_n)$ une base orthonormale de E, et A la matrice de passage de (e_i) à (v_i). Alors

$$(\langle v_i, v_j \rangle) = \left(\sum_{k,l} a_{ik} a_{jl} \langle e_k, e_l \rangle \right) = \left(\sum_{k} a_{ik} a_{jk} \right) = A\, {}^tA$$

d'où

$$v(H) = |\det A| = |\det(\langle v_i, v_j \rangle)|^{1/2}$$

√

Théorème 2.5.1.8 (Minkowski). *Soit H un réseau. Soit S une partie mesurable de E telle que $\mu(S) > v(H)$. Alors il existe deux éléments distincts de S, x et y tels que $x - y \in H$.*

Démonstration. Soit $\mathfrak{B}$ une base de H. On peut alors écrire :

$$E = \bigsqcup_{h\in H} (h + P_{\mathfrak{B}}) \qquad \text{et donc} \qquad S = \bigsqcup_{h\in H} S \cap (h + P_{\mathfrak{B}})$$

On en déduit que :

$$\mu(S) = \sum_{h\in H} \mu(S \cap (h + P_{\mathfrak{B}})) = \sum_{h\in H} \mu((-h + S) \cap P_{\mathfrak{B}})$$

Supposons que l'on ait $(-h + S) \cap (-h' + S) = \emptyset$ dès que $h \neq h'$, on aurait alors :

$$\mu(S) = \sum_{h\in H} \mu((-h + S) \cap P_{\mathfrak{B}}) = \mu\left(\bigsqcup_{h\in H} (-h + S') \cap P_{\mathfrak{B}}\right) \leq \mu(P_{\mathfrak{B}}) = v(H)$$

ce qui est supposé faux. On en déduit qu'il existe h et h' distincts dans H tel que $(-h + S) \cap (-h' + S) \neq \emptyset$. Et donc il existe x et y dans S vérifiant $-h + x = -h' + y$. Ainsi $x - y = h - h' \in H - \{0\}$, ce qu'il fallait démontrer. √

Corollaire 2.5.1.9. *Soient H un réseau et S une partie de E mesurable, convexe, symétrique par rapport à 0 et telle que $\mu(S) > 2^n v(H)$. Alors $S \cap H^\star \neq \emptyset$ (où $H^\star = H - \{0\}$)*

Démonstration. On pose $S' = \frac{1}{2}S$, alors $\mu(S') = \frac{1}{2^n}\mu(S) > v(H)$. On en déduit, par le théorème précédent qu'il existe x et y appartenant à S' tels que $x - y \in H^\star$. Mais on a $x - y = \frac{1}{2}((2x) + (-2y)) \in S$, d'où le résultat. √

Corollaire 2.5.1.10. *Soient H un réseau et S une partie de E mesurable, convexe, compacte, symétrique par rapport à 0 et telle que $\mu(S) \geq 2^n v(H)$. Alors $S \cap H^\star \neq \emptyset$.*

Démonstration. Notons, pour $\varepsilon > 0$, $S_\varepsilon = (1 + \varepsilon)S$. On a alors $\mu(S_\varepsilon) > 2^n v(H)$ et donc, d'après le corollaire précédent, $H^\star \cap S_\varepsilon \neq \emptyset$. D'autre part, comme S_ε est compact, $H^\star \cap S_\varepsilon$ est compact.

Comme S est convexe et symétrique par rapport à 0, on a pour $\varepsilon' < \varepsilon$, $S \subset S_{\varepsilon'} \subset S_\varepsilon$.

Comme une intersection décroissante de compacts non vides est non vide, on obtient :

$$\bigcap_{\varepsilon>0} H^\star \cap S_\varepsilon = H^\star \cap \left(\bigcap_{\varepsilon>0} S_\varepsilon\right) \neq \emptyset$$

Finalement, on a $\bigcap_{\varepsilon>0} S_\varepsilon \supset S$, d'après la remarque précédente. Réciproquement si $x \in S_\varepsilon$ pour tout $\varepsilon > 0$, on peut construire une suite (s_n) d'éléments de S telle que $x = \left(1 + \frac{1}{n}\right) s_n$ pour tout n. Par compacité, (s_n) admet une valeur d'adhérence $s \in S$. Par passage à la limite, on trouve que $x = s$ et donc $x \in S$. √

2.5.2 Discriminant

Définition 2.5.2.1. *Soient B un anneau et A un sous-anneau de B tel que B soit un A-module libre de dimension n. Soit $\mathfrak{B} = (x_1, \ldots, x_n)$ une base de B sur A. On appelle discriminant relativement à la base $\mathfrak{B}$ la quantité $D(\mathfrak{B}) = \det\left(Tr_{B/A}(x_i x_j)\right)$.*

Proposition 2.5.2.2. *Si $\mathfrak{B}$ et $\mathfrak{B}'$ sont deux bases de B sur A, alors $D(\mathfrak{B})$ et $D(\mathfrak{B}')$ différent multiplicativement d'un carré d'une unité.*

Démonstration. On vérifie que si P désigne la matrice de passage de $\mathfrak{B}$ à $\mathfrak{B}'$, on a :

$$\left(Tr_{B/A}(x_i x_j)\right) = {}^tP \left(Tr_{B/A}\left(x'_i x'_j\right)\right) P$$

et donc $D(\mathfrak{B}) = \det(P)^2 D(\mathfrak{B}')$. Comme la matrice P est inversible, son déterminant l'est également. √

Corollaire 2.5.2.3. *L'idéal engendré par $D(\mathfrak{B})$ ne dépend pas de la base $\mathfrak{B}$ choisie.*

Définition 2.5.2.4. *Cet idéal s'appelle le discriminant de B sur A et est noté $\mathfrak{D}_{B/A}$.*

Lemme 2.5.2.5 (Stabilité par passage au quotient). *Soient B un anneau et A un sous-anneau de B tel que B soit un A-module libre de dimension n. Soit $\mathfrak{a}$ un idéal de A de sorte que l'on a le diagramme commutatif suivant :*

$$\begin{array}{ccc} A & \twoheadrightarrow & A/\mathfrak{a} \\ \downarrow & \circlearrowleft & \downarrow \\ B & \twoheadrightarrow & B/\mathfrak{a}B \\ x & \longmapsto & \overline{x} \end{array}$$

Si $(x_1, \ldots, x_n)$ est une base de B, alors $(\overline{x}_1, \ldots, \overline{x}_n)$ est une base de $B/\mathfrak{a}B$ et $D(\overline{x}_1, \ldots, \overline{x}_n) = \overline{D(x_1, \ldots, x_n)}$.

Démonstration. Il suffit de vérifier $Tr(\overline{x}) = \overline{Tr(x)}$. √

Proposition 2.5.2.6. *Soit K une extension séparable de degré n de k. On note $\tau_1, \ldots, \tau_n$ les morphismes de k-algèbres de K dans $\overline{k}$. On considère $(x_1, \ldots, x_n)$ une base de K sur k. Alors $D(x_1, \ldots, x_n) = \det(\tau_i(x_j))^2 \neq 0$.*

Démonstration. On calcule :

$$D(x_1, \ldots, x_n) = |Tr(x_i x_j)| = \left| \sum_{k=1}^{n} \tau_k(x_i x_j) \right| = \left| \sum_{k=1}^{n} \tau_k(x_i)\, \tau_k(x_j) \right| = \det(\tau_i(x_j))^2$$

La non nullité est une conséquence immédiate du lemme de Dedekind qui dit que les τ_k forme une famille libre sur $\mathbb{C}$. √

Le cas qui nous intéresse et que l'on va développer dans la fin de ce paragraphe est celui où $A = \mathbb{Z}$.

Proposition 2.5.2.7. *Soit $\mathfrak{a}$ un idéal fractionnaire non nul de $\mathcal{O}_K$, c'est un $\mathbb{Z}$-module libre de dimension n.*

Démonstration. Il existe $d \in \mathcal{O}_K$ tel que $\mathfrak{a} \subset d^{-1}\mathcal{O}_K$. $\mathcal{O}_K$ et donc $d^{-1}\mathcal{O}_K$ est un $\mathbb{Z}$-module libre de dimension n, ce qui prouve que $\mathfrak{a}$ est un $\mathbb{Z}$-module libre de dimension inférieure ou égale à n.

D'autre part soit $(e_1, \ldots, e_n)$ une base de $\mathcal{O}_K$ sur $\mathbb{Z}$ et soit x un élément non nul de $\mathfrak{a}$. Alors $(xe_1, \ldots, xe_n)$ est une famille libre sur $\mathbb{Z}$ d'éléments de $\mathfrak{a}$. On en déduit le résultat annoncé. √

Soit $\mathfrak{B}$ une base de $\mathfrak{a}$ sur $\mathbb{Z}$. Le calcul effectué dans la démonstration de la proposition 2.5.2.2 prouve que $D(\mathfrak{B})$ ne dépend pas de la base $\mathfrak{B}$ choisie. On peut donc poser la définition suivante :

Définition 2.5.2.8. *Soit $\mathfrak{a}$ un idéal fractionnaire non nul de $\mathcal{O}_K$. On appelle discriminant de $\mathfrak{a}$ et on note $D(\mathfrak{a})$ le discriminant d'une base quelconque de $\mathfrak{a}$ sur $\mathbb{Z}$.*

Définition 2.5.2.9. *On appelle discriminant absolu du corps de nombre K le discriminant de $\mathcal{O}_K$, noté d_K.*

Proposition 2.5.2.10. *Soient $\mathfrak{a} \subset \mathfrak{a}'$ deux idéaux fractionnaires non nuls de K, alors l'indice $(\mathfrak{a}' : \mathfrak{a})$ est fini et vérifie*

$$D(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2 D(\mathfrak{a}')$$

Démonstration. $\mathfrak{a}$ est un sous-$\mathbb{Z}$-module de $\mathfrak{a}'$ libre de même dimension n. On sait donc qu'il existe une base (e_i) de $\mathfrak{a}'$ et des entiers (a_i) tels que la famille $(a_i e_i)$ soit une base de $\mathfrak{a}$. Avec ces bases, on a clairement

$$\mathfrak{a}'/\mathfrak{a} = \prod_{i=1}^{n} \mathbb{Z}/a_i\mathbb{Z}$$

et, si A est la matrice de changement de base,

$$\det A = \prod_{i=1}^{n} a_i$$

d'où la proposition. √

2.5.3 Norme d'un idéal

On allons étendre la notion de norme à un idéal de $\mathcal{O}_K$. Pour cela, on va avoir besoin de la proposition suivante :

Proposition 2.5.3.1. *Si $x \in \mathcal{O}_K$ et $x \neq 0$, alors $|N(x)| = (\mathcal{O}_K : \mathcal{O}_K x)$.*

Démonstration. $\mathcal{O}_K$ et $\mathcal{O}_K x$ sont des $\mathbb{Z}$-modules libres de dimension n. On peut donc trouver une base $(e_1, \ldots, e_n)$ de $\mathcal{O}_K$ et des entiers $c_1, \ldots, c_n$ tels que $(c_1 e_1, \ldots, c_n e_n)$ soit une base de $\mathcal{O}_K x$. On a alors $(\mathcal{O}_K : \mathcal{O}_K x) = |c_1 \ldots c_n|$.

D'autre part $(xe_1, \ldots, xe_n)$ est également une base de $\mathcal{O}_K x$ donc le déterminant de l'application qui a xe_i associe $c_i e_i$ est inversible dans $\mathbb{Z}$ donc il vaut 1 en valeur absolue. Ceci prouve que $N(x) = |c_1 \ldots c_n|$. √

Ceci nous incite à poser la définition suivante :

Définition 2.5.3.2. *Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$. On définit la norme de $\mathfrak{a}$ par $N(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})$.*

Proposition 2.5.3.3. *Si $\mathfrak{a}$ est un idéal non nul de $\mathcal{O}_K$, on a $N(\mathfrak{a}) < \infty$*

Démonstration. C'est un corollaire immédiat de la proposition 2.5.2.10. √

Proposition 2.5.3.4. *Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux non nuls de $\mathcal{O}_K$ alors $N(\mathfrak{ab}) = N(\mathfrak{a})\,N(\mathfrak{b})$.*

Démonstration. Grâce à la décomposition en idéaux maximaux dans un anneau de Dedekind, on peut supposer que $\mathfrak{b}$ est un idéal maximal. Comme on l'a vu dans la démonstration du théorème 2.2.2.9, $\mathfrak{a}/\mathfrak{ab}$ est un espace vectoriel de dimension 1 sur $\mathcal{O}_K/\mathfrak{b}$ et donc Card $(\mathfrak{a}/\mathfrak{ab})$ = Card $(\mathcal{O}_K/\mathfrak{b})$. L'égalité Card $(\mathcal{O}_K/\mathfrak{ab})$ = Card $(\mathcal{O}_K/\mathfrak{a})$ Card $(\mathfrak{a}/\mathfrak{ab})$ permet finalement de conclure. √

2.6 Démonstration

2.6.1 Discriminant et ramification

Nous allons montrer dans cette partie que K se ramifie en p si et seulement si p divise le discriminant absolu de K.

Lemme 2.6.1.1. *Soit $\mathcal{O}$ un anneau de Dedekind et $\mathfrak{a}$ un idéal entier non nul de $\mathcal{O}$. On a vu qu'alors on peut écrire $\mathfrak{a} = \prod_{i=1}^{q} \mathfrak{m}_i^{\alpha_i}$ où les $\mathfrak{m}_i$ sont des idéaux premiers de D et les α_i des entiers strictement positifs. Dans ces conditions on a l'isomorphisme suivant :*

$$\mathcal{O}/\mathfrak{a} \xrightarrow{\sim} \prod_{i=1}^{q} \mathcal{O}/\mathfrak{m}_i^{\alpha_i}$$

Démonstration. D'après le théorème des restes chinois, il suffit de prouver que les $\mathfrak{m}_i^{\alpha_i}$ sont deux à deux étrangers. Or ceci se déduit du formulaire 2.2.1.11 sur les anneaux de Dedekind. √

Dans notre situation, on obtient $\mathcal{O}_K/p\mathcal{O}_K \xrightarrow{\sim} \prod_{i=1}^{q} \mathcal{O}_K/\mathfrak{p}_i^{e_i}$ $\qquad (\star)$

Lemme 2.6.1.2. *Soit k un corps parfait et K une k-algèbre finie. Alors K est réduite (ie 0 est le seul élément nilpotent) si et seulement si $\mathfrak{D}_{K/k} \neq 0$.*

Démonstration. Supposons tout d'abord que K ne soit pas réduite. Considérons donc $x_1 \in K$ un élément nilpotent non nul. On peut alors former $(x_1, x_2, \dots x_n)$ une base de K sur k. Mais alors pour tout j entre 1 et n, $x_1 x_j$ est un élément nilpotent et donc l'endomorphisme de multiplication par $x_1 x_j$ l'est aussi. On en déduit que $Tr(x_1 x_j) = 0$ puis que $\mathfrak{D}_{K/k} = 0$.

Réciproquement supposons que K soit réduite. K est en particulier un anneau nœthérien donc, d'après le lemme 2.2.1.3 il existe des idéaux premiers $\mathfrak{q}_i$ et des entiers strictement positifs α_i tels que $\mathfrak{q}_1^{\alpha_1} \dots \mathfrak{q}_l^{\alpha_l} = 0$. Soit $x \in \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_l$, alors $x^{\alpha_1 + \dots + \alpha_l} = 0$ puis $x = 0$. On en déduit que $\mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_l = 0$.

D'autre part, $K/\mathfrak{q}_i$ est une k-algèbre intègre de dimension finie, c'est donc un corps. Ainsi $\mathfrak{q}_i$ est un idéal maximal de K. En appliquant le théorème des restes chinois, on obtient $K \sim \prod_{i=1}^{l} K/\mathfrak{q}_i$.

Considérons alors $\mathfrak{B} = (\mathfrak{B}_1, \dots, \mathfrak{B}_l)$ une base de K sur k adaptée à cette décomposition. En remarquant que si $x \in K/\mathfrak{q}_i$ et $y \in K/\mathfrak{q}_j$ (où $i \neq j$), alors $xy = 0$, on obtient $D(\mathfrak{B}) = D(\mathfrak{B}_1) \dots D(\mathfrak{B}_l)$, d'où il vient $\mathfrak{D}_{K/k} = \prod_{i=1}^{l} \mathfrak{D}_{(K/\mathfrak{q}_i)k}$. Or $K/\mathfrak{q}_i$ est un corps et même une extension séparable de k (car k est parfait) et donc la trace n'y est pas dégénérée, ce qui veut dire que $\mathfrak{D}_{(K/\mathfrak{q}_i)k} \neq 0$ ou encore $\mathfrak{D}_{(K/\mathfrak{q}_i)k} = k$, et puis $\mathfrak{D}_{K/k} = k \neq 0$. $\surd$

Théorème 2.6.1.3. *K se ramifie en p si et seulement si p divise le discriminant absolu de K.*

Démonstration. D'après $(\star)$, K se ramifie en p si et seulement si $\mathcal{O}_K/p\mathcal{O}_K$ n'est pas réduit. Le lemme précédent prouve que ceci équivaut à $\mathfrak{D}_{(\mathcal{O}_K/p\mathcal{O}_K)(\mathbb{Z}/p\mathbb{Z})} = 0$, c'est-à-dire, grâce à la stabilité par passage au quotient, $\mathfrak{D}_{\mathcal{O}_K/\mathbb{Z}} \subset p\mathbb{Z}$, ce qui veut bien dire que p divise le discriminant absolu de K. $\surd$

Corollaire 2.6.1.4. *Pour prouver que K se ramifie en au moins un idéal premier, il suffit de montrer que son discriminant absolu n'est jamais* 1, *ni* (-1).

2.6.2 L'espace de Minkowski

Pour obtenir ce résultat, on va plonger K dans un espace vectoriel euclidien et utiliser les propriétés des réseaux énoncées précédemment.

K est une extension séparable de $\mathbb{Q}$ donc il existe exactement n homomorphismes de corps de K dans $\mathbb{C}$. On pose $K_{\mathbb{C}} = \mathbb{C}^{\hom(K,\mathbb{C})}$ et on munit $K_{\mathbb{C}}$ du produit scalaire canonique.

On a l'application naturelle $j : \begin{pmatrix} K & \longrightarrow & K_{\mathbb{C}} \\ x & \longmapsto & (\tau x)_\tau \end{pmatrix}$.

Le groupe de Galois $gal(\mathbb{C}|\mathbb{R}) = \{1, F\}$ agit sur $K_{\mathbb{C}}$ de la façon suivante : si $z = (z_\tau)$, $(Fz)_\tau = \overline{z_{\overline{\tau}}}$. L'action de F est une isométrie de $K_{\mathbb{C}}$.

On appelle $K_{\mathbb{R}}$ le sous-espace stable par F ; le produit scalaire (hermitien) sur $K_{\mathbb{C}}$ induit sur $K_{\mathbb{R}}$ un produit scalaire réel qui en fait un espace vectoriel euclidien. Comme $F \circ j = j$, on a par restriction $j : K \longrightarrow K_{\mathbb{R}}$. Nous allons maintenant étudier l'*espace de Minkowski* $K_{\mathbb{R}}$.

Soit $\tau \in \hom(K, \mathbb{C})$. On dit que τ est réel si $\overline{\tau} = \tau$, complexe dans le cas contraire ; $\hom(K, \mathbb{C})$ contient r morphismes réels $\rho_1, \dots, \rho_r : K \longrightarrow \mathbb{R}$ et s paires de morphismes complexes conjugués $\sigma_1, \overline{\sigma_1}, \dots, \sigma_s, \overline{\sigma_s}$: $K \longrightarrow \mathbb{C}$, d'où $n = r + 2s$. Dans la suite, ρ décrira l'ensemble des ρ_i et σ l'ensemble des σ_j. Alors :

$$K_{\mathbb{R}} = \{(z_\tau) \in K_{\mathbb{C}} \,|\, z_\rho \in \mathbb{R}, z_{\overline{\sigma}} = \overline{z_\sigma}\}$$

Proposition 2.6.2.1. *On a un isomorphisme* $f : \begin{pmatrix} K_{\mathbb{R}} & \longrightarrow & \mathbb{R}^{\hom(K,\mathbb{C})} = \mathbb{R}^{r+2s} \\ (z_\tau) & \longmapsto & (x_\tau) \end{pmatrix}$ *défini par* $x_\rho = z_\rho$, $x_\sigma = \mathcal{R}e(z_\sigma)$, $x_{\overline{\sigma}} = \mathcal{I}m(z_\sigma)$.

Si on munit $\mathbb{R}^{\hom(K,\mathbb{C})}$ du produit scalaire $(x, y) \longmapsto \sum_\tau \alpha_\tau x_\tau y_\tau$, où $\alpha_\tau = 1$ si τ est réel, $\alpha_\tau = 2$ si τ est complexe, alors f est de plus une isométrie.

L'application $j : K \longrightarrow K_{\mathbb{R}}$ nous fournit les réseaux suivants dans $K_{\mathbb{R}}$:

Proposition 2.6.2.2. *Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$, alors $\Gamma = j\mathfrak{a}$ est un réseau de $K_\mathbb{R}$, de volume*

$$\mathrm{vol}\,(\Gamma) = \sqrt{|d_K|}N(\mathfrak{a})$$

Démonstration. $\mathfrak{a}$ est libre de rang n sur $\mathbb{Z}$; soit donc $(\alpha_1, \ldots, \alpha_n)$ une base de $\mathfrak{a}$. Alors $\Gamma = \mathbb{Z}j\alpha_1 + \ldots + \mathbb{Z}j\alpha_n$. En posant $\hom(K, \mathbb{C}) = \{\tau_1, \ldots, \tau_n\}$, et $A = (\tau_l\alpha_i)$, on a :

$$(\langle j\alpha_i, j\alpha_k\rangle) = \left(\sum_{l=1}^{n} \tau_l\alpha_i\overline{\tau_l}\alpha_k\right) = A\,{}^tA$$

et

$$(\det A)^2 = D(\mathfrak{a}) = N(\mathfrak{a})^2 d_K$$

d'où

$$v(\Gamma) = |\det(\langle j\alpha_i, j\alpha_k\rangle)|^{1/2} = |\det A| = \sqrt{|d_K|}N(\mathfrak{a})$$

√

Théorème 2.6.2.3. *Le discriminant d'un corps de nombres K de degré n vérifie $|d_K|^{1/2} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2}$.*

Démonstration. Le théorème de Minkowski sur les réseaux s'applique de la façon suivante : soit X une partie mesurable, convexe, compacte, symétrique par rapport à l'origine de $K_\mathbb{R}$, et telle que $\mu(X) \geq 2^n v(\Gamma)$, où $\Gamma = j\mathcal{O}_K$, alors il existe $a \in \mathcal{O}_K$ tel que $a \neq 0$ et $ja \in X$.

Pour $t > 0$, posons

$$X_t = \left\{(z_\tau) \in K_\mathbb{R} \;\middle|\; \sum_\tau |z_\tau| \leq t\right\}$$

X_t est clairement mesurable, convexe, compacte et symétrique par rapport à l'origine, et on montre (voir lemme suivant) que $\mu(X_t) = 2^r\pi^s\frac{t^n}{n!}$. Pour appliquer le résultat, on choisit donc $\mu(X_t) = 2^n v(\Gamma)$, ce qui correspond à $t^n = n!\left(\frac{4}{\pi}\right)^s\sqrt{|d_K|}$. On dispose donc du a désiré.

L'inégalité entre les moyennes arithmétique et géométrique nous donne :

$$\left(\prod_\tau |\tau a|\right)^{1/n} \leq \frac{1}{n}\sum_\tau |\tau a|$$

d'où

$$\left|N_{K/\mathbb{Q}}(a)\right| = \prod_\tau |\tau a| \leq \frac{1}{n^n}\left(\sum_\tau |\tau a|\right)^n \leq \frac{t^n}{n^n}$$

Comme $n = r + 2s$, on a $s \leq n/2$ et $\frac{t^n}{n^n} \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{n/2}\sqrt{|d_K|}$. Enfin, $a \in \mathcal{O}_K$ donc $N_{K/\mathbb{Q}}(a) \in \mathbb{Z}$ et en particulier $\left|N_{K/\mathbb{Q}}(a)\right| \geq 1$. On en déduit le résultat demandé. √

Lemme 2.6.2.4. *Dans l'espace de Minkowski $K_\mathbb{R}$, la partie mesurable*

$$X_t = \left\{(z_\tau) \in K_\mathbb{R} \;\middle|\; \sum_\tau |z_\tau| \leq t\right\}$$

a pour volume $\mu(X_t) = 2^r\pi^s\dfrac{t^n}{n!}$.

Démonstration. Si λ est la mesure de Lebesgue sur $\mathbb{R}^{\hom(K,\mathbb{C})}$, et $f : K_\mathbb{R} \longrightarrow \mathbb{R}^{\hom(K,\mathbb{C})}$ l'application précédemment définie, alors $\mu(X_t) = 2^s\lambda(f(X_t))$. On a :

$$f(X_t) = \left\{(x_\rho, x_\sigma, x_{\overline{\sigma}}) \;\middle|\; \sum_\rho |x_\rho| + 2\sum_\sigma \sqrt{{x_\sigma}^2 + {x_{\overline{\sigma}}}^2} \leq t\right\}$$

Le facteur 2 est dû au fait que $|z_{\overline{\sigma}}| = |z_\sigma|$.

On passe en coordonnées polaires

$$(u_\sigma, \theta_\sigma) \longmapsto \left(x_\sigma = \frac{u_\sigma}{2}\cos\theta_\sigma, x_{\overline{\sigma}} = \frac{u_\sigma}{2}\sin\theta_\sigma\right)$$

et on utilise la symétrie de X_t pour se restreindre au domaine où $x_\rho \geq 0$, ce qui divise le volume par 2^r. Ce travail nous permet d'obtenir l'expression

$$\lambda\left(f\left(X_t\right)\right) = \int_{Y_{r,s}(t)\times[0,2\pi]^s} 2^r 4^{-s} u_1 \ldots u_s \, dx_1 \ldots dx_r du_1 \ldots du_s d\theta_1 \ldots d\theta_s$$

où $Y_{r,s}\left(t\right) = \left\{(x_1, \ldots, x_r, u_1, \ldots, u_s) \in \mathbb{R}^{+r+s} \mid x_1 + \ldots + x_r + u_1 + \ldots + u_s \leq t\right\}$,

d'où finalement $\mu\left(X_t\right) = 2^r \pi^s I_{r,s}\left(t\right)$ avec

$$I_{r,s}\left(t\right) = \int_{Y_{r,s}(t)} u_1 \ldots u_s \, dx_1 \ldots dx_r du_1 \ldots du_s$$

On a clairement $I_{r,s}\left(t\right) = t^{r+2s} I_{r,s}\left(1\right)$. Si, en appliquant le théorème de Fubini, on intègre d'abord par rapport aux variables $x_1, \ldots, x_{r-1}, u_1, \ldots, u_s$, puis par rapport à x_r, on obtient :

$$I_{r,s}\left(1\right) = \int_0^1 I_{r-1,s}\left(1 - x_r\right) dx_r = \int_0^1 \left(1 - x_r\right)^{n-1} dx_r . I_{r-1,s}\left(1\right) = \frac{1}{n} I_{r-1,s}\left(1\right)$$

d'où, par récurrence, $I_{r,s}\left(1\right) = \frac{(n-r)!}{n!} I_{0,s}\left(1\right)$. De la même manière, on obtient

$$I_{0,s}\left(1\right) = \int_0^1 u_s (1 - u_s)^{2s-2} du_s . I_{0,s-1}\left(1\right)$$

et $I_{0,s}\left(1\right) = \frac{1}{(2s)!} I_{0,0}\left(1\right) = \frac{1}{(2s)!} = \frac{1}{(n-r)!}$. Finalement, $I_{r,s}\left(1\right) = \frac{1}{n!}$, d'où le résultat annoncé. √

Corollaire 2.6.2.5 (Théorème de Minkowski). *Tout corps de nombres différent de $\mathbb{Q}$ se ramifie en au moins un idéal premier.*

Démonstration. On a vu dans le paragraphe précédent qu'il suffisait de prouver que $|d_K| > 1$. Posons alors $u_n = \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2}$. On a alors $u_2 = \frac{\pi}{2} > 1$ et $\frac{u_{n+1}}{u_n} = \sqrt{\frac{\pi}{4}}\left(1 + \frac{1}{n}\right)^n > 1$, ce qui prouve le théorème. √

On a montré que $\mathbb{Z}$ est simplement connexe !

2.7 Compléments

2.7.1 Un résultat de finitude

Théorème 2.7.1.1. *Il n'y a qu'un nombre fini de corps de nombres de discriminant donné.*

Démonstration. La formule de Stirling permet de montrer que le discriminant d'un corps de nombre tend vers l'infini avec le degré du corps de nombres. Ainsi, on peut supposer que le degré n ainsi donc que les nombres r et s définis précédemment sont donnés.

Soit K un corps de nombres. Montrons qu'il existe un élément primitif de K « pas trop grand ».

Si $r = 0$, alors les résultats sur les réseaux prouvent qu'il existe une constante C_0 et un élément $x \in \mathcal{O}_K$ vérifiant $\mathcal{I}m\left(\sigma_1\left(x\right)\right) \leq C_0$, $\mathcal{R}e\left(\sigma_1\left(x\right)\right) \leq \frac{1}{2}$ et pour tout i supérieur ou égal à 2, $|\sigma_i\left(x\right)| \leq \frac{1}{2}$. Comme $x \in \mathcal{O}_K$, on a $|N\left(x\right)| \geq 1$ et donc $|\sigma_1\left(x\right)| \geq 1$. On en déduit que pour i supérieur ou égal à 2, $\sigma_1\left(x\right) \neq \sigma_i\left(x\right)$ et $\sigma_1\left(x\right) \neq \overline{\sigma}_i\left(x\right)$. D'autre part on a $\sigma_1\left(x\right) \neq \overline{\sigma}_1\left(x\right)$. Ceci prouve que x est un élément primitif.

Si $r > 0$, alors comme précédemment il existe une constante C_1 et $x \in \mathcal{O}_K$ tel que $|\rho_1\left(x\right)| \leq C_1$ et pour tout $\tau \in \hom\left(K, \mathbb{C}\right)$ différent de ρ_1, $|\tau\left(x\right)| \leq \frac{1}{2}$. On en déduit, grâce à la norme, que $|\rho_1\left(x\right)| \geq 1$ et donc que x est un élément primitif.

Les majorations ci-dessus prouvent que les fonctions symétriques élémentaires des τx appartiennent à un ensemble borné et donc ne peuvent prendre qu'un nombre fini de valeurs. On en déduit qu'il n'y a qu'un nombre fini de possibilités pour le polynôme caractéristique de x et donc également pour x. Comme $K = \mathbb{Q}[x]$, on obtient le théorème annoncé. √

2.7.2 Le théorème des unités

Soit K un corps de nombres, les entiers r et s sont définis comme précédemment. On notera $\mathcal{O}_K^\star$ le groupe des unités de l'anneau $\mathcal{O}_K$ et μ_K l'ensemble des racines de l'unité contenues dans K.

Le but de ce paragraphe est de démontrer le théorème suivant :

Théorème 2.7.2.1. *Avec les notations précédentes, $\mathcal{O}_K^\star$ est isomorphe au produit direct de μ_K par $\mathbb{Z}^{r+s-1}$.*

Proposition 2.7.2.2. *Les éléments de $\mathcal{O}_K^\star$ sont exactement les éléments de $\mathcal{O}_K$ de norme 1 ou (-1).*

Démonstration. Si x est inversible dans $\mathcal{O}_K$ alors on a $N(x)N\left(x^{-1}\right) = N(1) = 1$ et $N(x) \in \mathbb{Z}$ d'où la première implication.

Réciproquement si $N(x) \in \{1, -1\}$, on peut écrire l'équation de dépendance intégrale $x^n + a_{n-1}x^{n-1} + \ldots + N(x) = 0$, ce qui prouve bien que x est inversible dans $\mathcal{O}_K$. √

Définition 2.7.2.3 (Plongement logarithmique). *Avec les notations précédentes, on appelle plongement logarithmique le morphisme suivant :*

$$L : \left(\begin{array}{ccc} K^\star & \to & \mathbb{R}^{r+s} \\ x & \mapsto & (\ln|\rho_1(x)|, \ldots, \ln|\rho_r(x)|, ln|\sigma_1(x)|, \ldots, ln|\sigma_s(x)|) \end{array} \right)$$

On notera λ la restriction de ce morphime à $\mathcal{O}_K^\star$ et Γ l'image de λ.

Proposition 2.7.2.4. *Le noyau de λ est exactement μ_K.*

Démonstration. Si $x \in \ker\lambda$, alors les coefficients de son polynôme caractéristique (qui s'expriment comme les fonctions symétriques élémentaires de $\tau(x)$, $\tau \in \hom(K, \mathbb{C})$) sont bornées. Ceci prouve que $\ker\lambda$ est un sous-groupe fini de $K^\star$, il est donc formé de racines de l'unité.

D'autre part, si $x \in \mu_K$, alors il est clair que $|\tau(x)| = 1$ pour tout $\tau \in \hom(K, \mathbb{C})$ et donc $x \in \ker\lambda$. √

Remarque 2.7.2.5. *La proposition dit exactement que la suite suivante est exacte :*

$$1 \longrightarrow \mu_K \longrightarrow \mathcal{O}_K^\star \longrightarrow \Gamma \longrightarrow 1$$

Proposition 2.7.2.6. *Γ est un sous-groupe discret de $\mathbb{R}^{r+s}$.*

Démonstration. Il suffit de montrer que tout compact de $\mathbb{R}^{r+s}$ intersecte Γ sur un ensemble fini. Soit donc C un compact de $\mathbb{R}^{r+s}$ et soit $x \in \Gamma \cap C$. Alors il existe $x_0 \in \mathcal{O}_K$ et R tel que pour tout $\tau \in \hom(K, \mathbb{C})$, $|\ln|\tau(x)|| \leq R$ et puis $e^{-R} \leq |\tau(x)| \leq e^R$. Comme précédemment, on en déduit que les coefficients du polynôme caractéristique de x sont bornés et puis que $\Gamma \cap C$ est fini. √

Les résultats sur les sous-groupes discrets prouvent en particulier que Γ est un $\mathbb{Z}$-module libre de dimension inférieure ou égale à $r+s$. Ceci prouve que la suite exacte écrite au-dessus est scindée et donc que $\mathcal{O}_K^\star$ s'exprime comme produit direct de Γ par μ_K.

Il ne reste donc plus qu'à montrer que Γ est de dimension $r+s-1$.

Il est facile de voir tout d'abord que la dimension de Γ est inférieure ou égale à $r+s-1$.

Démonstration. Soit $x \in \mathcal{O}_K^\star$, on a vu qu'alors $N(x) = 1$, et donc

$$\prod_{\tau \in \hom(K,\mathbb{C})} |\tau(x)| = \left(\prod_{i=1}^{r} |\rho_i(x)| \right) \left(\prod_{j=1}^{s} |\sigma_j(x)|^2 \right) = 1.$$

Ceci prouve que Γ est inclus dans l'hyperplan d'équation $x_1 + \ldots + x_r + 2(y_1 + \ldots + y_s) = 0$. √

Notons H l'hyperplan d'équation $x_1 + \ldots + x_r + 2(y_1 + \ldots + y_s) = 0$.

Lemme 2.7.2.7. *Il existe deux constantes C et α telles que pour tout w dans H, il existe un élément a de $\mathcal{O}_K$ tel que $N(a) \leq \alpha$ et $||w - L(a)|| \leq C$.*

Démonstration. Notons H_α l'hyperplan affine d'équation $x_1 + \ldots + x_r + 2(y_1 + \ldots + y_s) = \alpha$.

Soit $v = (x_1, \ldots, x_r, y_1, \ldots, y_s) \in H_\alpha$. Considérons l'ensemble suivant :

$$X = \{(z_\tau) \in K_{\mathbb{R}} \,|\, |\rho_i| \leq e^{x_i},\ |\sigma_j| \leq e^{y_j}\}$$

X est alors un ensemble compact, convexe et symétrique par rapport à 0. Le volume de X vaut $\pi^s e^{x_1} \ldots e^{x_s} e^{2y_1} \ldots e^{2y_s}$ soit $\pi^s e^{\alpha}$. Donc si on choisit α suffisamment grand, il va exister $a \in \mathcal{O}_K$ tel que $ja \in X$. Autrement dit, on aura $|\rho_i(a)| \leq e^{x_i}$ et $|\sigma_j(a)| \leq e^{y_j}$. On a alors $|N(a)| \leq e^{\alpha}$. D'autre part $a \in \mathcal{O}_K$ donc $|N(a)| \geq 1$ et puis :

$$|\rho_i(a)| = |N(a)| \left(\prod_{k \neq i} |\rho_k(a)|\right) \left(\prod_{l=1}^{s} |\sigma_l(a)|^2\right) \geq \frac{e^{x_i}}{e^{\alpha}}$$

$$|\sigma_j(a)|^2 = |N(a)| \left(\prod_{k=1}^{r} |\rho_k(a)|\right) \left(\prod_{l \neq j} |\sigma_l(a)|^2\right) \geq \frac{e^{2y_j}}{e^{\alpha}}$$

On en déduit que $-\alpha \leq \ln|\rho_i(a)| - x_i \leq 0$ et $-\frac{\alpha}{2} \leq \ln|\sigma_j(a)| - y_j \leq 0$. Ainsi $||v - L(a)|| \leq \alpha\sqrt{r+s}$.

Remarquons finalement que le α peut être choisi indépendamment de v. √

Lemme 2.7.2.8. *Modulo les éléments de $\mathcal{O}_K^\star$, il n'y a qu'un nombre fini d'éléments de $\mathcal{O}_K$ de norme donnée a priori.*

Démonstration. Notons q la valeur de la norme donnée a priori. Soit $x \in \mathcal{O}_K$, on a alors Card $(\mathcal{O}_K/\mathcal{O}_K x) = |N(x)| = |q|$. On en déduit que $q \in \mathcal{O}_K x$ (car l'ordre dans $\mathcal{O}_K/\mathcal{O}_K x$, $1 * q = 0$) et donc $\mathcal{O}_K q \subset \mathcal{O}_K x$, d'où $\mathcal{O}_K/\mathcal{O}_K x \subset \mathcal{O}_K/\mathcal{O}_K q$. Or $\mathcal{O}_K/\mathcal{O}_K q$ est fini donc l'ensemble de $\mathcal{O}_K x$ qui conviennent également. On en déduit le lemme annoncé. √

On en déduit le résultat voulu de la façon suivante :

Démonstration. D'après le lemme précédent, il existe $a_1, \ldots, a_N$ des éléments de $\mathcal{O}_K$ tels que si $|N(a)| \leq e^{\alpha}$, alors $a = u a_k$ où $u \in \mathcal{O}_K^\star$. Notons B la boule de E de centre l'origine et de rayon C et posons :

$$M = \bigcup_{k=1}^{N} (B + L(a_k))$$

M est alors une partie bornée de E et si $w \in H$, alors il existe a de norme inférieure à α tel que $(w - L(a)) \in B$. D'autre part il existe $u \in \mathcal{O}_K^\star$ tel que $a = u a_k$. On a alors $(w - L(a_k) - \lambda(u)) \in B$ et donc $(w - \lambda(u)) \in M$. On en déduit par la caractérisation des réseaux que Γ est de dimension $r + s - 1$. √

2.8 L'exemple de $\mathbb{Q}[\sqrt{d}]$

Considérons d un entier positif non multiple d'un carré parfait. Prenons $K = \mathbb{Q}[\sqrt{d}]$.

Lemme 2.8.0.9. *Soit $x \in \mathbb{Q}$. On suppose que $x\sqrt{d} \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$. Alors $x \in \mathbb{Z}$.*

Démonstration. Supposons que $x\sqrt{d} \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$, on a alors l'équation de dépendance intégrale $\left(x\sqrt{d}\right)^n + a_{n-1}\left(x\sqrt{d}\right)^{n-1} + \ldots + a_0 = 0$. Si n est pair, on obtient puisque d n'est pas un carré parfait, l'équation $\left(x^2 d\right)^{\frac{n}{2}} + \ldots + a_0 = 0$. De même si n est impair, on obtient $x\left(x^2 d\right)^{\frac{n-1}{2}} + \ldots + a_1 x = 0$ puis $\left(x^2 d\right)^{\frac{n-1}{2}} + \ldots + a_1 = 0$. Dans tous les cas, $x^2 d \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]} \cap \mathbb{Q} = \mathbb{Z}$. Comme on a supposé que d n'est pas divisible par un carré parfait, il vient $x \in \mathbb{Z}$. √

2.8.1 Cas où d n'est pas congru à 1 modulo 4

Proposition 2.8.1.1. *Si d n'est pas congru à 1 modulo 4, l'anneau des entiers est $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \mathbb{Z}[\sqrt{d}]$.*

Démonstration. On a $1 \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ et $\sqrt{d} \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$. On en déduit que $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$.

Réciproquement, supposons que $x = a+b\sqrt{d} \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$. Alors $Tr(x) = 2a \in \mathbb{Z}$. On en déduit que $2b\sqrt{d} \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$ et donc d'après le lemme précédent $2b \in \mathbb{Z}$. Ainsi x s'écrit $x = \frac{a'+b'\sqrt{d}}{2}$. Supposons a' et b' impairs. On a alors $N(x) = \frac{a'^2-db'^2}{4} \in \mathbb{Z}$ et on en déduit que d est congru à 1 modulo 4 ce qui est supposé faux. On en déduit que a' ou b' est pair puis les deux par le lemme précédent. √

Regardons les nombres premiers p en lesquels K se ramifie.

Proposition 2.8.1.2. *K se ramifie en p si et seulement si p divise d ou $p = 2$.*

Démonstration. Calculons le discriminant absolu de K, il vaut :

$$\begin{vmatrix} Tr(1) & Tr(\sqrt{d}) \\ Tr(\sqrt{d}) & Tr(d) \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & d \end{vmatrix} = 4d$$

ce qui permet de conclure. √

Essayons de déterminer les idéaux au-dessus de $p\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$.

Si p divise d, considérons l'idéal $\mathfrak{p} = p\mathbb{Z} + \sqrt{d}\,\mathbb{Z}$. Montrons que c'est un idéal premier. Pour cela, supposons que $(a + b\sqrt{d})(a' + b'\sqrt{d}) \in \mathfrak{p}$. On obtient alors p divise $aa' + dbb'$ et donc p divise aa', soit p divise a ou p divise a', ce qui montre bien que $\mathfrak{p}$ est premier. Finalement, on vérifie que $p\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \mathfrak{p}^2$ et donc $\mathfrak{p}$ est le seul idéal premier au-dessus de $p\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$.

Si $p = 2$ et d est impair, considérons $\mathfrak{p} = \left\{ a + b\sqrt{d} \mid a \equiv b \pmod 2 \right\}$ et supposons que $(a+b\sqrt{d})(a' + b'\sqrt{d}) \in \mathfrak{p}$. On obtient alors $aa' + dbb' \equiv ab' + ba' \pmod 2$. Si a est pair et b est impair, on obtient $db' \equiv a' \pmod 2$ et donc $a' \equiv b' \pmod 2$. Si a est impair et b est pair, on obtient directement $a' \equiv b' \pmod 2$. On en déduit que $\mathfrak{p}$ est un idéal premier. Il ne reste plus qu'à vérifier que $2\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \mathfrak{p}^2$ pour prouver qu'il s'agit du seul idéal premier au-dessus de $p\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$.

Dans le cas où p est différent de 2 et p ne divise pas d, on suppose de plus de d est un carré modulo p. On considère alors ω un racine carrée de d et $\mathfrak{p}_1 = \left\{ a + b\sqrt{d} \mid a \equiv \omega b \pmod p \right\}$ et supposons que $(a + b\sqrt{d})(a' + b'\sqrt{d}) \in \mathfrak{p}_1$. On obtient alors $aa' + dbb' \equiv \omega\,(ab' + ba') \pmod p$ qui s'écrit également $(a - \omega b)\,(a' - \omega b') \equiv 0 \pmod p$, ce qui prouve que $\mathfrak{p}_1$ est premier. De même, $\mathfrak{p}_2 = \left\{ a + b\sqrt{d} \mid a \equiv -\omega b \pmod p \right\}$ est un idéal premier. On vérifie alors que $\mathfrak{p}_1 \neq \mathfrak{p}_2$ et donc ce sont les seuls idéaux premiers au-dessus de $p\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$.

Une application du théorème des unités.

Le théorème des unités de Dirichlet permet ici de retrouver la forme des solutions de l'équation de Pell-Fermat $a^2 - db^2 = \pm 1$. En effet, le dégré de l'extension $K/\mathbb{Q}$ est clairement 2 et comme $K \subset \mathbb{R}$, on trouve $r = 2$ et $s = 0$. Ainsi $\mathcal{O}^\star_{\mathbb{Q}[\sqrt{d}]}$ est isomorphe à $\{\pm 1\} \times \mathbb{Z}$.

Or les éléments de $\mathcal{O}^\star_{\mathbb{Q}[\sqrt{d}]}$ sont exactement les $a + b\sqrt{d}$ avec $a^2 - db^2 = \pm 1$.

2.8.2 Cas où d est congru à 1 modulo 4

Proposition 2.8.2.1. *Si d est congru à 1 modulo 4, l'anneau des entiers est $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \mathbb{Z} + \frac{1}{2}\left(1 + \sqrt{d}\right)\mathbb{Z}$.*

Démonstration. On a $1 \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$. D'autre part $\frac{1+\sqrt{d}}{2}$ est solution de l'équation $x^2 - x - \frac{d-1}{4} = 0$.

Réciproquement si $x = a + b\sqrt{d} \in \mathcal{O}_{\mathbb{Q}[\sqrt{d}]}$, on en déduit comme précédemment que x s'écrit $\frac{a'+b'\sqrt{d}}{2}$ où a' et b' sont des entiers et que 4 divise $a'^2 - db'^2$. En regardant, les congruences modulo 4, on trouve que a' et b' doivent être de même parité et donc le résultat voulu. √

Proposition 2.8.2.2. *K se ramifie en p si et seulement si p se ramifie en d.*

Démonstration. Calculons le discriminant absolu de K, il vaut :

$$\begin{vmatrix} Tr(1) & Tr\left(\frac{1+\sqrt{d}}{2}\right) \\ Tr\left(\frac{1+\sqrt{d}}{2}\right) & Tr\left(\frac{d+1+2\sqrt{d}}{4}\right) \end{vmatrix} = \begin{vmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{vmatrix} = d$$

ce qui permet de conclure. √

2.8.3 Extension au cas général

Dans le cas général, si $d = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ (où les p_i sont des nombres premiers distincts et les α_i des entiers strictement positifs), on remarque que $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[\sqrt{d'}]$ avec $d' = p_1^{\beta_1} \dots p_k^{\beta_k}$ où β_i est le reste de la division euclidienne de α_i par 2. Mais d' n'est alors multiple d'aucun carré parfait et ainsi on est ramené au cas précédent.

Bibliographie

[Dou79] R. et A. Douady. *Algèbre et théories galoisiennes*, volume vol. 2. Cedic/Fernand Nathan, Paris, 1979.

[Neu99] Jürgen Neukirch. *Algebraic number theory*. Springer, Berlin, 1999.

[Sam71] Pierre Samuel. *Théorie algébrique des nombres*. Hermann, Paris, 1971.

Chapitre 3

Mémoire de DEA

Le sujet de mon exposé de maîtrise m'ayant bien plu, j'ai décidé de continuer à étudier l'arithmétique. Pour le DEA, je me spécialise dans le p-adique et c'est Christophe Breuil qui me guide pour me faire découvrir ce terrain nouveau. Le sujet qu'il me propose reprend un cas particulier d'une conjection de Serre connue aujourd'hui depuis de nombreuses années. Le titre que je décide de donner à ce mémoire est « **Représentations géométriques du groupe de Galois absolu d'un corps local** ».

De nombreux rappels sont faits au début de sorte que ce mémoire doit rester accessible à tout élève ayant suivi un enseignement minimal de niveau DEA en algèbre.

Sommaire

Dans tout ce mémoire, K désignera un corps de caractéristique nulle (et donc parfait) complet pour une valuation discrète v. On supposera que la valuation est normalisée par $v(K^\star) = \mathbb{Z}$. On rappelle que l'anneau de la valuation, $\mathcal{O}_K = \{x \in K, v(x) \geqslant 0\}$, est un anneau local. Son idéal maximal est $\mathfrak{m}_K = \{x \in K, v(x) > 0\}$. C'est un idéal principal engendré par un élément π de valuation 1. Un tel élément s'appelle une *uniformisante* de K. Le corps résiduel $\mathcal{O}_K/\mathfrak{m}_K$ sera noté k. On supposera que k est un corps parfait, de caractéristique $p > 0$.

$\mathbb{F}_p$ désignera le corps fini à p élément $\mathbb{Z}/p\mathbb{Z}$. On fixe une fois pour toutes $\bar{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$. Finalement, on désignera par $\mathbb{F}_q$ l'unique sous-corps de $\bar{\mathbb{F}}_p$ à q éléments. On rappelle qu'il est formé exactement des $x \in \bar{\mathbb{F}}_p$ tels que $x^q = x$.

3.1 Structure du groupe de Galois absolu d'un corps local

Si l'on se donne une extension finie L de K, rappelons que la valuation v s'étend de manière unique à L. On notera encore v par la suite cette nouvelle valuation. v est encore une valuation discrète, seulement elle n'est peut-être plus normalisée dans le sens où $v(L^\star) = \mathbb{Z}$. En fait, on a toujours l'inclusion $\mathbb{Z} \subset v(L^\star)$ (puisque K est inclus dans L) et comme $v(L^\star)$ est un sous-groupe discret de $\mathbb{Z}$, il va exister un entier e tel que $v(L^\star) = \frac{1}{e}\mathbb{Z}$. e s'appelle l'*indice de ramification* de l'extension L/K. Il est en général noté $e(L/K)$ plutôt que e. On voit immédiatement que si l'on appelle $\mathfrak{m}_L$ l'idéal maximal de $\mathcal{O}_L$, $\mathfrak{m}_L$ est l'idéal engendré par un élément de L de valuation $\frac{1}{e}$. Ceci prouve en particulier que $m_K\mathcal{O}_L = \mathfrak{m}_L^e$.

Regardons maintenant $\ell = \mathcal{O}_L/\mathfrak{m}_L$ le corps résiduel de L. C'est naturellement une extension de k. En effet, l'application $\mathcal{O}_K \to \ell$ composée de l'inclusion $\mathcal{O}_K \to \mathcal{O}_L$ et de la projection $\mathcal{O}_L \to \ell$ se factorise par k. Le degré de l'extension ℓ/k est en général noté $f(L/K)$ ou plus simplement f s'il n'y a pas d'ambiguité. On l'appelle le degré résiduel de l'extension L/K. Il est utile de connaître la formule $e(L/K)\,f(L/K) = [L : K]$. Si $e(L/K) = 1$, l'extension L/K est dite *non ramifiée* et si $f(L/K) = 1$, elle est dite *totalement ramifiée*.

Finalement si l'on ne suppose plus que l'extension L/K est finie mais que l'on suppose simplement qu'elle est algébrique, il est encore vrai que la valuation v définie sur K se prolonge de façon unique à L. Par contre, il n'est plus vrai que celle-ci reste discrète et il n'est plus possible de définir de façon générale les nombres $e(L/K)$ et $f(L/K)$. Toutefois si ces quantités sont finies, les définitions données précédemment sont encore valides. En particulier, on sait donner un sens à la non-ramification ou la totale ramification de l'extension L/K. Plus précisément, on dira que l'extension L/K est *non ramifiée* si $v(L^\star) = \mathbb{Z}$. Ceci revient à dire que pour toute extension finie K' de K contenue dans L, K' est non ramifiée sur K. De même, on dira que l'extension L/K est *totalement ramifiée* si l'extension résiduelle ℓ/k est triviale. Là encore, cela revient à dire que toute extension finie de K contenue dans L est totalement ramifiée sur K.

Il est important de faire une remarque sur le cas galoisien. Si l'extension L/K est galoisienne (pas forcément finie), il en est de même de l'extension ℓ/k et on a une flèche naturelle du groupe de Galois de L/K dans celui de ℓ/k. Pour voir cela, il suffit de vérifier qu'un K-automorphisme de L laisse forcément stable l'anneau $\mathcal{O}_L$ et l'idéal $\mathfrak{m}_L$ et donc induit par passage au quotient un automorphisme de ℓ laissant fixe k. La flèche ainsi définie est toujours surjective. C'est un isomorphisme lorsque l'extension L/K est non ramifiée et seulement dans ce cas.

3.1.1 L'extension maximale non ramifiée

Fixons à partir de maintenant une clôture algébrique $\bar{K}$ du corps K. Comme nous l'avons déjà dit, la valuation v se prolonge à $\bar{K}$ et nous noterons encore v ce prolongement. Le corps résiduel de $\bar{K}$ n'est autre qu'une clôture algébrique de k, nous l'appelerons $\bar{k}$. Nous avons également vu qu'à toute extension de K contenue dans $\bar{K}$, on pouvait associer une extension de k contenue dans $\bar{k}$. La réciproque est également vraie. Autrement dit, si ℓ est une extension de k contenue dans $\bar{k}$, il va lui correspondre une extension L

de K contenue dans $\bar{K}$ dont le corps résiduel est précisément ℓ. On peut même faire un peu mieux, on peut choisir L non ramifiée sur K et dans ce cas, le corps L est uniquement déterminé.

Autrement dit, la fonction qui à une extension non ramifiée de K contenue dans $\bar{K}$ associe son corps résiduel est une bijection de l'ensemble des extensions non ramifiées de K contenues dans $\bar{K}$ dans l'ensemble des extensions de k contenues dans $\bar{k}$. Cette bijection est croissante (pour l'inclusion) et respecte les extensions galoisiennes. Ceci permet de prouver qu'il existe une extension maximale non ramifiée de K contenue dans $\bar{K}$, c'est précisément celle qui est en correspondance par la bijection précédente avec le corps $\bar{k}$. Cette extension, généralement notée K^{nr}, est galoisienne puis $\bar{k}/k$ l'est et donc définit un sous-groupe distingué de $\mathrm{Gal}\left(\bar{K}/K\right)$ qui correpondant à $\mathrm{Gal}\left(\bar{K}/K^{\mathrm{nr}}\right)$. Ce sous-groupe s'appelle le *groupe d'inertie* et est en général noté I.

Le quotient de $\mathrm{Gal}\left(\bar{K}/K\right)$ par I correspond au groupe de Galois de K^{nr} sur K et donc est isomorphe d'après ce que l'on a dit précédemment au groupe de Galois absolu de k, c'est-à-dire $\mathrm{Gal}\left(\bar{k}/k\right)$. Finalement, disons que I peut être décrit de façon plus terre à terre. En effet, un automorphisme σ appartient à I si et seulement s'il agit trivialement sur $\bar{k}$, ie si $\sigma(x) = x \pmod{\mathfrak{m}_{\bar{K}}}$ pour tout $x \in \mathcal{O}_{\bar{K}}$.

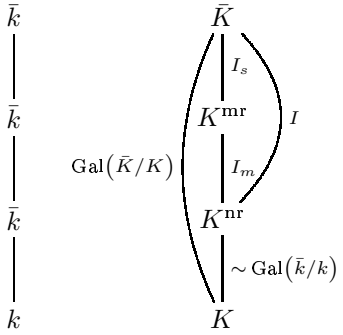
3.1.2 Description du groupe d'inertie

Là encore, il est possible de couper le groupe d'inertie en deux en intercalant une extension intermédiaire. Il s'agit de l'*extension maximale modérément ramifiée*. Rappelons quand même que l'on dit que l'extension finie L/K est *modérément ramifiée* si l'indice de ramification $e(L/K)$ est premier à p, caractéristique du corps résiduel k. Au contraire, une extension telle que $e(L/K)$ est une puissance de p sera dite *sauvagement ramifiée*. Bien entendu, il est possible d'étendre cela à toute extension algébrique en disant simplement que L/K est *modérément ramifiée* (resp. *sauvagement ramifiée*) si toutes les extensions K' de K qui sont finies et incluses dans L le sont.

Il existe une extension maximale modérément ramifiée de K qui bien sûr contient K^{nr} et que l'on note souvent K^{mr}. Il est assez facile de la décrire. Considérons un entier e premier à p et le corps K_e obtenu en rajoutant à K^{nr} une racine e-ième de l'uniformisante π (comme l'extension K^{nr}/K est non ramifiée, π est indifféremment uniformisante de K et de K^{nr}). Il est clair que l'extension K_e/K^{nr} est totalement ramifiée et que son indice de ramification vaut e, elle est donc modérément ramifiée et incluse dans K^{mr}. En réalité ces extensions suffisent à atteindre toute l'extension maximale modérément ramifiée. Ceci permet de décrire le groupe de Galois de K^{mr} sur K^{nr}. Il s'agit tout simplement de la limite projective des groupes finis $\mathbb{Z}/e\mathbb{Z}$ (l'extension K_e/K^{nr} est cyclique) où e décrit les nombres premiers à p et où les applications de transitions sont les projections habituelles. C'est également le produit des $\mathbb{Z}_\ell$ pour ℓ nombre premier différent de p. Il s'agit donc d'un groupe profini d'ordre premier à p. On l'appelle le *groupe d'inertie modérée* et on le note souvent I_m.

L'extension $K^{\mathrm{mr}}/\bar{K}$ est bien entendu galoisienne. Son groupe de Galois s'appelle le groupe d'*inertie sauvage* et se note souvent I_s. C'est un sous-groupe du groupe d'inertie qui est un pro-p-groupe. Pour comprendre bien ce groupe, il est encore nécessaire de le découper en faisant intervenir de nouvelles extensions intermédiaires. Nous n'allons toutefois pas le faire car il ne nous intéressera pas par la suite.

Récapitulons donc par le diagramme suivant les rappels que nous venons de faire :



3.1.3 Représentations

Une bonne façon de récupérer des informations sur un groupe G est de regarder ses représentations, ou ses représentations continues si le groupe G est naturellement muni d'une topologie. Rappelons qu'une représentation ρ est dite *irréductible* ou encore *simple* si son espace vectoriel sous-jacent V n'admet pas de sous-espaces stricts stables pour l'action du groupe G. Une représentation est dite *semi-simple* si elle peut s'écrire comme somme directe de représentations irréductibles. Cette terminologie est justifiée par le fait que si E est un corps, une représentation dans un E-espace vectoriel peut être vu comme un $E[G]$-module. Une représentation simple (resp. semi-simple) correspond alors à un module simple (resp. semi-simple). Rappelons finalement que si ρ est une représentation dans un E-espace vectoriel V de dimension finie, alors on peut trouver ce que l'on appelle une suite de Jordan-Hölder, c'est-à-dire une suite

$$0 = V_0 \subset V_1 \subset \ldots \subset V_n = V$$

de sous-représentations de V telle que les quotients successifs V_{i+1}/V_i soient des représentations simples. De surcroît, on montre que ces quotients successifs sont uniquement déterminés et ce que l'on appelle la *semi-simplifiée* de ρ est la représention somme directe de ces quotients.

Un des grands buts de la théorie des nombres est d'exhiber et de classifier les réprésentations (continues) du groupe de Galois absolu d'un corps, par exemple d'un corps local. Nous allons présenter par la suite un aspect de cela. Nous avons vu précédemment que l'on disposait d'une description particulièrement explicite du groupe d'inertie modérée I_m. Commençons donc par étudier les représentations continues de ce groupe. Il est bon de commencer par décrire les *caractères* (représentations de dimension 1) continues de I_m dans le groupe $\mu(\bar{k})$ formé des racines de l'unité de $\bar{k}$, celui-ci héritant de la topologie discrète. Un caractère est en réalité simplement un morphisme de groupes de I_m dans le groupe multiplicatif $\mu(\bar{k})$ qui est continu, c'est-à-dire dont le noyau est un sous-groupe ouvert de I_m. Notons par exemple X l'ensemble de ces caractères qui est naturellement muni d'une structure de groupe.

On a déjà en fait rencontré de tels morphismes. En effet, on a vu que si e était un entier premier à p, le corps K_e obtenu en rajoutant à K^{nr} une racine e-ième de l'uniformisante π était une extension de K^{nr} contenue dans K^{mr}. En particulier le groupe de Galois $\mathrm{Gal}(K_e/K^{\mathrm{nr}})$ est naturellement un quotient de I_m et donc on dispose de la projection canonique $I_m \to \mathrm{Gal}(K_e/K^{\mathrm{nr}})$. Mais K^{nr} contient les racines e-ième de l'unité et donc la théorie de Kummer nous dit que ce groupe de Galois s'identifie aux racines e-ième de l'unité de $\bar{K}$ ou encore via la réduction modulo $\mathfrak{m}_{\bar{K}}$ aux racines e-ième de l'unité de $\bar{k}$. On a ainsi construit un morphisme de groupes $\theta_e : I_m \to \mu(\bar{k})$, c'est-à-dire un caractère de I_m. On vérifie immédiatement que θ_e est continu, le noyau de θ_e étant le sous-groupe de I_m correspond à l'extension intermédiaire K_e qui est bien ouvert car K_e/K est finie. Il est amusant de remarquer que le θ_e ainsi construit ne dépend en fait d'aucun choix et plus particulièrement ne dépend pas de l'uniformisante π considérée.

Ainsi l'on vient d'exhiber des éléments du groupe X. En fait, ces éléments suffisent à engendrer X. En outre, ils sont soumis aux seules relations $\theta_1 = 1$, $\theta_{ne}^n = \theta_e$, pour n et e entiers naturels premiers à p. Une

autre façon de dire cette affirmation est de considérer le groupe additif $(\mathbb{Q}/\mathbb{Z})'$ constitué des éléments de $\mathbb{Q}/\mathbb{Z}$ dont les dénominateurs sont premiers à p. On a alors un morphisme naturel de $(\mathbb{Q}/\mathbb{Z})'$ qui est celui qui envoie le rationnel $\alpha = \frac{a}{b}$ sur le caractère $\psi_\alpha = \theta_b^a$. L'affirmation précédente s'énonce alors ainsi :

Proposition 3.1.3.1. *L'application $\alpha \mapsto \psi_\alpha$ est un isomorphisme de groupes abéliens.*

La démonstration est simple et laissée au lecteur. Le rationnel α associé à un caractère $\psi \in X$ s'appelle l'*invariant* de ψ. Un caractère qui a pour invariant un rationnel de la forme $\frac{p^i}{p^n-1}$ est appelé *caractère fondamental de niveau n.*

Soit désormais $q = p^r$ est une puissance de p. Bien entendu, un caractère de I_m à valeurs dans $\mu_{q-1}\left(\bar{k}\right)$, le groupe des racines $(q-1)$-ième de l'unité de $\bar{k}$ est aussi un caractère de I_m à valeurs dans $\mu\left(\bar{k}\right)$ et donc le groupe des caractères continus de I_m dans $\mu_{q-1}\left(\bar{k}\right)$ est un sous-groupe de X. Il n'est pas dur de voir qu'il s'agit précisément des $\psi \in X$ d'ordre $q-1$, il s'agit donc du sous-groupe cyclique de X engendré par le générateur θ_{q-1}. Autrement dit, un caractère continu de I_m à valeurs dans $\mathbb{F}_q$ est juste un entier compris entre 0 et $p^n - 2$. Cet entier en fait est souvent écrit en base p. Ainsi la donnée de $\psi : I_m \to \mu_{q-1}\left(\bar{k}\right)$ équivaut également à la donnée d'un r-uplet $(n_1, \ldots, n_r)$ d'entiers compris entre 0 et $p-1$, la correspondance étant :

$$\psi = \psi_1^{n_1} \ldots \psi_r^{n_r}$$

où $\psi_i = \theta_{q-1}^{p^i}$, les ψ_i sont donc les caractères fondamentaux de niveau n. Ceci n'est en fait pas une bijection, le caractère constant égal à 1 peut se représenter par les deux r-uplet $(0, \ldots, 0)$ et $(p-1, \ldots, p-1)$. Toutefois, si l'on excepte ce cas particulier, à tout caractère il correspond un et un unique r-uplet.

L'intérêt de la décomposition en base p est de rendre les choses canoniques. Expliquons-cela. Considérons E un corps fini à q éléments. Bien sûr E va être isomorphe en tant que corps à $\mu_{q-1}\left(\bar{k}\right)$ auquel on a ajouté 0 mais de façon non canonique. Fixons pour l'instant un isomorphisme, disons φ. Un caractère de I_m à valeurs dans $E^\star$ va via φ devenir un caractère de I_m à valeurs dans $\mu_{q-1}\left(\bar{k}\right)$ et donc va être décrit par un r-uplet d'entiers compris entre 0 et $p-1$ comme cela vient d'être expliqué. Mais bien sûr, cela dépend du choix de φ. Que se passe-t-il si on change φ en un autre isomorphisme φ'. φ' va être un composé de φ par un automorphisme d'un corps fini à q éléments, et donc $\varphi' = \varphi^{p^i}$ pour un certain i. Il n'est pas bien difficile de voir que cela se traduit simplement sur le r-uplet associé par un décalage de i. En particulier, l'ensemble des exposants qui apparaissent ne dépend pas de la façon d'identifier E à $\mu_{q-1}\left(\bar{k}\right)$. Une autre façon de voir les choses est la suivante. Il est tout à fait possible, une fois un isomorphisme φ fixé, de transporter les caractères fondamentaux de niveau r en des caractères à valeurs dans $E^\star$. Ce qui se passe, c'est que si l'on change φ en un autre isomorphisme φ', les caractères que l'on va obtenir ainsi vont juste être permutés, et qui plus est par une permutation circulaire. Autrement dit, il est tout à fait possible de définir les *caractères fondamentaux* des I_m à valeurs dans $E^\star$. On peut les noter ψ_i où i parcourt l'ensemble $\mathbb{Z}/r\mathbb{Z}$. et imposer pour tout i la relation $\psi_{i+1} = \psi_i^p$. Bien sûr ψ_1 n'est pas uniquement déterminée, mais une fois que l'on a choisi celui-ci tous les autres le sont. Tout caractère $\psi : I_m \to E^\star$ s'écrit alors sous la forme

$$\psi = \psi_1^{n_1} \ldots \psi_r^{n_r}$$

où les n_i sont des entiers compris entre 0 et $p-1$. En outre, cette écriture est unique sauf pour le caractère constant égal à 1 qui s'écrit à la fois $\psi_1^0 \ldots \psi_r^0$ et $\psi_1^{p-1} \ldots \psi_r^{p-1}$. Comme nous l'avons déjà dit, modifier le choix de ψ_1 revient simplement à permuter circulairement les n_i. En particulier, l'exposant ne dépend que du caractère fondamental sur lequel il porte. Autrement dit, on peut réénoncer encore une fois cette proposition.

Proposition 3.1.3.2. *Avec les notations précédentes, considérons $\psi : I_m \to E^\star$ un caractère. Alors ψ peut s'écrire sous la forme*

$$\psi = \prod_\sigma \sigma^{v_\sigma(\psi)}$$

où les $v_\sigma(\psi)$ sont des entiers compris entre 0 et $p-1$ et le produit est étendu à tous les caractères fondamentaux σ. En outre, cette écriture est unique sauf pour le caractère constant égal à 1 pour lequel on peut choisir soit tous les exposants égaux à 0, soit tous les exposants égaux à $p-1$. Dans ce cas, on choisira de poser $v_\sigma(1) = p-1$ pour tout caractère fondamental σ.

Ceci précède permet de décrire de façon explicite toutes les représentations continues et semi-simple de I_m dans un $\bar{\mathbb{F}}_p$-espace vectoriel V. Plus précisément, comme $\bar{\mathbb{F}}_p$ est algébriquement clos et que I_m est commutatif, il est facile de voir que pour tout telle représentation ρ admet une droite stable. Cela signifie exactement que les seules représentations simples sont celles de dimension 1, c'est-à-dire les caractères. En particulier, une représentation semi-simple de I_m dans un tel espace vectoriel sera diagonalisable et donnée par un certain nombre de caractères, précisément la dimension de V sur $\bar{\mathbb{F}}_p$. Nous ne pousserons pas plus loin l'étude, étant donné que par la suite nous semi-simplifierons systématiquement toutes nos représentations.

3.1.4 Représentations provenant de la géométrie

Il est une façon géométrique de décrire les représentations continues du groupe de Galois absolu $\mathrm{Gal}\left(\bar{K}/K\right)$ dans un $\mathbb{F}_q$-espace vectoriel de dimension finie. Pour cela, considérons S un $(\mathrm{Spec}\, K)$-schéma[1] fini et étale. S est affine et en fait simplement le spectre de $K_1 \times \ldots \times K_n$ où les K_i sont des extensions finies de K. Regardons les $\bar{K}$-points de S, $S\left(\bar{K}\right)$. Il s'agit tout simplement de l'ensemble $\mathrm{Hom}_{K-\mathrm{alg}}\left(K_1 \times \ldots \times K_n, \bar{K}\right)$ qui s'identifie naturellement à l'union disjointe $\coprod_{i=1}^n \mathrm{Hom}_{K-\mathrm{alg}}\left(K_i, \bar{K}\right)$. Si l'on désigne par d_i le degré de l'extension K_i/K, l'ensemble $\mathrm{Hom}_{K-\mathrm{alg}}\left(K_i, \bar{K}\right)$ est fini de cardinal d_i et donc $S\left(\bar{K}\right)$ est fini de cardinal $d = \sum_{i=1}^n d_i$. Cet ensemble est muni d'une action de $\mathrm{Gal}\left(\bar{K}/K\right)$, un K-automorphisme de $\bar{K}$ agissant simplement par composition. En outre, cette action est continue. Bien entendu, si S et S' sont deux K-schémas finis et étales, et $f : S \to S'$ est un morphisme de schémas, f va induire une application de $S\left(\bar{K}\right)$ dans $S'\left(\bar{K}\right)$ qui commute à l'action de Galois. On a ainsi défini un foncteur de la catégorie des K-schémas finis et étales dans la catégories des ensembles finis munis d'une action de $\mathrm{Gal}\left(\bar{K}/K\right)$, les flèches de cette dernière catégorie étant les applications d'ensembles commutant à l'action de Galois.

Proposition 3.1.4.1. *Ce foncteur est une équivalence de catégorie.*

Nous n'allons pas prouver complètement la proposition mais juste exhiber un quasi-inverse. Prenons donc Γ un ensemble fini muni d'une action de $\mathrm{Gal}\left(\bar{K}/K\right)$. On lui associe la sous-algèbre B de la K-algèbre des fonctions de Γ dans $\bar{K}$ constituée des fonctions f vérifiant $f(gx) = gf(x)$ pour tout $x \in \Gamma$ et tout $g \in \mathrm{Gal}\left(\bar{K}/K\right)$. Le K-schéma fini et étale associé à Γ est alors le spectre de B.

Cette proposition est en fait un cas extrêtement particulier d'une théorie générale. Cette dernière se propose, étant donné S un schéma connexe, de classifier les S-schémas étales. En fait, ils sont en correspondance avec des ensembles munis d'une action d'un certain groupe mais le groupe n'est plus ici bien entendu un groupe de Galois. C'est ce que l'on appelle le π_1 du schéma S. Nous n'en dirons pas plus sur le sujet.

On vient de trouver une origine géométrique aux ensembles finis munis d'une action de $\mathrm{Gal}\left(\bar{K}/K\right)$. Mais ce que l'on aimerait, c'est trouver une telle origine aux représentations mais une représentation c'est un espace vectoriel avec une action compatible de $\mathrm{Gal}\left(\bar{K}/K\right)$, pas seulement un ensemble. On voit donc bien ce qui va se passer. Ces structures supplémentaires vont se traduire par des structures supplémentaires sur le K-schéma fini et étale. D'autre part, le résultat précédent suggère qu'il sera plus simple de se restreindre aux représentation sur un espace vectoriel fini. En fait, on va se retreindre aux $\mathbb{F}_q$-espaces vectoriels de dimension finie, où $q = p^r$ est une puissance de p. Mais voyons tout de suite

[1] Par la suite, on notera souvent K à la place de $\mathrm{Spec}\, K$, et même R à la place de $\mathrm{Spec}\, R$ si R est un anneau.

quelles structures il faut ajouter au K-schéma S fini et étale. Ce que l'on souhaite en fait, c'est que l'ensemble $S\left(\bar{K}\right)$ ne soit pas seulement un ensemble, mais un $\mathbb{F}_q$-espace vectoriel. Mais il existe une description fonctorielle des schémas pour laquelle cette affirmation se traduit simplement. En effet, se donner un K-schéma S fini revient à se donner un foncteur contravariant de la catégorie des K-algèbres dans celle des ensembles, ce foncteur étant représentable par une K-algèbre finie. Ce foncteur est celui qui à une K-algèbre A associe l'ensemble des A-points de S. On aimerait donc considérer les foncteurs contravariants de la catégorie des K-algèbres dans celle des $\mathbb{F}_q$-espaces vectoriels qui une fois composé avec le foncteur d'oubli deviennent représentables par une K-algèbre finie. Se donner un tel objet est en fait équivalent à se donner un K-schéma S fini muni d'une structure de $\mathbb{F}_q$-espace vectoriel dans le sens suivant :

1. S est munie d'une loi de groupe commutatif. Cela se traduit par l'existence d'un morphisme de K-schémas $m : S \times_K S \to S$ vérifiant les axiomes suivants.
   – m est associative dans le sens où le diagramme suivant est commutatif

$$\begin{array}{ccc} S \times_K S \times_K S & \xrightarrow{\mathrm{id}\times m} & S \times_K S \\ \downarrow{\scriptstyle m\times\mathrm{id}} & & \downarrow{\scriptstyle m} \\ S \times_K S & \xrightarrow[m]{} & S \end{array}$$

   – il existe une section $e : K \to S$ telle que les diagrammes suivants commutent.

$$\begin{array}{ccc} S & \xrightarrow{\sim} & S \times_K K \\ \| & & \downarrow{\scriptstyle \mathrm{id}\times e} \\ S & \xleftarrow[m]{} & S \times_K S \end{array} \qquad \text{et} \qquad \begin{array}{ccc} S & \xrightarrow{\sim} & K \times_K S \\ \| & & \downarrow{\scriptstyle e\times\mathrm{id}} \\ S & \xleftarrow[m]{} & S \times_K S \end{array}$$

   Un tel morphisme e correspond bien entendu à l'existence d'un élément neutre pour la loi de groupe m. On peut montrer qu'un tel morphisme est unique.
   – il existe un morphisme de K-schémas $i : S \to S$ faisant commuter le diagramme suivant.

$$\begin{array}{ccccc} S & \xrightarrow{\mathrm{id}\times i} & S \times_K S & \xrightarrow{m} & S \\ \downarrow & & & \nearrow_{e} & \\ K & & & & \end{array}$$

   Un tel morphisme correspond à l'existence d'un inverse à tout élément du groupe. Ici également, on peut montrer qu'un tel morphisme est unique.
2. La loi m précédente est commutative dans le sens où le diagramme suivant commute.

$$\begin{array}{ccc} S \times_K S & \xrightarrow{m} & S \\ \downarrow{\scriptstyle \mathrm{pr}_2\times\mathrm{pr}_1} & & \| \\ S \times_K S & \xrightarrow{m} & S \end{array}$$

   (pr_i désigne la i-ème projection canonique)
3. Pour tout $\lambda \in \mathbb{F}_q$, il existe un morphisme de K-schémas $[\lambda] : S \to S$. On suppose que pour tous λ et μ dans $\mathbb{F}_q$,

$$\begin{aligned} [1] &= \mathrm{id}_S \\ [\lambda] \circ [\mu] &= [\lambda\mu] \\ m \circ (\lambda \times \mu) &= [\lambda + \mu] \end{aligned}$$

Définition 3.1.4.2. *Un K-schéma muni des structures précédentes est appelé en* K-schéma en $\mathbb{F}_q$-vectoriels. *Un K-schéma vérifiant simplement l'axiome* 1 *est appelé un* K-schéma en groupe. *Un K-schéma vérifiant les axiomes* 1 *et* 2 *est appelé un* K-schéma en groupe commutatif.

Remarque 3.1.4.3. *Bien entendu, on peut étendre les définitions précédentes à une base quelconque, simplement en remplaçant partout K par la base en question.*

Comme nous pouvons nous y attendre, il y a une correspondance entre les K-schémas en $\mathbb{F}_q$-vectoriels finis et étales et les représentations de $\mathrm{Gal}\left(\bar{K}/K\right)$ dans un $\mathbb{F}_q$-espace vectoriel de dimension finie. Cette correspondance est exactement que celle que l'on a décrite tout à l'heure. Rappelons-là tout de même. Soit S un K-schéma en $\mathbb{F}_q$-vectoriel, on peut lui associer le $\mathbb{F}_q$-espace vectoriel de dimension finie des $\bar{K}$-points de S, cet espace étant munie d'une action de $\mathrm{Gal}\left(\bar{K}/K\right)$ qui est compatible à la structure d'espace vectoriel. Bien entendu, un morphisme en K-schémas en $\mathbb{F}_q$-vectoriel induit une application $\mathbb{F}_q$-linéaire entre les espaces vectoriels associés, cette application respectant l'action de Galois. On a ainsi défini un foncteur allant de la catégorie des K-schémas en $\mathbb{F}_q$-vectoriel finis et étales dans celle des représentations de $\mathrm{Gal}\left(\bar{K}/K\right)$ dans un $\mathbb{F}_q$-vectoriel de dimension finie. On a une proposition analogue à la proposition précédente.

Proposition 3.1.4.4. *Ce foncteur est une équivalence de catégories.*

La démonstration est analogue à la démonstration de la proposition 3.1.4.1.

On a un petit rabiot dans ce cas. Les deux catégories sont des catégories abéliennes et il se trouve que le foncteur défini est additif. En particulier, il conserve les noyaux, les conoyaux, les quotients, et tout ce genre de choses.

L'intêret de ce parallèle est de pouvoir classifier les représentations de $\mathrm{Gal}\left(\bar{K}/K\right)$ dans un $\mathbb{F}_q$-espace vectoriel de dimension finie. En effet, il est des propriétés naturelles sur les K-schémas en $\mathbb{F}_q$-vectoriels qui se transportent ainsi sur les représentations et qui permettent de faire un peu de tri. Les notions de simplicité et de semi-simplicité sont purement catégoriques. Être simple signifie ne pas avoir de sous-objet non trivial et être semi-simple, c'est être somme directe d'objets simples. Ainsi ces deux notions existaient déjà aussi bien pour les K-schémas en $\mathbb{F}_q$-vectoriels finis et étales que pour les représentations de $\mathrm{Gal}\left(\bar{K}/K\right)$ dans un $\mathbb{F}_q$-espace vectoriel de dimension finie et bien entendu elles se correspondent. Les suites de composition de Jördan-Hölder existent également dans chacune de ces catégories et se correspondent via notre foncteur.

3.1.5 Énoncé du théorème principal

Prenons maintenant $\rho : \mathrm{Gal}\left(\bar{K}/K\right) \to \mathrm{GL}\left(V\right)$, où V est un $\mathbb{F}_p$-espace vectoriel[2], une représentation du groupe de Galois absolu de K. Notons G le K-schéma en $\mathbb{F}_p$-vectoriel associé à cette représentation ρ. On fait l'hypothèse selon laquelle il existe $\mathcal{G}$ un $\mathcal{O}_K$-schéma en $\mathbb{F}_p$-vectoriel fini et plat tel que $\mathcal{G} \times_{\mathcal{O}_K} K = \mathcal{G}_K = G$. Bien entendu cette dernière égalité a lieu en tant schéma en $\mathbb{F}_p$-vectoriel les lois définissant cette structure se transportant sans problème par extension des scalaires. Nous allons nous intéresser en fait à la restriction de la représentation ρ au groupe d'inertie I. Cette représentation n'est pas forcément semi-simple. Qu'à cela ne tienne, considérons $\rho' : I \to \mathrm{GL}\left(V'\right)$ un quotient de Jördan-Hölder de cette représentation. Par définition ρ' est simple.

Proposition 3.1.5.1. *Avec les notations précédentes, la restriction de ρ' au groupe d'inertie sauvage I_s est triviale.*

[2]Attention, c'est $\mathbb{F}_p$, plus $\mathbb{F}_q$.

En effet, regardons le sous-groupe $\rho'(I_s)$. Il s'agit d'un p-groupe agissant sur l'espace vectoriel V'. Si $x \in V'$, l'orbite de x est naturellement en bijection avec un quotient de $\rho'(I_s)$ et donc son cardinal est une puissance de p. En particulier, si x n'est pas fixe par $\rho'(I_s)$, le cardinal de cette orbite va être un multiple de p. Comme le cardinal de V est lui aussi un multiple de p, il en résulte que l'ensemble

$$V'_0 = \{x \in V',\ \forall g \in I_s, \rho'(g)(x) = x\}$$

a pour cardinal un multiple de p. En particulier $V'_0 \neq 0$. Mais V'_0 est une sous-représentation de V' et ρ' est simple. On déduit de tout cela que $V'_0 = V'$, ce qui démontre la proposition.

Ainsi ρ' se factorise en une représentation $\rho' : I_m \to \mathrm{GL}(V')$ qui est encore simple. L'anneau E des endomorphismes de ρ' (c'est-à-dire des endomorphismes de V' commutant à l'action de ρ') forme alors un corps a priori non commutatif. En effet, le noyau et l'image d'un tel endomorphisme f correspondent à des sous-représentations de ρ' et donc sont soit 0 soit V tout entier. Finalement, si f n'est pas nul, f est forcément bijectif, ce qui prouve notre assertion. Ce corps se plonge dans $\mathrm{M}_n(V')$, il est donc fini et de caractéristique p. Il est donc isomorphe (non canoniquement) à un $\mathbb{F}_q$ pour $q = p^r$ une certaine puissance bien choisie de p. Maintenant V' a une structure d'espace vectoriel sur E. Mais le fait que ρ soit simple entraîne directement de V' est de dimension 1 sur E. Cela veut dire qu'en fait l'on peut mettre sur V' une structure de corps, et cela prouve au passage qu'en fait $r = \dim V'$. La réprésentation ρ' devient alors tout simplement un caractère de I_m à valeurs dans $V'^\star$. D'après ce que l'on a expliqué précédemment, $\rho' = \prod_\psi \psi^{v_\psi(\rho')}$, le produit étant étendu à tous les caractères fondamentaux $\psi : I_m \to V'^\star$.

Théorème 3.1.5.2. *Avec les notations précédentes, les entiers $v_\psi(\rho')$ vérifient tous l'inégalité :*

$$v_\psi(\rho') \leqslant v(p)$$

où v désigne toujours la valuation sur K que l'on s'était fixée au tout début.

La quantité $v(p)$ qui intervient dans le théorème précédent est souvent notée e_K et s'appelle l'*indice de ramification absolu* du corps K. Cette terminologie se justifie de la façon suivante. Comme K est de caractéristique 0, on peut naturellement plonger $\mathbb{Q}$ dans K. Par complétude, ce plongement se prolonge en un plongement continu que $\mathbb{Q}_p$ dans K. Si d'autre part le corps résiduel k est fini et de cardinal $q = p^f$, on voit immédiatement que l'extension $K/\mathbb{Q}_p$ est également finie et que son indice de ramification est précisément l'entier e_K.

Ce résultat a été conjecturé la première fois par Serre dans l'article [Ser72]. Des calculs sur les courbes elliptiques et les groupes formels sont à l'origine de cette conjecture.

Le but de tout ce qui suit est de donner deux démonstrations de ce théorème. Elles reposent à peu près sur le même principe. Le premier objectif est de donner une classification des schémas finis et plats en $\mathbb{F}_q$-vectoriel ou en groupe commutatif sur les bases $\mathcal{O}_K$ et K. Il faut ensuite expliciter l'extension des scalaires et l'équivalence de catégories décrite précédemment via notre classification. Le théorème se déduit de tout cela par quelques calculs pas très difficiles à mener.

3.2 Classification des schémas en $\mathbb{F}_q$-vectoriel

La première démonstration que nous allons proposer date de 1974 et est due à Raynaud. Elle est décrite entièrement dans l'article [Ray74] que nous allons suivre d'assez près.

Commençons par une remarque générale. Pour énoncer notre théorème, on a pris une représentation du groupe de Galois absolu du corps K puis on l'a restreint au groupe d'inertie I. Il revenait au même donc de partir d'une représentation de $\mathrm{Gal}\left(\bar{K}/K^{\mathrm{nr}}\right)$. La propriété que l'on imposait, à savoir provenir d'un schéma en $\mathbb{F}_p$-vectoriel fini et plat sur l'anneau des entiers $\mathcal{O}_K$, se traduit directement. Ainsi il ne coûte rien de remplacer K par $\widehat{K^{\mathrm{nr}}}$. Il a l'avantage de contenir par exemple les racines d-ième de l'unité avec d premier à p. Dans toute la suite, on fera cette hypothèse.

3.2.1 Caractères de $\mathbb{F}_q$

Considérons maintenant un entier r et posons $q = p^r$. On suppose comme on vient de l'expliquer que K contient les racines $(q-1)$-ième de l'unité. Ceci implique en particulier que le corps résiduel k contient lui aussi les racines $(q-1)$-ième de l'unité. On notera $\mu_{q-1}(\mathcal{O}_K)$ (resp. $\mu_{q-1}(k)$) le groupe des racines $(q-1)$-ième de l'unité de $\mathcal{O}_K$ (resp. de k). La projection canonique $\mathcal{O}_K \to k$ induit un isomorphisme entre $\mu_{q-1}(\mathcal{O}_K)$ et $\mu_{q-1}(k)$. $\mu_{q-1}(k)$ est en fait le groupe multiplicatif de l'unique sous-corps de k à q éléments.

Avec ces hypothèses, il nous est possible d'étudier les caractères de $\mathbb{F}_q^\star$ à valeurs dans $K^\star$. Ceux-ci forment un groupe que l'on va noter M. Soit $\chi \in M$. Tout élément $x \in \mathbb{F}_q$ vérifie l'équation $x^q = x$ et donc comme χ est un morphisme de groupes, on a la relation $\chi(x)^q = \chi(x)$. Ceci prouve d'une part qu'il était judicieux de rajouter les racines $(q-1)$-ième de l'unité à K et que d'autre part χ est à valeurs dans le groupe de ces racines, qui est par exemple inclus dans l'anneau des entiers $\mathcal{O}_K$. En fait, il est d'usage de prolonger tout χ en une application de $\mathbb{F}_q$ dans $\mathcal{O}_K$ simplement en posant $\chi(0) = 0$.

Le groupe $\mathbb{F}_q^\star$ est cyclique. Ainsi, après le choix d'un générateur τ de $\mathbb{F}_q^\star$ se donner un caractère $\chi \in M$ revient simplement à se donner une racine $(q-1)$-ième de l'unité qui n'est autre que $\chi(\tau)$. Autrement dit M est isomorphe au groupe des racines $(q-1)$-ième de l'unité de K, mais cet isomorphisme n'est pas canonique, il dépend du choix d'un générateur τ. Une façon de rendre les choses canoniques est d'introduire la définition suivante.

Définition 3.2.1.1. *Un caractère $\chi : \mathbb{F}_q \to \mathcal{O}_K$ est dit* fondamental *si le morphisme composé $\mathbb{F}_q \to \mathcal{O}_K \to k$ est un morphisme d'anneaux.*

Étudions un peu plus en détail ces caractères fondamentaux. Fixons un isomorphisme φ entre $\mathbb{F}_q$ et le sous-corps de k à q éléments. La projection canonique $\mu_{q-1}(\mathcal{O}_K) \to \mu_{q-1}(k)$ est un isomorphisme. Son inverse fournit par composition avec φ un caractère fondamental tel que défini précédemment. Notons $\chi : \mathbb{F}_q \to \mathcal{O}_K$ ce caractère. Comme la composé de χ avec la projection canonique est un morphisme de corps, χ est forcément injectif et donc est un générateur du groupe cyclique M. Toutefois, on n'a toujours pas trouver ici un générateur canonique car il y a encore le choix de l'isomorphisme φ.

Mais, les autres caractères fondamentaux s'obtiennent simplement en composant χ par un automorphisme de corps de $\mathbb{F}_q$. Il s'agit donc des $\chi^{p^i} = \chi_i$. Bien sûr, comme $q = p^r$, on a $\chi_{i+r} = \chi_i$ pour tout i et donc les indices peuvent en fait être vus comme des éléments de $\mathbb{Z}/r\mathbb{Z}$. On a la relation immédiate $\chi_{i+1} = \chi_i^p$. Si maintenant $\chi : \mathbb{F}_q^\star \to \mathcal{O}_K$ est un caractère pas forcément fondamental, on pourra toujours écrire $\chi = \chi_1^n$ où n est un certain entier compris entre 0 et $q-1$. Écrivons n en base p, on obtient $n = n_1 + n_2 p + \ldots + n_r p^{r-1}$ et ensuite $\chi = \chi_1^{n_1} \ldots \chi_r^{n_r}$. L'important est que l'exposant n_i ne dépend que de χ_i. On vient donc de prouver la proposition :

Proposition 3.2.1.2. *Soit $\chi : \mathbb{F}_q \to \mathcal{O}_K$ un caractère. Alors χ peut s'écrire sous la forme*

$$\chi = \prod_\sigma \sigma^{v_\sigma(\chi)}$$

où les $v_\sigma(\chi)$ sont des entiers compris entre 0 et $p-1$ et le produit est étendu à tous les caractères fondamentaux σ. En outre, cette écriture est unique sauf pour le caractère constant égal à 1 pour lequel on peut choisir soit tous les exposants égaux à 0, soit tous les exposants égaux à $p-1$. Dans ce cas, on choisira de poser $v_\sigma(1) = p-1$ pour tout caractère fondamental σ.

Par la suite, nous choisirons quand même une indexation des caractères fondamentaux. Nous les noterons χ_i pour i décrivant $\mathbb{Z}/r\mathbb{Z}$. On rappelle que les χ_i sont soumis à la relation $\chi_{i+1} = \chi_i^p$.

3.2.2 Découpage de la bigèbre

Nous voulons classifier les schémas finis et plats en $\mathbb{F}_q$-vectoriel sur $\mathcal{O}_K$ et K. Nous allons en fait plus généralement étudier les schémas finis et plats en $\mathbb{F}_q$-vectoriel sur A où A est une $\mathcal{O}_K$-algèbre. Nous allons toutefois nous limiter à un certain type bien particulier de tels schémas qui vont nous suffir pour le théorème que l'on a en vue. Prenons donc A une $\mathcal{O}_K$-algèbre et G un K-schéma fini et plat en $\mathbb{F}_q$-vectoriel sur A. Comme G est fini (et donc affine) sur A et que A est affine, G est le spectre d'une certaine A-algèbre $\mathcal{A}$. Les structures supplémentaires que l'on a mises sur G vont se transporter naturellement sur $\mathcal{A}$. La multiplication $m : G \times_A G \to G$ va fournir sur $\mathcal{A}$ ce que l'on appelle une *comultiplication* qui est un morphisme de A-algèbres de $c : \mathcal{A} \to \mathcal{A} \otimes_A \mathcal{A}$. De même, pour tout $\lambda \in \mathbb{F}_q$, l'application $[\lambda] : G \to G$ va fournir une application $\mathcal{A} \to \mathcal{A}$ que l'on notera encore $[\lambda]$. Les axiomes que doivent vérifier ces morphismes se déduisent directement des axiomes déjà énoncés pour les schémas en $\mathbb{F}_q$-vectoriel. Nous laissons le lecteur soucieux réécrire les diagrammes adéquats. En particulier, il va exister un morphisme de A-algèbre $e : \mathcal{A} \to A$ qui va correspondre à la section (forcément unique) $e : \operatorname{Spec} A \to G$. Ce morphisme s'appelle l'*augmentation* de $\mathcal{A}$. Son noyau est l'*idéal d'augmentation* de $\mathcal{A}$. Nous le noterons $\mathcal{I}$ par la suite. De même $\mathcal{A}$ va hériter d'un morphisme $\varphi : \mathcal{A} \to \mathcal{A}$, appelé l'*antipodie*, correspondant au morphisme défini sur G donnant l'inverse d'un élément. $\mathcal{A}$ muni de ces nouvelles structures est ce que l'on appelle la *bigèbre* associé au schéma en $\mathbb{F}_q$-vectoriel G.

Il nous faut maintenant mettre à profit les caractères que nous avons introduit dans le paragraphe précédent. Pour tout $\chi \in M$, on introduit l'endomorphisme A-linéaire de $\mathcal{A}$, i_χ, défini de la façon suivante :

$$i_\chi = \frac{1}{q-1} \sum_{\lambda \in \mathbb{F}_q^\star} \chi^{-1}(\lambda)\,[\lambda]$$

cette écriture a bien un sens étant donné que $q-1$ est inversible dans $\mathcal{O}_K$ et donc dans A.

Calculons maintenant, pour χ' et χ'' deux caractères :

$$\begin{aligned} i_{\chi'} \circ i_{\chi''} &= \frac{1}{(q-1)^2} \sum_{\lambda,\mu \in \mathbb{F}_q^\star} \chi'^{-1}(\lambda)\,\chi''^{-1}(\mu)\,[\lambda\mu] \\ &= \frac{1}{(q-1)^2} \sum_{\lambda,\mu \in \mathbb{F}_q^\star} \chi'\chi''^{-1}(\mu)\,\chi'^{-1}(\lambda\mu)\,[\lambda\mu] \\ &= \left(\frac{1}{q-1} \sum_{\mu \in \mathbb{F}_q^\star} \chi'\chi''^{-1}(\mu) \right) i_{\chi'} \end{aligned}$$

La facteur entre parenthèses écrit ci-dessus vaut 1 si $\chi' = \chi''$ et 0 sinon. On en déduit que les i_χ forment une famille de projecteurs orthogonaux de $\mathcal{A}$. D'autre part, il est facile de voir que la somme des i_χ pour χ décrivant M est l'identité de A.

D'autre part en utilisant le fait que pour tout $\lambda \in \mathbb{F}_q$, $e \circ [\lambda] = e$, on prouve facilement que les i_χ stabilise l'idéal d'augmentation $\mathcal{I}$. On obtient ainsi une décomposition de cet idéal en somme directe :

$$\mathcal{I} = \bigoplus_{\chi \in M} \mathcal{I}_\chi$$

où $\mathcal{I}_\chi$ est l'image de $\mathcal{I}$ par l'application i_χ.

3.2.3 Description de la multiplication et de la comultiplication

À partir de maintenant, nous allons faire l'hypothèse suivante. Nous allons supposer que pour tout $\chi \in M$, le A-module $\mathcal{I}_\chi$ est libre de rang 1. On remarque que cela entraîne en particulier que G est fini

et plat sur A. On voit ici que la classification que nous allons proposer est en fait assez restrictive, mais comme nous l'avons déjà dit, cela va nous suffir pour l'instant.

L'égalité $\mathcal{A} = A \oplus \mathcal{I}$ nous donne une décomposition de $\mathcal{A}$ et de $\mathcal{A} \otimes_A \mathcal{A}$ en somme directe de A-modules libres de rang 1. On peut alors décomposer les applications A-linéaires $c : \mathcal{A} \to \mathcal{A} \otimes_A \mathcal{A}$ et $d : \mathcal{A} \otimes_A \mathcal{A} \to A$ définie par $d(x \otimes y) = xy$ sur ces sommes directes.

Remarquons que si χ est le caractère trivial, on a $i_1 = \frac{1}{q-1} \sum_{\lambda \in \mathbb{F}_q^\star} [\lambda]$. Mais $[\lambda]$ est un morphisme de A-algèbres, donc $[\lambda] x = x$ pour tout $x \in A$. On déduit de cela que i_1 laisse fixe les points de A. En particulier, les projections i_χ respecte les décompositions données ci-dessus. Cette décomposition permet en fait de diagonaliser simultanément tous les opérateurs $[\lambda]$. Plus précisément, on vérifie immédiatement que si $a \in A$, $[\lambda](a) = a$ et que si $x \in \mathcal{I}_\chi$, $[\lambda](x) = \chi(\lambda) x$, et ce pour tout $\lambda \in \mathbb{F}_q$.

Faisons une seconde remarque. Si χ', χ'' sont deux caractères de M, $x' \in \mathcal{I}_{\chi'}$ et $x'' \in \mathcal{I}_{\chi''}$, alors le produit $x'x''$ appartient à $\mathcal{I}_{\chi'\chi''}$. En effet, les hypothèses impliquent qu'il existe x'_0 et x''_0 dans $\mathcal{I}$ tels que :

$$\begin{aligned} x' &= \frac{1}{q-1} \sum_{\mu \in \mathbb{F}_q^\star} \chi'^{-1}(\mu) [\mu](x'_0) \\ x'' &= \frac{1}{q-1} \sum_{\nu \in \mathbb{F}_q^\star} \chi''^{-1}(\mu) [\mu](x''_0) \end{aligned}$$

Calculons alors pour $\chi \in M$, $i_\chi(x'x'')$. Cela donne :

$$\begin{aligned} i_\chi(x'x'') &= \frac{1}{(q-1)^3} \sum_{\lambda \in \mathbb{F}_q^\star} \chi^{-1}(\lambda) \sum_{\mu,\nu \in \mathbb{F}_q^\star} \chi'^{-1}(\mu) \chi''^{-1}(\nu) [\mu](x'_0) [n] u(x''_0) \\ &= \frac{1}{(q-1)^3} \sum_{\lambda,\mu,\nu \in \mathbb{F}_q^\star} \chi^{-1}(\lambda) \chi'^{-1}(\mu) \chi''^{-1}(\nu) [\lambda\mu](x'_0) [\lambda\nu](x''_0) \\ &= \frac{1}{(q-1)^3} \sum_{\lambda,\mu,\nu \in \mathbb{F}_q^\star} \left(\chi^{-1}\chi'\chi''\right)(\lambda) \chi'^{-1}(\mu) \chi''^{-1}(\nu) [\mu](x'_0) [\nu](x''_0) \\ &= \left(\frac{1}{q-1} \sum_{\lambda \in \mathbb{F}_q^\star} \left(\chi^{-1}\chi'\chi''\right)(\lambda) \right) x'x'' \end{aligned}$$

On voit donc que si $\chi \neq \chi'\chi''$, $i_\chi(x'x'') = 0$, ce qui prouve bien que $x'x'' \in I_{\chi'\chi''}$. En particulier, l'application d est entièrement décrite par les applications

$$d_{\chi',\chi''} : \mathcal{I}_{\chi'} \otimes_A \mathcal{I}_{\chi''} \to \mathcal{I}_{\chi'\chi''}$$

qui sont d'ailleurs précisément $x' \otimes x'' \mapsto x'x''$.

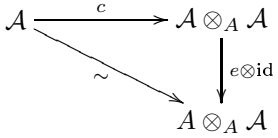
On peut faire un raisonnement analogue pour la comultiplication c. Essayons de voir, pour $x \in \mathcal{I}_\chi$, $\chi \in M$, comment se décompose $c(x)$ sur notre somme directe. On est donc amené à calculer $i_{\chi'} \otimes i_{\chi''}(x)$ pour χ' et χ'' décrivant M et à regarder quand cette quantité s'annule. Mais cela revient à voir que $d \circ (i_{\chi'} \otimes i_{\chi''})(x)$ s'annule. On va donc calculer cette dernière expression :

$$\begin{aligned} d \circ (i_{\chi'} \otimes i_{\chi''})(x) &= \frac{1}{(q-1)^3} \sum_{\lambda,\mu,\nu \in \mathbb{F}_q^\star} \chi^{-1}(\lambda) \chi'^{-1}(\mu) \chi''^{-1}(\nu) d \circ ([\mu] \otimes [\nu]) \circ c \circ [\lambda](x) \\ &= \frac{1}{(q-1)^3} \sum_{\lambda,\mu,\nu \in \mathbb{F}_q^\star} \chi^{-1}(\lambda) \chi'^{-1}(\mu) \chi''^{-1} [\lambda(\mu+\nu)](x) \\ &= \left(\frac{1}{q-1} \sum_{\lambda \in \mathbb{F}_q^\star} \left(\chi^{-1}\chi'\chi''\right)(\lambda) \right) \left(\frac{1}{(q-1)^2} \sum_{\mu,\nu \in \mathbb{F}_q^\star} \chi'^{-1}(\mu) \chi''^{-1}(\nu) [\mu+\nu](x) \right) \end{aligned}$$

Cela prouve donc que $c(x)$ est uniquement porté par les $\mathcal{I}_{\chi'} \otimes_A \mathcal{I}_{\chi''}$ pour $\chi'\chi'' = \chi$. Les applications A-linéaires

$$c_{\chi',\chi''} : \mathcal{I}_{\chi'\chi''} \to \mathcal{I}_{\chi'} \otimes_A I_{\chi''}$$

suffisent donc à décrire sa restriction (à gauche et à droite) $c : \mathcal{I} \to \mathcal{I} \otimes_A \mathcal{I}$. D'autre part, le fait que le diagramme



commute prouve que pour tout $x \in \mathcal{A}$, $c(x) - x \otimes 1 \in \mathcal{I} \otimes_A \mathcal{A}$. De même, $c(x) - 1 \otimes x \in \mathcal{A} \otimes \mathcal{I}$. On en déduit, en regardant la décomposition sur la somme directe, que pour tout $x \in \mathcal{I}$, $c(x) - x \otimes 1 - 1 \otimes x \in \mathcal{I} \otimes_A \mathcal{I}$ et donc en particulier :

$$c(x) = x \otimes 1 + 1 \otimes x + \sum_{\chi',\chi'' \in M} c_{\chi',\chi''}(x)$$

Finalement, si $a \in A$, comme c est un morphisme de A-algèbres, on a $c(a) = a(1 \otimes 1)$ et donc c est entièrement décrit par les morphismes $c_{\chi',\chi''}$.

On peut de même considérer la comultiplication (resp. multiplication) itérée et définir pour tous caractères $\chi_1, \ldots, \chi_n \in M$, des applications A-linéaires :

$$c_{\chi_1,\ldots,\chi_n} : \mathcal{I}_\chi \to \mathcal{I}_{\chi_1} \otimes_A \ldots \otimes_A I_{\chi_n}$$

$$d_{\chi_1,\ldots,\chi_n} : \mathcal{I}_{\chi_1} \otimes_A \ldots \otimes_A \mathcal{I}_{\chi_n} \to \mathcal{I}_\chi$$

où χ désigne le produit des χ_i, i variant de 1 à n.

Pour tous $\chi_1, \ldots, \chi_n$, l'application composée $d_{\chi_1,\ldots,\chi_n} \circ c_{\chi_1,\ldots,\chi_n}$ est un endormophisme du A-module libre de rang 1, $\mathcal{I}_{\chi_1 \ldots \chi_n}$. Il s'agit donc simplement de la multiplication par un élément $\omega_{\chi_1,\ldots,\chi_n} \in A$.

On veut voir également cela sous forme de matrices. Considérons pour tout $\chi \in M$, un générateur e_χ de $\mathcal{I}_\chi$. La famille B formée de 1 et des éléments e_χ précédemment définis forme alors une base de $\mathcal{A}$ sur A. De même la famille de $x_1 \otimes \ldots \otimes x_n$ pour x_i décrivant B forme une base de $\mathcal{A} \otimes_A \ldots \otimes_A \mathcal{A}$ sur A. Les calculs que l'on a fait précédemment explicitent totalement en fonction des $\omega_{\chi_1,\ldots,\chi_n}$ les matrices de la multiplication et de la comultiplication itérées dans ces bases. Nous laissons le lecteur écrire explicitement ces matrices. Cette description des choses n'apporte en fait pas de nouvelles lumières et est même plus pénible à utiliser que la précédente. Elle permet quand même de se rassurer quelque part.

Regardons maintenant comment les axiomes de structure de schémas en $\mathbb{F}_q$-vectoriels se traduisent sur les quantités que l'on vient d'introduire. Le fait que $[1] = \mathrm{id}_\mathcal{A}$ dit simplement que $\chi(1) = 1$ pour tout caractère χ. Le fait que $[\lambda] \circ [\mu] = [\lambda\mu]$ se traduit en $\chi(\lambda)\chi(\mu) = \chi(\lambda\mu)$ pour tout $\lambda, \mu \in \mathbb{F}_q$ et $\chi \in M$. C'est certes rassurant mais ça ne nous donne pas grand chose de nouveau. La dernière condition, à savoir $d \circ ([\lambda] \otimes [\mu]) \circ c = [\lambda + \mu]$, va par contre nous fournir une nouvelle relation. Pour $\chi \in M$, $x \in \mathcal{I}_\chi$ et λ et μ deux éléments de $\mathbb{F}_q$. On a $[\lambda + \mu](x) = \chi(\lambda + \mu)x$. Calculons l'autre terme :

$$\begin{aligned} d \circ ([\lambda] \otimes [\mu]) \circ c(x) &= d \circ ([\lambda] \otimes [\mu]) \left(x \otimes 1 + 1 \otimes x + \sum_{\chi'\chi''=\chi} c_{\chi',\chi''}(x) \right) \\ &= d\left(\chi(\lambda) x \otimes 1 + \chi(\mu) 1 \otimes x\right) + \sum_{\chi'\chi''=\chi} \chi'(\lambda)\chi''(\mu)\omega_{\chi',\chi''} x \\ &= \left(\chi(\lambda) + \chi(\mu) + \sum_{\chi'\chi''=\chi} \chi'(\lambda)\chi''(\mu)\omega_{\chi',\chi''} \right) x \end{aligned}$$

Et donc finalement, pour tout $\chi \in M$, $\lambda, \mu \in \mathbb{F}_q$, la formule est :

$$\chi(\lambda+\mu) = \chi(\lambda) + \chi(\mu) + \sum_{\chi'\chi''=\chi} \chi'(\lambda)\chi''(\mu)\omega_{\chi',\chi''}$$

On peut en fait *inverser* cette dernière égalité pour exprimer les $\omega_{\chi',\chi''}$ en fonction des valeurs des caractères χ' et χ''. On procède ainsi. En multipliant cette égalité par $\chi'^{-1}(\lambda)\chi''^{-1}(\mu)$ et en sommant sur tous les λ et μ dans $\mathbb{F}_q^\star$, on obtient directement :

$$\omega_{\chi',\chi''} = \frac{1}{(q-1)^2}\left(\sum_{\lambda,\mu\in\mathbb{F}_q^\star} \chi'^{-1}(\lambda)\chi''^{-1}(\mu)\chi(\lambda+\mu) - \chi'\left(\lambda^{-1}\mu\right) - \chi''\left(\lambda\mu^{-1}\right)\right)$$

Cette dernière formule se simplifie quelque peu. On trouve :

$$\omega_{\chi',\chi''} = \frac{(\chi'\chi'')(-1)}{q-1} \sum_{u+v=-1} \chi'(u)\chi''(v)$$

si χ' et χ'' sont différents de 1. Sinon :

$$\omega_{1,\chi} = \omega_{\chi,1} = -\frac{q}{q-1}$$

Cela prouve en particulier que les constantes $\omega_{\chi',\chi''}$ ne dépendent ni de la base A choisie, ni du A-schéma en $\mathbb{F}_q$-vectoriel, ni même en fait du corps K, pourvu qu'il contienne les racines $(q-1)$-ième de l'unité. On remarque également que les constantes $\omega_{\chi_1,\ldots,\chi_n}$ s'obtiennent en fonction des $\omega_{\chi',\chi''}$ et donc elles aussi ne dépendent ni de la base ni du schéma. En particulier, ces constantes sont des éléments de $\mathcal{O}_K$. Avant de continuer, il va nous être nécessaire d'estimer quelques unes de ces constantes. Plus précisément, soit $\chi \in M$. On a vu que l'on pouvait écrire $\chi = \chi_1^{n_1}\ldots\chi_r^{n_r}$ où les χ_i sont ici les r caractères fondamentaux de M et les n_i sont des entiers compris entre 0 et $p-1$. En outre, on a vu que si l'on imposait que les n_i ne soient pas tous simultanément nuls, cette écriture était unique. Ainsi on peut poser :

$$\begin{aligned} d_\chi &= d_{\chi_1,\ldots,\chi_1,\chi_2,\ldots,\chi_2,\ldots,\chi_r,\ldots,\chi_r} \\ c_\chi &= c_{\chi_1,\ldots,\chi_1,\chi_2,\ldots,\chi_2,\ldots,\chi_r,\ldots,\chi_r} \\ \omega_\chi &= \omega_{\chi_1,\ldots,\chi_1,\chi_2,\ldots,\chi_2,\ldots,\chi_r,\ldots,\chi_r} \end{aligned}$$

où parmi les indices, il y a n_i χ_i.

Pour tout i, on définit également :

$$\begin{aligned} d_i &= d_{\chi_i,\ldots,\chi_i} \\ c_i &= c_{\chi_i,\ldots,\chi_i} \\ \omega_i &= \omega_{\chi_i,\ldots,\chi_i} \end{aligned}$$

où ce coup-ci χ_i est répété p fois.

Ce qu'il va nous falloir, c'est montrer que les constantes ω_χ sont inversibles dans $\mathcal{O}_K$ puis déterminer la valuation des ω_i.

3.2.4 Un calcul de $\omega_{\chi_1,\ldots,\chi_n}$

D'après les remarques précédentes, pour faire ce calcul, on peut choisir presque librement la base ainsi que le schéma en $\mathbb{F}_q$-vectoriel. Notre base va être l'anneau des entiers $\mathcal{O}_L$ du corps L obtenu en rajoutant à K les racines p-ième de l'unité. L'extension L/K est totalement ramifiée. Appelons ℓ le corps résiduel de L. Il s'identifie à k.

On va en fait définir deux schémas en $\mathbb{F}_q$-vectoriel sur $\mathcal{O}_L$. Considérons tout d'abord G, le *groupe diagonalisé* par $\mathbb{F}_q$. Il est décrit par la bigèbre $\mathcal{A}$ suivante. L'algèbre sous jacente est $\mathcal{O}_L[\mathbb{F}_q]$. En tant que A-module, il s'agit simplement du module libre engendré par des générateurs e_a, pour a décrivant $\mathbb{F}_q$. La loi de multiplication est donnée par la formule $e_a e_b = e_{a+b}$ valable pour tous a et b dans $\mathbb{F}_q$. La comultiplication c est donnée par $c(e_a) = e_a \otimes e_a$ et l'action de $\lambda \in \mathbb{F}_q^\star$ est définie par $[\lambda](e_a) = e_{\lambda a}$, et ce pour tout $a \in \mathbb{F}_q$.

L'augmentation e est l'unique morphisme de $\mathcal{O}_L$-algèbres qui envoie e_a sur 1 pour tout a. On peut également décrire les espaces $\mathcal{I}_\chi$ (en gardant les notations précédentes) pour $\chi \in M$. I_χ est un $\mathcal{O}_L$-module libre de rang 1 engendré, si $\chi \neq 1$, par le vecteur

$$e_\chi = \sum_{a \in \mathbb{F}_q} \chi^{-1}(a)\, e_a$$

et sinon par

$$e_1 = \sum_{a \in \mathbb{F}_q} e_a - q e_0$$

Le second $\mathcal{O}_L$-schéma en $\mathbb{F}_q$-vectoriel que l'on aura à considérer que ce que l'on appelle le *dual de Cartier* de G. Appelons-le G'. Sa bigèbre $\mathcal{A}'$ est simplement le dual de $\mathcal{A}$, c'est-à-dire l'ensemble des applications A-linéaires de $\mathcal{A}$ dans A. La comultiplication (resp. la multiplication, resp. l'action de $\lambda \in \mathbb{F}_q^\star$) de G' est simplement définie comme la transposée de la multiplication (resp. comultiplication, resp. l'action de $\lambda \in \mathbb{F}_q^\star$) de G. $\mathcal{A}'$ peut en fait être simplement vu comme la $\mathcal{O}_L$-algèbres des fonctions de $\mathbb{F}_q$ dans $\mathcal{O}_L$. En tant que module, elle est engendrée par les ε_a, fonction caractéristique de l'élément $a \in \mathbb{F}_q$. Les ε_a sont soumis aux relations de commutation $\varepsilon_a^2 = \varepsilon_a$ et $\varepsilon_a \varepsilon_b = 0$ si $a \neq b$. La comultiplication c' se décrit alors simplement par :

$$c'(\varepsilon_a) = \sum_{a'+a''=a} \varepsilon_{a'} \otimes \varepsilon_{a''}$$

L'action de $\lambda \in \mathbb{F}_q^\star$ est décrite par le morphisme $[\lambda] : \mathcal{A} \to \mathcal{A}$ défini par $[\lambda](\varepsilon_a) = \varepsilon_{\lambda^{-1}a}$. Autrement dit si $f : \mathbb{F}_q \to \mathcal{O}_L$ est une fonction, $[\lambda](f)$ sera défini par $[\lambda](f)(x) = f(\lambda x)$ et ce pour tout $x \in \mathbb{F}_q$. L'augmentation $e : \mathcal{A}' \to \mathcal{O}_L$ est le morphisme de $\mathcal{O}_L$-algèbres qui à une fonction $f : \mathbb{F}_q \to \mathcal{O}_L$ associe sa valeur en 0. L'idéal d'augmentation $\mathcal{I}'$ est donc l'idéal engendré par les ε_a pour $a \in \mathbb{F}_q^\star$. On peut finalement décrire les $\mathcal{I}'_\chi$. Ce sont des A-modules libres de dimension 1. $\mathcal{I}'_\chi$ est engendré par le vecteur :

$$\varepsilon_\chi = \sum_{a \in \mathbb{F}_q} \chi(a)\, \varepsilon_a$$

Il est immédiat, au vu des relations de commutation sur les ε_a, $a \in \mathbb{F}_q$, de vérifier que pour tous caractères χ et χ' dans M, on a $\varepsilon_{\chi'}\varepsilon_{\chi''} = \varepsilon_{\chi'\chi''}$. Si l'on se rappelle bien de la description faite pour annoncer l'introduction des quantités $\omega_{\chi',\chi''}$, on déduit directement de cela que :

$$c(\varepsilon_\chi) = \varepsilon_\chi \otimes 1 + 1 \otimes \varepsilon_\chi + \sum_{\chi'\chi''=\chi} \varepsilon_{\chi'} \otimes \varepsilon_{\chi''}$$

Le fait que, pour tout χ' et χ'' dans M, la quantité $\sum_{\lambda\in\mathbb{F}_q}\left(\chi'\chi''^{-1}\right)(\lambda)$ fasse $q-1$ dans le cas où $\chi'=\chi''$ et 0 sinon, nous dit précisément que la base duale de la base $(\varepsilon_\chi)_{\chi\in M}$ de $\mathcal{I}'$ est formée des vecteurs $\frac{1}{q-1}e_\chi$, χ décrivant M. On déduit de cela les relations :

$$e_{\chi'}e_{\chi''}=(q-1)\,\omega_{\chi',\chi''}\,e_{\chi'\chi''}$$

$$c'(e_\chi)=e_\chi\otimes 1+1\otimes e_\chi+\sum_{\chi'\chi''=\chi}e_{\chi'}\otimes e_{\chi''}$$

Considérons maintenant $\psi:\mathbb{F}_q\to\mathcal{O}_L$ un caractère non trivial, $\mathbb{F}_q$ étant aussi considéré pour sa structure additive. Un tel caractère existe car l'on a pris soin de rajouter dans L les racines p-ième de l'unité. ψ permet de définir un morphisme u de $\mathcal{O}_L$-schémas en groupe entre G et G'. Sur les bigèbres, il est défini par :

$$u(e_a)=\sum_{\lambda\in\mathbb{F}_q}\psi(\lambda a)\,\varepsilon_\lambda$$

Bien sûr, on prolonge u par linéarité. On vérifie facilement que u est bien un morphisme de bigèbres. Calculons, pour $\chi\in M$, $\chi\neq 1$:

$$\begin{aligned}u(e_\chi) &= \sum_{a\in\mathbb{F}_q,\lambda\in\mathbb{F}_q^\star}\chi^{-1}(a)\,\psi_{\lambda a}\varepsilon_\lambda\\ &= \sum_{a\in\mathbb{F}_q,\lambda\in F_q^\star}\chi(\lambda)\,\chi^{-1}(\lambda a)\,\psi(\lambda a)\,\varepsilon_\lambda\\ &= \sum_{a\in\mathbb{F}_q}\chi^{-1}(a)\,\psi(a)\cdot\sum_{\lambda\in\mathbb{F}_q^\star}\chi(\lambda)\,\varepsilon_\lambda=g(\chi)\,\varepsilon_\chi\end{aligned}$$

où la fonction g est définie par :

$$g(\chi)=\sum_{a\in\mathbb{F}_q}\chi^{-1}(a)\,\psi(a)$$

On remarque que cette relation reste vraie pour $\chi=1$ à condition de poser $g(1)=-q$.

La fonction g précédemment définie permet en fait d'exprimer facilement les constantes $\omega_{\chi',\chi''}$. Plus précisément, la relation de commutation entre les e_χ fournit

$$u(e_{\chi'}e_{\chi''})=(q-1)\,\omega_{\chi',\chi''}u(e_{\chi',\chi''})$$

et donc

$$\omega_{\chi',\chi''}=\frac{1}{q-1}\cdot\frac{g(\chi')\,g(\chi'')}{g(\chi'\chi'')}$$

Plus généralement, on déduit de cette formule la formule suivante, simplement en utilisant les relations d'associativité sur les constantes $\omega_{\chi_1,\ldots,\chi_n}$ que toutefois nous n'avons pas écrites. Cela donne :

$$\omega_{\chi_1,\ldots,\chi_n}=\frac{1}{(q-1)^{n-1}}\cdot\frac{g(\chi_1)\ldots g(\chi_n)}{g(\chi_1\cdots\chi_n)}$$

3.2.5 Quelques estimations

Avant de commencer, faisons deux remarques. Tout d'abord on n'a fait aucune hypothèse sur le caractère ψ à part le fait qu'il soit non trivial. On peut par exemple prendre pour ψ le composé de l'application $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ par un caractère non trivial de $\mathbb{F}_p$. Autrement dit, on peut supposer que ψ vérifie en outre $\psi(x^p)=\psi(x)$ pour tout $x\in\mathbb{F}_q$. Cela prouve directement que si $\chi\in M$, $g(\chi^p)=g(\chi)$. En

particulier la quantité ω_i que nous avons définie précédemment ne dépend en fait pas de i. On la notera ω par la suite.

Nous allons modifier le corps L. Nous allons simplement prendre le corps $\mathbb{Q}_p$ auquel on a ajouté les racines $(q-1)$-ième de l'unité. On a déjà expliqué pourquoi on avait le droit de faire une telle chose. On considère toujours sur l'anneau des entiers $\mathcal{O}_L$ le schéma en $\mathbb{F}_q$-vectoriel constant égal à $\mathbb{F}_q$. Sa bigèbre est bien entendu encore $\mathcal{O}_L[\mathbb{F}_q]$, la comultiplication et les éléments e_χ sont encore définis comme précédemment. En particulier ils vérifient toujours les relations de commutation :

$$e_{\chi'} e_{\chi''} = (q-1)\,\omega_{\chi',\chi''} e_{\chi'\chi''}$$

valables pour tous caractères χ' et χ'' de M. Par une récurrence simple, et en utilisant les lois d'associativité des ω, on prouve que, pour tout $\chi_1, \ldots, \chi_n \in M$, on a :

$$e_{\chi_1} \ldots e_{\chi_n} = (q-1)^{n-1}\,\omega_{\chi_1,\ldots,\chi_n} e_{\chi_1 \cdots \chi_n}$$

En particulier si $\chi = \chi_i^{n_1} \ldots \chi_r^{n_r}$ est la décomposition en caractères fondamentaux de χ, on a la relation :

$$(q-1)^{n-1}\,\omega_\chi e_\chi = e_1^{n_1} \ldots e_r^{n_r}$$

où $e_i = e_{\chi_i}$.

Nous allons donc nous intéresser aux éléments e_i et plus particulièrement à leur résidu modulo p, que l'on notera par exemple $\bar{e_i}$. Ils vivent naturellement dans la réduction modulo p de $\mathcal{A}$, disons $\bar{\mathcal{A}}$. Celle-ci s'identifie à la bigèbre $k[\mathbb{F}_q]$ munie de la comultiplication et de l'action de $\mathbb{F}_q$ habituelle. En particulier, on peut considérer l'idéal d'augmentation $\bar{\mathcal{I}}$ de cette bigèbre. C'est bien entendu la réduction modulo p de $\mathcal{I}$. Nous allons prouver que les $\bar{e_i}$ engendre le $\mathbb{F}_q$-espace vectoriel $\bar{\mathcal{I}}/\bar{\mathcal{I}}^2$. Pour cela, on remarque que l'action de $\mathbb{F}_q$ respecte $\bar{\mathcal{I}}$ et donc se factorise en une action sur $\bar{\mathcal{I}}/\bar{\mathcal{I}}^2$, puis même en une action sur $\mathrm{Hom}_{l-\mathrm{alg}}\left(\bar{\mathcal{I}}/\bar{\mathcal{I}}^2, l\right)$. Considérons maintenant la ℓ-algèbre, $\ell(\varepsilon)$, engendré par l'élément ε soumis à la seule relation $\varepsilon^2 = 0$. Notons $p : \ell(\varepsilon) \to \ell$ l'unique morphisme de l-algèbre qui envoie ε sur 0. p induit une flèche :

$$\mathrm{Hom}_{\ell-\mathrm{alg}}\left(\bar{\mathcal{A}}, \ell(\varepsilon)\right) \longrightarrow \mathrm{Hom}_{\ell-\mathrm{alg}}\left(\bar{\mathcal{A}}, \ell\right)$$

Ces deux ensembles sont des espaces vectoriels sur $\mathbb{F}_q$. En tant que groupes, ils s'identifient respectivement à $\mathrm{Hom}_{\mathrm{gr}}\left(\mathbb{F}_q, l(\varepsilon)^\star\right)$ et $\mathrm{Hom}_{\mathrm{gr}}\left(\mathbb{F}_q, l^\star\right)$. D'autre part, l'élément neutre du groupe $\mathrm{Hom}_{l-\mathrm{alg}}\left(\bar{\mathcal{A}}, l\right)$ est donné par le morphisme d'augmentation de $\bar{\mathcal{A}}$. On déduit de tout cela, que l'on est en présence du diagramme suivant.

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_{l-\mathrm{alg}}\left(\bar{\mathcal{I}}/\bar{\mathcal{I}}^2, l\right) & \longrightarrow & \mathrm{Hom}_{l-\mathrm{alg}}\left(\bar{\mathcal{A}}, l(\varepsilon)\right) & \xrightarrow{p\circ\cdot} & \mathrm{Hom}_{l-\mathrm{alg}}\left(\bar{\mathcal{A}}, l\right) \\
 & & & & \downarrow \sim & & \downarrow \sim \\
0 & \longrightarrow & \mathrm{Hom}_{\mathrm{gr}}\left(\mathbb{F}_q, l\right) & \longrightarrow & \mathrm{Hom}_{\mathrm{gr}}\left(\mathbb{F}_q, l(\varepsilon)^\star\right) & \xrightarrow{p\circ\cdot} & \mathrm{Hom}_{\mathrm{gr}}\left(\mathbb{F}_q, l^\star\right)
\end{array}$$

En appliquant par exemple le lemme de cinq on trouve un isomorphisme canonique entre les groupes $\mathrm{Hom}_{\ell-\mathrm{alg}}\left(\bar{\mathcal{I}}/\bar{\mathcal{I}}^2, \ell\right)$ et $\mathrm{Hom}_{\mathrm{gr}}\left(\mathbb{F}_q, \ell\right)$. La structure d'espace vectoriel sur ce dernier est donnée par la formule $\lambda \cdot f(x) = f(\lambda x)$ où λ et x sont dans $\mathbb{F}_q$ et $f \in \mathrm{Hom}_{\mathrm{gr}}\left(\mathbb{F}_q, \ell\right)$. Considérons $f \in \mathrm{Hom}_{\mathrm{gr}}\left(\mathbb{F}_q, \ell\right)$ un vecteur propre commun à l'action de tous les $\lambda \in \mathbb{F}_q$. Quitte à diviser par $f(1) \neq 0$, on peut supposer que $f(1) = 1$. Mais alors, pour tout $\lambda \in \mathbb{F}_q$, il existe une constante c_λ telle que $h(\lambda x) = c_\lambda h(x)$ pour tout $x \in \mathbb{F}_q$. On voit alors que $c_\lambda = h(\lambda)$ puis que h est multiplicatif. Cela signifie que les caractères qui interviennent pour l'action de $\mathbb{F}_q$ sur $\bar{\mathcal{I}}/\bar{\mathcal{I}}^2$ sont précisément les caractères multiplicatifs ou encore que les $\bar{e_i}$ forment une base de $\bar{\mathcal{I}}/\bar{\mathcal{I}}^2$. Finalement, il est facile de voir que pour tout $a \in \mathbb{F}_q$, $e_a^p = e_0$ et donc que $\bar{\mathcal{I}}^p = 0$. On déduit de tout ça que les e_i^n pour n variant sur $\mathbb{N}$ engendrent $\mathcal{I}$. Finalement, pour des questions de dimension, $\mathcal{I}$ est engendré en tant que $\mathbb{F}_q$-algèbre par les e_i, ceux-ci étant simplement liés par les relations $e_i^p = 0$.

On est maintenant en mesure de fournir les estimations désirées. La dernière formule écrite prouve après réduction modulo p, que ω_χ est non nul modulo p. Cela revient à dire que ω_χ est inversible. De même, on voit que $\omega = 0 \pmod{p}$. Nous allons donner des estimations un peu meilleures. On appelle à nouveau G' le dual de Cartier de G. Sa bigèbre $\mathcal{A}'$ est, comme nous l'avons décrit précédemment, l'ensemble des fonctions de $\mathbb{F}_q$ dans $\mathcal{O}_L$. Nous noterons encore ε_a la fonction caractéristique d'un élément $a \in \mathbb{F}_q$. On rappelle que $\mathcal{I}_\chi$ est alors un $\mathcal{O}_L$-module libre de rang 1, il est engendré par

$$\varepsilon_\chi = \sum_{a \in \mathbb{F}_q} \chi(a)\, \varepsilon_a$$

Nous allons dans un premier temps estimer $c(\varepsilon_{\chi_i})$ où χ_i est le i-ième caractère fondamental. On prend pour cela χ' et χ'' deux caractères de M tels que $\chi'\chi'' = \chi_i$. Décomposons $\chi' = \chi_1^{n'_1} \dots \chi_r^{n'_r}$ et $\chi'' = \chi_1^{n''_1} \dots \chi_r^{n''_r}$. Comme leur produit est fondamental, il existe forcément un indice j tel que $n'_j + n''_j \geqslant p$. On déduit de cela que $\omega_{\chi'\chi''} = 0 \pmod{p}$ et donc que

$$c(\varepsilon_{\chi_i}) = \varepsilon_{\chi_i} \otimes 1 + 1 \otimes \varepsilon_{\chi_i} \pmod{p}$$

En utilisant la co-associativité de c, on généralise immédiatement cette formule :

$$c_n(\varepsilon_{\chi_i}) = \varepsilon_{\chi_i} \otimes 1 \otimes \dots \otimes 1 + \dots + 1 \otimes \dots \otimes 1 \otimes \varepsilon_{\chi_i} \pmod{p}$$

Prenons maintenant $\chi = \chi_1^{n_1} \dots \chi_r^{n_r}$. En appliquant la formule précédente à $n = n_1 + \dots + n_r$, on voit que

$$\omega_\chi = n_1! \dots n_r! \pmod{p}$$

En regardant la décomposition de $c_p\left(\varepsilon_{\chi_i}^p\right)$, on trouve

$$\omega = p! \pmod{p^2}$$

Cette dernière congruence permet finalement de calculer la valuation de ω dans $\mathcal{O}_K$. En effet, le thérorème de Wilson nous dit que $(p-1)! = -1 \pmod{p}$ et donc $v(\omega) = e_K$ où on rappelle que e_K est l'indice de ramification absolu de corps K, par définition $e_k = v(p)$.

3.2.6 Classification proprement dite

On a vu et utilisé abondamment que la bigèbre $\mathcal{A}$ peut se décomposer en tant que A-module de la façon suivante :

$$\mathcal{A} = A \oplus \left(\bigoplus_{\chi \in M} \mathcal{I}_\chi \right)$$

Prenons maintenant $\chi \in M$, χ s'écrit alors $\chi = \chi_1^{n_1} \dots \chi_r^{n_r}$ où les χ_i sont les caractères fondamentaux, les n_i sont entiers compris entre 0 et $p-1$ non tous nuls. Étant donné que ω_χ est inversible, l'application $d_\chi : \mathcal{I}_{\chi_1}^{\otimes n_1} \otimes_A \dots \otimes_A \mathcal{I}_{\chi_r}^{\otimes n_r} \to \mathcal{I}_\chi$ est un isomorphisme de A-modules. Ainsi en tant que A-modules, $\mathcal{A}$ peut s'écrire simplement à l'aide des $\mathcal{I}_{\chi_i}$. Plus précisément, on a :

$$\mathcal{A} = \bigoplus_{0 \leqslant n_i \leqslant p-1} \mathcal{I}_{\chi_1}^{\otimes n_1} \otimes_A \dots \otimes_A \mathcal{I}_{\chi_r}^{\otimes n_r}$$

le terme où tous les n_i sont nuls correspondant à la composante A.

Nous allons voir que la donnée des applications d_i et c_i suffisent à reconstruire respectivement la multiplication et la comultiplication de $\mathcal{A}$. Commençons par la multiplication. Il suffit de décrire pour χ'

et χ'' deux caractères l'application $d_{\chi',\chi''}$. Décomposons $\chi' = \chi_1^{n'_1} \dots \chi_r^{n'_r}$ et $\chi'' = \chi_1^{n''_1} \dots \chi_r^{n''_r}$ où les χ_i sont les caractères fondamentaux. Si pour tout indice i, on a $n'_i + n''_i \leqslant p-1$, $d_{\chi',\chi''}$ est par construction simplement l'isomorphisme canonique :

$$d_{\chi',\chi''} : \left(\mathcal{I}_{\chi_1}^{\otimes n'_1} \otimes_A \dots \otimes_A \mathcal{I}_{\chi_r}^{\otimes n'_r}\right) \otimes \left(\mathcal{I}_{\chi_1}^{\otimes n''_1} \otimes_A \dots \otimes_A \mathcal{I}_{\chi_r}^{\otimes n''_r}\right) \xrightarrow{\sim} I_{\chi_1}^{\otimes n'_1+n''_1} \otimes_A \dots \otimes_A \mathcal{I}_{\chi_r}^{\otimes n'_r+n''_r}$$

Sinon c'est pareil. Simplement un exposant supérieur à p va apporter une *retenue* et celles-ci sont gérées par définition par les applications :

$$d_i : \mathcal{I}_{\chi_i}^{\otimes p} \to \mathcal{I}_{\chi_{i+1}}$$

Traitons maintentant la comultiplication. Comme on l'a expliqué au tout début, il suffit de décrire les applications $c_{\chi',\chi''}$ pour $\chi', \chi'' \in M$. Écrivons donc $\chi' = \chi_1^{n'_1} \dots \chi_r^{n'_r}$ et $\chi'' = \chi_1^{n''_1} \dots \chi_r^{n''_r}$ où les χ_i sont encore les caractères fondamentaux. Comme précédemment si pour tout indice i, $n'_i + n''_i \leqslant p-1$, la description ne pose pas de problèmes. Il s'agit simplement de la multiplication par l'élément $\omega_{\chi',\chi''}$ (qui est bien défini) une fois les identifications canoniques étant faites :

$$c_{\chi',\chi''} : I_{\chi_1}^{\otimes n'_1+n''_1} \otimes_A \dots \otimes_A \mathcal{I}_{\chi_r}^{\otimes n'_r+n''_r} \xrightarrow{\times \omega_{\chi',\chi''}} \left(\mathcal{I}_{\chi_1}^{\otimes n'_1} \otimes_A \dots \otimes_A \mathcal{I}_{\chi_r}^{\otimes n'_r}\right) \otimes \left(\mathcal{I}_{\chi_1}^{\otimes n''_1} \otimes_A \dots \otimes_A \mathcal{I}_{\chi_r}^{\otimes n''_r}\right)$$

Là encore, s'il existe un indice i tel que $n'_i + n''_i \geqslant p$, il faut expliquer comment on gère les *retenues*. C'est un peu penible à présenter dans le cas général. Nous allons donc travailler sur un exemple ne possédant qu'une retenue. Supposons donc que l'on ait $c_{\chi_1^n,\chi_1^{p-n}}$ où n est un entier compris entre 1 et $p-1$. On a alors le diagramme suivant :

$$\mathcal{I}_{\chi_1^p} = \mathcal{I}_{\chi_2} \xrightarrow{c_{\chi_1^n,\chi_1^{p-n}}} \mathcal{I}_{\chi_1^n} \otimes_A \mathcal{I}_{\chi_1^{p-n}} \xrightarrow{c_{\chi_1^n} \otimes c_{\chi_1^{p-n}}} \mathcal{I}_{\chi_1}^{\otimes n} \otimes_A \mathcal{I}_{\chi_1}^{\otimes p-n}$$
$$\mathcal{I}_{\chi_1^p} \xrightarrow[c_1]{} \mathcal{I}_{\chi_1}^{\otimes n} \otimes_A \mathcal{I}_{\chi_1}^{\otimes p-n}$$

D'après le cas précédent, les c_χ ne sont en fait que la multiplication par ω_χ qui est inversible, ce qui donne une expression de $c_{\chi^n,\chi^{p-n}}$.

Ainsi l'on vient de voir que la donnée des modules $\mathcal{I}_{\chi_i}$ et des applications d_i et c_i suffisent à reconstruire (à isomorphisme près) la bigèbre $\mathcal{A}$ et donc le schéma en $\mathbb{F}_q$-vectoriel dont on était parti. On a en fait plus précisément le théorème suivant :

Théorème 3.2.6.1. *Soit A une $\mathcal{O}_K$-algèbre. L'application*

$$G \mapsto \left(\mathcal{I}_{\chi_i}, d_i : \mathcal{I}_{\chi_i}^{\otimes p} \to \mathcal{I}_{\chi_{i+1}}, c_i : \mathcal{I}_{\chi_{i+1}} \to \mathcal{I}_{\chi_i}^{\otimes p}\right)$$

est une bijection de l'ensemble des classes d'isomorphismes de A-schémas en $\mathbb{F}_q$-vectoriels G qui sont tels que $\mathcal{I}_\chi$ est un A-module libre de rang 1 et les classes d'isomorphismes de "triplet" (A_i, d_i, c_i) où les A_i sont des A-modules libres de rang 1, $d_i : A_i^{\otimes p} \to A_{i+1}$ et $c_i : A_{i+1} \to A_i^{\otimes p}$, le tout vérifiant $d_i \circ c_i = \omega id_{A_{i+1}}$.

Pour finir de prouver ce théorème, il suffit de construire une application inverse. Bien entendu, partant d'un triplet (A_i, d_i, c_i) vérifiant les conditions de l'énoncé précédent, on construit la bigèbre $\mathcal{A}$ avec les formules données ci-dessus. Il faut alors vérifier les axiomes de bigèbres. Nous n'allons pas le faire. Pour plus de détails, se reporter à [Ray74]. Ce dernier article traite un cas un peu plus général (mais pas plus difficile) que nous allons tout de même exposer.

Considérons C le corps obtenu en ajoutant à $\mathbb{Q}$, le corps des nombres rationnels, les racines $(q-1)$-ième de l'unité. Notons D' la fermeture intégrale de $\mathbb{Z}$ dans C et $\mathfrak{p}$ un idéal premier de D' au dessus de p. On rend ensuite $(q-1)$ inversible dans D' et on enlève au spectre de l'anneau obtenu les idéaux premiers au-dessus de p qui sont différents de $\mathfrak{p}$. Le schéma obtenu est le spectre d'un anneau de valuation

discrète que l'on va noter D. Plus algébriquement D s'obtient à partir de D' d'abord en rendant $(q-1)$ inversible puis en localisant par rapport à la partie multiplicative complémentaire de la réunion des idéaux premiers au-dessus de p et différents de $\mathfrak{p}$. Les caractères χ sont encore définis. Ils sont ce coup-ci à valeurs dans D et un tel caractère est dit *fondamental* si son composé avec la projection de D dans le corps résiduel en $\mathfrak{p}$ est additif. Il est encore vrai que tout caractère s'écrit de façon unique comme produit de caractères fondamentaux avec des exposants compris entre 0 et $p-1$, non tous nuls. Si maintenant S est un schéma, un S-schéma en $\mathbb{F}_q$-vectoriels G est alors décrit par un faisceaux de bigèbres muni d'une action compatible de $\mathbb{F}_q$. En particulier, si S est un schéma sur $\operatorname{Spec} D$, on peut encore définir les $\mathcal{I}_\chi$, il s'agira de $\mathcal{O}_S$-modules. La classification de RAYNAUD porte sur les S-schémas en $\mathbb{F}_q$-vectoriels pour lesquels tous les $\mathcal{I}_\chi$ sont localement libres de rang 1.

Théorème 3.2.6.2. *Soit S un schéma sur $\operatorname{Spec} D$. L'application*

$$G \mapsto \left(\mathcal{I}_{\chi_i}, d_i : \mathcal{I}_{\chi_i}^{\otimes p} \to \mathcal{I}_{\chi_{i+1}}, c_i : \mathcal{I}_{\chi_{i+1}} \to \mathcal{I}_{\chi_i}^{\otimes p}\right)$$

est une bijection de l'ensemble des classes d'isomorphismes de S-schémas en $\mathbb{F}_q$-vectoriels G qui sont tels que $\mathcal{I}_\chi$ est un $\mathcal{O}_S$-module localement libre de rang 1 et les classes d'isomorphismes de "triplet" (L_i, d_i, c_i) où les L_i sont des $\mathcal{O}_S$-modules localement libres de rang 1, $d_i : L_i^{\otimes p} \to L_{i+1}$ et $c_i : L_{i+1} \to L_i^{\otimes p}$, le tout vérifiant $d_i \circ c_i = \omega id_{L_{i+1}}$.

3.2.7 Une autre description

On peut donner une autre description peut-être un peu plus terre à terre de la classification précédente. Donnons-nous un triplet (A_i, d_i, c_i) vérifiant les conditions du théorème 3.2.6.1. On peut alors choisir pour tout indice i, un générateur X_i de A_i. $X_i \otimes \ldots \otimes X_i$ (p fois) est alors un générateur de $A_i^{\otimes p}$. Une fois, ces choix faits, la donnée de l'application $d_i : A_i^{\otimes p} \to A_{i+1}$ revient tout simplement à se donner un élément $\delta_i \in A$ défini par $d_i(X_i \otimes \ldots \otimes X_i) = \delta_i X_{i+1}$. De même $c_i : A_{i+1} \to A_i^{\otimes p}$ est décrit par un élément $\gamma_i \in A$. La condition $d_i \circ c_i = \omega \mathrm{id}_{A_{i+1}}$ se traduit par l'égalité $\gamma_i \delta_i = \omega$.

Décrivons la bigèbre $\mathcal{A}$ du schéma en $\mathbb{F}_q$-vectoriel correspondant à notre triplet. Elle est engendrée en tant qu'algèbre par les vecteurs X_i qui sont soumis aux seules relations $X_i^p = \delta_i X_{i+1}$. L'action de $\mathbb{F}_q$ est également simple à décrire. Elle est linéaire et déterminée par la relation :

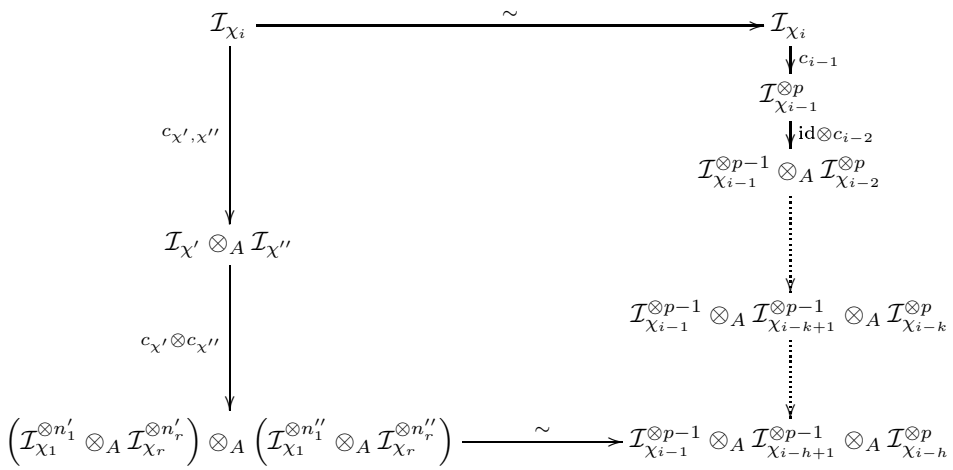
$$[\lambda]\left(X_1^{n_1} \ldots X_r^{n_r}\right) = \left(\chi_1^{n_1} \ldots \chi_r^{n_r}\right)(\lambda) \cdot X_1^{n_1} \ldots X_r^{n_r}$$

et ce pour tout $\lambda \in \mathbb{F}_q$ et tous entiers n_i compris entre 0 et $p-1$. On vérifie à part que la formule reste valable pour tous les n_i nuls.

La comultiplication, elle, demande un peu de travail. Nous allons donner simplement la valeur de $c(X_i)$. Il s'agit donc de calculer $c_{\chi',\chi''}$ pour $\chi'\chi'' = \chi_i$. Décomposons comme à l'habitude $\chi' = \chi_1^{n_1'} \ldots \chi_r^{n_r'}$ et $\chi'' = \chi_1^{n_1''} \ldots \chi_r^{n_r''}$. Notons qu'il existe un entier h tel que :

$$\begin{aligned}
n'_{i-1} + n''_{i-1} &= p-1 \\
&\vdots \\
n'_{i-h+1} + n''_{i-h+1} &= p-1 \\
n'_{i-h} + n''_{i-h} &= p \\
n'_{i-h-1} + n''_{i-h-1} &= 0 \\
&\vdots \\
n'_{i-r} + n''_{i-r} &= 0
\end{aligned}$$

Il y a donc h retenues à gérer. On regarde pour cela le diagramme suivant :



On déduit de cela que :

$$c_{\chi',\chi''}(X_i) = \frac{\gamma_{i-1}\cdots\gamma_{i-h}}{\omega_{\chi'}\omega_{\chi''}} \cdot \left(X_1^{n'_1}\ldots X_r^{n'_r}\right) \otimes \left(X_1^{n''_1}\ldots X_r^{n''_r}\right)$$

Finalement on utilise la formule $c(X_i) = 1\otimes X_i + X_i \otimes 1 + \sum_{\chi'\chi''=\chi_i} c_{\chi',\chi''}(X_i)$ pour avoir l'expression souhaitée.

Les constantes γ_i et δ_i dépendent bien entendu du choix des éléments générateurs X_i. Mais un générateur de A_i s'écrit de façon générale $u_i X_i$ où u_i est une certaine unité de A. Pour cette nouvelle famille, les quantités qui interviennent vont être $\delta'_i = u_i^p \delta_i u_{i+1}^{-1}$ et $\gamma'_i = u_i^{-p}\delta_i u_{i+1}$. Le théorème 3.2.6.1 peut donc se réénoncer de la façon suivante.

Théorème 3.2.7.1. *Soit A une $\mathcal{O}_K$-algèbre. La donnée d'un A-schéma en $\mathbb{F}_q$-vectoriel G qui est tel que les A-modules $\mathcal{I}_\chi$ soient libres de dimension 1 équivaut à la donnée de r couples (γ_i,δ_i) d'éléments de A, vérifiant la condition $\gamma_i\delta_i = \omega$ pour tout i et ayant pris soin d'identifier les familles de couples (γ_i,δ_i) et (γ'_i,δ'_i) dès qu'il existe des u_i, unités de A, telles que $\delta'_i = u_i^p\delta_i u_{i+1}^{-1}$ et $\gamma'_i = u_i^{-p}\delta_i u_{i+1}$.*

Terminons par une remarque. Dans le cas où $A = \mathcal{O}_{\widehat{K^{\mathrm{nr}}}}$, cet énoncé se simplifie encore. En effet, on voit facilement que si $v(\delta_i) = v(\delta'_i)$ pour tout i, les familles (δ_i,γ_i) et (δ'_i,γ'_i) sont équivalentes au sens précédent. Ainsi se donner un $\mathcal{O}_{\widehat{K^{\mathrm{nr}}}}$-schéma en $\mathbb{F}_q$-vectoriel tel que les A-modules $\mathcal{I}_\chi$ soient libres de dimension 1 équivaut à se donner une famille de r entiers compris entre 0 et e_K, qui rappelons-le est la valuation de ω. En particulier, il y a $(e_K)^r$ classes d'isomorphisme de tels schémas.

3.3 Première preuve du théorème

Nous pouvons désormais nous attaquer à la preuve du théorème 3.1.5.2. Celle-ci est également dû à Raynaud et a été pour la première fois publiée dans [Ray74], c'est-à-dire le même article que celui qui nous a servi de support pour la classification des schémas en $\mathbb{F}_q$-vectoriel.

Rappelons brièvement l'énoncé du théorème. On garde les mêmes notations que précédemment. K désigne un corps de caractéristique nulle complet pour une valuation v discrète. On note $\mathcal{O}_K$ son anneau des entiers et k son corps résiduel. On suppose que k est parfait de caractéristique p. On pose $e_K = v(p)$, c'est l'indice de ramification absolu du corps K. $\bar{K}$ désigne une clôture algébrique K. K^{nr} (resp. K^{mr})

est la fermeture non ramifiée (resp. modérément ramifiée) de K dans $\bar{K}$. On note I_m le groupe d'inertie modérée de K, c'est-à-dire le groupe de Galois de l'extension $K^{\mathrm{mr}}/K^{\mathrm{nr}}$. On se donne maintenant un schéma en $\mathbb{F}_p$-vectoriel fini et plat $\mathcal{G}$ sur l'anneau des entiers $\mathcal{O}_K$. Le K-schéma $\mathcal{G} \times_{\mathcal{O}_K} K$ est alors fini et étale[3] et donc va nous fournir une représentation $\rho : \mathrm{Gal}\left(\bar{K}/K\right) \to \mathrm{GL}\left(V\right)$ où V est un espace vectoriel de dimension finie sur $\mathbb{F}_p$. La restriction de ρ au groupe d'inertie n'est pas forcément semi-simple. On en considère un quotient de Jordan-Hölder qui donne une nouvelle représentation simple $\rho' : I_m \to \mathrm{GL}\left(V'\right)$ où V' est encore un espace vectoriel de dimension finie sur $\mathbb{F}_p$. On a vu qu'en fait V' hérite alors d'une structure de corps et que ρ' peut ainsi être vue comme un caractère. Le théorème dit alors que $v_\sigma\left(\rho'\right) \leqslant e_K$ pour tout caractère fondamental σ.

3.3.1 Adhérence schématique

On commence par prendre une suite de composition de Jordan-Hölder du schéma $\mathcal{G}_K = \mathcal{G} \times_{\mathcal{O}_K} K$, c'est-à-dire :

$$0 = \mathcal{G}_K^0 \subset \mathcal{G}_K^1 \subset \mathcal{G}_K^2 \subset \ldots \subset \mathcal{G}_K^m = \mathcal{G}_K$$

telle que les quotients successifs $\mathcal{G}_K^{i+1}/\mathcal{G}_K^i$ soient des objets simples de la catégorie des K-schémas en groupe finis. On va voir dans un premier temps qu'une telle suite de composition peut se remonter de façon canonique sur l'anneau des entiers $\mathcal{O}_K$.

De façon plus générale, prenons $\mathcal{X}$ un $\mathcal{O}_K$-schéma de type fini et regardons $\mathcal{X}_K = \mathcal{X} \times_{\mathcal{O}_K} K$ sa fibre générique. On considère en outre $\mathcal{Y}_K$ un sous-schéma fermé de $\mathcal{X}_K$. L'*adhérence schématique* $\mathcal{Y}$ de $\mathcal{Y}_K$ dans $\mathcal{X}$ est définie comme étant le plus petit sous-schéma fermé de $\mathcal{X}$ contenant $\mathcal{Y}_K$. Comme on a supposé $\mathcal{Y}_K$ fermé dans $\mathcal{X}_K$, la fibre générique de $\mathcal{Y}$, c'est-à-dire $\mathcal{Y} \times_{\mathcal{O}_K} K$, est exactement $\mathcal{Y}_K$. Supposons désormais que le schéma $\mathcal{X}$ soit fini et notons $\mathcal{A}$ son anneau. $\mathcal{X}_K$ est alors tout autant fini et a pour anneau $\mathcal{A}_K = \mathcal{A} \otimes_{\mathcal{O}_K} K$. Le schéma $\mathcal{Y}_K$ est défini par un idéal $\mathcal{I}_K$ de $\mathcal{A}_K$. Dans ces conditions, il est facile de voir que le schéma $\mathcal{Y}$ est défini par l'idéal $\mathcal{I}$, image réciproque de $\mathcal{I}_K$ par l'application canonique $\mathcal{A} \to \mathcal{A}_K$. On déduit de cela d'une part que $\mathcal{Y}$ est fini sur $\mathcal{O}_K$ et d'autre part que l'application $\mathcal{A}/\mathcal{I} \to \mathcal{A}_K/\mathcal{I}_K$ est injective, ce qui prouve que l'anneau $\mathcal{A}/\mathcal{I}$ est sans torsion. Comme la base $\mathcal{O}_K$ est un anneau principal, cela est équivalent à la platitude de $\mathcal{Y}$.

De cela, on déduit que la formation de l'adhérence schématique commute aux produits fibrés. En particulier, en gardant les notations précédentes, si $\mathcal{X}$ est un $\mathcal{O}_K$-schéma en groupe commutatif fini et si $\mathcal{Y}_K$ est un sous-schéma en groupe de $\mathcal{X}_K$, l'adhérence schématique $\mathcal{Y}$ va hériter d'une structure de $\mathcal{O}_K$-schéma en groupe commutatif fini et plat. En outre, le quotient $\mathcal{X}/\mathcal{Y}$ est représentable par un $\mathcal{O}_K$-schéma en groupe commutatif fini et plat.

Appliquons cela à notre situation. Pour tout i considérons l'adhérence schématique dans $\mathcal{G}$ de $\mathcal{G}_K^i$. Il s'agit d'un $\mathcal{O}_K$-schéma en groupe commutatif fini et plat, au même titre que les quotients $\mathcal{G}^{i+1}/\mathcal{G}^i$. Ces derniers donnent après extension des scalaires à K les quotients $\mathcal{G}_K^{i+1}/\mathcal{G}_K^i$. Ceux-ci sont, comme nous l'avons déjà vu, naturellement muni d'une structure de schéma en $\mathbb{F}_q$-vectoriel de dimension 1 mais il n'est pas clair que cette structure supplémentaire puisse se remonter à $\mathcal{G}^{i+1}/\mathcal{G}^i$. Toutefois, il va être possible de remplacer $\mathcal{G}^{i+1}/\mathcal{G}^i$ par un autre schéma en groupe qui, lui, va pouvoir hériter de la structure de $\mathbb{F}_q$-espace vectoriel. C'est ce que nous allons faire.

3.3.2 Prolongement de la structure d'espace vectoriel

Nous allons nous placer dans la situation suivante. On prend $\mathcal{G}$ un schéma en groupe commutatif fini et plat sur l'anneau $\mathcal{O}_K$. On considère $\mathcal{G}_K = \mathcal{G} \times_{\mathcal{O}_K} K$ sa fibre générique que l'on munit d'une structure de schéma en $\mathbb{F}_q$-vectoriel. Le but est de construire un nouveau $\mathcal{O}_K$-schéma en groupe commutatif fini et

[3]Cela est dû au fait que K est de caractéristique nulle. Plus précisément si G est un schéma en groupe fini et plat sur un anneau A, et que le rang de G est inversible dans A alors G est étale. C'est un théorème de Deligne.

plat $\mathcal{G}'$ qui puisse être muni d'une strcture de $\mathbb{F}_q$-vectoriel et qui soit tel que $\mathcal{G}' \times_{\mathcal{O}_K} K$ soit isomorphe à $\mathcal{G}_K$, l'isomorphisme respectant la structure d'espace vectoriel.

Pour cela, on va s'intéresser à la catégorie formée des couples $(\mathcal{H}, \varphi_{\mathcal{H}})$ où $\mathcal{H}$ est un $\mathcal{O}_K$-schéma en groupe commutatif fini et plat et $\varphi_{\mathcal{H}}$ un isomorphisme entre $\mathcal{H} \times_{\mathcal{O}_K} K$ et $\mathcal{G}_K$. Si $(\mathcal{H}, \varphi_{\mathcal{H}})$ et $(\mathcal{H}', \varphi_{\mathcal{H}'})$ sont deux objets de cette catégorie, un morphisme entre eux sera un morphisme de schéma en groupe $f : \mathcal{H}' \to \mathcal{H}$ faisant commuter le diagramme suivant :

$$\begin{array}{ccc} \mathcal{H}' \times_{\mathcal{O}_K} K & \xrightarrow{f \times \mathrm{id}} & \mathcal{H} \times_{\mathcal{O}_K} K \\ & {\scriptstyle \varphi_{\mathcal{H}'}} \searrow \quad \swarrow {\scriptstyle \varphi_{\mathcal{H}}} & \\ & \mathcal{G}_K & \end{array}$$

Comme ici, tous les schémas considérés sont affines, la catégorie précédente peut se redécrire en termes d'anneaux. Notons $\mathcal{A}$ la bigèbre de $\mathcal{G}$ et $\mathcal{A}_K = A \otimes_{\mathcal{O}_K} K$. Les objets de cette catégorie seront les couples $(\mathcal{B}, \varphi_{\mathcal{B}})$ où $\mathcal{B}$ est une $\mathcal{O}_K$-bigèbre sans torsion et $\varphi_{\mathcal{B}} : \mathcal{B} \otimes_{\mathcal{O}_K} K \to \mathcal{A}_K$ est un isomorphisme de K-algèbres. Un morphisme de $(\mathcal{B}, \varphi_{\mathcal{B}})$ dans $(\mathcal{B}', \varphi_{\mathcal{B}'})$ sera la donnée de $f : \mathcal{B} \to \mathcal{B}'$ un morphisme de $\mathcal{O}_K$-bigèbres vérifiant :

$$\begin{array}{ccc} \mathcal{B} \otimes_{\mathcal{O}_K} K & \xrightarrow{f \otimes \mathrm{id}} & \mathcal{B}' \otimes_{\mathcal{O}_K} K \\ & {\scriptstyle \varphi_{\mathcal{B}'}} \searrow \quad \swarrow {\scriptstyle \varphi_{\mathcal{B}}} & \\ & \mathcal{A}_K & \end{array}$$

Cette catégorie est en fait celle d'un pré-ordre. Nous entendons par là que étant donné deux objets $(\mathcal{B}, \varphi_{\mathcal{B}})$ et $(\mathcal{B}', \varphi_{\mathcal{B}'})$, l'ensemble $\mathrm{Hom}\left((\mathcal{B}, \varphi_{\mathcal{B}}), (\mathcal{B}', \varphi_{\mathcal{B}'})\right)$ est soit vide, soit réduit à un élément. En effet, supposons qu'il ne soit pas vide. Alors il existe une flèche $f : \mathcal{B} \to \mathcal{B}'$ faisant commuter le diagramme suivant :

$$\begin{array}{ccccc} \mathcal{B} & \longrightarrow & \mathcal{B} \otimes_{\mathcal{O}_K} K & \overset{\sim}{\searrow} & \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f \otimes \mathrm{id}} & & \mathcal{A}_K \\ \mathcal{B}' & \longrightarrow & \mathcal{B}' \otimes_{\mathcal{O}_K} K & \overset{\sim}{\nearrow} & \end{array}$$

Comme $\mathcal{B}$ et $\mathcal{B}'$ sont sans torsion, les flèches $\mathcal{B} \to \mathcal{B} \otimes_{\mathcal{O}_K} K$ et $\mathcal{B}' \to \mathcal{B}' \otimes_{\mathcal{O}_K} K$ sont injectives. On déduit directement de cela que f est uniquement déterminé par ce diagramme et qu'en outre il s'agit d'une injection. Ainsi l'ordre associé à notre catégorie est l'inclusion sur les sous-$\mathcal{O}_K$-bigèbres $\mathcal{B}$ de la fermeture intégrale de $\mathcal{O}_K$ dans $\mathcal{A}_K$ telles que $\mathcal{B}\left[\frac{1}{\pi_i}\right] = \mathcal{A}_K$ où π_i est une uniformisante du corps K_i si $\mathcal{A}_K$ s'écrit en tant que K-algèbre $\mathcal{A}_K = K_1 \times \ldots \times K_g$, les K_i étant des extensions finies séparables de K.

Proposition 3.3.2.1. *La catégorie définie précédemment admet des produits finis. Autrement dit, l'ordre qui lui est associé admet des bornes supérieures finies.*

Commençons par construire les produits. On considère donc $(\mathcal{H}, \varphi_{\mathcal{H}})$ et $(\mathcal{H}', \varphi_{\mathcal{H}'})$ deux objets de notre catégorie. Le produit $\mathcal{H} \times_{\mathcal{O}_K} \mathcal{H}'$ a pour fibre générique $\mathcal{G}_K \times_K \mathcal{G}_K$ via le morphisme $\varphi_{\mathcal{H}} \times \varphi_{\mathcal{H}'}$. Le noyau $\mathcal{S}_K$ du morphisme $\mathcal{G}_K \times_K \mathcal{G}_K \to \mathcal{G}_K$, $(x, y) \mapsto x - y$, s'identifie à la diagonale de $\mathcal{G}_K \times_K \mathcal{G}_K$ et donc est isomorphe à $\mathcal{G}_K$. Notons $\mathcal{S}$ son adhérence schématique dans le produit $\mathcal{H} \times_{\mathcal{O}_K} \mathcal{H}'$. On vérifie immédiatement qu'il s'agit du produit recherché.

Remarquons que la dualité de Cartier (rappelée au tout début du paragraphe 3.4.3) prouve directement que la catégorie admet également des sommes finies.

On déduit de cette proposition que notre catégorie admet un objet final, c'est-à-dire l'ordre qui lui est associé admet un plus grand élément. En effet, il faut d'abord voir que toute chaîne strictement croissante de sous-$\mathcal{O}_K$-bigèbres de la fermeture intégrale de $\mathcal{O}_K$ dans $\mathcal{A}_K$ est finie. Cela provient du fait que $\mathcal{A}_K$ est un $\mathcal{O}_K$-module de type fini et donc en particulier en $\mathcal{O}_K$-module nœthérien. On est en fait ramené à démontrer un résultat très général sur les ensembles ordonnés.

Soit donc E un ensemble ordonné non vide. On veut prouver que si E n'admet pas de suite infinie strictement croissante et que si toute paire d'éléments de E admet une borne supérieure alors E admet un élément maximal. Bien entendu, le fait que la première hypothèse prouve ipso facto que toute chaine de E est majorée et donc que E admet un élément maximal par le lemme de Zorn. Il est toutefois possible de s'en passer dans ce cas particulier avec cette hypothèse bien plus forte. Pour cela, on choisit arbitrairement x_1 un élément de E. S'il est maximal on a trouvé ce que l'on cherchait. S'il ne l'est pas, on choisit $x_2 > x_1$ et on continue ainsi. L'hypothèse faite prouve que cette construction s'arrête au bout d'un nombre fini d'étapes[4]. Supposons maintenant que E admette deux éléments maximaux M_1 et M_2. Par hypothèse, il existe x à la fois plus grand que M_1 et M_2. En effet, il suffit de prendre pour M la borne supérieure de la paire $\{M_1, M_2\}$. Mais la maximalité nous dit que $M = M_1$ et d'autre part que $M = M_2$. Ainsi $M_1 = M_2$ et E admet un unique élément maximal que l'on va appeler M. Considérons maintenant $E' = \{x \in E,\ x \not\leqslant M\}$. On veut montrer que E' est vide. Supposons le contraire. E' n'admet pas plus que E de suite infinie strictement croissante. Donc, E' admet un élément maximal, disons M'. Prenons maintenant un $x \in E$. Si $x \in E'$ il ne peut pas être strictement supérieur à M'. Sinon, par définition $x \leqslant M$, ainsi si $x > M'$, on aurait $M' < M$, ce qui n'est pas possible puisque $M' \in E'$. De tout cela, on déduit que M' est un élément maximal de E et donc que $M = M'$, ce qui est absurde.

L'application de ce lemme à notre cas particulier assure l'existence d'un objet final à notre catégorie. On l'appelle le *prolongement maximal* de $\mathcal{G}_K$ à $\mathcal{O}_K$ et on le notera $\mathcal{G}_{\max}$. Là encore, grâce à la dualité de Cartier, on prouve que la catégorie admet également un objet initial qui s'appelle le *prolongement minimal* de $\mathcal{G}_K$ à $\mathcal{O}_K$ et que l'on notera $\mathcal{G}_{\min}$.

La bigèbre de $\mathcal{G}_{\min}$ est en fait assez facile à décrire. Notons pour cela, $\mathcal{B}_0$ la fermeture intégrale de $\mathcal{O}_K$ dans $\mathcal{A}_K$. Si K s'écrit $K = K_1 \times \ldots \times K_G$, $\mathcal{B}_0$ n'est autre que $\mathcal{O}_{K_1} \times \ldots \times \mathcal{O}_{K_g}$. Seulement B_0 n'est en général pas une bigèbre, il n'y a en effet aucune raison pour que la comultiplication c vérifie $c(\mathcal{B}_0 \otimes_{\mathcal{O}_K} \mathcal{B}_0) \subset \mathcal{B}_0$. Qu'à cela ne tienne, on construit une suite $\mathcal{B}_i$ par la formule suivante :

$$\mathcal{B}_{i+1} = \{b \in \mathcal{B}_i, \quad c(b) \in \mathcal{B}_i \otimes_{\mathcal{O}_K} \mathcal{B}_i\}$$

Il s'agit d'une suite décroissante et stationnaire. notons $\mathcal{B}_\infty$ sa limite, c'est-à-dire $\mathcal{B}_\infty = \cap_{n\in\mathbb{N}} B_n$. $\mathcal{B}_\infty$ est par construction $\mathcal{O}_K$-bigèbre. On peut montrer qu'il s'agit de la bigèbre associé au prolongement minimal $\mathcal{G}_{\min}$.

Il reste peut-être à souligner que pour avoir ces résultats, on a été obligé de supposer que le schéma $\mathcal{G}_K$ provenait d'un $\mathcal{O}_K$-schéma en groupe fini et plat. S'il n'en est pas ainsi, bien sûr, $\mathcal{G}_K$ ne va admettre ni de prolongement minimal ni de prolongement maximal puisque par hypothèse il n'admet aucun prolongement. Toutefois la construction précédente de $\mathcal{B}_\infty$ a encore un sens. Ce qu'il se passe alors, c'est que la suite des $\mathcal{B}_n$ n'est plus stationnaire mais strictement décroissante et que le bigèbre $\mathcal{B}_\infty$ ainsi construite va être de rang strictement inférieur à celui de $\mathcal{G}_K$, et donc ne pourra pas être un prolongement de $\mathcal{G}_K$.

Supposons maintenant qu'en plus $\mathcal{G}_K$ est muni d'une structure de schéma en $\mathbb{F}_q$-vectoriel. Alors comme nous l'avons déjà dit, il n'est pas vrai en général que celle-ci se prolonge à $\mathcal{G}$ mais cela devient vrai avec les schémas en groupe $\mathcal{G}_{\min}$ et $\mathcal{G}_{\max}$. Pour voir cela, il suffit de constater que tout automorphisme de $\mathcal{G}$ peut se prolonger en un automorphisme de $\mathcal{G}_{\min}$ et $\mathcal{G}_{\max}$ et cela se voit formellement par exemple au niveau des bigèbres.

[4]Il est amusant de remarquer que cette démonstration se généralise en ces termes pour prouver le lemme de Zorn. Cependant, on n'est pas ce coup-ci assuré de terminer en un nombre fini d'étapes, il faut continuer cette construction transfiniment.

Récapitulons finalement ce que l'on a vu dans ce paragraphe au moyen de la proposition suivante :

Proposition 3.3.2.2. *Soit $\mathcal{G}_K$ un K-schéma en groupe commutatif fini (et donc plat). On a alors l'alternative suivante. Soit $\mathcal{G}_K$ ne provient pas d'un schéma en groupe commutatif fini et plat sur $\mathcal{O}_K$, soit c'est le cas et alors parmi tous les prolongements possibles, il y en a deux particuliers notés $\mathcal{G}_{min}$ et $\mathcal{G}_{max}$ caractérisés par le fait que si $\mathcal{G}$ est un autre prolongement fini et plat de $\mathcal{G}_K$, il existe un unique diagramme $\mathcal{G}_{max} \to \mathcal{G} \to \mathcal{G}_{min}$ qui induit l'identité de $\mathcal{G}_K$ après extension des scalaires. Si en outre, $\mathcal{G}_K$ est muni d'une structure de $\mathbb{F}_q$-vectoriel, celle-ci se transmet aux schémas en groupe $\mathcal{G}_{min}$ et $\mathcal{G}_{max}$.*

3.3.3 Fin de la preuve

Rappelons l'endroit où nous avions abouti dans la démonstration. On a vu que l'on pouvait sans perte de généralité supposer $K = \widehat{K^{\mathrm{nr}}}$ et donc que la représentation ρ' introduite dans l'introduction de ce chapitre correspondait à un certain schéma en $\mathbb{F}_q$-vectoriel de dimension 1 sur K, que l'on va appeler $\mathcal{G}_K$ à partir de maintenant. On a également vu que ce schéma admettait un prolongement $\mathcal{G}$ à $\mathcal{O}_K$. D'après la proposition précédente, on peut supposer que la structure de $\mathbb{F}_q$-espace vectoriel s'étend également à $\mathcal{G}$.

On est alors presque dans la situation étudiée dans le chapitre précédemment. Notons $\mathcal{A}$ la bigèbre de $\mathcal{G}$, $\mathcal{I}$ son idéal d'augmentation et $[\lambda] : \mathcal{A} \to \mathcal{A}$ le morphisme donnant l'action de $\lambda \in \mathbb{F}_q$. Si χ est un caractère de $\mathbb{F}_q$ à valeurs dans $\mathcal{O}_K$, on note encore

$$i_\chi = \frac{1}{q-1} \sum_{\lambda \in \mathbb{F}_q^\star} \chi^{-1}(\lambda)\,[\lambda]$$

et finalement $\mathcal{I}_\chi = i_\chi(\mathcal{I})$. Il reste alors juste à vérifier que les $\mathcal{I}_\chi$ sont des $\mathcal{O}_K$-modules libres de dimension 1. Tout d'abord les $\mathcal{I}_\chi$ sont des facteurs directs de $\mathcal{A}$ qui est libre sur un anneau principal. On en déduit que les $\mathcal{I}_\chi$ sont libres. La dimension des $\mathcal{I}_\chi$ n'est pas modifiée par changement de base, il suffit donc par exemple de la calculer pour le $\bar{K}$-schéma en $\mathbb{F}_q$-vectoriel $\mathcal{G}_{\bar{K}} = \mathcal{G} \otimes_{\mathcal{O}_K} \bar{K} = \mathcal{G}_K \otimes_K \bar{K}$. Mais, ce schéma est étale[5] et puis constant, puisque le groupe de Galois absolu de $\bar{K}$ est trivial et donc tous les ensembles à q éléments munis d'une action de ce groupe sont isomorphes. On conclut alors par l'équivalence de catégorie énoncée par la proposition 3.1.4.4. On a déjà fait le calcul pour le groupe constant et on avait alors vérifié que les $\mathcal{I}_\chi$ étaient bien de dimension 1. On peut donc utiliser la description donnée dans le paragraphe 3.2.7.

On peut trouver des couples (δ_i, γ_i) d'éléments de $\mathcal{O}_K$ vérifiant $\delta_i \gamma_i = \omega$ tels que $\mathcal{A}$ soit en tant que $\mathcal{O}_K$-algèbre engendré par des générateurs X_i, i variant dans $\mathbb{Z}/r\mathbb{Z}$, soumis aux seules relations $X_i^p = \delta_i X_{i+1}$. On rappelle que ω a été défini dans le chapitre précédent, tout ce dont on aura besoin par la suite sera de savoir que $v(\omega) = e_K$, l'indice de ramification absolu du corps K. On rappelle également que l'action de $\lambda \in \mathbb{F}_q$ sur $\mathcal{A}$ se traduit par la formule suivante :

$$[\lambda]\left(X_1^{n_1} \dots X_r^{n_r}\right) = \left(\chi_1^{n_1} \dots \chi_r^{n_r}\right)(\lambda) \cdot X_1^{n_1} \dots X_r^{n_r}$$

valable pour tout r-uplet d'entiers compris entre 0 et $p-1$, $(n_1, \dots, n_r)$. On avait également établi une formule pour la comultiplication mais étant donné que nous n'aurons pas à l'utiliser, nous ne la rappelons pas ici.

Par définition le caractère fondamental $\chi_1 : \mathbb{F}_q \to \mathcal{O}_K$ est additif. Il fournit donc, après réduction modulo l'idéal maximal $\mathfrak{m}_K$, un isomorphisme de corps entre $\mathbb{F}_q$ et $\mu_{q-1}\left(\bar{k}\right)$ auquel on a pris soin d'ajouter 0. On notera $\chi_1^{-1} : \mu_{q-1}\left(\bar{k}\right) \to \mathbb{F}_q^\star$ l'isomorphisme réciproque. Encore par définition et en reprenant les notations du paragraphe 3.1.3, $\psi_1 = \chi_1^{-1} \circ \theta_{q-1}$ est un caractère fondamental de I_m à valeurs dans $\mathbb{F}_q^\star$. Les autres caractères fondamentaux sont les $\psi_i = \psi_1^{p^i}$ pour i variant dans $\mathbb{Z}/r\mathbb{Z}$.

[5] Il s'agit encore du théorème de Deligne.

D'autre part, l'espace vectoriel sous-jacent à la représentation ρ' est le $\mathbb{F}_q$-espace vectoriel de dimension 1 de $\bar{K}$-points de $\mathcal{G}_K$, $\mathcal{G}_K$ qui bien entendu est décrit par la même présentation que $\mathcal{G}$. Notons $\mathcal{A}_K$ sa bigèbre et $V' = \mathrm{Hom}_{K-\mathrm{alg}}\left(\mathcal{A}_K, \bar{K}\right) = \mathrm{Hom}_{K-\mathrm{alg}}\left(\mathcal{A}_K, K^{\mathrm{mr}}\right)$ l'espace vectoriel en question. L'action de $\sigma \in I_m$ sur V' est simplement la composition. Autrement dit ρ' est simplement l'application :

$$\rho' : \left(\begin{array}{ccc} I_m & \to & \mathrm{GL}\left(V'\right) \\ \sigma & \mapsto & \left(f \mapsto \sigma \circ f\right) \end{array} \right)$$

Les caractères fondamentaux de I_m à valeurs dans $\mathrm{GL}\left(V'\right)$ peuvent se décrire via la bijection φ suivante qui est par définition additive :

$$\varphi : \left(\begin{array}{ccc} \mathbb{F}_q^\star & \to & \mathrm{GL}\left(V'\right) \\ \lambda & \mapsto & \left(f \mapsto f \circ [\lambda]\right) \end{array} \right)$$

Il nous faut donc calculer l'application composée $\varphi^{-1} \circ \rho'$. L'image de $\sigma \in I_m$ par cette application est l'unique λ faisant commuter le diagramme suivant :

$$\begin{array}{ccc} \mathcal{A}_K & \xrightarrow{f} & \bar{K} \\ {\scriptstyle [\lambda]}\downarrow & & \downarrow{\scriptstyle \sigma} \\ \mathcal{A}_K & \xrightarrow{f} & \bar{K} \end{array}$$

pour tout élément f de V'. Pour le déterminer, il nous suffira de comparer l'image de $X_1 \in \mathcal{A}_K$ par les deux chemins envisageables. Notons pour cela $x_i = f\left(X_i\right)$. Ces éléments sont soumis aux relations :

$$\begin{array}{rcl} x_1^p & = & \delta_1 x_2 \\ x_2^p & = & \delta_2 x_3 \\ & \vdots & \\ x_r^p & = & \delta_r x_1 \end{array}$$

Cela implique en particulier que x_1 est solution de l'équation

$$x_1^q = \delta_1^{p^{r-1}} \delta_2^{p^{r-2}} \ldots \delta_r \cdot x_1$$

et puis que l'action de σ sur x_1 est

$$\sigma\left(x_1\right) = \theta_{q-1}\left(\sigma\right)^{v\left(\delta_1^{p^{r-1}} \delta_2^{p^{r-2}} \ldots \delta_r\right)} \cdot x_1 = \theta_{q-1}\left(\sigma\right)^{p^{r-1} v(\delta_1) + p^{r-2} v(\delta_2) + \ldots + v(\delta_r)} \cdot x_1$$

La commutativité de précédent diagramme se traduit donc par la formule :

$$\theta_{q-1}\left(\sigma\right)^{p^{r-1} v(\delta_1) + p^{r-2} v(\delta_2) + \ldots + v(\delta_r)} \cdot x_1 = \chi_1\left(\lambda\right) \cdot x_1$$

Bien entendu, on a toute liberté pour choisir f et donc on peut prendre un $x_1 \neq 0$. On en déduit que :

$$\lambda = \psi_r\left(\sigma\right)^{v(\delta_1)} \ldots \psi_1\left(\sigma\right)^{v(\delta_r)}$$

On vient ainsi de décomposer $\varphi^{-1} \circ \rho'$ sur les caractères fondamentaux. Les exposants qui apparaissent sont les $v\left(\delta_i\right)$, il ne reste plus qu'à voir que ces nombres sont inférieurs ou égaux à e_K. Mais il suffit pour cela de se rappeler que l'on avait $\delta_i \gamma_i = \omega$ où $\gamma_i \in \mathcal{O}_K$ et $v\left(\omega\right) = e_K$. Ceci termine la première démonstration du théorème principal.

3.3.4 Quelques compléments

Nous allons voir dans ce paragraphe que dans le cas où $e_K < p-1$ la catégorie des $\mathcal{O}_K$-schémas en groupe commutatif finis et plats annulés par une puissance de p est abélienne. Nous allons pour cela la comparer à la catégorie des K-schémas en groupe commutatif finis annulés par une puissance de p dont on peut voir facilement qu'elle l'est via l'équivalence de catégories avec les représentations de $\mathrm{Gal}\left(\bar{K}/K\right)$.

Montrons dans un premier temps que tout K-schéma en groupe commutatif fini annulé par une puissance de p admet au plus un prolongement à $\mathcal{O}_K$. On prouve cela par récurrence sur la longueur du schéma en question. Prenons donc pour commencer $\mathcal{G}_K$, un K-schéma en groupe commutatif fini simple annulé par une puissance de p et supposons qu'il provienne d'un schéma en groupe commutatif fini et plat $\mathcal{G}$ sur $\mathcal{O}_K$. Le fait que $\mathcal{G}_K$ soit simple prouve dans un premier temps, qu'il est en fait annulé par p, et donc un schéma en $\mathbb{F}_p$-vectoriel. On a alors vu que dans ce cas, $\mathcal{G}_K$ hérite directement d'une structure de schéma en $\mathbb{F}_q$-vectoriel pour lequel il est de dimension 1, où $q = p^r$ est une certaine puissance de p. Cette structure se transporte aux $\mathcal{O}_K$-schémas en groupe commutatif finis et plats $\mathcal{G}_{\min}$ et $\mathcal{G}_{\max}$ définis précédemment. On va prouver qu'en fait $\mathcal{G}_{\min}$ et $\mathcal{G}_{\max}$ sont isomorphes, ce qui entrainera bien l'unicité du prolongement de $\mathcal{G}_K$ à l'anneau des entiers $\mathcal{O}_K$.

On aimerait pour cela appliquer la classification du paragraphe 3.2.7, il nous faut donc vérifier les hypothèses nécessaires, ce qui se fait sans problèmes comme dans le paragraphe précédent. Ainsi, en notant $\mathcal{A}_{\min}$ (resp. $\mathcal{A}_{\max}$) la bigèbre de $\mathcal{G}_{\min}$ (resp. $\mathcal{G}_{\max}$), il existe r couples d'éléments de $\mathcal{O}_K$ (δ_i, γ_i) (resp. (Δ_i, Γ_i)) vérifiant $\delta_i\gamma_i = \omega$ (resp. $\Delta_i\Gamma_i = \omega$ tels que la bigèbre $\mathcal{A}_{\min}$ (resp. $\mathcal{A}_{\max}$) est engendrée par des éléments x_i (resp. X_i) pour i variant dans $\mathbb{Z}/r\mathbb{Z}$ soumis aux seules relations $x_i^p = \delta_i x_{i+1}$ (resp. $X_i^p = \Delta_i X_{i+1}$).

Le fait que les fibres génériques de $\mathcal{G}_{\min}$ et $\mathcal{G}_{\max}$ soient isomorphes à $\mathcal{G}_K$ et donc entre elles entraîne conformément au théorème 3.2.7.1 l'existence d'éléments $u_i \in K$ tels que $\delta_i = u_i^p \Delta_i u_{i+1}^{-1}$. En outre, comme il existe un $\mathcal{O}_K$-morphisme de $\mathcal{G}_{\max}$ dans $\mathcal{G}_{\min}$, on a $v(u_i) \geqslant 0$ pour tout i. Autrement dit $u_i \in \mathcal{O}_K$. Considérons maintenant un indice i pour lequel $v(u_i)$ est maximal. On a alors :

$$e \geqslant v(\delta_i) = pv(u_i) + v(\Delta_i) - v(u_{i+1}) \geqslant (p-1)\, v(u_i)$$

On en déduit que $v(u_i) \leqslant \frac{e}{p-1} < 1$. Il en résulte qu'en fait $v(u_i) = 0$, autrement dit que u_i est une unité de $\mathcal{O}_K$, puis qu'il en est de même pour tous les u_i. Ceci prouve à nouveau en vertu du théorème 3.2.7.1 que $\mathcal{G}_{\min}$ et $\mathcal{G}_{\max}$ sont isomorphes et finalement que le prolongement de $\mathcal{G}_K$ à $\mathcal{O}_K$ est unique.

Poursuivons la récurrence. Prenons donc $\mathcal{G}_K$ un K-schéma en groupe commutatif fini annulé par une puissance de p de longueur n. $\mathcal{G}_K$ admet un sous-groupe simple, disons $\mathcal{H}_K$. La catégorie des K-schémas en groupe commutatif fini étant abélienne, le quotient $\mathcal{G}_K/\mathcal{H}_K$ est bien défini et on a la suite exacte suivante :

$$0 \longrightarrow \mathcal{H}_K \longrightarrow \mathcal{G}_K \longrightarrow \mathcal{G}_K/\mathcal{H}_K \longrightarrow 0$$

Supposons que $\mathcal{G}_K$ admette deux prolongement $\mathcal{G}$ et $\mathcal{G}'$ à $\mathcal{O}_K$. $\mathcal{H}_K$ étant un sous-groupe fermé de $\mathcal{G}_K$, on peut considérer son adhérence schématique $\mathcal{H}$ dans $\mathcal{G}$. Le quotient $\mathcal{G}/\mathcal{H}$ est alors défini et est un $\mathcal{O}_K$-schéma en groupe commutatif fini et plat annulé par une puissance de p. De même, on construit $\mathcal{H}'$ et $\mathcal{G}'/\mathcal{H}'$. Les groupes $\mathcal{H}$ et $\mathcal{H}'$ sont de longueur strictement inférieure à n, ils sont donc isomorphes d'après l'hypothèse de récurrence. Il en est de même de $\mathcal{G}/\mathcal{H}$ et de $\mathcal{G}'/\mathcal{H}'$. Si l'on suppose en outre que l'on a un morphisme de $\mathcal{G}'$ dans $\mathcal{G}$ faisant commuter le diagramme suivant :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{H}' & \longrightarrow & \mathcal{G}' & \longrightarrow & \mathcal{G}'/\mathcal{H}' & \longrightarrow & 0 \\
 & & \sim\downarrow & & \downarrow & & \downarrow\sim & & \\
0 & \longrightarrow & \mathcal{H} & \longrightarrow & \mathcal{G} & \longrightarrow & \mathcal{G}/\mathcal{H} & \longrightarrow & 0
\end{array}$$

on peut conclure en voyant les objets du diagramme simplement comme des faisceaux et en leur appliquant le lemme des cinq. Pour le cas général, on considère la borne supérieure de $\mathcal{G}$ et de $\mathcal{G}'$ définie par la proposition 3.3.2.1 qui est naturellement munie de flèches vers $\mathcal{G}$ et $\mathcal{G}'$. On applique alors deux fois le résultat précédent pour conclure.

On déduit plus ou moins de cela la proposition suivante :

Proposition 3.3.4.1. *Soient $\mathcal{G}$ et $\mathcal{H}$ deux $\mathcal{O}_K$-schémas en groupe commutatif finis et plats annulés par une puissance de p. On note $\mathcal{G}_K$ (resp. $\mathcal{H}_K$) la fibre générique de $\mathcal{G}$ (resp. $\mathcal{H}$). Dans ces conditions, tout morphisme de $\mathcal{G}_K$ dans $\mathcal{H}_K$ se remonte de façon unique en un morphisme de $\mathcal{G}$ dans $\mathcal{H}$. En outre, le noyau de le conoyau de ce dernier morphisme sont plats sur $\mathcal{O}_K$.*

Cette proposition dit en fait exactement que le foncteur extension des scalaires des $\mathcal{O}_K$ à K allant de la catégories des $\mathcal{O}_K$-schémas en groupe commutatif finis et plats annulés par une puissance de p dans celle des K-schémas en groupe commutatif finis annulés par une puissance de p est pleinement fidèle et que son image essentielle est stable par noyau et conoyau. Le fait que nous voulions prouver en résulte.

Il est intéressant de remarquer que ce résultat devient faux dès que $e_K \geqslant p-1$. En effet, en faisant un raisonnement analogue à celui présenté au début de ce paragraphe, on peut prouver dans ce cas qu'il existe un K-schéma en groupe commutatif fini et plat annulé par une puissance de p, disons $\mathcal{G}_K$, qui peut se prolonger à $\mathcal{O}_K$ mais pour lequel les prolongements minimal et maximal ne sont pas isomorphes. On prouve alors que l'unique flèche de $\mathcal{G}_{\max}$ dans $\mathcal{G}_{\min}$ qui n'est pas un isomorphisme est à la fois un monomorphisme et un épimorphisme.

3.4 Une classification plus complète des schémas en groupe sur $\mathcal{O}_K$

Certes, la classification de Raynaud nous a suffi pour démontrer le théorème central de ce mémoire, mais ce dernier prête facilement à généralisation et dans ce cas, la méthode précédemment proposée devient impuissante. Nous allons donc proposer une classification beaucoup plus générale des schémas en groupe commutatif finis et plats sur l'anneau des entiers $\mathcal{O}_K$. Il va falloir procéder par étape. On va tout d'abord donner une description assez explicite de cet anneau $\mathcal{O}_K$ au moins quand l'indice de ramification absolu du corps K est 1. On donnera ensuite une classification des schémas en groupe commutatif finis (forcément plats) sur le corps résiduel k. On sera alors en mesure d'établir une équivalence de catégories entre la catégorie des $\mathcal{O}_K$-schémas en groupe commutatif finis et plats et une autre dont les objets sont a priori plus simples à manipuler, dans un premier temps dans le cas où l'indice de ramification e_K vaut 1, puis ensuite dans le cas où $e_K < p-1$.

3.4.1 L'anneau des vecteurs de Witt

Le but de ce paragraphe est, étant donné un corps k parfait de caractéristique p, de construire un anneau de valuation discrète et de caractéristique nulle $W(k)$, qui soit non ramifié (ce qui signifie que p est une uniformisante de $W(k)$) et de corps résiduel k. L'idée pour faire cela est de rappeler que l'on peut décrire $\mathbb{Z}_p$ comme les suites infinies de chiffres (souvent écrites de droite à gauche) de $\mathbb{F}_p$ que l'on ajoute et multiplie avec les mêmes règles que celles qui nous ont été enseignées dans notre jeunesse à l'école. Ainsi, copiant cela, on va considérer l'ensemble des suites à valeur dans le corps k et essayer de le munir d'une structure d'anneau de valuation discrète, la valuation étant le nombre de termes nuls qui débutent la suite.

Pour faire cela, il va falloir nous donner un niveau de généralité supplémentaire. En fait, on ne va pas définir $W(k)$ pour tout corps k parfait de caractéristique p mais plutôt pour tout anneau A. En

tant qu'ensemble on définit $W(A)$ comme l'ensemble des suites à valeurs dans A. W ainsi défini est même un foncteur d'une façon évidente. Pour définir les lois de composition, on commence par définir les applications suivantes appelées les *composantes fantômes* :

$$\Phi_n(A) : \left(\begin{array}{ccc} W(A) & \longrightarrow & A \\ (a_0, \ldots, a_n, \ldots) & \mapsto & a_0^{p^n} + p a_1^{p^{n-1}} + \ldots + p^{n-1} a_{n-1}^p + p^n a_n \end{array} \right)$$

Ce que l'on veut faire c'est mettre sur tout $W(A)$ une structure d'anneaux qui soit telle que le foncteur W soit un foncteur de la catégorie des anneaux et qui soit telle également que les W_n que l'on vient de définir soient des transformations naturelles entre W et le foncteur identité. Autrement dit, on souhaite que dans le diagramme suivant, tous les flèches soient des homomorphismes d'anneaux et que de surcroît il commute, et ce pour tout morphisme d'anneaux $f : A \to B$ et tout entier n.

$$\begin{array}{ccc} W(A) & \xrightarrow{\Phi_n(A)} & A \\ {\scriptstyle W(f)}\downarrow & & \downarrow{\scriptstyle f} \\ W(B) & \xrightarrow{\Phi_n(B)} & B \end{array}$$

Mais voyons comment cela impose et définit une structure d'anneaux sur tous les $W(A)$. Prenons donc un anneau A et deux éléments $a = (a_0, \ldots, a_n, \ldots)$ et $b = (b_0, \ldots, b_n, \ldots)$ de $W(A)$. Écrivons $s = a + b = (s_0, \ldots, s_n, \ldots)$ et $p = ab = (p_0, \ldots, p_n, \ldots)$ et voyons comment se traduisent nos conditions sur les s_n et les p_n. Dire que Φ_0 est un morphisme d'anneaux fournit directement $s_0 = a_0 + b_0$ et $p_0 = a_0 b_0$, ce qui est raisonnable, pour multiplier deux nombres, on commence par multiplier leur chiffre des unités. Le morphisme Φ_1 donne les conditions

$$\begin{array}{rcl} s_0^p + s_1 p & = & a_0^p + a_1 p + b_0^p + b_1 p \\ p_0^p + p_1 p & = & (a_0^p + a_1 p)(b_0^p + b_1 p) \end{array}$$

Si p est inversible dans A, ces équations se résolvent et on trouve :

$$\begin{array}{rcl} s_1 & = & a_1 + b_1 - \dfrac{(a_0 + b_0)^p - a_0^p - b_0^p}{p} \\ p_1 & = & a_1 b_0^p + a_0^p b_1 + a_1 b_1 p \end{array}$$

Ainsi, au moins lorsque p est inversible dans A (et cela explique pourquoi l'on avait besoin d'un plus grand degré de généralité), ces deux expressions définissent s_1 et p_1 de façon unique. On voit même bien que par récurrence l'on va trouver une formule polynômiale qui définit de façon unique s_n et p_n pour tout entier n, disons $s_n = S_n(a_0, \ldots, a_n, b_0, \ldots, b_n) = S_n(a, b)$ et $p_n = P_n(a_0, \ldots, a_n, b_0, \ldots, b_n) = P_n(a, b)$, S_n et P_n étant a priori des polynômes à coefficients dans $\mathbb{Z}\left[\frac{1}{p}\right]$. Ceci n'est donc à première vue valable que si p est inversible dans A. Cependant, comme on peut déjà le remarquer pour s_1 et p_1 les polynômes qui vont intervenir vont en fait être à coefficients dans $\mathbb{Z}$. On montre ce fait en général en procédant à diverses estimations de valuation. Cela est un peu pénible et nous n'allons pas le faire.

Toutefois pour l'addition, il est possible de parvenir à cette conclusion par une autre voie que nous allons présenter. On va supposer que A est un anneau dans lequel tout entier non nul est inversible. On considère $\Lambda(A) = 1 + tA[\![t]\!]$. C'est un groupe pour la multiplication. On regarde alors l'application :

$$E : \left(\begin{array}{ccc} W(A) & \longrightarrow & \Lambda(A) \\ a = (a_0, \ldots, a_n, \ldots) & \mapsto & \exp\left(-\Phi_0(a)\, t - \Phi_1(a)\, \frac{t^p}{p} - \ldots - \Phi_n(a)\, \frac{t^{p^n}}{p^n} - \ldots \right) \end{array} \right)$$

On remarque tout d'abord que cette application est bien défini car il n'est nécessaire que faire qu'un nombre fini d'opérations pour calculer un coefficient donné. Bien entendu E est un morphisme de groupes. Nous allons donner une nouvelle expression de E. Calculons donc :

$$\begin{aligned} E(a) &= \exp\left(-a_0 - (a_0^p + a_1 p)\frac{t^p}{p} - \left(a_0^{p^2} + p a_1^p + p^2 a_2\right)\frac{t^{p^2}}{p^2} - \dots\right) \\ &= \exp\left(-a_0 t - \frac{(a_0 t)^p}{p} - \frac{(a_0 t)^{p^2}}{p^2} - \dots - a_1 t^p - \frac{(a_1 t^p)^p}{p} - \frac{(a_1 t^p)^{p^2}}{p^2} - \dots - \dots\right) \\ &= F(a_0 t)\, F(a_1 t^p) \dots F(a_n t^{p^n}) \dots \end{aligned}$$

où l'on a pris soin de poser :

$$F(x) = \exp\left(-x - \frac{x^p}{p} - \dots - \frac{x^{p^n}}{p^n} - \dots\right)$$

On se rappelle maintenant que l'on dispose de la formule suivante :

$$\exp(-x) = \prod_{n \geqslant 1} (1 - x^n)^{\mu(n)/n}$$

où μ désigne la fonction d'inversion de Moëbius. Rappelons comment elle est définie. Par définition, $\mu(1) = 1$. Si $p_1, \dots, p_r$ sont des nombres premiers distincts, $\mu(p_1 \dots p_r) = (-1)^r$ et sinon, c'est-à-dire, dès que n est divisible par un carré distinct de 1, $\mu(n) = 0$. Elle vérifie la relation suivante valable pour tout $n > 1$:

$$\sum_{d|n} \mu(d) = 0$$

On peut maintenant démontrer la formule que nous venons de rappeler. Il suffit pour cela de prendre le logarithme et de développer. On obtient :

$$\sum_{n \geqslant 1} \frac{\mu(n)}{n} \log(1 - x^n) = -\sum_{n \geqslant 1} \frac{\mu(n)}{n} \sum_{m \geqslant 1} \frac{x^{nm}}{m} = -\sum_{n \geqslant 1} \sum_{d|n} \mu(d) \frac{x^n}{n} = -x$$

En fait, on a une décomposition similaire en produit pour la fonction F. Il s'agit de :

$$F(x) = \prod_{\text{PGCD}(n,p)=1} (1 - x^n)^{\mu(n)/n}$$

Pour voir cela, on écrit simplement :

$$\prod_{\text{PGCD}(n,p)=1} (1 - x^n)^{\mu(n)/n} = \exp(-x) \prod_{n \geqslant 1} (1 - x^{pn})^{-\mu(pn)/pn}$$

Or par définition de μ, $\mu(pn)$ vaut 0 si n est un multiple de p et vaut $-\mu(n)$ sinon. On obtient ainsi :

$$\begin{aligned} \prod_{\text{PGCD}(n,p)=1} (1 - x^n)^{\mu(n)/n} &= \exp(-x) \prod_{\text{PGCD}(n,p)=1} (1 - x^{pn})^{\mu(n)/pn} \\ &= \exp\left(-x - \frac{x^p}{p}\right) \prod_{\text{PGCD}(n,p)=1} \left(1 - x^{p^2 n}\right)^{\mu(n)/p^2 n} = \dots = F(x) \end{aligned}$$

Cette dernière expression prouve qu'en fait les coefficients de la série entière F dans l'anneau $\mathbb{Z}_{(p)}$, le localisé de $\mathbb{Z}$ en l'idéal premier $p\mathbb{Z}$. Le fait que E soit un homomorphisme de groupes se traduit par l'égalité :

$$F(a_0 t)\, F(b_0 t) \ldots F(a_n t^{p^n}) F(b_n t^{p^n}) \ldots = F(S_0(a,b)\, t) \ldots F(S_n(a,b)\, t^{p^i}) \ldots$$

La valuation p-adique du terme de gauche est nulle comme on vient de le voir. La valuation de $F(S_i(a,b))$, quant à elle, est négative ou nulle. On déduit qu'elle est en fait nulle et donc que celle de $S_i(a,b)$ est positive, ce qui est bien ce que l'on voulait voir.

On peut définir des "endormorphismes" sur W. Il y a tout d'abord celui que l'on appelle le *Verschiebung* ou encore la *translation*. Si A est un anneau, il est simplement donné par :

$$V(A)(a_0, \ldots, a_n, \ldots) = (0, a_0, \ldots, a_n, \ldots)$$

Sur les composantes fantômes, $V(A)$ agit par $\Phi_n(V(A)(a)) = p\Phi_{n-1}(a)$ pour tout $n \geqslant 1$ et $\Phi_0(V(A)(a)) = 0$. Il faut faire attention que $V(A)$ n'est pas un homomorphisme d'anneaux, il est simplement additif. V définit donc une transformation naturelle de W vu comme foncteur de la catégorie des anneaux dans celles des groupes abéliens.

On peut également définir ce que l'on appelle le *Frobenius*. Il s'agit ce coup-ci d'une véritable transformation naturelle du foncteur W. Il est défini par son action sur les composantes fantômes. Autrement dit F est l'unique transformation naturelle de W faisant commuter le diagramme suivant pour tout entier n :

$$\begin{array}{ccc} W(A) & \xrightarrow{\Phi_n(A)} & A \\ {\scriptstyle F(A)}\downarrow & & \| \\ W(A) & \xrightarrow{\Phi_{n-1}(A)} & A \end{array}$$

Il n'est pas facile de donner une formule explicite décrivant F dans le cas général. Toutefois, si A est de caractéristique p, cette formule existe comme nous allons le voir tout à l'heure.

Comme on le voit sur les composantes fantômes, le composée de F est de V dans un sens se calcule bien. Plus précisément, de façon générale, $F \circ V$ n'est autre que la multiplication par p.

Il est également possible de définir ce que l'on appelle l'anneau des vecteurs de Witt *tronqués*. Pour tout anneau A, on définit $W_n(A)$ comme l'ensemble des $n+1$-uplets $(a_0, \ldots, a_n)$ d'éléments de A que l'on munit des opérations décrites par les polynômes S_i et P_i précédemment introduits. On a une suite exacte de groupes abéliens valable pour tout anneau A :

$$0 \longrightarrow W(A) \xrightarrow{V(A)^n} W(A) \longrightarrow W_n(A) \longrightarrow 0$$

tout cela étant fonctoriel en A. La flèche de $W(A)$ dans $W_n(A)$ consiste simplement à tronquer la suite aux $n+1$ premiers termes. $W(A)$ s'identifie à la limite projective des $W_n(A)$ pour les morphismes canoniques $W_{n+1}(A) \to W_n(A)$.

Finalement, on dispose d'une section mutliplicative de la projection $W(A) \to A$ qui consiste à envoyer une suite $(a_0, \ldots, a_n, \ldots)$ sur a_0. Il s'agit bêtement de l'application qui à $a \in A$ fait correspondre l'élément $[a] = (a, 0, \ldots, 0, \ldots)$. $[a]$ s'appelle le *représentant de Teichmüller* de A.

3.4.2 En caractéristique p

Il est un peu plus aisé de décrire les choses lorsque A est un anneau de caractéristique p, c'est ce que nous allons faire. Tout d'abord les composantes fantômes s'expriment simplement, on a $\Phi_n(a) = a_0^{p^n}$ si $a = (a_0, \ldots, a_n, \ldots)$. Toutefois elles n'ont plus un intêret immense.

Le Frobenius quant à lui s'exprime désormais de façon sympathique. En effet, on a la formule :

$$F(a_0, \ldots, a_n, \ldots) = (a_0^p, \ldots, a_n^p, \ldots)$$

et l'on comprend désormais pourquoi on a appelé cet endomorphisme ainsi. La relation $F \circ V = p$ permet d'exprimer la multiplication par p de façon simple :

$$p(a_0, \ldots, a_n, \ldots) = (0, a_0^p, \ldots, a_n^p, \ldots)$$

On remarque déjà que ces écritures entraînent que non seulement $F \circ V = p$ mais également que $V \circ F = p$.

Supposons désormais que k soit un corps parfait de caractéristique p. $W(k)$ peut alors être muni d'une valuation discrète, la valuation de la suite $(a_0, \ldots, a_n, \ldots)$ étant le plus petit entier n tel que $a_n \neq 0$. Le corps résiduel s'identifie à k et la projection canonique est, comme précédemment, l'application qui envoie $(a_0, \ldots, a_n, \ldots)$ sur a_0. En réalité $W(k)$ est complet pour cette valuation. On a plus précisément le théorème suivant :

Théorème 3.4.2.1. *Soient k un corps parfait de caractéristique p et A un anneau local nœthérien complet de corps résiduel k. Notons $\pi : A \to k$ la projection canonique. Il existe alors un* unique *homomorphisme d'anneaux $u : W(k) \to A$ qui fasse commuter*

$$\begin{array}{ccc} W(k) & \xrightarrow{u} & A \\ \downarrow & & \downarrow \pi \\ k & = & k \end{array}$$

Si en outre, A est un anneau de valuation discrète de caractéristique nulle, il devient par u un $W(k)$ module libre de rang $e_A = v_A(p)$ où v_A est la valuation normalisée sur A.

On suppose que k est un corps parfait de caractéristique p. D'après les descriptions précédentes, l'image de $V(k)$ coïncide avec celle de la multiplication par p. En particulier $W_n(k)$ s'identifie au quotient $W(k)/p^n W(k)$.

On est maintenant en mesure de donner un nouveau point de vue sur l'anneau des vecteurs de Witt à coefficients dans k parfait de caractéristique p. Prenons A un anneau complet pour une valuation discrète de corps résiduel k admettant p pour uniformisante. On vient de voir que A et $W(k)$ sont canoniquement isomorphes. En particulier, si $a \in k$, on peut définir le représentant de Teichmüller de a comme un élément de A. Il existe une façon plus intrinsèque de voir cela. Prenons a un élément de k. Pour tout entier n, considérons $x_n = a_n^p$ où a_n est un relèvement arbitraire de a^{1/p^n} (cela existe et est unique car k est supposé parfait de caractéristique p). On montre que la suite x_n est de Cauchy et donc converge. Sa limite est le représentant de Teichmüller de a. Nous le noterons encore $[a]$. Mais maintenant, l'ensemble des $[a]$ pour a décrivant k forme un système de représentant de A pour la relation de congruence modulo p. Donc, par un lemme connu, tout élément $x \in A$ s'écrit comme limite d'une série convergeante :

$$x = \sum_{n \geqslant 0} [a_n] p^n$$

pour des éléments $a_n \in k$. Il n'est pas difficile de voir alors que l'élément x vu dans $W(k)$ via l'isomorphisme canonique n'est autre que $a = (a_0, \ldots, a_n^{p^n}, \ldots)$. En particulier, les polynômes S_n disent comment se comportent les représentants de Teichmüller vis-à-vis de l'addition.

L'exemple primordial à donner est sans doute celui de $k = \mathbb{F}_p$. $W(k)$ s'identifie alors à l'anneau $\mathbb{Z}_p$ et $W_n(k)$ s'identifie à $\mathbb{Z}/p^n\mathbb{Z}$. Le Frobenius n'est alors autre que l'identité et en conséquence le Verschiebung correspond à la multiplication par p.

3.4.3 Décomposition des k-schémas en groupe commutatif finis

Faisons tout d'abord quelques rappels généraux sur les schémas en groupe commutatif. Soit A un anneau. Un *schéma en groupe commutatif* sur A est simplement la donnée d'un schéma $\mathcal{G}$ sur $\operatorname{Spec} A$ et d'un morphisme $m : \mathcal{G} \times_A \mathcal{G} \to G$ vérifiant les axiomes usuels de groupe commutatif. Si $\mathcal{G}$ est affine sur $\operatorname{Spec} A$, on a $\mathcal{G} = \operatorname{Spec} B$ pour une certaine A-algèbre B. La structure de groupe commutatif sur $\mathcal{G}$ va alors se transformer en une structure de cogèbre de B. Ainsi les A-schémas en groupe commutatif affines sont simplement décrits par des A-bigèbres.

Donnons-nous maintenant $\mathcal{G}$ un A-schéma en groupe commutatif affine de bigèbre B. Le A-module dual de $B = \operatorname{Hom}_A(B, A)$ va hériter d'une structure de bigèbre, sa multiplication est donnée par la transposée de la comultiplication de B tandis que sa comultiplication est donnée par la transposée de la multiplication de B. Elle correspond ainsi à un nouveau A-schéma en groupe commutatif affine $\mathcal{G}'$ que l'on appelle le *dual de Cartier* de $\mathcal{G}$. Cette terminologie est un peu abusive parce que ceci ne réalise effectivement une dualité que si l'on se restreint aux A-schémas en groupes commutatif finis et plats, essentiellement car le foncteur $\operatorname{Hom}(\cdot, A)$ ne réalise pas une dualité en général, mais c'est le cas lorsqu'il est restreint aux A-modules libres de type fini. Supposons donc désormais que $\mathcal{G}$ est un A-schéma en groupe commutatif fini et plat. Il est facile de décrire les C-points de $\mathcal{G}'$ où C est une A-algèbre. En effet, $\mathcal{G}'(C)$ est le groupe des morphismes de A-algèbres de B' dans C. C'est donc un sous-ensemble de $\operatorname{Hom}_A(B', C) = \operatorname{Hom}_C(B' \otimes_A C, C) \sim B' \otimes_A C$. $B' \otimes_A C$ est naturellement une C-bigèbre. Notons c_C sa comultiplication. $\mathcal{G}'(C)$ est alors décrit par :

$$\mathcal{G}'(C) = \{x \in B \otimes_A C, \quad c_C(x) = x \otimes x\}$$

À partir de maintenant, k désigne un corps parfait de caractéristique p. Notre but est d'étudier les k-schémas en groupe commutatif affines. Nous allons notre Aff_k leur catégorie. Notons tout de suite le théorème suivant dû à Grothendieck.

Théorème 3.4.3.1 (Grothendieck). *La catégorie Aff_k est une catégorie abélienne.*

Nous n'allons pas prouver ce théorème. Disons simplement que l'objet nul de cette catégorie est le k-schéma $\operatorname{Spec} k$ muni de la seule structure de groupe possible. Nous le noterons 0 dans la suite. Les noyaux se décrivent simplement en regardant les R-points est une k-algèbres. Plus précisément, si $f : \mathcal{G} \to \mathcal{H}$ est un morphisme entre k-schémas en groupe commutatif affines, f va induire pour toute k-algèbre R un morphisme de groupes abéliens $f_R : \mathcal{G}(R) \to \mathcal{H}(R)$. Le foncteur qui à un tel R associe le noyau de f_R est représentable par un k-schéma en groupe commutatif, c'est lui le noyau de f. Cela ne fonctionne hélas plus pour les conoyaux. Une méthode pour les définir est d'invoquer la dualité de Cartier.

La somme directe de deux k-schémas en groupe affines est le produit des deux schémas en question au-dessus de k. Le produit des deux lois fournit une loi de groupe commutatif sur ce schéma. Au niveau des bigèbres, il s'agit simplement de prendre le produit tensoriel et de la munir de la comultiplication produit tensoriel des comultiplications.

Frobenius et Verschiebung

Prenons $\mathcal{G}$ un k-schéma affine. Notons A l'anneau de $\mathcal{G}$, c'est une k-algèbre. On peut regarder une nouvelle k-algébre, $\underline{k}$. En tant qu'anneau il s'agit simplement de k, mais le morphisme définissant la structure d'algèbre est l'élévation à la puissance p de k dans $\underline{k}$. Autrement dit, si $x \in \underline{k}$ et $\lambda \in k$, $\lambda \cdot x = \lambda^p x$. Maintenant, on peut regarder la $\underline{k}$-algèbre $A^{(p)}$ défini par $A^{(p)} = A \otimes_k \underline{k}$. C'est également une k-algèbre puisque k et $\underline{k}$ ont les mêmes anneaux sous-jacents. L'action d'un élément $\mu \in k$ sur le produit tensoriel $x \otimes \lambda \in A^{(p)}$ est $\mu \cdot (x \otimes \lambda) = x \otimes (\mu\lambda)$. L'action de μ est donc moralement la multiplication par l'élément $\mu^{1/p}$, et même ici précisément puisque l'on a supposé k parfait. $A^{(p)}$ correspond à un nouveau k-schéma affine que l'on notera $\mathcal{G}^{(p)}$. On a en outre un morphisme k-linéaire de $A^{(p)}$ dans A défini par $x \otimes \lambda \mapsto x^p\lambda$. On obtient ainsi un morphisme de k-schéma $\mathcal{G} \to \mathcal{G}^{(p)}$, c'est celui-ci que l'on appelle le *Frobenius* que l'on note traditionnellement $F_{\mathcal{G}}$.

Avant de poursuivre, nous allons décrire pour R une $\underline{k}$-algèbre fixée, les R-points de $\mathcal{G}^{(p)}$ vu comme $\underline{k}$-schéma. Se donner un tel point, c'est par définition se donner un morphisme de $\underline{k}$-algèbres de $\varphi : A^{(p)} \to R$. Définissons alors ψ par $\psi(x) = \varphi(x \otimes 1)$. ψ est pour l'instant simplement un morphisme d'anneaux de A dans R. Il est soumis aux relations suivantes :

$$\psi(\lambda x) = \varphi(\lambda x \otimes 1) = \varphi(x \otimes \lambda^p) = \lambda^p \varphi(x \otimes 1) = \lambda^p \psi(x)$$

Ainsi ψ est un morphisme de k-algèbres de A dans $\underline{R}$, où $\underline{R}$ est la k-algèbre obtenue par restriction des scalaires de $\underline{k}$ à k. Cette correspondance est bijective, et donc on en déduit que $\mathcal{G}^{(p)}(R) = \mathcal{G}(\underline{R})$.

Le Frobenius quant à lui se décrit aussi simplement sur les R-points. Si R est une k-algèbre, on a un morphisme de R dans $\underline{R}$ qui est simplement celui qui à x associe x^p. Un tel morphisme fournit par fonctorialité une flèche $\mathcal{G}(R) \to \mathcal{G}(\underline{R})$. C'est le Frobenius.

Si le corps k est $\mathbb{F}_p$, l'élévation à la puissance p est l'identité et donc $\mathcal{G}^{(p)} = \mathcal{G}$ et le morphisme de Frobenius est l'identité. Toutefois, les choses ne sont plus aussi triviales dès que k est un peu plus grand.

Voyons maintenant ce qu'il se passe si l'on suppose en outre que $\mathcal{G}$ est muni d'une structure de k-schéma en groupe commutatif. L'anneau de $\mathcal{G}$, A, est alors une bigèbre. On vérifie formellement que la comultiplication de A fournit une comultiplication sur la k-algèbre $A^{(p)}$ et donc en fait une bigèbre. Autrement dit, le k-schéma affine $\mathcal{G}^{(p)}$ défini précédemment est un k-schéma en groupe commutatif. On vérifie également que le morphisme de Frobenius $F_{\mathcal{G}}$ est compatible avec les structures de groupes.

Mais maintenant grâce à la dualité de Cartier, on peut aller dans l'autre sens. Plus précisément, si $\mathcal{G}'$ désigne le dual de Cartier de $\mathcal{G}$, alors le dual de Cartier de $\mathcal{G}^{(p)}$ s'identifié à $\mathcal{G}'^{(p)}$. En effet, il s'agit juste de voir que se donner un morphisme k-linéaire de $A^{(p)} \to k$ revient à se donner un élément de $A'^{(p)}$ où A (resp A') désigne la bigèbre de $\mathcal{G}$ (resp $\mathcal{G}'$). À l'élément $\varphi \otimes \lambda \in A'^{(p)}$, on associe le morphisme $x \otimes \mu \mapsto \lambda\mu\varphi(x)^p$. k étant parfait, il s'agit bien ainsi d'une correspondance bijective. Ainsi le Frobenius de $\mathcal{G}'$ fournit par dualité un morphisme de k-schémas en groupe de $\mathcal{G}^{(p)}$ dans $\mathcal{G}$. C'est lui que l'on appelle le *Verschiebung* et que l'on note souvent $V_{\mathcal{G}}$.

Si $\mathcal{G}$ et $\mathcal{H}$ sont deux k-schémas en groupe commutatif finis, une flèche $f : \mathcal{G} \to \mathcal{H}$ induit de façon évident une flèche $f^{(p)} : G^{(p)} \to \mathcal{H}^{(p)}$. Elle fait commuter le diagramme suivant :

$$\begin{array}{ccccc}
\mathcal{G}^{(p)} & \xrightarrow{V_{\mathcal{G}}} & \mathcal{G} & \xrightarrow{F_{\mathcal{G}}} & \mathcal{G}^{(p)} \\
\downarrow{\scriptstyle f^{(p)}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f^{(p)}} \\
\mathcal{H}^{(p)} & \xrightarrow{V_{\mathcal{H}}} & \mathcal{H} & \xrightarrow{F_{\mathcal{H}}} & H
\end{array}$$

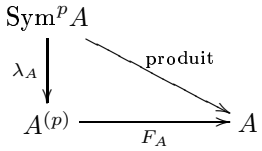
Il est peut-être utile de donner une description du Verschiebung directement en terme de bigèbres. Pour cela, notons $\mathrm{Sym}^p A \subset \otimes^p A$ la k-algèbre des tenseurs symétriques sur A. On peut alors définir les

deux applications suivantes, qui sont k-linéaires :

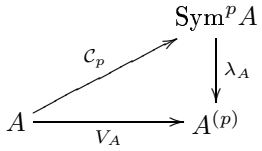
$$s_A : \begin{pmatrix} \otimes^p A & \longrightarrow & \mathrm{Sym}^p A \\ a_1 \otimes \ldots \otimes a_p & \mapsto & \sum_{\sigma \in S_p} a_{\sigma(1)} \otimes \ldots \otimes a_{\sigma(p)} \end{pmatrix}$$

$$\alpha_A : \begin{pmatrix} A^{(p)} & \longrightarrow & \mathrm{Sym}^p A \\ a \otimes \lambda & \mapsto & \lambda\,(a \otimes \ldots \otimes a) \end{pmatrix}$$

Le morphisme α_A est injectif. En outre on a la décomposition en somme directe $\mathrm{Sym}^p A = (\mathrm{im}\, s_A) \oplus (\mathrm{im}\, \alpha_A)$. Ceci permet de définir une application k-linéaire $\lambda_A : \mathrm{Sym}^p A \to A^{(p)}$ en disant que λ_A est l'application nulle sur $(\mathrm{im}\, s_A)$ et l'inverse de α_A sur $(\mathrm{im}\, \alpha_A)$. On vérifie dans un premier temps, que le diagramme suivant commute :



Le Verschiebung, quant à lui, est décrit par le diagramme suivant :



où c_p désigne la comultiplication itérée, comme on le vérifie plus ou moins fastidieusement.

On déduit de cela, en recollant les deux diagrammes précédemment que Frobenius et Verschiebung sont soumis à la relation de commutation $F_{\mathcal{G}} \circ V_{\mathcal{G}} = p$ où p désigne la multiplication par p. En considérant le schéma en groupe dual $\mathcal{G}'$, on voit que l'on a de même $V_{\mathcal{G}} \circ F_{\mathcal{G}} = p$.

On remarquera que l'on a pris soin de donner des définitions suffisamment générales pour qu'elles restent valables si k n'est pas forcément parfait. En outre, si k' est une extension de k et si $\mathcal{G}$ est un k-schéma en groupe commutatif fini, $\mathcal{G}_{k'} = \mathcal{G} \otimes_k k'$ va être un k'-schéma en groupe commutatif fini. $(\mathcal{G}_{k'})^{(p)}$ s'identifie alors naturellement à $\mathcal{G}^{(p)} \times_k k' = \mathcal{G}^{(p)}_{k'}$ et le Frobenius $F_{\mathcal{G}_{k'}} : \mathcal{G}_{k'} \to \mathcal{G}^{(p)}_{k'}$ se déduit du Frobenius $F_{\mathcal{G}}$ par extension des scalaires. Il en est de même du Verschiebung. D'autre part si $\mathcal{G}$ et $\mathcal{G}'$ sont deux k-schémas en groupe commutatif finis, le k-schéma $(\mathcal{G} \times_k \mathcal{G}')^{(p)}$ s'identifie au produit $\mathcal{G}^{(p)} \times_k \mathcal{G}'^{(p)}$ et le Frobenius et le Verschiebung au produit des morphismes correspondants. Finalement, il ne faut pas oublier de dire que Frobenius et Verschiebung s'échangent par dualité de Cartier.

Il est possible bien entendu de parler de Frobenius et de Verschiebung itérés. On définit pour cela par récurrence le groupe $\mathcal{G}^{(p^n)}$ par $\mathcal{G}^{\left(p^{n+1}\right)} = \left(\mathcal{G}^{(p^n)}\right)^{(p)}$. Il s'agit alors des applications $V^n_{\mathcal{G}} : \mathcal{G} \to \mathcal{G}^{(p^n)}$ et $F^n_{\mathcal{G}} : \mathcal{G}^{(p^n)} \to \mathcal{G}$.

Signalons également qu'il est possible d'étendre ces notions à tout k-schéma en groupe commutatif affine et que l'on garde toutes les propriétés annoncées dans ce paragraphe. Toutefois, cela demande l'introduction des schémas en groupe commutatif formels, c'est pour cela que nous avons présenté la théorie seulement dans ce cas particulier qui nous suffira pour la suite.

Groupes constants et étales

Prenons Γ un groupe commutatif fini. On aimerait construire un k-schéma en groupe commutatif fini, disons $C(\Gamma)$, qui soit tel que pour tout k-algèbre R, le groupe des R-points de $C(\Gamma)$ s'identifie fonctoriellement à Γ. Seulement, cela n'est pas possible, on va donc être moins ambitieux.

On remarque que si l'on pose $A = k^\Gamma$, la k-algèbre des fonctions de Γ dans k, on a une application naturelle de Γ dans $\mathrm{Hom}_{k-\mathrm{alg}}(A, R)$ pour tout k-algèbre R. Il s'agit simplement que celle qui à $\gamma \in \Gamma$ fait correpondre la fonction ε_γ qui envoie γ sur 1 et γ' sur 0 dès que $\gamma' \neq \gamma$. Évidemment, elle est toujours injective. De surcroît, dans le cas où $p \neq 2$ et où R est une algèbre connexe, il n'est pas bien difficile de montrer qu'il s'agit là d'un isomorphisme. Finalement, le k-schéma $\mathrm{Spec}\, A$ est un bon candidat pour ce que l'on cherche à définir.

Il reste à mettre sur A une structure de bigèbre qui induise sur $\mathrm{Hom}_{k-\mathrm{alg}}(A, R)$ une structure de groupe qui soit telle que l'application mentionnée ci-dessus devienne un homéomorphisme. Un petit calcul montre que la comultiplication à retenir est définie par la formule :

$$c(\varepsilon_\gamma) = \sum_{\gamma'+\gamma''=\gamma} \varepsilon_{\gamma'} \otimes \varepsilon_{\gamma''}$$

Comme k est parfait, il en est de même de A, et le morphisme de k-algèbre $A \to A^{(p)}$, $x \mapsto x^{1/p} \otimes 1$ est bien défini et bijectif. Via cette identification, le frobenius F_A devient un endormorphisme de k-algèbres de A, c'est l'identité.

On a ainsi défini notre k-schéma en groupe commutatif $C(\Gamma)$. Il n'est pas bien malin de voir qu'il est fini puisque A est un k-espace vectoriel de dimension finie. Un point important à remarquer est que si $f : \Gamma \to \Gamma'$ est un morphisme de groupes entre deux groupes finis Γ et Γ', il induit un morphisme de k-algèbres de $k^{\Gamma'}$ dans k^Γ. Celui-ci respecte la comultiplication définie précédemment et on obtient ainsi une flèche de $C(\Gamma) \to C(\Gamma')$. Autrement dit, C définit un foncteur de la catégorie des groupes abéliens finis dans celle des k-schémas en groupe commutatif finis. Il est pleinement fidèle. Son image essentielle forme la catégorie des groupes constants.

Il existe une caractérisation sympathique des k-schémas en groupe commutatif finis et étales. Bien sûr, comme l'on est sur un corps parfait, son anneau va être simplement un produit d'extensions finies k_i de k. Ainsi l'on voit qu'un k-schéma en groupe commutatif $\mathcal{G}$ va être étale si et seulement si son anneau est séparable ou ce qui revient au même réduit. On a également la proposition suivante qui caractérise les groupes étales en terme de Frobenius.

Proposition 3.4.3.2. *Soit $\mathcal{G}$ un k-schéma en groupe commutatif fini. $\mathcal{G}$ est étale si et seulement si le groupe $\mathcal{G} \times_k \bar{k}$ est constant, si et seulement si le Frobenius $F_\mathcal{G}$ est injectif, ou ce qui revient au même bijectif.*

Comme corollaire de ce qui précède, on a de nombreuses notions de stabilité. Plus précisément, tout sous-groupe, tout quotient et tout produit fini de k-schémas en groupe commutatif finis et étales l'est encore.

Citons pour finir le théorème de Deligne. Il dit dans ce cas particulier que si $\mathcal{G}$ est un k-schéma en groupe commutatif fini dont le rang n'est pas un multiple de p, alors $\mathcal{G}$ est étale. Plus généralement, on a :

Théorème 3.4.3.3 (Deligne). *Soit A un anneau et $\mathcal{G}$ un A-schéma en groupe commutatif fini et plat. Si le rang de $\mathcal{G}$ est inversible dans A, alors $\mathcal{G}$ est étale.*

Groupes connexes

On rappelle qu'un schéma en dit *connexe* si son espace topologique sous-jacent l'est. On rappelle également que si $S = \mathrm{Spec}\, A$, la connexité de S équivaut au fait que A ne peut pas s'écrire comme produit de deux anneaux non nuls. Si e est un *idempotent* de A, c'est-à-dire un élément vérifiant $e^2 = e$, on a toujours la décomposition $A = eA \times (1-e)A$, et réciproquement toute décomposition s'obtient ainsi. Elle est non triviale dès que e est différent de 0 et de 1. Ainsi S est connexe si et seulement si les seules solutions de l'équation $e^2 = e$ sont 0 et 1.

Prenons maintenant A une k-algèbre finie. C'est un anneau artinien. Un tel anneau ne possède qu'un nombre fini d'idéaux maximaux, notons les $\mathfrak{m}_1, \ldots, \mathfrak{m}_l$. On a en outre la décomposition suivante :

$$A = \prod_{i=1}^{l} A_{\mathfrak{m}_i}$$

où $A_{\mathfrak{m}_i}$ est le localisé de A en $\mathfrak{m}_i$. En fait la suite $\mathfrak{m}_i^n$ est stationnaire, on peut donc appeler $\mathfrak{m}_i^\infty$ sa limite. $A_{\mathfrak{m}_i}$ s'identifie alors simplement au quotient $A/\mathfrak{m}_i^\infty$. Cet anneau est connexe et donc la décomposition écrite précédemment correspond bien au découpage en composantes connexes de $\operatorname{Spec} A$. On déduit de cela en particulier qu'une k-algèbre finie est connexe si et seulement si elle est locale.

Soit $\mathcal{G}$ un k-schéma en groupe commutatif fini. Supposons $\mathcal{G}$ connexe. Notons A la bigèbre de $\mathcal{G}$, il s'agit d'une k-algèbre finie connexe et donc d'après ce que l'on vient de rappeler A est local d'idéal maximal $\mathfrak{m}$ et il existe un entier r tel que $\mathfrak{m}^r = 0$. Le morphisme d'augmentation $A \to k$ a pour noyau un idéal maximal de A, c'est donc $\mathfrak{m}$. On déduit de cela que $A/\mathfrak{m} = k$. On déduit de cela et du fait que k est parfait que si $p^n \geqslant r$, alors le Frobenius itéré $F_A^n : A^{(p^n)} \to A$ a pour image k. Du point de vue schéma, cela signifie que si $\mathcal{G}$ est connexe, il existe un entier n, tel que le Frobenius itéré $F_{\mathcal{G}}^n$ soit le morphisme nul, autrement dit le Frobenius est nilpotent. La réciproque est également vraie.

Là encore, on a des notions de stabilité. Tout quotient d'un k-schéma en groupe commutatif fini et connexe est encore connexe car un sous-anneau d'un anneau connexe l'est. De même tout sous-groupe d'un k-schéma en grope commutatif fini et connexe est encore connexe, ceci car un quotient d'un anneau local reste local. Finalement, les k-schémas en groupe commutatif fini et connexe sont également stables par produit finis.

Première décomposition d'un k-schéma en groupe commutatif fini

Soit $\mathcal{G}$ un k-schéma en groupe commutatif fini. Notons $\mathcal{G}^0$ la composante connexe de l'élément neutre de $\mathcal{G}$, celui-ci étant défini comme le point de $\mathcal{G}$ image de l'unique point de $\operatorname{Spec} k$ par la section neutre. Comme l'application définissant la multiplication sur $\mathcal{G}$ est continue, elle stabilise $\mathcal{G}^0$. On a vu que l'on peut décomposer la bigèbre A de $\mathcal{G}$ sous la forme

$$A = \prod_{i=1}^{l} A_{\mathfrak{m}_i}$$

où les $\mathfrak{m}_i$ sont les idéaux maximaux de A. Le morphisme d'augmentation $A \to k$ a pour noyau un de ces idéaux maximaux, disons par exemple $\mathfrak{m}_1$. La bigèbre de $\mathcal{G}^0$ est alors simplement l'anneau $A_{\mathfrak{m}_1}$ auquel la comultiplication de A s'étend.

Le théorème 3.4.3.1 nous dit que l'on peut définir le quotient $\mathcal{G}/\mathcal{G}^0$ est qu'il s'agit a priori d'un k-schéma en groupe commutatif affine. En réalité les choses se passent bien mieux que cela.

Théorème 3.4.3.4. *On garde les notations précédentes. $\pi_0(\mathcal{G}) = \mathcal{G}/\mathcal{G}^0$ est un k-schéma en groupe commutatif fini et étale et la suite exacte :*

$$0 \longrightarrow \mathcal{G}^0 \longrightarrow \mathcal{G} \longrightarrow \pi_0(\mathcal{G}) \longrightarrow 0$$

est scindée. Autrement dit $\mathcal{G}$ est canoniquement isomorphe au produit $\mathcal{G}^0 \times \pi_0(G)$.

En outre, si l'on arrive à écrire $\mathcal{G} = \mathcal{G}_c \times \mathcal{G}_e$ où $\mathcal{G}_c$ (resp. $\mathcal{G}_e$) est un k-schéma en groupe commutatif fini connexe (resp. étale), il existe deux isomorphismes $\varphi_c : \mathcal{G}^0 \to \mathcal{G}_c$ et $\varphi_e : \pi_0(G) \to \mathcal{G}_e$ uniquement déterminés tels que $\varphi_c \times \varphi_e = id_{\mathcal{G}}$.

Nous allons en fait construire $\pi_0(\mathcal{G})$ par une autre méthode et prouver que l'on a bien un produit direct. Notons A la bigèbre de $\mathcal{G}$. Si B_1 et B_2 sont deux sous-algèbres séparables de A, le produit B_1B_2 est également séparable car il s'identifie à un quotient du produit tensoriel $B_1 \otimes_k B_2$. Ainsi, comme A est par hypothèse de dimension finie sur k, il existe une plus grande sous-algèbre séparable de A. C'est celle que nous allons noter $\pi_0(A)$.

Bien entendu, la définition précédente s'étend à toute k-algèbre finie B. D'autre part, si B et B' sont deux k-algèbres finies et $f : B \to B'$ un morphisme de k-algèbres, f envoie $\pi_0(B)$ dans $\pi_0(B')$ et donc induit un morphisme de k-algèbre $\pi_0(f) : \pi_0(B) \to \pi_0(B')$. π_0 définit ainsi un foncteur. Voyons tout d'abord quelques propriétés générales de celui-ci :

Proposition 3.4.3.5. *Si B et B' sont deux k-algèbres finies, on a :*

$$\begin{aligned} \pi_0(B \times B') &= \pi_0(B) \times \pi_0(B') \\ \pi_0(B \otimes_k B') &= \pi_0(B) \times_k \pi_0(B') \end{aligned}$$

Si B est une k-algèbre finie et k' une extension de k, on a $\pi_0(B \otimes_k k') = \pi_0(B) \otimes_k k'$.

Si N est le nilradical de B, k-algèbre finie, la projection canonique $B \to B/N$ induit un isomorphisme $\pi_0(B) \sim \pi_0(B/N)$. En particulier, si k est parfait (ce que nous supposons ici), B/N va être réduit puis séparable et $\pi_0(B) \sim B/N$.

Pour les démonstrations, se reporter à [Wat79]

Revenons à notre situation. Il est passablement clair que la structure de bigèbre de A se restreint à $\pi_0(A)$, qui devient donc une sous-bigèbre de A. En notant $\pi_0(\mathcal{G})$ le k-schéma en groupe commutatif associé à cette bigèbre, on a directement une flèche $\mathcal{G} \to \pi_0(\mathcal{G})$ qui provient de l'inclusion de $\pi_0(A)$ dans A. Cette flèche est surjective. Nous voulons voir que son noyau s'identifie à $\mathcal{G}^0$. Ce noyau est défini par le quotient $A/(I \cap \pi_0(A))A$ où I est l'idéal d'augmentation de A. Si on appelle $\mathfrak{m}_i$ les idéaux maximaux de A, on a vu que A se décompose de la façon suivante :

$$A = \prod_{i=1}^{l} A/\mathfrak{m}_i^{r_i}$$

où les r_i sont des entiers suffisamment grands. Supposons encore $\mathfrak{m}_1$ est l'idéal d'augmentation I. Notons $f \in A$ l'idempotant $(1, 0, \ldots, 0)$ vu dans la décomposition. L'élément $(1 - f)$ appartient à $\pi_0(A) \cap I$. On déduit de cela et de la connexité de $A/\mathfrak{m}_1^{r_1}$ que le quotient $A/(I \cap \pi_0(A))A$ s'identifie à $A/\mathfrak{m}_1^{r_1}$. Autrement dit le noyau du morphisme $\mathcal{G} \to \pi_0(G)$ est bien $\mathcal{G}^0$, et les deux définitions coïncident.

Mais maintenant il est facile de voir que la suite exacte

$$0 \longrightarrow \mathcal{G}^0 \longrightarrow \mathcal{G} \longrightarrow \pi_0(\mathcal{G}) \longrightarrow 0$$

est scindée. En effet, la proposition 3.4.3.5 nous dit que $\pi_0(N)$ est isomorphe en tant que k-algèbre au quotient A/N, N désignant le nilradical de A. Il est facile de voir que la comultiplication se prolonge à A/N et que l'isomorphisme ci-dessus la respecte. En termes de groupes, cela signifie que $\pi_0(G)$ s'identifie à un sous-schéma en groupe commutatif fini de $\mathcal{G}$ et donc que la suite est scindée.

On déduit facilement de ce qui précède la proposition suivante :

Proposition 3.4.3.6. *Soit $\mathcal{G}$ un k-schéma en groupe commutatif fini. $\mathcal{G}$ est connexe si et seulement si $\mathcal{G}^0 = \mathcal{G}$. $\mathcal{G}$ est étale si et seulement si $\mathcal{G} = \pi_0(G)$.*

Si $\mathcal{G}'$ est un autre k-schéma en groupe commutatif fini, on a le formulaire suivant :

$$\begin{aligned} (\mathcal{G} \times_k \mathcal{G}')^0 &= \mathcal{G}^0 \times_k \mathcal{G}'^0 \\ \pi_0(\mathcal{G} \times_k \mathcal{G}') &= \pi_0(\mathcal{G}) \times_k \pi_0(\mathcal{G}') \end{aligned}$$

Groupes diagonalisables et de type multiplicatif

Ces notions sur les notions duales de celles présentées dans le paragraphe 3.4.3. Plus précisément, considérons $\mathcal{G}$ un schéma en groupe commutatif fini et notons $\mathcal{G}'$ son dual de Cartier. On dira que $\mathcal{G}$ est *diagonalisable* si $\mathcal{G}'$ est un groupe constant. On dira que $\mathcal{G}$ est de *type multiplicatif* si $\mathcal{G}'$ est étale.

Considérons Γ un groupe commutatif fini. On définit le k-schéma en groupe commutatif fini $D(\Gamma)$ simplement comme étant le dual de Cartier de $C(\Gamma)$. L'on obtient ainsi une nouveau foncteur D qui va de la catégorie des groupes commutatifs finis dans celle des k-schémas en groupe commutatif finis. Comme précédemment, ce foncteur est pleinement fidèle, comme composé de deux foncteurs pleinement fidèles. Son image essentielle constitue la catégorie des groupes diagonalisables.

Voyons à quoi ressemble $D(\Gamma)$. Notons A sa bigèbre, il s'agit de la bigèbre duale de A', k-algèbre des fonctions de Γ dans k munie de la comultiplication définie par :

$$c'(\varepsilon_\gamma) = \sum_{\gamma'+\gamma''=\gamma} \varepsilon_{\gamma'} \otimes \varepsilon_{\gamma''}$$

Un calcul simple montre alors qu'en tant que k-algèbre A s'identifie canoniquement à $k[\Gamma]$. Cela signifie qu'en tant que k-espace vectoriel, A admet pour base une famille d'éléments e_γ indexée par Γ et que la multiplication sur A est donnée par $e_\gamma e_{\gamma'} = e_{\gamma+\gamma'}$. La comultiplication, quant à elle, est donnée par $c(e_\gamma) = e_\gamma \otimes e_\gamma$.

Bien entendu, on a une proposition duale de la proposition 3.4.3.2 pour les groupes de type multiplicatif. Plus précisément :

Proposition 3.4.3.7. *Soit $\mathcal{G}$ un k-schéma en groupe commutatif fini. $\mathcal{G}$ est de type multiplicatif si et seulement si le groupe $\mathcal{G} \times_k \bar{k}$ est diagonalisable, si et seulement si le Verschiebung $V_\mathcal{G}$ est surjectif, ou ce qui revient au même bijectif.*

Il nous faut peut-être justifier légèrement la terminologie. En réalité un k-schéma en groupe commutatif fini est de type multiplicatif si et seulement si il n'admet de morphisme non nul dans ce que l'on appelle le *groupe additif*. Le groupe additif n'est pas un groupe fini. C'est celui qui est associé à la bigèbre $k[X]$, la comultiplication étant donnée par $c(X) = 1 \otimes X + X \otimes 1$. Il s'appelle ainsi car si R est une k-algèbre, le groupe de ses R-points n'est autre que le groupe additif de R.

Deuxième décomposition d'un k-schéma en groupe commutatif fini

Soit $\mathcal{G}$ un k-schéma en groupe commutatif fini. $\mathcal{G}$ est dit *unipotent* si son dual de Cartier $\mathcal{G}'$ est connexe. Par dualité, on voit immédiatement que $\mathcal{G}$ est unipotent si et seulement si le Verschiebung est nilpotent. On voit également que tout schéma en groupe commutatif fini $\mathcal{G}$ se décompose de façon unique à isomorphisme près comme produit d'un groupe unipotent par un groupe de type multiplicatif. On a en fait la proposition suivante un peu plus précise.

Proposition 3.4.3.8. *Soit $\mathcal{G}$ un k-schéma en groupe commutatif fini. Alors il existe $\mathcal{G}_{em}$, $\mathcal{G}_{eu}$, $\mathcal{G}_{cm}$, $\mathcal{G}_{cu}$ quatre k-schémas en groupe commutatif finis tels que*

1. *$\mathcal{G}_{em}$ soit étale et de type multiplicatif*
2. *$\mathcal{G}_{eu}$ soit étale et unipotent*
3. *$\mathcal{G}_{cm}$ soit connexe et de type multiplicatif*
4. *$\mathcal{G}_{cu}$ soit connexe et unipotent*
5. *$\mathcal{G} = \mathcal{G}_{em} \times \mathcal{G}_{eu} \times \mathcal{G}_{cm} \times \mathcal{G}_{cu}$*

En outre, si les schémas en groupe commutatif finis $\mathcal{G}'_{em}$, $\mathcal{G}'_{eu}$, $\mathcal{G}'_{cm}$, $\mathcal{G}'_{cu}$ vérifient les cinq conditions précédentes, il existe des isomorphismes de k-schémas en groupes $\varphi_{em} : \mathcal{G}_{em} \to \mathcal{G}'_{em}$, $\varphi_{eu} : \mathcal{G}_{eu} \to \mathcal{G}'_{eu}$, $\varphi_{cm} : \mathcal{G}_{cm} \to \mathcal{G}'_{cm}$, $\varphi_{cu} : \mathcal{G}_{cu} \to \mathcal{G}'_{cu}$ uniquement déterminés tels que $\varphi_{em} \times \varphi_{eu} \times \varphi_{cm} \times \varphi_{cu} = id_{\mathcal{G}}$.

Finalement cette décomposition est conservée par extension des scalaires à un autre corps parfait.

On peut voir la proposition précédente d'un point de vue plus catégorique. Notons $\underline{\mathrm{G}}_k$ la catégorie des k-schémas en groupe commutatif finis. Notons $\underline{\mathrm{Gem}}_k$ (resp. $\underline{\mathrm{Geu}}_k$, resp. $\underline{\mathrm{Gcm}}_k$, resp. $\underline{\mathrm{Gcu}}_k$) la sous-catégorie pleine de $\underline{\mathrm{G}}_k$ formée des k-schémas en groupe commutatif étales et de type multiplicatif (resp. étales et unipotents, resp. connexes et de type multiplicatif, resp. connexes et unipotents). La proposition précédente dit alors que la catégorie $\underline{\mathrm{G}}_k$ s'identifie aux produits des quatre catégories $\underline{\mathrm{Gem}}_k$, $\underline{\mathrm{Geu}}_k$, $\underline{\mathrm{Gcm}}_k$ et $\underline{\mathrm{Gcu}}_k$. La dualité de Cartier induit des dualités sur $\underline{\mathrm{Gem}}_k$ et $\underline{\mathrm{Gcu}}_k$ et une anti-équivalence de catégories entre $\underline{\mathrm{Geu}}_k$ et $\underline{\mathrm{Gcm}}_k$.

Il n'est pas anodin de noter que chacune des quatre catégories définies précédemment est stable par produit fini. Cela se voit par exemple en regardant les caractérisations par le Frobenius ou le Verschiebung que l'on a données précédemment.

Cela permet de donner une description assez explicite des k-schémas en groupe commutatif finis lorsque k est un corps algébriquement clos, disons de caractéristique p. Dans un premier temps, il est facile de décrire les schémas étales. Le groupe de Galois absolu de k étant ici trivial, un k-schéma en groupe commutatif fini et étale est simplement donné par le groupe de ces k-points. Autrement dit, se donner un tel schéma revient exactement à se donner un groupe commutatif fini, les propriétés de dévissage se transposant également. Il est assez simple de vérifier que parmi les groupes commutatifs finis, ceux qui correspondent aux schémas unipotents sont ceux qui sont d'ordre une puissance de p et ceux qui correspondent aux schémas de type multiplicatif sont ceux qui sont d'ordre premier à p.

Il reste à regarder ce qu'il se passe pour les k-schémas en groupe commutatif finis et connexes. Commençons par le cas connexe de type multiplicatif. Comme l'on est toujours sur un corps algébriquement clos, un groupe de type multiplicatif va être diagonalisable. Ainsi un tel groupe va s'écrire $D(\Gamma)$ où Γ est un certain groupe fini commutatif. Notons A la bigèbre de $\mathcal{G}$. Il s'agit en tant que k-algèbre de l'algèbre du groupe $k[\Gamma]$. Notons e_γ le représentant dans $k[\Gamma]$ de l'élément $\gamma \in \Gamma$. Si H est un sous-groupe non trivial de Γ, définissons :

$$e_H = \sum_{h \in H} e_h$$

Il est facile de vérifier que $e_H^2 = (\operatorname{Card} H)\, e_H$. Ainsi si $\operatorname{Card} H$ est inversible dans k, l'élément $\frac{e_H}{\operatorname{Card} H}$ va être un idempotent de A différent de 1 et de 0. Mais ceci n'est pas possible car l'on a supposé A connexe. Ainsi, tout sous-groupe non trivial de Γ a pour ordre un multiple de p, on déduit facilement de cela que l'ordre de Γ est une puissance de p. Réciproquement si Γ est un groupe commutatif d'ordre une puissance de p, Γ va s'écrire comme une extension de $\mathbb{Z}/p^n\mathbb{Z}$ et il est alors facile de vérifier que $D(\Gamma)$ est bien un k-schéma en groupe commutatif fini, connexe et de type multiplicatif.

De tout cela, on déduit que, sur un corps k algébriquement clos, dans la décomposition de la proposition 3.4.3.8 $\mathcal{G} = \mathcal{G}_{\mathrm{em}} \times \mathcal{G}_{\mathrm{eu}} \times \mathcal{G}_{\mathrm{cm}} \times \mathcal{G}_{\mathrm{cu}}$, le groupe $\mathcal{G}_{\mathrm{em}}$ est d'ordre premier à p et les groupes $\mathcal{G}_{\mathrm{eu}}$, $\mathcal{G}_{\mathrm{cm}}$ et $\mathcal{G}_{\mathrm{cu}}$ sont d'ordre une puissance de p. Comme on a également dit que la décomposition était conservée par extension des scalaires, cette propriété reste vraie pour un corps parfait k de caractéristique p quelconque. Notons à présent $\underline{\mathrm{G}}_{p,k}$ la catégorie des k-schémas en groupe fini dont l'ordre est une puissance de p (ou ce qui revient au même qui sont tués par une puissance de p). D'après ce que l'on vient de dire, cette catégorie s'identifie au produit $\underline{\mathrm{Geu}}_k \times \underline{\mathrm{Gcm}}_k \times \underline{\mathrm{Gcu}}_k$. C'est les objets de cette dernière catégorie auxquels on va s'intéresser par la suite. Nous allons en fait définir un foncteur partant de cette catégorie qui va s'avérer être une équivalence de catégories.

3.4.4 Modules de Dieudonné

On définit en fait ce foncteur plus ou moins séparément sur chacun des morceaux intervenant dans la catégorie qui nous intéresse. Commençons par les groupes unipotents. Dans toute la suite, nous noterons $W = W(k)$ l'anneau de vecteurs de Witt à coefficients dans k et $K = \operatorname{Frac} W$ son corps des fractions. Nous noterons également indifféremment F ou σ le Frobenius agissant sur k ou sur W. Rappelons que k étant supposé parfait de caractéristique p, σ est toujours bijectif.

Pour les groupes unipotents

Considérons donc $\mathcal{G}$ un k-schéma en groupe fini unipotent (et donc dont le rang est une puissance de p), c'est-à-dire en fait un objet de la catégorie $\underline{\mathrm{Geu}}_k \times \underline{\mathrm{Gcu}}_k$. On définit dans un premier temps le schéma en groupe sur k des vecteurs de Witt tronqués W_n. Il est tout simplement décrit par le foncteur qui à une k-algèbre A associe le groupe $W_n(A)$, le groupe des vecteurs de Witt tronqués à coefficients dans A.

Si A est une k-algèbre finie, on peut munir $W_n(A)$ d'une structure de W-module. Si $w \in W$ et si $a \in W_n(A)$, on définit la multiplication externe par :

$$w \cdot a = \sigma^{1-n}(w)\, a$$

où la multiplication à droite correspond à la multiplication dans l'anneau des vecteurs de Witt dont le résultat est éventuellement tronqué aux $n+1$ premières composantes. L'intêret de cela est qu'ainsi le Verschiebung V, qui rappelons-le à un vecteur de Witt $(a_0, \ldots, a_n, \ldots)$ associe le vecteur de Witt $(0, a_0, \ldots, a_n, \ldots)$, induit un morphisme W-linéaire entre $W_n(A)$ et $W_{n+1}(A)$.

Par fonctorialité on obtient un morphisme de k-schémas en groupe $W_n \to W_{n+1}$. Cela fournit par composition une flèche de l'ensemble $\operatorname{Hom}(G, W_n)$ dans l'ensemble $\operatorname{Hom}(G, W_{n+1})$ de W-modules. On rappelle qu'un k-schéma en groupe fini définit un foncteur de la catégorie de k-algèbres finies dans la catégorie des groupes, simplement en considérant les points. En fait, W_n décrit comme précédemment provient d'un k-schéma en groupe fini qui plus est unipotent, mais il n'est pas nécessaire de le savoir ici, on peut considérer les Hom précédents comme l'ensembles des transformations naturelles entre les deux foncteurs définis de la catégorie des k-algèbres finies dans celles des groupes abéliens. On peut ensuite considérer la limite inductive suivante :

$$M(\mathcal{G}) = \varinjlim_n \operatorname{Hom}(\mathcal{G}, W_n)$$

Cela définit pour l'instant un foncteur contravariant de la catégorie produit $\underline{\mathrm{Geu}}_k \times \underline{\mathrm{Gcu}}_k$ dans la catégorie de W-modules. Mais, nous allons voir qu'il est possible de rajouter des structures sur l'objet $M(\mathcal{G})$.

Déjà, si M est un W-module, on peut lui associer le W-module $M^{(p)}$ obtenu en tensorisant M par W au-dessus de W, le facteur W étant vu comme un W-module via le Frobenius σ. Comme k est supposé parfait, le Frobenius est bijectif sur W et il est possible de donner une nouvelle description de $M^{(p)}$. En tant que groupe, il s'agit simplement de M, la multiplication par un élément de W est donnée par la formule :

$$w \cdot m = \sigma^{-1}(w)\, m$$

valable pour tout $w \in W$ et tout $m \in M = M^{(p)}$.

Il est intéressant que remarquer que si $\mathcal{G}$ est un k-schéma en groupe fini unipotent, alors $M\left(G^{(p)}\right)$ s'identifie canonique à $(M(\mathcal{G}))^{(p)}$. Pour voir cela, on commence par prendre f un élément de $M(\mathcal{G})$, c'est-à-dire un morphisme de G dans $W_{n,k}$ pour un certain entier n. Le morphisme $f^{(p)} : \mathcal{G}^{(p)} \to W_{n,k}^{(p)} = W_{n,k}$ permet de définir une application de $M(\mathcal{G})$ dans $M\left(G^{(p)}\right)$. On vérifie qu'elle est semi-linéaire et induit en fait un isomorphisme entre $(M(\mathcal{G}))^{(p)}$ et $M\left(G^{(p)}\right)$.

C'est à ce moment que l'on se rappelle que l'on avait défini deux applications entre $\mathcal{G}$ et $\mathcal{G}^{(p)}$, le Frobenius $F_{\mathcal{G}} : \mathcal{G} \to \mathcal{G}^{(p)}$ et le Verschiebug $V_{\mathcal{G}} : \mathcal{G}^{(p)} \to \mathcal{G}$ (*cf* 3.4.3). Celles-ci induisent donc par application du foncteur M et via les identifications précédentes, des applications :

$$M(F_{\mathcal{G}}) : (M(\mathcal{G}))^{(p)} \to M(\mathcal{G})$$

$$M(V_{\mathcal{G}}) : M(\mathcal{G}) \to (M(\mathcal{G}))^{(p)}$$

Ces applications peuvent également être vues comme des endomorphismes semi-linéaires du W-module $M(\mathcal{G})$.

Notons à présent D_k l'anneau unitaire non commutatif (en général, il n'est commutatif que si $k = \mathbb{F}_p$) engendré par $W(k)$ et deux éléments F et V soumis aux relations suivantes :

1. $Fw = \sigma(w) F$
2. $wV = V\sigma(w)$
3. $FV = VF = p$

et ce pour tout $w \in W$.

Tout ce que l'on a dit précédemment montre qu'en fait $M(\mathcal{G})$ est un D_k-module à gauche[6]. C'est ce D_k-module que l'on va appeler le *module de Dieudonné* associé au k-schéma en groupe fini unipotent $\mathcal{G}$. On peut faire tout de suite quelques remarques. Le fait que $\mathcal{G}$ soit unipotent peut se traduire en disant que le Verschiebung $V_{\mathcal{G}}$ est nilpotent, c'est-à-dire nul lorsqu'on l'élève à une certaine puissance. Ainsi dans le module de Dieudonné de $\mathcal{G}$, $M(\mathcal{G})$, il va exister un entier n tel que pour tout $m \in M(\mathcal{G})$, on aura $V^n m = 0$. Un D_k-module vérifiant cette condition sera dit de *V-torsion*.

Faisons également une deuxième remarque. Gardons k notre corps parfait, et considérons ℓ une extension de k, elle aussi parfaite. Si $\mathcal{G}$ est un k-schéma en groupe fini unipotent, on peut considérer son extension à ℓ, disons $\mathcal{G}_\ell$. On a vu qu'elle restait unipotente. On obtient ainsi deux modules de Dieudonné qui sont reliés par une application :

$$M(\mathcal{G}) \otimes_{W(k)} W(\ell) \to M(\mathcal{G}_\ell)$$

le produit tensoriel héritant bien entendu du Frobenius et du Verschiebung définis sur $M(\mathcal{G})$. On peut vérifier en fait que cette application est un isomorphisme, ce qui peut se redire en disant que l'extension des scalaires commute à la formation du module de Dieudonné.

Cette dernière remarque permet de démontrer simplement, en fait en étendant les scalaires à une clôture séparable, que si $\mathcal{G}$ est un k-schéma en groupe unipotent de rang p^n, alors $M(\mathcal{G})$ est en fait un W-module de longueur finie, la longueur étant en fait précisément n.

Énonçons maintenant un théorème précis qui récapitule entre autres ce qui précède :

Théorème 3.4.4.1. *Le foncteur M défini précédemment induit une anti-équivalence entre la catégorie des k-schémas en groupe finis unipotents, c'est-à-dire la catégorie produit $\underline{Geu}_k \times \underline{Gcu}_k$ et la catégorie des D_k-modules de V-torsion qui sont de longueur finie en tant que W-modules.*

En outre, si $\mathcal{G}$ est un objet de $\underline{Geu}_k \times \underline{Gcu}_k$, on a l'égalité

$$rg(\mathcal{G}) = p^{lg(M(\mathcal{G}))}$$

De plus, les objets de $\underline{Gcu}_k$ correpondent précisément aux D_k-modules de F-torsion ou les objets de $\underline{Geu}_k$, eux, correspondent aux D_k-modules M sur lesquels le Frobenius est bijectif, cela signifiant tels que pour tout $m \in M$, il existe un unique $m' \in M$ tel que $m = Fm'$.

Finalement si ℓ est une extension parfaite de k et si G_ℓ désigne l'extension des scalaires de k à ℓ du groupe $\mathcal{G}$, il existe un isomorphisme canonique et fonctoriel entre les D_ℓ-modules $M(\mathcal{G}_\ell)$ et $M(\mathcal{G}) \otimes_{W(k)} W(l)$.

[6]Par la suite, on dira toujours D_k-module pour D_k-module à gauche.

Nous n'allons par démontrer ce théorème ici, nous reportons le lecteur à [Dem72]. Disons toutefois que la caractérisation des groupes étales et des groupes connexes par le Frobenius permet de démontrer directement le troisième point.

Dualité sur les modules de Dieudonné

Nous avons déjà vu que l'on pouvait définir une dualité, en l'occurrence la dualité de Cartier, sur les k-schémas en groupe finis. En fait, on peut lui trouver ce qui sera un équivalent au niveau des modules de Dieudonné, enfin plus précisément des D_k-modules qui sont des W-modules de longueur finie.

Pour cela, on commence par définir un objet particulier. Il s'agit de :

$$CW^u(k) = \varinjlim_n W_n(k)$$

où les applications de transition sont encore les Verschiebung. Comme précédemment on peut mettre sur $CW^u(k)$ une structure de W-module. On peut donner une autre description de ce module : $W_n(k)$ est isomorphe canoniquement au quotient W/p^nW et les flèches de transition deviennent via cet isomorphisme la multiplication par p. Ainsi :

$$CW^u(k) = \varprojlim_n W/p^nW = K/W$$

Il est possible d'interpréter cette nouvelle description de façon très terre à terre. Autant, l'anneau des vecteurs de Witt W permettait de construire un anneau de valuation discrète non absolument ramifié dont le corps résiduel était précisément k, en remarquant que moralement tout nombre d'un tel anneau se décompose de façon unique en base p, autant $CW^u(k)$ s'intéresse aux *chiffres après la virgule.*

Prenons maintenant M un D_k-module qui est de longueur finie en tant que W-module. On définit alors $M^\star$. En tant que W-module, il s'agit de l'ensemble $\mathrm{Hom}(M, CW^u(k))$ des applications W-lineaires de M dans $CW^u(k)$. Si f est une telle application, on définit les applications les applications Ff et Vf par les relations suivantes :

$$(Ff)(m) = \sigma \circ f(Vm)$$

$$(Vf)(m) = \sigma^{-1} \circ f(Fm)$$

Cela fait de $M^\star$ un D_k-module. C'est lui que l'on appelle le *dual* de M.

Prenons $\mathcal{G}$ un k-schéma en groupe fini connexe et unipotent. Le dual de Cartier de $\mathcal{G}$, $D(\mathcal{G})$ est alors lui aussi connexe et unipotent. Il est alors vrai que si l'on note $M(\mathcal{G})$ le module de Dieudonné de $\mathcal{G}$, le module de Dieudonné de $D(\mathcal{G})$ s'identifie canoniquement au dual de M, $M^\star$ tel que l'on vient de le définir. Pour une démonstration de cette propriété, il est possible de se reporter à [Dem72]. Nous allons finalement utiliser cette notion de dualité pour définir le foncteur de Dieudonné M sur le troisième morceau de notre catégorie.

Classification générale

Prenons $\mathcal{G}$ un k-schéma en groupe fini connexe et de type multiplicatif. Son dual $D(\mathcal{G})$ est alors unipotent et étale, en particulier il est unipotent et donc on peut parler de son module de Dieudonne $M(D(\mathcal{G}))$. On définit donc naturellement le module de Dieudonné de $\mathcal{G}$ comme le dual de $M(D(\mathcal{G}))$ dans le sens précédent.

On peut faire tout de suite quelques remarques simples. Sur $M(D(\mathcal{G}))$, F était bijectif et V de torsion comme nous l'avons déjà dit. Sur son dual, c'est-à-dire $M(\mathcal{G})$, c'est le contraire : F est de torsion et V est bijectif. La seconde remarque est la suivante. Soit M un D_k-module qui est de longueur finie en tant que W-module. En utilisant par exemple la description des modules sur un anneau principal, on voit que p est

forcément de torsion dans M. D'autre part comme $FV = FV = p$, il n'existe pas de sous-espaces stables à la fois par V et par F sur lesquels ces deux endomorphismes sont des bijections. Un peu d'algèbre linéaire permet alors de prouver que M se décompose comme somme directe de trois W-modules, disons M_1, M_2 et M_3, tous trois stables à la fois par F et V, le tout tel que F et V soit de torsion sur M_1, F soit bijection et V de torsion sur M_2 et finalement F soit de torsion et V bijectif sur M_3. Cela résume les grandes lignes de la démonstration du théorème suivant qui donne la classification des k-schémas en groupe finis de rang une puissance de p par leur module de Dieudonné.

Théorème 3.4.4.2. *Le foncteur M défini* par morceaux *sur la catégorie produit $\underline{Geu}_k \times \underline{Gcm}_k \times \underline{Gcu}_k$ réalise une anti-équivalence de catégorie avec la catégorie des D_k-modules qui sont de longueur finie en tant que W-modules.*

Dans cette équivalence les objets de $\underline{Geu}_k$ correspondent aux modules M sur lesquels F est bijectif et V de torsion. Les objets de $\underline{Gcm}_k$ correspondent aux modules M sur lesquels F est de torsion et V est bijectif. Les objets de $\underline{Gcu}_k$ correspondent aux modules M sur lesquels F est bijectif et V est de torsion.

En outre, on a l'égalité :

$$rg(\mathcal{G}) = p^{lg(M(\mathcal{G}))}$$

Finalement, si ℓ est une extension parfaite du corps k et si G_ℓ désigne l'extension des scalaires de k à ℓ de $\mathcal{G}$, il existe un isomorphisme canonique et fonctoriel entre les D_ℓ-modules $M(\mathcal{G}) \otimes_W W(\ell)$ et $M(G_\ell)$.

Covecteurs de Witt

On peut en fait donner une autre description du foncteur précédent qui a l'avantage de ne pas séparer plusieurs cas et de ne pas parler de dualité.

Commençons par prendre $\mathcal{G}$ un k-schéma en groupe fini unipotent. On avait alors défini $M(\mathcal{G})$ comme la limite inductive suivante :

$$M(\mathcal{G}) = \varinjlim_n \mathrm{Hom}(\mathcal{G}, W_n)$$

Définissons alors, si A est une k-algèbre finie, le W-module :

$$CW_k^u(A) = \varinjlim_n W_n(A)$$

Cela définit un foncteur CW_k^u, et il est alors facile de voir que $M(\mathcal{G})$ s'identifie en tant que W-module à $\mathrm{Hom}(\mathcal{G}, CW_k^u)$.

Donnons tout de suite une description plus explicite de $CW_k^u(A)$ où A est une k-algèbre finie. Un bon moyen peut-être de voir ses éléments est le suivant. Un tel élément sera simplement une suite *infinie à gauche* $(\ldots, a_{-n}, \ldots, a_{-1}, a_0)$ nulle à partir d'un certain rang. Il s'agit de donner maintenant des formules plus ou moins explicites pour décrire la structure de W-modules. Si $a = (\ldots, a_{-n}, \ldots, a_{-1}, a_0)$ et $b = (\ldots, b_{-n}, \ldots, b_{-1}, b_0)$ sont deux éléments de $CW_k^u(A)$, on définit $a + b = (\ldots, c_{-n}, \ldots, c_{-1}, c_0)$ par les relations suivantes :

$$c_{-n} = \lim_{k \to \infty} S_k(a_{-n-k}, \ldots, a_{-n}, b_{-n-k}, \ldots, b_{-n})$$

où S_k est le polynôme universel définissant l'addition sur les anneaux de vecteurs de Witt (*cf* 3.4.1). Le fait que les suites (a_{-n}) et (b_{-n}) sont nulles à partir d'un certain rang assure que la limite considérée est en fait stationnaire, il n'y a donc aucun problème de convergence comme on aurait pu le croire a priori.

La structure de W-module est un peu plus pénible à décrire, nous allons commencer par donner l'action d'un élément de k, c'est-à-dire, un élément de la forme $[\lambda] = (\lambda, 0, \ldots, 0, \ldots)$ où $\lambda \in k$. On a la formule :

$$[\lambda] \cdot (\ldots, a_{-n}, \ldots, a_0) = \left(\ldots, \sigma^{-n}(\lambda)\, a_{-n}, \ldots, \lambda a_0\right)$$

valable pour tout élément $(\ldots, a_{-n}, \ldots, a_0) \in CW_k^u(A)$.

Tout élément de W peut s'écrire comme un somme de $[\lambda_n] p^n$, donc pour terminer de décrire l'action, il suffit de donner celle de l'élément $p \in W$. Là encore, il ne s'agit pas d'une formule compliquée :

$$p \cdot (\ldots, a_{-n}, \ldots, a_0) = \left(\ldots, a_{-n-1}^p, \ldots, a_{-1}^p\right)$$

Il est également possible de définir sur $CW_k^u(A)$ un Frobenius et un Verschiebung. Les formules doivent être celles auxquelles on pense :

$$F(\ldots, a_{-n}, \ldots, a_0) = \left(\ldots, a_{-n}^p, \ldots, a_0^p\right)$$

$$V(\ldots, a_{-n}, \ldots, a_0) = (\ldots, a_{-n-1}, \ldots, a_{-1})$$

Bien entendu, F et V sont semi-linéaires dans le sens qu'il convient, et la relation $FV = VF = p$ est encore vérifiée. Autrement dit, le W-module $CW_k^u(A)$ hérite en fait d'une structure de D_k-module.

Donnons un peu de terminologie. Le D_k-module $CW_k^u(A)$ s'appelle *le module des covecteurs de Witt unipotents* à coefficients dans A. Le foncteur CW_k^u s'appelle, quant à lui le *foncteur des covecteurs de Witt unipotents*.

Remarquons que les applications F et V définies précédemment définissent en fait des transformations naturelles du foncteur CW_k^u et donc qu'ainsi le W-module $\mathrm{Hom}(\mathcal{G}, CW_k^u)$ hérite lui aussi d'une structure de D_k-module. C'est alors juste une simple vérification de voir que la structure de D_k-module définie ainsi coïncide avec la structure de D_k-module décrite dans le paragraphe précédent.

On vient donc de donner une nouvelle description, sûrement plus utilisable, du module de Dieudonné associé à k-schéma en groupe fini et unipotent. Toutefois, cette nouvelle description ne se généralise pas encore directement à tous les k-schémas en groupe finis de rang une puissance de p. Il faut faire encore quelques modifications et introduire le covecteurs de Witt.

La description des *covecteurs de Witt* ressemble grandement à ce que l'on vient de faire. On commence par prendre une k-algèbre finie A et on considère l'ensemble des suites *infinies à gauche* $(\ldots, a_{-n}, \ldots a_0)$ d'éléments de A, sauf que ce coup-ci on se restreint pas aux suites nulles à partir d'un certain rang, mais plutôt aux suites dont tous les termes deviennent nilpotents à partir d'un certain rang. Autrement dit, si l'on note par exemple $\mathfrak{r}_A$ le nilradical de A, l'ensemble que l'on vient de définir est :

$$CW_k(A) = \left\{ (\ldots, a_{-n}, \ldots, a_0) \;\middle|\; \begin{array}{l} a_{-n} \in A, \forall n \\ a_{-n} \in \mathfrak{r}_A, \forall n \geqslant N \end{array} \right\}$$

Exactement de la même façon que précédemment, on munit cet ensemble d'une structure de W-module puis d'une structure de D_k-module. Il est simplement plus difficile de prouver que la limite considérée pour la définition de la somme est encore stationnaire. Toutefois, cela reste vrai, une démonstration étant donnée dans [Fon77], le fait important utilisé est qu'une k-algèbre finie est un anneau artinien. Le D_k-module $CW_k(A)$ s'appelle le *module de covecteurs de Witt* à coefficients dans A, le foncteur CW_k qui s'en déduit s'appelle le *foncteur des covecteurs de Witt*.

Une remarque importante à faire à ce niveau est la suivante. Considérons $\mathcal{G}$ un k-schéma en groupe fini unipotent. On a alors vu que le Verschiebung V était de torsion sur $M(\mathcal{G})$. Cela va impliquer que l'inclusion canonique $\mathrm{Hom}(\mathcal{G}, CW_k^u) \to \mathrm{Hom}(\mathcal{G}, CW_k)$ bien entendu déduite de l'inclusion de CW_k^u dans CW_k est en réalité un isomorphisme. Autrement dit, on vient de voir que si l'on définit le foncteur contravariant $\tilde{M}$ par :

$$\tilde{M}(\mathcal{G}) = \mathrm{Hom}(\mathcal{G}, CW_k)$$

il coïncide canoniquement avec le foncteur M défini précédemment du moins sur les k-schémas en groupe finis et unipotents. En fait, on peut montrer que c'est le cas partout, c'est-à-dire sur tous les k-schémas en groupe finis de rang une puissance de p. On déduit le théorème suivant, copie conforme du théorème 3.4.4.2 :

Théorème 3.4.4.3. *Le foncteur $\tilde{M}$ réalise une anti-équivalence entre la catégorie des k-schémas en groupe finis d'ordre une puissance de p et la catégorie des D_k-modules qui sont de longueur finie en tant que W-modules.*

En outre, on a l'égalité :

$$rg(\mathcal{G}) = p^{lg\left(\tilde{M}(\mathcal{G})\right)}$$

Finalement, si ℓ est une extension parfaite du corps k et si G_ℓ désigne l'extension des scalaires de k à ℓ de $\mathcal{G}$, il existe un isomorphisme canonique et fonctoriel entre les D_ℓ-modules $\tilde{M}(\mathcal{G}) \otimes_W W(\ell)$ et $\tilde{M}(G_\ell)$.

À partir de maintenant, on désignera simplement par M le foncteur $\tilde{M}$. On peut finalement donner une description d'un quasi-inverse de M. Soit $\mathcal{G}$ un k-schéma en groupe fini de rang une puissance de p, $M(\mathcal{G})$ son module de Dieudonné. $\mathcal{G}$ se retrouve à partir de $M(\mathcal{G})$ grâce à la formule suivante :

$$\mathcal{G}(A) = \mathrm{Hom}\left(M(\mathcal{G}), CW_k(A)\right)$$

valable pour tout k-algèbre finie A, le Hom étant bien évidemment pris dans la catégorie des D_k-modules, cela voulant dire que l'on s'intéresse aux applications W-linéaires entre $M(\mathcal{G})$ et $CW_k(A)$ qui commutent au Frobenius et au Verschiebung.

3.4.5 Systèmes de Honda finis

Dans cette partie, on considère à nouveau K un corps de caractéristique nulle complet pour une valuation discrète v supposée normalisée. On notera $\mathcal{O}_K$ l'anneau des entiers, $\mathfrak{m}$ son idéal maximal et $k = \mathcal{O}_K/\mathfrak{m}$ son corps résiduel. k est encore supposé parfait et de caractéristique p. Le but est de classifier les $\mathcal{O}_K$-schémas en groupe finis et plats de rang une puissance de p. Bien entendu si $\mathcal{G}$ est un tel schéma, on peut regarder sa fibre spéciale $\mathcal{G}_k = \mathcal{G} \times_{\mathcal{O}_K} k$ et d'après ce que l'on a dit précédemment, celle-ci est classifiée par son module de Dieudonné. L'idée est donc d'équiper ce module de Dieudonné d'une structure supplémentaire qui va permettre de reconstruire tout le $\mathcal{O}_K$-schéma. C'est ici qu'interviennent les systèmes de Honda.

Les démonstrations des résultats qui vont suivre sont bien détaillées dans [Con99].

Le cas non ramifié

Dans un premier temps, on va supposer que l'anneau $\mathcal{O}_K$ est non ramifié, c'est-à-dire qu'il est isomorphe canoniquement à $W = W(k)$. Ce qui va nous permettre de retrouver $\mathcal{G}$ est simplement la donnée supplémentaire d'un sous-W-module de $M(\mathcal{G}_k)$ vérifiant certaines conditions que nous allons énoncer.

Mais commençons plutôt par expliquer comment l'on construit ce sous-module. Prenons A une W-algèbre finie, et définissons l'application suivante :

$$w_A : \left(\begin{array}{rcl} CW_k(A/pA) & \to & (A \otimes_W K)/A \\ (\ldots, a_{-n}, \ldots, a_0) & \mapsto & \displaystyle\sum_{n=0}^{\infty} p^{-n-1} \hat{a}_{-n}^{p^n} \end{array} \right)$$

où $\hat{a}_{-n-1}$ est un rélèvement quelconque dans A de l'élément $a_{-n-1} \in A/pA$. On peut vérifier ([Fon77], chap. 2, prop. 5.1.) que la série écrite précédemment converge toujours et que la limite ne dépend pas des choix faits. En outre, w_A est une application W-linéaire.

Il est peut-être bon de remarquer que cela n'a rien de mystique. L'ensemble de départ représente les chiffres après la virgule d'un certain nombre que l'application w_A ne fait qu'évaluer finalement.

Remarquons maintenant que le module $M(\mathcal{G}_k)$ s'injecte naturellement dans le W-module $CW_k(\mathcal{A}/p\mathcal{A})$ où $\mathcal{A}$ désigne la bigèbre de $\mathcal{G}$. Pour cela, on voit dans un premier temps que $\mathcal{A}/p\mathcal{A}$ n'est autre que la bigèbre de la fibre spéciale $\mathcal{G}_k$. On voit ensuite que l'on a l'inclusion suivante :

$$\mathrm{Hom}(\mathcal{G}_k, CW_k) \subset \mathrm{Hom}_{\underline{\mathrm{Set}}}(\mathcal{G}_k, CW_k)$$

Le Hom de gauche désigne comme à l'habitude les morphismes de k-schémas en groupe, ou plutôt les transformations naturelles entre foncteurs de la catégorie des k-algèbres finies dans celle des groupes abéliens. Le $\mathrm{Hom}_{\underline{\mathrm{Set}}}$ de droite désigne quant à lui les mêmes transformations naturelles, mais ce coup-ci les foncteurs sont vus comme allant de la catégorie des k-algèbres finies dans celles des ensembles. L'inclusion provient alors simplement du fait qu'un morphisme de groupes est en particulier une application ensembliste.

Le lemme de Yoneda nous dit finalement que l'ensemble $\mathrm{Hom}_{\underline{\mathrm{Set}}}(\mathcal{G}_k, CW_k)$ s'identifie canoniquement à l'ensemble $CW_k(\mathcal{A}/p\mathcal{A})$ puisque $\mathcal{G}_k$ n'est autre que le foncteur $\mathrm{Hom}(\mathcal{A}/p\mathcal{A}, \cdot)$, et on obtient l'inclusion que l'on recherchait.

Rappelons toutefois comment cette flèche se construit de façon explicite. Considérons donc un morphisme $f : \mathcal{G}_k \to CW_k$, il induit par définition un morphisme de groupes $g : \mathcal{G}_k(\mathcal{A}/p\mathcal{A}) \to CW_k(\mathcal{A}/p\mathcal{A})$. Mais encore par définition $\mathcal{G}_k(\mathcal{A}/p\mathcal{A}) = \mathrm{Hom}(\mathcal{A}/p\mathcal{A}, \mathcal{A}/p\mathcal{A})$ et donc cet ensemble contient un élément priviligié qui est l'identité. Son image par g est un élément de $CW_k(\mathcal{A}/p\mathcal{A})$ qui est précisément l'image de f que l'on voulait construire. Après ce rappel, il est facile de se convaincre que l'application définie est W-linéaire.

On regarde alors la flèche composée :

$$M(\mathcal{G}_k) \longrightarrow CW(\mathcal{A}/p\mathcal{A}) \xrightarrow{w_{\mathcal{A}}} (\mathcal{A} \otimes_W K)/\mathcal{A}$$

Son noyau est un sous-W-module de $M(G_k)$ que l'on va noter $L(\mathcal{G})$ et c'est lui qui va permettre d'expliciter notre classification.

Proposition 3.4.5.1. *Ce noyau que l'on vient de définir n'est en fait pas totalement quelconque, il vérifie au moins les trois propriétés suivantes :*

1. $F(M(\mathcal{G}_K)) \cap L(\mathcal{G}) = pL(\mathcal{G})$
2. $M(\mathcal{G}_K) = F(M(\mathcal{G}_K)) + L(\mathcal{G})$
3. $V_{|L(\mathcal{G})}$ *est une application injective*

où F et V désignement respectivement le Frobenius et le Verschiebung.

On définit à ce moment un *système fini de Honda* comme la donnée d'un D_k-module M qui est de longueur finie en tant que W-module et d'un sous-W-module L de M vérifiant les trois conditions suivantes :

1. $F(M) \cap L = pL$
2. $M = F(M) + L$
3. $V_{|L}$ est une application injective

On peut définir bien entendu la catégorie des systèmes finis de Honda. Les objets sont évidemment les systèmes finis de Honda tels que nous venons de les décrire, un morphisme entre (M, L) et (M', L') est tout simplement une application D_k-linéaire de M dans M' qui envoie L sur un sous-W-module de L'. Il est intéressant de remarquer tout de suite que cette catégorie est abélienne.

La propriété précédente dit alors exactement que si $\mathcal{G}$ est un $\mathcal{O}_K$-schéma en groupe fini et plat de rang une puissance de p, le couple $(M(\mathcal{G}_k), L(\mathcal{G}))$ est un système de Honda. On a même un peu mieux, on a en fait défini un foncteur contravariant de la catégorie des $\mathcal{O}_K$-schémas en groupe finis et plats de rang une puissance de p dans la catégorie des systèmes finis de Honda. Notons-le LM.

Théorème 3.4.5.2 (Fontaine). *Si $p > 2$, le foncteur LM réalise une anti-équivalence de catégorie.*

La preuve de ce théorème est assez complexe, se décompose en plusieurs étapes et fait appel à d'autres résultats. Elle est très bien traitée dans [Con99]. Faisons toutefois quelques remarques. Insistons tout d'abord sur l'hypothèse $p > 2$ qui est réellement nécessaire, il existe un résultat un peu plus faible pour $p = 2$ qui ne classifie que les $\mathcal{O}_K$-schémas en groupe finis, plats et unipotents. Nous n'en aurons pas besoin ici, nous n'allons donc pas l'énoncer. Pour plus de détails, se reporter par exemple à [Fon75a].

Un corollaire de ce résultat est le fait que la catégorie des O_K-schémas en groupe finis et plats de rang une puissance de p est abélienne si $p > 2$. Ceci est en fait un cas particulier du résultat principal énoncé dans le paragraphe 3.3.4. En outre, si $p = 2$, il est annoncé dans ce même paragraphe que la catégorie en question n'est plus abélienne (en effet $e_K = 1$ n'est plus strictement inférieur à $p - 1 = 1$).

Pour finir, nous allons donner un quasi-inverse du foncteur LM. Prenons donc (M, L) un système de Honda fini. Le $\mathcal{O}_K$-schéma en groupe $\mathcal{G}$ dont il est l'image se décrit par exemple par la formule :

$$\mathcal{G}(A) = \mathrm{Hom}\left((M, L), (CW(A/pA), \ker w_A)\right)$$

valable pour toute W-algèbre finie et plate (ou libre) A.

On peut en particulier retrouver facilement la représentation galoisienne associée à un $\mathcal{O}_K$-schéma en groupe fini et plat de rang une puissance de p, disons $\mathcal{G}$, simplement à partir du système de Honda qui lui est associé disons (M, L). En effet, par définition, cette représentation galoisienne s'identifie à $\mathcal{G}_K\left(\bar{K}\right)$ muni de l'action du groupe de Galois, où bien entendu $\mathcal{G}_K = \mathcal{G} \times_{\mathcal{O}_K} K$ et $\bar{K}$ est une clôture algébrique de K. Mais on a :

$$\mathcal{G}_K\left(\bar{K}\right) = \varinjlim_L \mathcal{G}_K(L) = \varinjlim_L \mathcal{G}(\mathcal{O}_L) = \varinjlim_L \mathrm{Hom}\left((M, L), (CW(\mathcal{O}_L/p\mathcal{O}_L), \ker w_{\mathcal{O}_L})\right)$$

toutes les limites inductives étant étendues aux extensions finies L de K.

Si l'on pose finalement :

$$\mathcal{CW}_K = \varinjlim_L CW(\mathcal{O}_L/p\mathcal{O}_L)$$

et

$$\mathcal{L}_K = \varinjlim_L \ker w_{\mathcal{O}_L}$$

le groupe de Galois $\mathrm{Gal}\left(\bar{K}/K\right)$ agit sur le couple $(\mathcal{CW}_K, \mathcal{L}_K)$ et donc l'ensemble :

$$\mathrm{Hom}\left((M, L), (\mathcal{CW}_K, \mathcal{L}_K)\right)$$

a naturellement une structure de représentation de Galois et c'est bien celle qui est associée à notre $\mathcal{O}_K$-schéma de départ $\mathcal{G}$. On remarquera que le couple $(\mathcal{CW}_K, \mathcal{L}_K)$ n'est pas un système fini de Honda, mais il n'y a quand même aucun problème pour définir le Hom.

Le cas $e_K < p-1$

Il est encore possible de généraliser la classification précédente par les systèmes finis de Honda dans le cas de faible ramification. Dans ce paragraphe, donc, le corps K est supposé d'indice de ramification $e_K < p-1$[7] et on s'intéresse toujours à décrire les $\mathcal{O}_K$-schémas en groupe finis et plats de rang une puissance de p. On a vu qu'il existait alors un unique application de $W = W(k)$ dans $\mathcal{O}_K$ faisant commuter le diagramme suivant :

$$\begin{array}{ccccc} k & \longleftarrow & \mathcal{O}_K & \longrightarrow & K \\ \uparrow & & \uparrow{\scriptstyle e_K} & & \\ k & \longleftarrow & W & & \end{array}$$

Soit $\mathcal{G}$ un $\mathcal{O}_K$-schéma en groupe fini et plat de rang une puissance de p. Comme tout à l'heure, on commence par regarder la fibre générique $\mathcal{G}_k = \mathcal{G} \times_{\mathcal{O}_K} k$, et son module de Dieudonné $M(\mathcal{G}_k)$.

Définir l'équivalent du L est un peu plus compliqué, en particulier, il ne sera pas un sous-module de $M(\mathcal{G}_k)$ mais d'un autre objet construit à partir de ce $M(\mathcal{G}_k)$. Commençons donc par présenter celui-ci.

Nous allons en fait faire cette construction de façon plus générale, en partant d'un D_k-module, peu importe qu'il soit le module de Dieudonné de la fibre générique de quelqu'un. Dans un premier temps, on pose $M^{(p)} = M \otimes_W W$ où le facteur W est vu comme un W-module via le Frobenius $\sigma : W \to W$. Comme σ est bijectif, il est facile de décrire $M^{(p)}$: en tant que groupe abélien, il s'agit simplement de M, l'action d'un élément $w \in W$ sur $m \in M^{(p)}$ est donnée par :

$$w \cdot m = \sigma^{-1}(w)\, m$$

Le Frobenius F et le Verschiebung V définis sur M induisent alors des applications $\mathcal{O}_K$-linéaires $F_0 : M^{(p)} \to M$ et $V_0 : M \to M^{(p)}$.

On considère maintenant le diagramme suivant, qui pour une fois n'a aucune raison d'être commutatif :

$$\begin{array}{ccc} \mathfrak{m} \otimes_W M & \xrightarrow{V^M} & p^{-1}\mathfrak{m} \otimes_W M^{(p)} \\ \downarrow{\scriptstyle \varphi_0^M} & & \uparrow{\scriptstyle \varphi_1^M} \\ \mathcal{O}_K \otimes_W M & \xleftarrow{F^M} & \mathcal{O}_K \otimes_W M^{(p)} \end{array}$$

Il s'agit maintenant de décrire les flèches. φ_0^M (resp. φ_1^M) proviennent de l'inclusion de $\mathfrak{m}$ dans $\mathcal{O}_K$ (resp. de $\mathcal{O}_K$ dans $p^{-1}\mathfrak{m}$). Attention, ce n'est pas pour cela que ces flèches sont forcément injectives, elles ne le sont pas en général. Les applications V^M et F^M sont, quant à elles, définies par les formules suivantes :

$$V^M(x \otimes m) = p^{-1}x \otimes V_0(m)$$

$$F^M(x \otimes m) = x \otimes F_0(m)$$

Une chose importante à remarquer finalement est que tous les objets écrits dans ce diagramme sont en fait des $\mathcal{O}_K$-modules et que toutes les applications sont $\mathcal{O}_K$-linéaires. On considère donc, dans la catégorie des $\mathcal{O}_K$-modules, la limite directe de ce diagramme. Elle peut être décrite de façon explicite comme le quotient suivant :

$$M_{\mathcal{O}_K} = \frac{(\mathcal{O}_K \otimes_W M) \oplus \left(p^{-1}\mathfrak{m} \otimes_W M^{(p)}\right)}{\left\{\left(\varphi_0^M(u) - F^M(v), \varphi_1^M(v) - V^M(u)\right) \;\middle|\; u \in \mathfrak{m} \otimes_W M,\, v \in \mathcal{O}_K \otimes_W M^{(p)}\right\}}$$

[7] On remarquera que cette nouvelle classification ne donne encore aucun renseignement sur le cas $p = 2$ qui échappait à la théorie précédente.

Le module $M_{\mathcal{O}_K}$ ne vient toutefois pas seul, il est muni de plusieurs applications, qui vont notamment jouer le rôle du Frobenius et du Verschiebung. Le Frobenius sera l'application $F_M : p^{-1}\mathfrak{m}\otimes_W M^{(p)} \to M_{\mathcal{O}_K}$ déduite de l'inclusion canonique de $p^{-1}\mathfrak{m}\otimes_W M^{(p)}$ dans $(\mathcal{O}_K \otimes_W M)\oplus\left(p^{-1}\mathfrak{m}\otimes_W M^{(p)}\right)$. Le Verschiebung lui sera l'application $V_M : M_{\mathcal{O}_K} \to \mathcal{O}_K\otimes_W M^{(p)}$ que l'on définit en remarquant que l'application $(1\otimes V_0)\oplus(p\otimes \mathrm{id}) : (\mathcal{O}_K\otimes_W M)\oplus\left(p^{-1}\mathfrak{m}\otimes_W M^{(p)}\right) \to \mathcal{O}_K\otimes_W M^{(p)}$ passe au quotient. Il est facile de vérifier que tout cela fait commuter le diagramme suivant :

$$\begin{array}{ccccc} M^{(p)} & \xrightarrow{F_0} & M & \xrightarrow{V_0} & M^{(p)} \\ \downarrow & & \downarrow & & \downarrow \\ p^{-1}\mathfrak{m}\otimes_W M^{(p)} & \xrightarrow{F_M} & M_{\mathcal{O}_K} & \xrightarrow{V_M} & \mathcal{O}_K\otimes_W M^{(p)} \end{array}$$

En choisissant une uniformisante de $\mathcal{O}_K$, il est possible de rendre tous les modules et toutes les applications décrits ici totalement explicites. Nous n'allons toutefois pas le faire précisément, cela étant un peu laborieux et ne nous sera pas utile. Toutefois ces descriptions permettent de voir par exemple que si M est de longueur finie en tant que W-module, alors $M_{\mathcal{O}_K}$ est aussi de longueur finie en tant que W-module et que l'on a la relation :

$$\lg_{\mathcal{O}_K}(M_{\mathcal{O}_K}) = e_K \cdot \lg_W(M)$$

De même, cela permet de montrer que, encore sous l'hypothèse que M est de longueur finie en tant que W-module, les flèches du diagramme précédent induisent des isomorphismes entre $\ker F_M$ et $\ker F_0$, entre $\operatorname{coker} F_M$ et $\operatorname{coker} F_0$, entre $\ker V_M$ et $\ker V_0$ et finalement entre $\operatorname{coker} V_M$ et $\operatorname{coker} V_0$. On montre également que tous les modules que l'on vient de citer sont tués par $\mathfrak{m}$ et donc en fait des k-espaces vectoriels.

Il peut être finalement intéressant de définir l'application $\iota_M : \mathcal{O}_K\otimes_W M \to M_{\mathcal{O}_K}$ déduite de l'inclusion canonique de $\mathcal{O}_K\otimes_W M$ dans $(\mathcal{O}_K\otimes_W M)\oplus\left(p^{-1}\mathfrak{m}\otimes_W M^{(p)}\right)$.

Avant de poursuivre, il va nous falloir décrire un peu plus précisément le $\mathcal{O}_K$-module $CW_{k,\mathcal{O}_K}(A) = (CW_k(A))_{\mathcal{O}_K}$ où A est une $\mathcal{O}_K$-algèbre finie. Une proposition générale prouvée dans [Fon77] (page 195) dit que l'application :

$$\iota_{CW_k(A)} : \mathcal{O}_K\otimes_W CW_k(A) \to CW_{k,\mathcal{O}_K}(A)$$

est surjective et que son noyau s'identifie à :

$$K = \sum_{n=1}^{\infty} \operatorname{im}\left(\mathfrak{m}^{p^{n-1}}\otimes_W \ker V^n\right)$$

où V désigne bien entendu toujours le Verschiebung, ce coup-ci sur $CW_k(A)$. Cela prouve donc que $CW_{k,\mathcal{O}_K}(A)$ s'identifie au quotient $(\mathcal{O}_K\otimes_W CW_k(A))/K$.

Rappelons-nous désormais que l'on avait défini une application W-linéaire :

$$w_A : CW_k(A/pA) \to (A\otimes_W K)/A$$

En étendant les scalaires à $\mathcal{O}_K$, on obtient une application $\mathcal{O}_K$-linéaire :

$$\tilde{w}_A : \mathcal{O}_K\otimes_W CW_k(A/pA) \to (A\otimes_W K)/A$$

le module de droite étant déjà un $\mathcal{O}_K$-module.

On peut alors montrer (*cf* [Fon77], page 197) que le noyau de cette application contient K et que donc celle-ci se factorise par $CW_{k,\mathcal{O}_K}(A)$. On obtient ainsi ce qui va généraliser au cas peu ramifié le rôle de w_A à savoir l'application $\mathcal{O}_K$-linéaire :

$$w'_A : CW_{k,\mathcal{O}_K}(A/pA) \to (A\otimes_W K)/A$$

Désignons à nouveau par $\mathcal{A}$ la bigèbre de $\mathcal{G}$. On a vu que le module de Dieudonné $M(\mathcal{G}_k)$ était naturellement inclus dans $CW_k(\mathcal{A}/p\mathcal{A})$. Cette flèche d'inclusion induit un morphisme $M(\mathcal{G}_k)_{\mathcal{O}_K} \to CW_{k,\mathcal{O}_K}(\mathcal{A}/p\mathcal{A})$. On regarde alors comme précédemment la composée :

$$M(\mathcal{G}_k)_{\mathcal{O}_K} \longrightarrow CW_{k,\mathcal{O}_K}(\mathcal{A}/p\mathcal{A}) \xrightarrow{w'_{\mathcal{A}}} (\mathcal{A}\otimes_W K)/\mathcal{A}$$

On va noter finalement $L(\mathcal{G})$ le noyau de cette flèche composée. Là encore, le couple $(M(\mathcal{G}_k), L(\mathcal{G}))$ n'est pas quelconque, il vérifie certaines propriétés qui correspondent à celles de la proposition 3.4.5.1. Plus précisément on a la proposition suivante :

Proposition 3.4.5.3. *Avec les définitions précédentes, le couple $(M(\mathcal{G}_k), L(\mathcal{G}))$ vérifie :*

1. *$L(\mathcal{G})/\mathfrak{m}L(\mathcal{G}) \to \operatorname{coker} F_{M(\mathcal{G}_k)}$ est un isomorphisme*
2. *$V_{M|L(\mathcal{G})}$ est une application injective*

On remarquera que l'application $L(\mathcal{G})/\mathfrak{m}L(\mathcal{G}) \to \operatorname{coker} F_{M(\mathcal{G}_k)}$ est bien définie, car nous avons vu que le conoyau $\operatorname{coker} F_M$ était tué par $\mathfrak{m}$. On remarquera également que dans le cas particulier $e_K = 1$, toutes les définitions que nous avons données se simplifient magiquement et redonnent la description présentée dans le paragraphe précédent. La proposition ci-dessus est alors vraiment une copie conforme de la proposition 3.4.5.1.

Ceci bien entendu nous incite à définir un *système fini de Honda* sur $\mathcal{O}_K$ comme la donnée d'un D_k-module M qui est de longueur finie en tant que W-module et d'un sous-$\mathcal{O}_K$-module L de $M_{\mathcal{O}_K}$, le tout vérifiant les deux conditions suivantes :

1. $L/\mathfrak{m}L \to \operatorname{coker} F_M$ est un isomorphisme
2. $V_{M|L}$ est une application injective

La proposition précédente dit donc exactement que le couple $(M(\mathcal{G}_k), L(\mathcal{G}))$ est un système fini de Honda sur $\mathcal{O}_K$. En fait cette construction définit un foncteur LM de la catégorie des $\mathcal{O}_K$-schémas en groupe finis plats de rang une puissance de p dans la catégorie des systèmes finis de Honda, un morphisme entre deux systèmes finis de Honda (M, L) et (M', L') étant bien évidemment une application D_k-linéaires de M dans M' qui soit telle que l'application induite $M_{\mathcal{O}_K} \to M'_{\mathcal{O}_K}$ envoie L sur un sous-$\mathcal{O}_K$-module de L'. Le théorème principal est le suivant :

Théorème 3.4.5.4 (Conrad). *Le foncteur LM est une anti-équivalence de catégorie.*

La démonstration de ce résultat est en fait une généralisation pas toujours facile de la démonstration du théorème du paragraphe précédent. Nous n'allons pas du tout la détailler ici, cela est fait dans [Con99]. Ce papier regroupe d'autres résulats intéressants que nous citons en vrac ici. La catégorie des systèmes finis de Honda sur $\mathcal{O}_K$ est abélienne et dans celle-ci les noyaux et les conoyaux sont exactement ce à quoi l'on pourrait s'attendre. Ceci a notamment pour corollaire le fait déjà vu selon lequel la catégorie des $\mathcal{O}_K$-schémas en groupe finis et plats de rang une puissance de p est abélienne (on rappelle que depuis le début de ce paragraphe, on a supposé $e_K < p-1$).

Disons finalement que cette classification s'étend, avec quelques modifications, au cas $e_K = p-1$ mais n'est alors plus valable que pour les groupes unipotents.

Terminons ce paragraphe en décrivant un quasi-inverse du foncteur LM. Partons donc d'un système fini de Honda sur $\mathcal{O}_K$, disons (M, L). Pour décrire $\mathcal{G}$, le $\mathcal{O}_K$-schéma en groupe qui lui est associé, il suffit de donner les groupes $\mathcal{G}(A)$ pour toute $\mathcal{O}_K$-algèbre finie et plate (ou libre) A. On a en fait la formule suivante :

$$\mathcal{G}(A) = \operatorname{Hom}\left((M, L), (CW_k(A/pA), \ker w'_A)\right)$$

là encore, le couple de droite n'est pas un système de Honda fini mais cela n'a aucune importance pour définir le Hom.

3.4.6 Quelques mots sur le cas général

Il existe finalement une classification des $\mathcal{O}_K$-schémas en groupe finis et plats de rang une puissance de p, sans aucune restriction sur la ramification. Nous n'allons pas du tout la présenter, mais juste la signaler.

Le papier détaillant cela est [Bre00]. Disons toutefois que cette classification se fait en termes de modules filtrés, et donc ne peut pas spécialement être vue comme une généralisation des systèmes de Honda.

3.5 Deuxième preuve du théorème

Berthelot a utilisé la classification précédente pour donner une nouvelle preuve de notre théorème, du moins dans le cas non ramifié, dans l'article [Ber77]. C'est elle que nous allons présenter dans ce chapitre.

3.5.1 Rappel de la situation

On part toujours de K un corps de caractéristique nulle, complet pour une valuation discrète v. On note $\mathcal{O}_K$ l'anneau des entiers, $\mathfrak{m}$ son idéal maximal et $k = \mathcal{O}_K/\mathfrak{m}$ le corps résiduel. On suppose que ce dernier est parfait de caractéristique $p > 0$. Dans la suite, on va supposer que K est non ramifié, c'est-à-dire que l'indice de ramification absolu $e_K = 1$, en particulier $\mathcal{O}_K$ sera canoniquement isomorphe à l'anneau $W(k)$ que l'on notera encore W.

On se donne maintenant un $\mathcal{O}_K$-schéma en $\mathbb{F}_p$-vectoriel fini et plat. Son extension des scalaires à K, $\mathcal{G}_K = \mathcal{G} \times_{\mathcal{O}_K} K$ correspond à une représentation du groupe de Galois $\mathrm{Gal}\left(\bar{K}/K\right)$, où $\bar{K}$ est une clôture algébrique de K fixée une fois pour toutes. On rappelle que cette représentation est simplement le F_p-espace vectoriel $\mathcal{G}_K\left(\bar{K}\right)$ sur lequel $\mathrm{Gal}\left(\bar{K}/K\right)$ agit naturellement.

On restreint alors cette représentation au groupe d'inertie I. Cette restrictiom n'a aucune raison d'être simple, mais on en considère un quotient de Jordan-Hölder, ce qui fournit une réprésentation simple $\rho : I \to \mathrm{GL}(V)$ où V est un certain espace vectoriel de dimension finie sur $\mathbb{F}_p$. On a vu que dans ces conditions, ρ se factorisait par le groupe d'inertie modérée I_m et donc fournit une nouvelle représentation $\rho' : I_m \to \mathrm{GL}(V)$. On a vu également que V était muni d'une structure de corps fini. ρ' se réduit donc à un caractère $I_m \to V^\star$. Si l'on choisit une indexation $\psi_1, \ldots, \psi_r$ des caractères fondamentaux de I_m à valeurs dans $V^\star$, ρ' va s'écrire de la façon suivante :

$$\rho' = \psi_1^{n_1} \ldots \psi_r^{n_r}$$

où les n_i sont des entiers compris entre 0 et $p-1$ non tous nuls et ainsi uniquement déterminés. r est par définition la dimension de la représentation ρ' et le cardinal de V est alors $q = p^r$.

Le théorème 3.1.5.2 affirme alors que les entiers n_i sont tous inférieurs ou égaux à l'indice de ramification $e_K = 1$.

Une première remarque est que si $p = 2$, le théorème n'apporte aucun élément nouveau. Enfin, de façon plus générale, le théorème a un réel intêret que dans le cas où $e_K < p - 1$, ce qui justifie un peu le soin particulier que l'on a porté à présenter la classification par les systèmes de Honda dans ce cas. Tout cela pour dire que par la suite, on supposera $p > 2$, et on utilisera la classification par les systèmes de Honda dans le cas non ramifié.

Par la suite $\mathcal{G}$ et $\mathcal{G}_K$ désigneront les schémas en $\mathbb{F}_p$-vectoriels associés à cette nouvelle représentation ρ' simple. $\mathcal{G}_K$ existe bien car toute telle représentation correspond à un K-schéma en groupe fini et étale. Quant à $\mathcal{G}$, il existe bien, car on appelle que l'on a vu que sous l'hypothèse $e_K < p - 1$, toute suite de

composition de Jordan-Hölder de schémas en groupe finis de rang une puissance de p sur K se relève sur $\mathcal{O}_K$.

Une deuxième remarque est que l'on peut supposer sans perte de généralité que le corps résiduel k est algébriquement clos. En effet, rappelons que le groupe d'inertie peut-être vu comme un groupe de Galois, précisément celui de l'extension $\bar{K}/K^{\mathrm{nr}}$ où K^{nr} désigne l'extension maximale non ramifiée de K incluse dans $\bar{K}$ et a pour corps résiduel $\bar{k}$. Ainsi le fait de restreindre la représentation au groupe d'inertie revient en fait à supposer que $K = \widehat{K^{\mathrm{nr}}}$ et donc que k est algébriquement clos.

Maintenant que cela est dit, considérons le système de Honda fini associé au $\mathcal{O}_K$-schéma en groupe fini et plat tué par p (et donc de rang une puissance de p), et notons-le par exemple (M, L). Nous allons traduire les propriétés de $\mathcal{G}$ sur M et sur L et vérifier ensuite notre théorème.

3.5.2 Description du système fini de Honda (M, L)

$\mathcal{G}_K$ hérite lui aussi d'une structure de K-schéma en $\mathbb{F}_q$-vectoriel et on a vu que, comme on a supposé que l'indice de ramification $e_K < p - 1$, cette structure se prolonge en fait à $\mathcal{G}$. On dispose donc, pour tout $\lambda \in \mathbb{F}_q$, d'un morphisme $[\lambda] : \mathcal{G} \to \mathcal{G}$ qui induit donc un endomorphisme que l'on va encore noter $[\lambda]$ du système de Honda fini (M, L).

$\mathcal{G}$ est par hypothèse tué par p, cela se traduit directement en disant que le W-module (on rappelle que $W = \mathcal{O}_K$) est tué par p. Ainsi M est un espace vectoriel sur le corps résiduel k, et L en est un sous-k-espace vectoriel. Les applications $[\lambda]$ sont simplement des endomorphismes k-linéaires de M qui stabilisent L et qui commutent au Frobenius et au Verschiebung que nous allons bientôt décrire.

Une dernière remarque à faire avant d'entamer la description est de voir que $\mathcal{G}_K$ a pour rang $p^r = q$. La longueur de M en tant que W-module est donc r, ce qui est représente encore la dimension de M comme k-espace vectoriel.

Pour tout caractère $\chi : \mathbb{F}_q^\star \to k^\star$, on commence par définir le sous-k-espace vectoriel de M suivant :

$$M_\chi = \{m \in M \mid [\lambda]\, m = \chi(\lambda)\, m\}$$

Si on définit en outre :

$$\pi_\chi = \frac{1}{q-1} \sum_{\lambda \in \mathbb{F}_q^\star} \chi(\lambda)^{-1}\, [\lambda]$$

on remarque que les π_χ sont des projecteurs deux à deux orthogonaux de somme l'identité, et que M_χ est exactement l'image de π_χ. Cela prouve que M se décompose en tant que k-espace vectoriel de la façon suivante :

$$M = \bigoplus_{\chi : \mathbb{F}_q^\star \to k^\star} M_\chi$$

Un *caractère fondamental*, comme nous l'avons déjà défini (*cf* 3.2.1), est un caractère $\chi : \mathbb{F}_q^\star \to k^\star$ qui est en outre additif. Supposons que l'espace M_χ soit non nul, et considérons $x \in M_\chi$, $x \neq 0$. On a alors :

$$[\lambda + \mu](x) = [\lambda](x) + [\mu](x)$$

et donc :

$$\chi(\lambda + \mu)\, x = [\chi(\lambda) + \chi(\mu)]\, x$$

ce qui prouve que χ est un caractère fondamental et donc la somme :

$$M = \bigoplus_{\chi} M_\chi$$

peut être simplement étendue aux caractères fondamentaux. Rappelons que les caractères fondamentaux sont au nombre de r, et qu'on peut choisir de les indexer par les éléments de $\mathbb{Z}/r\mathbb{Z}$ de sorte que $\chi_{i+1} = \chi_i^p$. On notera $M_i = M_{\chi_i}$ de sorte que finalement la décomposition précédente, s'écrive :

$$M = \bigoplus_{i \in \mathbb{Z}/r\mathbb{Z}} M_i$$

Regardons maintenant comment Frobenius et Verschiebung s'expriment dans cette décomposition. $[\lambda]$ étant un endomorphisme du système de Honda, son action commute à celle de F, on en déduit que si $x \in M_i$:

$$[\lambda](F(x)) = F([\lambda]x) = F(\chi_i(\lambda)x) = \chi_i(\lambda)^p F(x) = \chi_{i+1}(\lambda) F(x)$$

et donc que $F(x) \in M_{i+1}$. Cela prouve donc que $F(M_i) \subset M_{i+1}$. De même, on a $V(M_{i+1}) \subset M_i$.

Nous allons maintenant montrer qu'aucun des M_i ne peut être nul. Supposons donc qu'il existe un i tel que $M_i = 0$. D'après ce qui précède, cela impliquerait que le Frobenius F est nul sur M_{i-1}. Ainsi en vertu de l'inclusion $\ker F \subset \operatorname{im} V$ valable car (M, L) est un système fini de Honda, tout élément $x \in M_{i-1}$ est dans l'image de V et donc s'écrit $V(y)$ pour un certain $y \in M$. Finalement, le fait que V envoie M_j sur M_{j-1} prouve que $x = 0$. On a ainsi montré que $M_{i-1} = 0$. De même on montre que tous les M_i sont nuls et donc M aussi, mais cela n'est pas vrai. On en déduit en définitive qu'aucun des M_i n'est nul.

Mais les M_i sont au nombre de r et la dimension de M est également r. Il n'y a donc qu'une seule possibilité : tous les M_i sont de dimension 1 sur k. Choisissons donc maintenant pour tout i, un générateur de l'espace vectoriel M_i, disons e_i. En vertu de l'égalité $\ker F = \operatorname{im} V$ (on n'oublie pas que $FV = VF = p = 0$), il existe pour tout i, un élément $\alpha_i \in k^\star$ tel que soit $F(e_i) = \alpha e_{i+1}$ soit $V(\alpha_i e_{i+1}) = e_i$. Comme k est supposé algébriquement clos, on peut multiplier chacun des e_i par une certaine constante de telle façon que les α_i disparaissent. Plus précisément on a la proposition suivante qui résume tout ce que l'on vient de dire :

Proposition 3.5.2.1. *Il existe une base $(e_1, \ldots, e_r)$ de M dans laquelle :*

1. *la matrice du Frobenius*[8] *s'écrit :*

$$\begin{pmatrix} 0 & \cdots & 0 & \varepsilon_r \\ \varepsilon_1 & & & 0 \\ 0 & & & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix}$$

   où les ε_i sont égaux soit à 0 soit à 1

2. *la matrice du Verschiebung*[9] *s'écrit :*

$$\begin{pmatrix} 0 & \bar{\varepsilon}_1 & 0 & \cdots & 0 \\ \vdots & & & & \\ & & & & 0 \\ 0 & & & & \bar{\varepsilon}_{r-1} \\ \bar{\varepsilon}_r & 0 & \cdots & & 0 \end{pmatrix}$$

   où $\bar{\varepsilon}_i = 1 - \varepsilon_i$

[8] Il s'agit de faire attention au fait que le Frobenius n'est pas une application linéaire, du moins si on le voit de M dans M. Parler de matrice est peut-être donc un peu abusif. On peut voir toutefois le Frobenius comme une application de $M^{(p)}$ dans M, ce coup-ci k-linéaire et de dire que la matrice donnée correspond à la matrice de cette application lorsque M est munie de la base $(e_1, \ldots, e_r)$ et $M^{(p)}$ est munie de la base $(e_1^{(p)}, \ldots, e_r^{(p)})$ où $e_i^{(p)} = e_i \otimes 1$ (c'est-à-dire $e_i^{(p)} = e_i$ si l'on identifie $M^{(p)}$ à M en tant que groupe additif.

[9] Même remarque.

3. pour tout $\lambda \in \mathbb{F}_q$, la matrice de $[\lambda]$ s'écrit :

$$\begin{pmatrix} \chi_1(\lambda) & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \chi_r(\lambda) \end{pmatrix}$$

Comme p est nul dans M, le fait que (M, L) soit un système fini de Honda prouve que $F(M) \oplus L = M$. Mais vu les descriptions précédentes, il est facile de déterminer $F(M)$, il s'agit précisément de :

$$F(M) = \bigoplus_{i \text{ tq } \varepsilon_i = 1} M_i$$

D'autre part, comme les $[\lambda]$ sont des morphismes du système fini de Honda (M, L), ils stabilisent L et donc en particulier L s'écrit comme une somme de certains des M_i. Cela prouve directement que :

$$L = \bigoplus_{i \text{ tq } \varepsilon_i = 0} M_i$$

Une façon un peu plus algébrique de redire la chose est la suivante :

Proposition 3.5.2.2. *Il existe un entier s et des entiers n_i et m_i pour $i \in \mathbb{Z}/s\mathbb{Z}$ tel que le D_k-module M soit engendré par des éléments $x_1, \ldots, x_s$ soumis aux seules relations :*

1. $px_i = 0$
2. $F^{n_i}(x_i) = V^{m_{i+1}}(x_{i+1})$

En outre L est engendré en tant que W-modules par les éléments $V^j(x_i)$ pour $0 \leqslant j < m_i$.

Pour voir cela, il suffit de regarder les j tels que $\varepsilon_j = 0$ et $\varepsilon_{j+1} = 1$ et d'écrire les choses qui en découle. Si x_i correspond à e_{α_i}, l'entier m_i donne le nombre de 0 qui précèdent directement ε_{α_i}, lui-même inclus et l'entier n_i donne le nombre de 1 qui suivent directement ε_{α_i}. En particulier $\sum_{i \in \mathbb{Z}/s\mathbb{Z}} n_i$ donne le nombre d'indices j tels que $\varepsilon_j = 1$ et $\sum_{i \in \mathbb{Z}/s\mathbb{Z}} m_i$ donne le nombre d'indices j tels que $\varepsilon_j = 0$. On a ainsi la relation :

$$\sum_{i \in \mathbb{Z}/s\mathbb{Z}} m_i + n_i = r$$

3.5.3 Description de la représentation associée

Le but de ce paragraphe est de décrire l'espace vectoriel $\mathcal{G}_K(\bar{K})$. On se rappelle pour cela que l'on a vu que :

$$\mathcal{G}_K(\bar{K}) = \mathrm{Hom}((M, L), (\mathcal{CW}_K, \mathcal{L}_K))$$

et que l'on vient de donner une description par générateurs et relations de (M, L). On rappelle peut-être également que, par définition :

$$CW_K = \varinjlim_L CW(\mathcal{O}_L / p\mathcal{O}_L)$$

et

$$\mathcal{L}_K = \varinjlim_L \mathcal{L}_K$$

où la limite inductive est étendue à toutes les extensions finies L de K.

Un élément de $\mathcal{G}_K\left(\bar{K}\right)$ se résumé donc à la donnée d'éléments $y_i = \left(a_{-j,i}\right)_{j\in\mathbb{N}} \in CW_k\left(\mathcal{O}_L/p\mathcal{O}_L\right)$ pour i variant dans $\mathbb{Z}/s\mathbb{Z}$. Ces éléments sont soumis aux relations :

$$\forall i,\, \forall j \geqslant 1, \quad a_{-j,i}^{p} = 0$$

$$\forall i,\, \forall j \geqslant 0, \quad a_{-j,i}^{p^{n_i}} = a_{-j-m_{i+1},i+1}$$

D'autre part, il ne faut pas oublier que l'on a affaire à des morphismes dans la catégorie des systèmes finis de Honda, et donc que l'on doit vérifier la condition supplémentaire d'envoyer L sur un sous-W-module de $\mathcal{L}_K$. Cela se traduit par les équations :

$$\forall i,\, \forall j < m_i, \quad \sum_{n=0}^{\infty} p^{-n-1} b_{-j-n,i}^{p^n} \in \mathcal{O}_L$$

où $b_{-j,i} \in \mathcal{O}_L$ désigne un relèvement quelconque de $a_{-j,i}$.

Il s'agit maintenant d'expliciter sur les y_i l'action naturelle de $\mathrm{Gal}\left(\bar{K}/K\right)$ sur $\mathcal{G}_K\left(\bar{K}\right)$. On a en fait la proposition suivante :

Proposition 3.5.3.1. *Avec les notations précédentes, l'action de $\sigma \in Gal\left(\bar{K}/K\right)$ est donnée par :*

$$\sigma\left(y_i\right) = \theta_{q-1}\left(\sigma\right)^{\mu_i} y_i$$

où μ_i est défini par l'expression suivante :

$$\mu_i = \sum_{n=n_i+1}^{n_i+m_i+1} p^{r-n} + \ldots + \sum_{n=r-m_i+1}^{r} p^{r-n}$$

Rappelons quand même encore une fois la définition de θ_{q-1}. Il s'agit d'un caractère de $\mathrm{Gal}\left(\bar{K}/K\right)$ à valeurs dans $\mu_{q-1}\left(\bar{k}\right)$. Si l'on choisit dans $\bar{K}$ une racine $(q-1)$-ième de p, disons ζ, c'est celui qui vérifie pour tout $\sigma \in \mathrm{Gal}\left(\bar{K}/K\right)$ la relation :

$$\sigma\left(\zeta\right) = \theta_{q-1}\left(\sigma\right)\zeta$$

Donnons quelques indications sur la preuve de cette proposition. On commence en fait par prouver que les congruences données sur les $b_{-j,i}$ impliquent :

1. $\forall i,\, b_{0,i}^{p^{n_i}} = b_{-m_i+1,i+1} \pmod{p}$
2. $\forall i,\, \forall j < m_i,\, b_{-j,i} + p^{-1} b_{-j-1,i}^{p} = 0 \pmod{p}$

On peut montrer également que si $j \geqslant m_i$, $b_{-j,i}$ est congru à 0 modulo p, sauf dans le cas où tous les $\varepsilon_j = 0$, on a alors $b_{-j,i}$ congru à $b_{-j',i}$ modulo p, où j' est le reste de la division euclidienne de j par r. Tout cela pour dire que l'on aura pas à s'inquiéter des $b_{-j,i}$ avec $j \geqslant m_i$.

Ces nouvelles conditions impliquent, pour $j < m_i$ la congruence suivante :

$$b_{-j,i}^{q} = (-p)^{\mu_{i,j}}\, b_{-j,i} \pmod{p^{\mu_{i,j}+1}}$$

où, par définition :

$$\mu_{i,j} = \sum_{n=1}^{j} p^{r-n} + \sum_{n=j+n_i+1}^{j+n_i+m_i+1} p^{r-n} + \sum_{n=j+n_i+m_{i+1}+n_{i+1}+1}^{j+n_i+m_{i+1}+n_{i+1}+m_{i+2}} p^{r-n} + \ldots + \sum_{n=r-m_i+j+1}^{r} p^{r-n}$$

En particulier, on remarque que $\mu_{i,0} = \mu_i$.

Avant de poursuivre, remarquons que $\mu_{i,j}$ est défini comme une somme de puissance de p toutes distinctes. Cela implique en particulier que l'on a ici la décomposition de $\mu_{i,j}$ en base p, et on voit que les seuls chiffres qui peuvent intervenir sont 0 et 1. Cela implique aussi que $\mu_{i,j} < p^r = q$.

En fait, si μ est un entier tel que $0 \leqslant \mu < q$ et $x \in \mathcal{O}_L$ vérifiant $x^q = (-p)^\mu x \pmod{p^{\mu+1}}$, il existe toujours un $x' \in \mathcal{O}_{\bar{K}}$ congru à x modulo p tel que $x'^q = (-p)^\mu x'$. Cela prouve que l'on peut supposer sans problème que la dernière congruence annoncée est en fait une égalité.

Mais prouvons le fait que l'on vient d'annoncer. On cherche pour cela x' sous la forme $x' = x + py$. y est alors solution de l'équation polynômiale :

$$\sum_{i=0}^{q} C_q^i x^{q-i} (py)^i - (-p)^\mu (x + py) = 0$$

Autrement, y est racine du polynôme $P(X) = \sum_{i=0}^{q} \alpha_i X^i$ où les α_i sont donnés par :

$$\begin{aligned} & \alpha_0 = x^q - (-p)^\mu x \\ & \alpha_1 = qpx^{q-1} + (-p)^{\mu+1} \\ \forall i \geqslant 2 \qquad & \alpha_i = C_q^i x^{q-i} p^i \end{aligned}$$

Nous allons pour prouver que ce polynôme a une racine dans $\mathcal{O}_{\bar{K}}$ utiliser la méthode des polygônes de Newton. Nous n'allons pas la rappeler ici en détail, disons simplement qu'une condition suffisante est $v(\alpha_0) \geqslant v(\alpha_1)$ et $v(\alpha_i) < v(\alpha_1)$ pour tout $i \geqslant 2$, v désigne toujours la valuation sur $\mathcal{O}_K$ normalisée par $v(\mathcal{O}_K) = \mathbb{Z}$ ou ce qui revient au même puisque K est supposé non ramifié par $v(p) = 1$. Essayons donc d'estimer ces valuations.

Par hypothèse α_0 est divisible par $p^{\mu+1}$, ce qui se traduit directement par :

$$v(\alpha_0) \geqslant \mu + 1$$

α_1 est une somme de deux termes, nous allons donc estimer la valuation de chacun d'entre eux. Bien entendu, la valuation de $(-p)^{\mu+1}$ est $\mu + 1$. Il ne reste donc qu'à estimer celle de x. Écrivons pour cela :

$$v(x^q - (-p)^\mu x) = v(x) + v\left(x^{q-1} - (-p)^\mu\right) \geqslant \mu + 1$$

et supposons que $v(x) < \frac{\mu}{q-1}$. Dans ce cas, $v\left(x^{q-1}\right) < \mu = v((-p)^\mu)$. Cela permet donc de calculer la valuation de la somme est de prouver finalement que :

$$v(x^q - (-p)^\mu x) = qv(x)$$

On en déduit que $v(x) \geqslant \frac{\mu+1}{q}$. Le fait que $\mu < q$, et donc que $\mu \leqslant q-1$, prouve que $\frac{\mu+1}{q} \geqslant \frac{\mu}{q-1}$ et conduit donc à une absurdité. De tout cela, on déduit que :

$$v(x) \geqslant \frac{\mu}{q-1}$$

et puis que :

$$v(\alpha_1) = \mu + 1$$

Finalement le fait que C_i^q soit toujours un entier prouve que sa valuation est toujours positive et donc que, pour tout $i \geqslant 2$:

$$v(\alpha_i) \geqslant \mu + i > \mu + 1$$

Il ne reste plus qu'à rassembler tout ce que l'on vient de dire pour conclure : x' existe toujours bien.

On suppose donc à partir de maintenant que $b_{-j,i}$ est solution de l'équation :

$$b_{-j,i}^{q} = (-p)^{\mu_{i,j}}\, b_{-j,i}$$

Si ζ désigne à nouveau une racine $(q-1)$-ième de l'unité, $b_{-j,i}$ va s'écrire sous la forme $b_{-j,i} = u\zeta^{\mu_{i,j}}$ où u est une unité de W. Cela prouve que, pour tout $\sigma \in \mathrm{Gal}\left(\bar{K}/K\right)$ et pour tout $j < m_i$:

$$\sigma\left(b_{-j,i}\right) = \theta_{q-1}^{\mu_{i,j}} b_{-j,i}$$

La proposition s'ensuit finalement si l'on a remarqué que $p^j \mu_{i,j} = \mu_i \pmod{(q-1)}$.

3.5.4 Fin de la preuve

La façon de conclure est alors quasiment analogue à celle du paragraphe 3.3.3. Si l'on fait les bons choix, les caractères χ_i et ψ_i sont toujours reliés par la relation $\psi_i = \chi_i^{-1} \circ \theta_{q-1}$.

L'espace vectoriel sur lequel agit la représentation ρ' s'identifie à $\mathcal{G}_K\left(\bar{K}\right)$ que l'on vient de décrire et ρ' n'est autre que :

$$\rho' : \left(\begin{array}{ccc} I_m & \to & \mathrm{GL}\left(\mathcal{G}_K\left(\bar{K}\right)\right) \\ \sigma & \mapsto & (f \mapsto \sigma \circ f) \end{array} \right)$$

Pour connaître la décomposition de notre caractère sur les caractères fondamentaux, il suffit de trouver le $\lambda \in \mathbb{F}_q$ qui fait commuter le diagramme suivant :

$$\begin{array}{ccc} (M,L) & \xrightarrow{f} & (\mathcal{CW}_K, \mathcal{L}_K) \\ {\scriptstyle [\lambda]}\downarrow & & \downarrow{\scriptstyle \sigma} \\ (M,L) & \xrightarrow{f} & (\mathcal{CW}_K, \mathcal{L}_K) \end{array}$$

et ce pour tout $f \in \mathrm{Hom}\left((M,L), (\mathcal{CW}_K, \mathcal{L}_K)\right)$.

Regardons par exemple comment est envoyé l'élément $x_1 \in M$ par chacun de deux chemins présentés. Si on pose par exemple $f(x_1) = y_1$ et si l'on dit que x_i correpond au caractère fondamental χ_j, on obtient la relation :

$$\chi_j(\lambda)\, y_1 = \theta_{q-1}(\sigma)^{\mu_1}\, y_1$$

On a toute liberté dans le choix de f, et donc on peut supposer que $y_1 \neq 0$. Ainsi on obtient l'égalité :

$$\chi_j(\lambda) = \theta_{q-1}(\sigma)^{\mu_1}$$

puis

$$\lambda = \psi_j(\sigma)^{\mu_1}$$

Il s'agit donc pour conclure simplement de vérifier que l'écriture en base p du nombre μ_1 ne fait intervenir que les chiffres 0 et 1 mais cela se voit directement sur la définition.

Bibliographie

[Ber77] P. Berthelot. Systèmes de honda des schémas en $\mathbb{F}_q$-vectoriels. *Bull. Soc. math. France*, 105 :225–239, 1977.

[Bre00] C. Breuil. Groupes p-divisibles, groupes finis et modules filtrés. *Annals of Mathematics*, 152 :489–549, 2000.

[Con99] B. Conrad. Finite group schemes over bases with low ramification. *Compositio Math.*, 119 :239–320, 1999.

[Dem72] M. Demazure. *Lectures on p-divisible groups*, volume 302. Springer-Verlag, 1972. Lecture note in mathematics.

[Fon75a] J.M. Fontaine. Groupes finis commutatifs sur les vecteurs de witt. *C.R. Acad. Sc. Paris*, 280 :1423–1425, 1975.

[Fon75b] J.M. Fontaine. Groupes p-divisibles sur les vecteurs de witt. *C.R. Acad. Sc. Paris*, 280 :1353–1356, 1975.

[Fon75c] J.M. Fontaine. Sur la construction du module de dieudonné d'un groupe formel. *C.R. Acad. Sc. Paris*, 280 :1273–1276, 1975.

[Fon77] J.M. Fontaine. *Groupes p-divisibles sur les corps locaux*. Société mathématique de France, 1977. Astérisque 47-48.

[Ray74] M. Raynaud. Schémas en groupes de type $(p, \ldots, p)$. *Bull. Soc. math. France*, 102 :241–280, 1974.

[Ser72] J.P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones math.*, 15 :259–331, 1972.

[Wat79] W.C. Waterhouse. *Introduction to Affine Group Schemes*. Springer-Verlag, Paris, 1979.

Troisième partie

Vulgarisation

Chapitre 4

L'axiome du choix

J'ai décidé de rédiger cet article suite à la lecture du groupe de discussion `fr.sci.maths`. L'axiome du choix possède quand même une certaine notoriété et est en fait souvent mal compris et surinterprété.

Cet article a pour but de présenter les choses, simplement d'un point de vue mathématique sans porter de jugement philosophique quelconque sur les droits ou l'intuition. Afin de toucher un plus large public, sans toutefois tomber dans la simplicité consistant à contourner les difficultés, cet article commence par faire de nombreux (r)appels sur les fondements des mathématiques. Ces rappels ne sont *a posteriori* peut-être pas aussi bienheureux qu'on aurait pu le croire, un lecteur non habitué pouvant facilement être rapidement submergé et découragé.

Sommaire

4.1 Introduction

Nous allons parler de l'axiome du choix, spécifiquement dans un contexte mathématique et spécifiquement en logique classique dans l'axiomatisation des ensembles usuelle appelée ZF. Nous allons donc dans un premier temps présenter cette axiomatisation et faire tous les (r)appels nécessaires à un énoncé précis de l'axiome du choix.

Il est important d'avoir constamment en tête que la logique ne cherche pas à construire le "monde" à partir de rien, mais plutôt à supposer qu'il est là et à l'étudier. Bien entendu, pour cela, on se donne des a priori sur ce monde, ce que l'on appelle les axiomes, et on voit comment il réagit. Dans la suite, quand on parlera de modèle de ZF, il faut sans doute avoir à l'esprit qu'il s'agit simplement d'une boîte qui se comporte comme on lui demande et qui est censée se comporter comme le monde qui nous entoure. Ce sont ces boîtes, extérieures à nous osons le dire, que nous allons étudier.

Bon arrêtons de mal philosopher et parlons un peu de maths pour changer :-).

4.2 Présentation de la théorie des ensembles

Avant de parler de l'axiome du choix, il s'agit de formaliser les ensembles. La formalisation classique, que l'on appelle ZF (pour théorie de Zermelo-Fraenkel), est celle que nous allons présenter. Pour se mettre dans l'esprit de ZF, il faut oublier la description des ensembles tels des patates qui contiennent des points. Dans ZF, il n'y a pas de typage, il n'y a pas non plus de distinction entre ensemble et élément. Plus précisément dans ZF, tout est ensemble. En particulier, les éléments d'un ensemble sont encore des ensembles qui ont à leur tour des éléments qui sont encore des ensembles, etc. Ce point de vue a priori un peu barbare permet en fait d'écrire les choses de façon simple. Paradoxalement, la bonne façon de se représenter ces ensembles ne passe pas par des patates incluses les unes dans les autres, mais plutôt par une grosse patate que l'on appelle l'univers et dont les éléments sont précisément les ensembles, ces ensembles étant reliés par des flèches orientées qui indiquent l'appartenance. Informellement, l'univers représente l'ensemble de tous les ensembles mais celui-ci n'en est pas un au sens où il ne correspondra à aucun point dans la grosse patate.

Mais commençons tout de suite à dire les choses de façon plus précise.

4.2.1 Les axiomes de ZF

Un *modèle de ZF* ou encore un *univers* est un "ensemble" non vide (dans un sens intuitif) que l'on va appeler U muni d'une relation binaire vérifiant certains axiomes que l'on va lister. Rappelons dans un premier temps, qu'une relation binaire sur U est simplement une partie de $U \times U$, autrement dit pour tout couple (x, y) d'éléments de U, on est capable de dire si x est en relation avec y, ou si ce n'est pas le cas. Attention, l'ordre ici est important, la relation n'est pas du tout supposée symétrique. Une façon de représenter une relation binaire est de placer une flèche orientée entre x et y lorsqu'ils sont en relation dans cet ordre.

Les éléments de U vont être ce que l'on appelle les *ensembles* et le fait que x soit en relation avec y se notera "$x \in y$" (lire x appartient à y). Il faut faire attention au fait que le mot "ensemble" est à ce stade très ambigu. Par la suite, lorsque nous l'emploierons, il désignera toujours (sauf mention expresse du contraire) un élément de l'univers U.

Disons finalement que si A est un ensemble (donc un élément de U), un élément de A sera simplement un ensemble x tel que $x \in A$. Il est temps maintenant de donner les axiomes que doit vérifier la relation d'appartenance donnée sur U.

On utilisera l'abréviation "$A \subset B$" pour "$\forall x(x \in A) \Rightarrow (x \in B)$". On dira dans ce cas que A est un sous-ensemble (ou une partie) de B.

Remarquons aussi que par convention, tous les quantificateurs portent sur tous les ensembles. On utilisera aussi ce que l'on appelle des quantificateurs bornés, cela veut dire que l'on se permettra encore

les abréviations suivantes :

$$\begin{array}{lll} \forall x \in A, [...] & \longrightarrow & \forall x(x \in A) \Rightarrow [...] \\ \exists x \in A, [...] & \longrightarrow & \exists x(x \in A) \text{ et } [...] \end{array}$$

1. *Axiome d'extensionnalité*

$$\forall A \forall B[(\forall x(x \in A) \Leftrightarrow (x \in B)) \Rightarrow A = B]$$

Il dit que si A et B sont deux ensembles ayant exactement les mêmes éléments, alors ils sont égaux. Ainsi pour définir un ensemble A il suffira de définir ses éléments.

2. *Axiome de la paire*

$$\forall x \forall y \exists A(\forall z(z \in A) \Leftrightarrow (z = x \text{ ou } z = y))$$

Il dit qu'étant donné deux ensembles x et y, il existe un ensemble A qui n'a pour éléments que x et y. Cet ensemble est unique par l'axiome d'extensionnalité et on le notera $\{x, y\}$.

3. *Axiome de l'union*

$$\forall I \exists A(\forall z(z \in A) \Leftrightarrow (\exists y \in I, z \in y))$$

Cela veut dire que les éléments de A sont exactement les éléments des éléments de I. Encore une fois un tel ensemble est unique, on le notera $\cup I$ (lire *union* de I). Cela correspond informellement à une union indexée par l'ensemble d'indices I, les ensembles que l'on réunit étant précisément les éléments de I.

4. *Axiome des parties*

$$\forall A \exists B(\forall X(X \in B) \Leftrightarrow (X \subset A))$$

L'ensemble B est unique, il s'agit de l'ensemble des parties de A, que l'on note $\mathcal{P}(A)$.

5. *Schéma d'axiomes de compréhension*

Un schéma d'axiomes regroupe en général une infinité d'axiomes indexée par les formules logiques. Plus précisément il dit que pour toute formule F on a un certain axiome. Le schéma de compréhension permet de parler de sous-ensembles, il est décrit par :

$$\forall u_1 \ldots \forall u_n \forall X \exists Y(\forall x(x \in Y) \Rightarrow ((x \in X) \text{ et } (F(x, u_1, \ldots, u_n))))$$

où F est une formule quelconque à $(n+1)$ variables libres, c'est-à-dire dans laquelle on peut substituer $(n+1)$ variables, ici en l'occurrence $x, u_1, \ldots, u_n$. Le schéma de compréhension dit quels sous-ensembles de X doivent exister, il s'agit de ceux qui sont définissables par une formule. Les autres ont le droit d'exister mais on ne leur impose pas. C'est le maximum que l'on peut imposer étant donné que l'on aimerait au moins que les axiomes soient décrits par des formules logiques.

Ce schéma implique en particulier l'existence d'un ensemble n'ayant aucun élément. En effet, prenons X un ensemble quelconque de l'univers (qui existe puisque U est non vide) alors l'ensemble Y défini par :

$$\forall x(x \in Y) \Leftrightarrow ((x \in X) \text{ et } x \neq x)$$

existe justement par l'axiome de compréhension et est vide. Un tel ensemble est unique par extensionnalité, on le notera $\emptyset$ par la suite.

Ce schéma permet aussi de définir l'intersection de deux ensembles, disons A et B. Il s'agit simplement de l'ensemble X défini par :

$$\forall z(z \in X) \Leftrightarrow ((z \in A) \text{ et } (z \in B))$$

(en le voyant ici comme un sous-ensemble de A). Encore l'extensionnalité prouve l'unicité d'un tel ensemble, on le notera $(A \cap B)$.

6. *Schéma d'axiomes de remplacement*
   Les axiomes précédents ne permettent en fait pas de parler de tous les ensembles dont on aurait envie. Il faut encore ajouter la chose suivante. On dit que $F(x, y, u_1, \ldots, u_n)$ une formule à $(n+2)$ variables libres est une fonctionnelle en x et y si elle vérifie la condition suivante :

   $$\forall x \forall y \forall y' \forall u_1 \ldots \forall u_n (F(x, y, u_1, \ldots, u_n) \text{ et } F(x, y', u_1, \ldots, u_n)) \Rightarrow (y = y')$$

   Cela veut exactement dire qu'étant donné $x, u_1, \ldots, u_n$, il y a au plus un y qui vérifie $F(x, y, u_1, \ldots, u_n)$. C'est moralement l'image de x par la fonctionnelle F.
   Le schéma de remplacement dit que pour toute fonctionnelle F, si A est un ensemble, il en est de même de $F(A)$ (avec des notations évidentes, je l'espère mais de toute façon l'axiome précis sera écrit plus bas), on aimerait donc indexer les axiomes par des fonctionnelles. Seulement cela n'est pas possible, car la propriété d'être une fonctionnelle dépend fortement de l'univers considéré et on aimerait que les axiomes n'en dépendent pas quand même. Pour pallier cela, on indexe en fait les axiomes par toutes les formules et on procède ainsi :

   $$(F(x, y, u_1, ..., u_n) \text{ fonctionnelle}) \Rightarrow [\forall u_1 ... \forall u_n \forall A \exists B (\forall y (y \in B) \Rightarrow (\exists x \in A F(x, y, u_1, ..., u_n)))]$$

   L'ensemble B sera noté $F(A)$.
7. *Axiome de l'infini*
   Il est censé dire qu'il existe au moins un ensemble infini... on remarquera que toutes les constructions précédentes n'en ont pas encore fourni. Il y a plein de façons de le formuler, par exemple :

   $$\exists X ((\exists x \in X) \text{ et } (\forall x \in X, x \cup \{x\} \in X))$$

   où $\{x\}$ est l'ensemble contenant uniquement x, il existe en vertu de l'axiome de la paire.
8. *Axiome de fondation*
   Il dit intuitivement que l'on ne peut pas trouver une suite infinie d'ensemble x_i "décroissante" pour l'appartenance... je veux dire par là qui vérifie $x_{i+1} \in x_i$ pour tout entier i. Je vous laisse vous convaincre que cela revient exactement à dire que tout ensemble peut se construire seulement à partir de l'ensemble vide à l'aide des opérations précédentes. La façon la plus simple d'écrire cela sous forme d'un axiome est sans doute la suivante :

   $$\forall x (x \neq \emptyset) \Rightarrow (\exists y \in x, (x \cap y) = \emptyset)$$

   Il n'est pas si évident de montrer que cette condition simple équivaut aux énoncés plus intuitifs que l'on a donnés juste ci-dessus, nous ne le prouverons pas ici.

Voilà pour la liste. À ce niveau, il est peut-être légitime de se demander si un tel univers existe. On ne sait pas répondre à cette question, et même mieux, on peut montrer que l'on ne peut pas répondre à une formalisation dans cet univers de cette question... enfin bon, ce n'est pas le sujet. Pour plus d'informations, aller voir `http://www.eleves.ens.fr:8080/home/ollivier/goedel/goedel.html`

Il est sans doute amusant de remarquer que moyennant l'existence des entiers naturels, on peut construire un modèle de ZF auquel on a retiré l'axiome de l'infini. On laisse au lecteur le soin de vérifier que si l'on met sur $\mathbb{N}$ la relation suivante (x et y donc sont deux entiers) :

$$x \in y \text{ ssi l'écriture binaire de } y \text{ contient un 1 en } x\text{-ième position}$$

on obtient ce que l'on souhaite.

4.2.2 Constructions mathématiques usuelles

Ensembles "finis"

Si x et y sont deux ensembles, l'axiome de la paire assure l'existence d'un ensemble dont les seuls éléments sont x et y, que l'on a pris soin de noter $\{x, y\}$. En fait, étant donné des ensembles $x_1, \ldots, x_n$, on peut montrer l'existence d'un ensemble ne contenant que $x_1, \ldots, x_n$ que l'on va bien entendu noter $\{x_1, ..., x_n\}$.

On montre bien entendu cela par récurrence. Pour $n = 1$ et $n = 2$, c'est déjà fait. Supposons donc que $n \geqslant 2$. On note alors $X = \{x_1, ..., x_{n-1}\}$ et $Y = \{x_n\}$ dont l'hypothèse de récurrence assure l'existence. On appelle maintenant $I = \{X, Y\}$. La réunion de I, $\cup I$, est alors précisément l'ensemble $\{x_1, ..., x_n\}$ que l'on cherchait à construire.

Couples, triplets, n-uplets

On définit le *couple* (x, y), noté donc "(x, y)", comme l'ensemble $\{\{x\}, \{x, y\}\}$. C'est un petit jeu laissé au lecteur de démontrer que $(x, y) = (x', y')$ si et seulement si $x = x'$ et $y = y'$.

On définit ensuite les *n-uplets* par récurrence sur n, il y a plein de définitions possibles, par exemple $(x_1, \ldots, x_n) = ((x_1, \ldots, x_{n-1}), x_n)$

Il n'est pas possible de prendre $(x, y, z) = \{\{x\}, \{x, y\}, \{x, y, z\}\}$ par exemple. En effet, dans ce cas les triplets (a, b, b) et (a, b, a) seraient égaux, ce qui est indésirable.

Si A et B sont deux ensembles, on notera pas la suite $A \cup B$ la réunion de la paire $I = \{A, B\}$.

Produits "finis"

Commençons par le produit de deux ensembles, disons X et Y. On aimerait définir le produit $X \times Y$ comme l'ensemble dont les éléments sont précisément les couples (x, y) où x est un élément de X, et y un élément de Y. Il reste juste à voir que cet ensemble existe effectivement. Une méthode générale pour ça est de voir l'ensemble en question comme un sous-ensemble *définissable* (ie dont les éléments sont caractérisés par une formule) d'un certain ensemble dont on connaît par ailleurs l'existence. Ici par exemple, il suffit de remarquer qu'un couple (x, y) est, tel qu'on vient de le définir, un élément de l'ensemble $\mathcal{P}(\mathcal{P}(X \cup Y))$ et donc que le produit $X \times Y$ est naturellement inclus dans $\mathcal{P}(\mathcal{P}(X \cup Y))$. Maintenant il ne reste plus qu'à écrire une formule qui identifie ces couples à l'intérieur de cet ensemble. C'est un peu laborieux mais pas difficile et nous laissons le lecteur sceptique le faire par lui-même.

Maintenant si $X_1, \ldots, X_n$ sont des ensembles, on définit le produit $X_1 \times \ldots \times X_n$ encore par récurrence via la formule

$$X_1 \times \ldots \times X_n = (X_1 \times \ldots \times X_{n-1}) \times X_n$$

On vérifie alors que ses éléments sont exactement les n-uplets $(x_1, \ldots, x_n)$ où x_i est un élément de X_i pour tout i compris entre 1 et n.

Relations

Soit E un ensemble. Une relation sur E est par définition un ensemble R inclus dans le produit $E \times E$. Bien entendu, on dira que x est en relation avec y si et seulement si le couple (x, y) appartient à R. Il est bien sûr possible de définir l'ensemble des relations sur E, il s'agit tout simplement de l'ensemble $\mathcal{P}(E \times E)$.

Bien entendu, on peut définir les relations réflexives, symétriques, anti-symétriques, transitives par les axiomes habituels. En particulier, on peut sans problème parler de relation d'ordre, de relation d'ordre total, de relation de bon ordre, de relation d'équivalence, etc. On peut même, étant donné un ensemble

E, parler de l'ensemble des relations d'ordre sur E, des relations d'ordre total sur E, des relations de bon ordre sur E, des relations d'équivalence sur E... cela se définissant par des formules, certes longues à écrire mais qui existent bien.

Si E est un ensemble et R une relation d'équivalence sur E, on peut définir l'ensemble quotient E/R. Pour cela, il faut d'abord donner une formule explicite qui dit qu'une partie A de E est une classe d'équivalence pour R. On peut par exemple prendre :

$$\exists x \in A, \forall y \in E, (y \in A) \Leftrightarrow ((x, y) \in R)$$

L'ensemble E/R est alors le sous-ensemble de $\mathcal{P}(E)$ formé des éléments qui sont des classes d'équivalence pour la relation R. L'axiome de compréhension assure son existence.

Fonctions

Une fonction f est par définition un ensemble dont les éléments sont des couples, c'est-à-dire des ensembles de la forme $\{\{x\}, \{x, y\}\}$, qui vérifie de surcroît :

$$(\forall x \forall y \forall y'((x, y) \in f \text{ et } (x, y') \in f) \Rightarrow (y = y'))$$

Étant donnée une fonction f, on peut définir son domaine et son image. Un ensemble x est dans le domaine de f s'il existe un ensemble y tel que $(x, y) \in f$. Le fait que le domaine de f soit un ensemble peut se voir avec l'axiome de remplacement (mais ce n'est pas nécessaire). Voyons comment cela fonctionne. On définit la fonctionnelle $P_1(X, x)$ suivante :

$$\exists y, X = (x, y)$$

Cette fonctionnelle n'est définie que sur les couples et pour ceux-ci est simplement la première projection. L'image par P_1 de l'ensemble f est alors précisément le domaine de f.

L'image de f est bien ce que l'on pense. Il s'agit de l'ensemble des y tels qu'il existe x vérifiant $(x, y) \in f$. On utilise l'axiome de remplacement avec ce coup-ci la deuxième projection pour voir qu'il s'agit bien d'un ensemble.

Les notations traditionnelles sont $\mathrm{Dom}(f)$ pour le domaine de la fonction f et $\mathrm{Im}(f)$ pour l'image de f.

Il faut préciser qu'il n'existe pas d'ensemble dont les éléments soient précisément les fonctions. Par contre si E et F sont deux ensembles, on définit une fonction de E dans F comme étant une fonction f de domaine E et d'image incluse dans F (f est donc en particulier inclus dans $E \times F$). L'axiome de compréhension prouve que les fonctions de E dans F forment bien un ensemble (puisqu'il est inclus dans $\mathcal{P}(E \times F)$) que l'on note souvent F^E ou encore $\mathrm{Fonc}(E, F)$. Remarquons qu'une fois précisés les ensembles de départ et d'arrivée, il est possible de définir une injection, une surjection et une bijection par les axiomes habituels. Une *injection* $f : E \to F$ est une fonction de E dans F vérifiant :

$$\forall x \in E, \forall x' \in E, (\exists y \in F, (x, y) \in f \text{ et } (x', y) \in f) \Rightarrow (x = x')$$

Une *surjection* $f : E \to F$ est une fonction de E dans F vérifiant :

$$\forall y \in F, \exists x \in E, (x, y) \in f$$

Une *bijection* $f : E \to F$ est une fonction de E dans F qui est à la fois une injection et une surjection.

Remarquons qu'une fonction f est toujours une fonction de $\mathrm{Dom}(f)$ dans $\mathrm{Im}(f)$. Remarquons également que l'ensemble $\mathrm{Fonc}(\emptyset, F)$ est toujours réduit à un unique élément, qui est précisément l'ensemble vide, l'ensemble $\mathrm{Fonc}(E, \emptyset)$ quant à lui est vide dès que E est non vide.

Il s'agit de dire finalement que par la suite les termes "fonction", "injection", "surjection" et "bijection" désigneront toujours les objets précis que l'on vient de définir. Cela est très important pour la bonne compréhension de l'axiome du choix.

Produits quelconques

On aimerait définir le produit d'une famille quelconque d'ensembles. Mais avant de faire cela, il s'agit d'abord de dire ce que c'est une famille quelconque d'ensembles. Pour cela, on considère un certain ensemble I que l'on appelle ensemble d'indices et on définit une famille d'ensembles indexée par I. C'est simplement une fonction (au sens précédent donc) de domaine I. Une famille quelconque d'ensembles sera alors une famille d'ensembles indexée par un certain ensemble.

Remarquez qu'il n'est pas clair qu'il existe un ensemble ayant exactement pour éléments les familles indexées par l'ensemble I. En effet, ici on ne peut pas a priori borner ces éléments (c'est-à-dire tous les mettre dans un gros ensemble) et donc le fait que l'on dispose d'une jolie formule ne permet pas de conclure. De fait, il est faux de façon générale qu'un tel ensemble existe. Un exercice éducatif est sans doute de démontrer que cet ensemble existe si et seulement si I est vide.

Soit donc $F = (X_i)$ une famille d'ensembles indexée par l'ensemble I. Il existe un ensemble dont les éléments sont exactement les X_i, il s'agit par définition de l'image de F. La réunion de cet ensemble fournit ce que l'on appelle habituellement la réunion des X_i pour i parcourant I. Notons-la par exemple X. Un élément du produit des X_i est alors une fonction x de I dans X telle que l'image de l'élément i de I appartienne à l'ensemble X_i. Formellement x est un élément du produit des X_i si :

$$x \in \mathrm{Fonc}(I, X) \quad \text{et} \quad \forall i \forall y \forall Y ((i, y) \in x \text{ et } (i, Y) \in F)) \Rightarrow (y \in Y)$$

On voit alors directement que l'axiome de compréhension permet de définir le produit des X_i.

Les nombres

Toutes les constructions données précédemment permettent de construire dans un univers U la plupart des objets que l'on utilise couramment en mathématiques. Enfin, presque... la construction de l'ensemble des entiers naturels $\mathbb{N}$ muni des opérations classiques ne se déduit pas directement de tout cela. Admettons pour l'instant son existence, nous en donnerons une construction plus tard.

Une fois que l'on a $\mathbb{N}$, il n'est pas bien difficile par exemple de construire $\mathbb{Z}$. On met sur l'ensemble $\mathbb{N} \times \mathbb{N}$ la relation d'équivalence suivante :

$$(x, y)\, R\, (x', y') \quad \text{ssi} \quad x + y' = x' + y$$

(où bien sûr, $x + y$ désigne l'image par la fonction $+$ qui va de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$ du couple (x, y))

Le quotient de $\mathbb{N} \times \mathbb{N}$ par cette relation d'équivalence fournit précisément $\mathbb{Z}$. Il s'agit alors de prolonger les opérations. On définit pour cela le sous-ensemble $+$ de $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ en disant qu'un triplet (A, B, C) est dans $+$ si et seulement si :

$$\exists (a_1, a_2) \in A,\ \exists (b_1, b_2) \in B,\ \exists (c_1, c_2) \in C,\ a_1 + b_1 + c_2 = a_2 + b_2 + c_1$$

(là encore, il y a beaucoup d'abus d'écriture, nous laissons au lecteur le soin d'écrire cette formule aussi rigoureusement que possible...)

Pour la multiplication on procède de même. $\times$ est le sous-ensemble de $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ formé des triplets (X, Y, Z) vérifiant :

$$\exists (a_1, a_2) \in A,\ \exists (b_1, b_2) \in B,\ \exists (c_1, c_2) \in C,\ a_1 \times b_1 + a_2 \times b_2 + c_2 = a_1 \times b_2 + a_2 \times b_1 + c_1$$

Il faut ensuite vérifier que $+$ et $\times$ ainsi définies sont bien des fonctions de $\mathbb{Z} \times \mathbb{Z}$ dans $\mathbb{Z}$, ce qui se fait sans difficulté particulière.

Maintenant on peut construire $\mathbb{Q}$ en mettant à nouveau la bonne relation d'équivalence sur $\mathbb{Z} \times \mathbb{Z}$. On peut également construire $\mathbb{R}$, en prenant l'ensemble des suites à valeurs rationnelles (ie des fonctions de $\mathbb{N}$ dans $\mathbb{Q}$) qui sont de Cauchy, et en quotientant cet ensemble par la relation d'équivalence qui dit deux suites sont équivalentes si et seulement si leur différence tend vers 0. Là encore, il faut prolonger les opérations, mais ces constructions ne requièrent pas plus d'astuce du côté théorie des ensembles que celle détaillée précédemment.

4.2.3 Et les démonstrations dans tout ça

Avant d'entrer dans le vif du sujet, il nous faut faire une dernière précision. En effet, dans la suite, nous allons parler d'axiome du choix, d'axiome du choix dénombrable, d'axiome du choix dépendant, etc. et nous allons nous demander lorsqu'un tel énoncé l'"utilise", mais nous n'avons pas encore défini ce que cela pouvait bien vouloir dire formellement.

Prenons donc un certain énoncé, qui s'exprime sous la forme d'une formule F. Dire que F est démontrable (ou encore prouvable) dans ZF signifie que la formule F est vérifiée dans tous les modèles de ZF. Comme on l'a dit, on ne sait pas construire un modèle de ZF, on ne sait même pas s'il en existe un. Il se pourrait donc que tous les énoncés soient démontrables dans ZF. Et effectivement... personne n'a encore trouvé de contradiction interne dans les axiomes que l'on a listés précédemment mais personne non plus ne peut prouver qu'il n'y en a pas. Il faut donc faire avec et par la suite, on supposera toujours implicitement qu'il existe au moins un modèle de ZF.

Voyons brièvement comment on peut voir qu'un énoncé est ou n'est pas démontrable. Pour prouver qu'il est démontrable comme on vient de le dire, il "suffit" de montrer qu'il est vrai dans tous les modèles de ZF, en gros il "suffit" de triturer les axiomes que l'on a pour en sortir le théorème que l'on veut. Il existe une définition précise de ce "triturer" pour laquelle la phrase qui précède est vraie, mais nous n'allons pas entrer plus en avant dans les détails, cela n'étant pas notre sujet. Signalons toutefois que le théorème cité précédemment est ce que l'on appelle classiquement le théorème de complétude de Gödel.

Mais comment faire pour voir qu'un énoncé n'est pas démontrable ? Ben, il s'agit de construire un modèle de ZF dans lequel cet énoncé est faux. Ouille, construire un modèle de ZF, c'est difficile, on a déjà dit que l'on ne savait pas faire. Oui, mais on a dit aussi que l'on allait sans vergogne supposer qu'il en existe un. Ainsi les méthodes classiques pour ce faire consistent à construire plus ou moins explicitement à partir d'un modèle donné, un nouveau modèle dans lequel l'énoncé en question est faux. Ce n'est pas quelque chose de facile. Une méthode générale pour construire ces modèles est ce que l'on appelle le "forcing". Nous n'allons là encore pas détailler davantage. Pour plus d'informations, aller voir `http://www-math.mit.edu/~tchow/mathstuff/forcingdum` (en anglais).

Bien sûr, il y a des cas où prouver qu'une formule F n'est pas démontrable dans ZF est plus simple. Par exemple, mais c'est un peu de la triche, si la formule (non F) est démontrable, F ne va pas l'être. En effet, si on prend un modèle quelconque de ZF (dont on rappelle que l'on suppose l'existence), la formule F va y être vérifiée et donc (non F) ne le sera pas. Une autre façon qui porte ses fruits est de prouver dans ZF que F implique une formule G que l'on sait par ailleurs ne pas être démontrable.

Un peu de terminologie peut-être. Si la formule (non F) est démontrable, on dit que F est réfutable. Si F n'est ni démontrable, ni réfutable, on dit que F est indécidable.

Bien entendu, on a expliqué ici les choses avec les axiomes de ZF, mais tout ce que l'on vient de dire s'étend sans problème à tout système d'axiomes cohérent (c'est-à-dire pour lequel il existe un modèle...). Par la suite, on va énoncer l'axiome du choix et dire qu'il est indécidable (au sens précédent donc) dans ZF. Ainsi la théorie formée des axiomes de ZF auxquels on ajoute l'axiome du choix, que l'on note ZFC, est encore cohérente. Dire qu'un énoncé F "utilise" l'axiome du choix, c'est précisément dire que celui-ci est prouvable dans ZFC mais ne l'est pas dans ZF. Ainsi, en général, prouver effectivement qu'un énoncé "utilise" l'axiome du choix n'est pas quelque chose de facile, alors que prouver qu'il ne l'"utilise" pas est quand même relativement plus simple.

4.3 Axiome du choix

4.3.1 Énoncé

Ne perdons plus de temps et énonçons enfin cet axiome. Il dit que pour tout ensemble E, il existe une fonction f de $\mathcal{P}(E)\backslash\{\emptyset\}$ dans E qui soit telle que pour toute partie A non vide de E, $f(A)$ appartient à A. De façon plus formelle, cela s'écrit :

$$\forall E \exists f (f \text{ fonction de } \mathcal{P}(E)\backslash\{\emptyset\} \text{ dans } E) \text{ et } (\forall A \in \mathcal{P}(E)\backslash\{\emptyset\}, (A, a) \in f \Rightarrow a \in A)$$

Une fonction f qui vérifie cette propriété s'appelle une *fonction de choix* sur E. L'axiome du choix dit exactement que tout ensemble admet une fonction de choix.

De façon équivalente et plus compacte, il dit qu'un produit non vide (ie indexé par un ensemble non vide) d'ensembles non vides est non vide. Cette formulation est un peu plus dangereuse dans le sens où il faut bien garder à l'esprit que le mot "produit" a le sens précis que l'on a introduit dans la première partie. De nombreuses confusions proviennent surtout de cela. (Pour les algébristes convaincus, cela peut se reformuler en disant que toute surjection ensembliste est scindée, c'est-à-dire que si $p : A \to B$ est une application surjective, alors il existe une application $s : B \to A$, que l'on appelle une section, vérifiant $p \circ s = \mathrm{id}_B$).

Il n'est peut-être pas clair a priori que ces deux énoncés sont bien équivalents. Démontrons cela. Supposons dans un premier temps le premier énoncé. Il s'agit de montrer que si I est un ensemble non vide et $F = (X_i)$ une famille d'ensembles non vides indexée par I, alors on peut exhiber une fonction de I dans l'union des X_i, telle que $f(i)$ soit dans X_i pour tout i. Pour faire cela, on considère une fonction de choix, disons g, sur l'union des X_i. Il ne reste plus alors qu'à définir $f(i)$ comme étant $g(X_i)$. Réciproquement, prenons E un ensemble quelconque et montrons que le deuxième énoncé assure l'existence d'une fonction de choix sur E. On considère pour cela comme ensemble d'indices l'ensemble $\mathcal{P}(E)\backslash\{\emptyset\}$. La famille indexée par cet ensemble sera également $\mathcal{P}(E)\backslash\{\emptyset\}$. On laisse au lecteur le soin de se persuader qu'un élément du produit de cette famille correspond précisément à une fonction de choix sur E.

Il est bon de dire tout de suite que l'axiome du choix n'est pas une conséquence formelle des autres axiomes de ZF. La négation de l'axiome du choix, non plus. Autrement dit, l'axiome du choix est indécidable dans ZF. La théorie constituée des axiomes de ZF et de l'axiome du choix est donc cohérente, c'est elle que l'on appelle ZFC (C pour "Choice").

4.3.2 Commentaires

L'axiome du choix est souvent sur-interprété ou mal interprété. Essayons de mettre les choses au clair en détaillant quelques exemples. Donnons-nous pour commencer un singleton I et une famille (X_i) indexée par I, c'est-à-dire en fait simplement un ensemble X. On suppose X non vide. Le produit des X_i

s'identifie alors à X et est non vide puisque nous venons de le supposer. Tout ça pour dire que l'on n'a pas besoin de l'axiome du choix pour choisir un élément dans un ensemble.

Par récurrence, on peut montrer que même que si I est fini, exhiber un élément du produit est possible. Dit en termes plus concrets, on n'utilise pas l'axiome du choix pour choisir simultanément un élément dans un nombre fini d'ensembles.

Attention par contre, si ce sont les X_i (ie les ensembles dans lesquels on va choisir les éléments) qui sont des ensembles finis mais que I ne l'est pas, la construction par récurrence a priori ne marche plus. Et en fait cet énoncé plus faible où l'on suppose les ensembles X_i finis n'est pas non plus démontrable dans ZF même si I est l'ensemble des entiers naturels.

Mais à côté de cela, il est des cas où l'axiome du choix n'est pas nécessaire pour construire une telle fonction. Supposons par exemple que l'on veuille construire une fonction de choix sur l'ensemble des entiers naturels $\mathbb{N}$. Il est vrai que l'on n'a toujours pas construit cet ensemble (mais il est vrai aussi que cela viendra plus tard :-) mais supposons pour l'instant qu'il existe et qu'il est muni des opérations usuelles et de la relation d'ordre usuelle. C'est cette dernière qui va nous être utile. En effet, elle a la particularité remarquable que toute partie non vide de $\mathbb{N}$ admet pour cette relation d'ordre un plus petit élément. Ainsi l'idée vient de considérer la fonction f qui à une partie non vide de $\mathbb{N}$ associe son plus petit élément qui sera bien une fonction de choix. Voyons pour une fois que cela est bien possible, c'est-à-dire qu'il existe bien un ensemble f qui correspond à une telle fonction. Il est défini par la formule :

$$f \subset (\mathcal{P}(\mathbb{N}) - \{\emptyset\}) \times \mathbb{N} \quad \text{et} \quad (X, x) \in f \Rightarrow (x \in X \text{ et } \forall y \in X,\, x \leqslant y)$$

Le schéma de compréhension, finalement, assure bien l'existence d'un tel ensemble f.

De façon très informelle et imagée, on peut dire que choisir une chaussette par paire parmi une infinité de paires en vrac dans une bassine requiert l'axiome du choix, alors que ce n'est pas le cas pour les chaussures car il suffit par exemple de prendre toutes les chaussures gauches.

4.3.3 Axiome du choix dénombrable, axiome du choix dépendant

Avant de dire ce que sont ces axiomes, il est peut-être nécessaire de faire le point sur la notion de dénombrabilité. Soit X un ensemble. On dit que X est dénombrable s'il peut être mis en bijection avec $\mathbb{N}$. Mais là, encore "bijection" est à prendre dans le sens défini dans la première partie et $\mathbb{N}$ désigne encore l'ensemble des entiers naturels qu'effectivement nous n'avons toujours pas construit mais ça viendra... Attention, cela ne veut pas du tout dire que la sous-patate de l'univers regroupant tous les ensembles éléments de X est "dénombrable". Aussi étonnant que cela puisse paraître, il existe des univers qui comptent un nombre "dénombrable" d'ensembles (bien entendu toujours sous l'hypothèse qu'il existe au moins un modèle de ZF) et pourtant on peut montrer que l'ensemble des réels n'est jamais dénombrable.

Maintenant cette mise au point faite, on peut énoncer l'axiome du choix dénombrable. On le note souvent CC pour "Countable Choice". Il dit qu'un produit dénombrable d'ensembles non vides est non vide. Cela signifie que si I est un ensemble dénombrable, si (X_i) est une famille d'ensembles non vides indexée par I, alors le produit des X_i est non vide. Il est important de bien remarquer que la condition de dénombrabilité porte sur l'ensemble d'indices I et non sur les ensembles indexés. Comme être dénombrable signifie être en bijection avec $\mathbb{N}$, ce dernier énoncé peut se reformuler en disant que toute famille (X_n) d'ensembles non vides indexée par $\mathbb{N}$ est telle que le produit des X_n est non vide.

L'axiome du choix dépendant, que l'on note souvent DC pour "Dependent Choice", lui, dit quelque chose de plus fort. On part d'un ensemble E que l'on suppose simplement non vide. On se donne en outre une fonction $f : E \to \mathcal{P}(E)\backslash\{\emptyset\}$ quelconque. L'axiome du choix dépendant dit alors que pour tout x de E, il existe une suite (x_n) d'éléments de E telle que

1. $x_0 = x$
2. $x_{n+1} \in f(x_n)$

Il est peut-être nécessaire de préciser ce que l'on entend par "suite" : là encore, il y a une définition formelle. Une suite à valeurs dans E est simplement une fonction de $\mathbb{N}$ (oui, oui, on ne l'a toujours pas construit, je sais :-) dans E, fonction bien entendu au sens formel, celui dont on parle depuis le début. Ce que l'on note communément x_n est bien entendu l'image de n, élément de $\mathbb{N}$, par cette fonction.

Il s'agit sans doute de la forme de l'axiome du choix la plus couramment utilisée, du moins en analyse. C'est celle que l'on emploie par exemple typiquement pour construire une suite par récurrence.

Voyons les rapports qu'entretiennent tous ces axiomes. Déjà, il est clair que l'axiome du choix, dans sa deuxième formulation, implique l'axiome du choix dénombrable. Il est peut-être un peu moins clair que l'axiome du choix implique l'axiome du choix dépendant, et comme l'on n'a toujours pas défini ce qu'était $\mathbb{N}$, on aura du mal à démontrer quoi que ce soit en fait. Disons quand même plus ou moins informellement comment on fait les choses. On considère donc E un ensemble non vide et f une fonction de E dans $\mathcal{P}(E)\backslash\{\emptyset\}$. D'après l'axiome du choix justement il existe sur E une fonction de choix, disons $g : \mathcal{P}(E)\backslash\{\emptyset\} \to E$. Il suffit alors, étant donné un élément x de E, de construire la suite (x_n) de la façon suivante :

1. $x_0 = x$
2. $x_{n+1} = g(f(x_n))$

On verra en que cela définit bien une fonction de $\mathbb{N}$ dans E.

Il est finalement vrai que l'axiome du choix dépendant implique l'axiome du choix dénombrable. Prenons donc une famille (X_n) d'ensembles non vides indexée par $\mathbb{N}$. Il s'agit de montrer que le produit des X_n est non vide. Pour cela, on commence par construire ce que l'on appelle l'union disjointe des X_n, que l'on va noter X. Il s'agit de l'ensemble des couples (n, x) où n est un entier naturel (ie un élément de $\mathbb{N}$) et x un élément de X_n. Montrons tout d'abord que cet ensemble existe. Notons X' l'union des X_n que l'on a déjà considérée plusieurs fois. Bien entendu, on va voir X comme une partie de $\mathbb{N} \times X'$, elle est définie par la formule $(n, x) \in X \Rightarrow x \in X_n$. L'axiome de compréhension prouve donc que l'union disjointe existe.

Il nous faut maintenant définir une fonction $f : X \to \mathcal{P}(X)\backslash\{\emptyset\}$. On prend celle qui au couple (n, x) associe $\{n+1\} \times X_{n+1}$ qui est bien une partie non vide de X. (Le lecteur encore sceptique pourra s'amuser à écrire lui-même une formule et se convaincre qu'une telle fonction existe encore grâce à l'axiome de compréhension). Il ne reste alors plus qu'à prendre un élément x dans X_0 et à appliquer l'axiome du choix dépendant au couple $(0, x_0)$ élément de X. Il faut encore construire un élément du produit des X_n à partir de la suite obtenue mais cela se fait sans difficulté.

Finalement on a :

$$\text{Axiome du choix} \Rightarrow \text{Axiome du choix dépendant} \Rightarrow \text{Axiome du choix dénombrable}$$

Il est à noter que toutes les réciproques sont fausses, dans le sens où, comme nous l'avons déjà expliqué, il existe un modèle de ZF vérifiant l'axiome du choix dépendant mais pas l'axiome du choix, et un modèle de ZF vérifiant l'axiome du choix dénombrable mais pas l'axiome du choix dépendant. Construire de tels modèles n'est pas quelque chose de facile, et nous n'allons pas le faire.

4.3.4 Énoncés équivalents classiques

Il est peut-être nécessaire au préalable de faire quelques rappels sur les notions d'ordre. Prenons donc E un ensemble muni d'une relation binaire que l'on va noter $\leqslant$. On dit que cette relation est un *ordre* si elle vérifie les trois propriétés suivantes :

1. *(réflexivité)* $\forall x \in E,\ x \leqslant x$
2. *(transitivité)* $\forall x \in E, \forall y \in E, \forall z \in E,\ (x \leqslant y \text{ et } y \leqslant z) \Rightarrow (x \leqslant z)$
3. *(antisymétrie)* $\forall x \in E, \forall y \in E,\ (x \leqslant y \text{ et } y \leqslant x) \Rightarrow (x = y)$

Une relation sur E qui vérifie juste les deux premières conditions est ce que l'on appelle un *pré-ordre*.

On dit que l'ordre est *total*, ou encore que E est *totalement ordonné*, si la relation $\leqslant$ vérifie en outre la condition :

4. $\forall x \in E, \forall y \in E,\ (x \leqslant y \text{ ou } y \leqslant x)$

On dira souvent de E qu'il est un ensemble *partiellement ordonné* s'il est juste muni d'une relation d'ordre. Le mot "partiellement" ne sous-entend aucunement que la relation d'ordre n'est pas totale, il est juste là pour préciser qu'elle ne l'est pas forcément.

Prenons donc E un ensemble partiellement ordonné. Ce que l'on appelle un *plus grand élément* de E, c'est un élément x de E plus grand que tous les autres, c'est-à-dire vérifiant $y \leqslant x$ pour tout y dans E. La propriété d'antisymétrie prouve directement que s'il existe un plus grand élément, alors celui-ci est unique.

Il est important de ne pas confondre cette notion avec la notion d'élément maximal. Un *élément maximal* de E, c'est un élément x de E tel qu'il n'existe pas de y strictement supérieur (ie supérieur et différent) à x. Pour illustrer la distinction, il est intéressant de remarquer que si E est un ensemble muni de la relation "égalité" (ie $x \leqslant y$ si et seulement si $x = y$) qui est une relation d'ordre, alors tout élément de E est un élément maximal mais E n'admet pas de plus grand élément dès qu'il est de cardinal plus grand que 2. Il est intéressant aussi de remarquer que cet exemple prouve qu'un élément maximal n'est pas du tout forcément unique.

Il est cependant vrai que si E est *totalement* ordonné, alors un élément maximal est forcément unique et que les notions d'élément maximal et de plus grand élément coïncident. Il est également vrai que si E est un ensemble partiellement ordonné qui admet un plus grand élément x, alors il admet un unique élément maximal qui est précisément x.

Reprenons maintenant E un ensemble partiellement ordonné. Si A est une partie de E, la relation d'ordre, $\leqslant$ disons, se restreint à A (formellement il s'agit de faire l'intersection de l'ensemble $\leqslant$ avec l'ensemble $A \times A$). On dit que A est *majoré* dans E s'il existe un élément x de E plus grand que tous les éléments de A, c'est-à-dire tel que $y \leqslant x$ pour tout y dans A. On dit que A est une *chaîne* si l'ordre induit sur A est total. On dit que E est *inductif* si toute chaîne de E est majorée.

Finalement, on dit que E est *bien ordonné* si toute partie A non vide admet un plus petit élément (oui, je sais, je n'ai pas défini plus petit élément mais bon :-). Bien entendu, on peut donner encore plein de définitions et de propriétés intéressantes sur les ordres mais ici sont rassemblées celles qui vont nous servir par la suite.

Ouf. On est maintenant en mesure d'énoncer quelques équivalents de l'axiome du choix. Commençons par le théorème de maximalité de Hausdorff. Il dit la chose suivante. On prend E un ensemble partiellement ordonné. On peut regarder alors le sous-ensembles de $\mathcal{P}(E)$ formé des chaînes. Cet ensemble est muni d'un ordre naturel, celui donné par l'inclusion. Le théorème de maximalité de Hausdorff dit que ce dernier ensemble muni de ce dernier ordre admet un élément maximal. On résume cela en général en disant que tout ensemble partiellement ordonné admet une chaîne "maximale".

Une autre formulation plus courante de cet énoncé est le lemme de Kuratowski-Zorn, sans doute plus connu sous le nom de lemme de Zorn. Il dit que tout ensemble partiellement ordonné inductif admet un élément maximal. Voyons peut-être rapidement le pourquoi de l'équivalence de ces deux énoncés.

Supposons dans un premier temps le théorème de maximalité de Haussdorf et prenons E un ensemble partiellement ordonné inductif. Il s'agit de prouver que E admet un élément maximal. On considère pour cela A un sous-ensemble de E qui est une chaîne maximale. Elle est majorée par hypothèse, notons x un majorant. S'il existait dans E y strictement supérieur à x, alors l'ensemble $A \cup \{y\}$ serait une chaîne de E contenant strictement A, ce qui est exclu. Cela prouve bien que x est un élément maximal de E.

Réciproquement, supposons le lemme de Zorn. Soit E un ensemble partiellement ordonné. On considère X le sous-ensemble de $\mathcal{P}(E)$ formé des chaînes de E que l'on ordonne par inclusion. J'affirme que cet ensemble est inductif. En effet, étant donné une partie X' de X (bien réfléchir à ce dont il s'agit), il est immédiat de constater que la réunion de X' (qui est une partie de E) majore X'. Le lemme de Zorn appliqué à X fournit précisément ce que l'on cherche.

Un autre énoncé est le théorème de Zermelo qui stipule que tout ensemble peut être muni d'un bon ordre. Précisément pour tout ensemble E, il existe une partie de $E \times E$ qui est un bon ordre sur E. Celui-ci aussi est équivalent à l'axiome du choix.

Un dernier. L'axiome du choix est encore équivalent à ce que l'on appelle le lemme de trichotomie. Il dit que si X et Y sont deux ensembles quelconques, alors soit il existe une injection de X dans Y, soit il existe une injection de Y dans X. Pour une bonne définition de cardinal, il dit que les cardinaux sont totalement ordonnés.

Nous démontrerons au paragraphe 4.4.5 l'équivalence de toutes ces propriétés avec l'axiome du choix mais admettons-les pour le moment et voyons comment on les utilise.

4.3.5 Quelques exemples

Pour un nombre beaucoup plus impressionnant d'énoncés équivalents, plus faibles, plus forts, strictement plus faibles, strictement plus forts que l'axiome du choix, vous pouvez aller voir :

1. `http://www.eleves.ens.fr:8080/home/nesme/maths/choix.html`
2. `http://www.eleves.ens.fr:8080/home/madore/math/ac\_var.html`
3. `http://math.vanderbilt.edu/~schectex/ccc/choice.html` (en anglais).

Existence de bases dans les espaces vectoriels

Prenons k un corps quelconque et E un espace vectoriel sur k. Le but est de montrer que E admet une base sur k. Pour cela, on considère l'ensemble F des familles libres d'éléments de E. On ordonne cet ensemble par inclusion. On obtient ainsi un ensemble partiellement ordonné inductif. En effet si F' est un sous-ensemble de F totalement ordonné, il n'est pas très difficile de voir que l'union de F' est encore une famille libre. Le lemme de Zorn s'applique donc et nous fournit ainsi une famille libre maximale. Montrer qu'il s'agit d'une base est encore un exercice simple que nous n'allons pas faire ici.

Évidemment, la démonstration que nous venons de présenter utilise l'axiome du choix, via justement le lemme de Zorn. Évidemment aussi, le fait de donner une démonstration qui utilise l'axiome du choix ne démontre aucunement que le résultat l'utilise. Ici, c'est le cas. On peut construire des modèles de ZF dans lesquels il existe un espace vectoriel qui n'admet pas de bases. On peut faire les choses un peu plus explicitement comme par exemple construire des modèles de ZF dans lesquels $\mathbb{R}$ n'admet pas de base en tant que $\mathbb{Q}$-espace vectoriel, et même dans lesquels les seules endomorphismes $\mathbb{Q}$-linéaires de $\mathbb{R}$ sont les multiplications par les éléments de $\mathbb{R}$.

Théorème de Tychonov

Ce paragraphe traite essentiellement de topologie générale. Comme l'objet de cet article n'est pas de parler de cela, nous n'allons pas rappeler les définitions usuelles. Ainsi, si vous n'avez jamais entendu les mots "quasi-compact" ou "ultrafiltre", vous pouvez passer directement à la section suivante.

Une application directe du lemme de Zorn est le fait que tout filtre se prolonge en un ultrafiltre. En effet étant donné un ensemble X et un filtre F sur X, il suffit de regarder l'ensemble des filtres F' prolongeant F. Il est alors facile de voir que cet ensemble est inductif. Le lemme de Zorn fournit alors l'existence d'un filtre maximal, ie d'un ultrafiltre, prolongeant F.

Utilisant la puissance des filtres et des ultrafiltres, il est facile de voir que :

1. un espace topologique est quasi-compact si et seulement si tout filtre admet une valeur d'adhérence si et seulement si tout ultrafiltre est convergent.
2. un ultrafiltre sur un produit est convergent si et seulement si chacune de ses projections l'est.

Il est alors facile d'en déduire qu'un produit d'espaces topologiques quasi-compacts est encore quasi-compact.

On présente plus souvent le théorème de Tychonov en disant qu'un produit quelconque d'espaces topologiques compacts est compact. Mais cette version se déduit directement de la précédente. Il est amusant de remarquer que la version avec "quasi-compact" est équivalente à l'axiome du choix alors que la version avec simplement "compact" est strictement plus faible mais nécessite quand même l'axiome du choix. Là encore, nous n'allons donner aucune démonstration.

Théorème de Cantor-Bernstein

Prenons A et B deux ensembles. Le théorème de Cantor-Bernstein dit que s'il existe une injection de A dans B et une injection de B dans A, alors il existe une bijection de A dans B.

Voyons comment on peut le démontrer. Tout d'abord notons B' l'image de B par l'injection de B dans A. C'est un sous-ensemble de A qui est en bijection avec B (justement par l'injection en question). Il s'agit donc simplement de construire une bijection de B' dans A sachant que l'on dispose d'une injection $i : A \to B'$. On commence pour cela par définir l'ensemble $C = A - B'$ et on construit une suite (c'est-à-dire une fonction d'ensemble de départ $\mathbb{N}$, que l'on n'a toujours pas construit effectivement mais ça viendra :-) de sous-ensembles de A par la formule de récurrence suivante :

1. $C_0 = C$
2. $C_{n+1} = i(C_n)$

($i(C_n)$ est l'image de C_n par l'injection i, on laisse au lecteur le soin de montrer qu'il s'agit bien d'un ensemble)

Comme nous l'avons déjà utilisé mais toujours pas prouvé (voir 4.3.5), cette construction définit bien une suite.

On note finalement C_∞ la réunion des ensembles C_n (cela existe comme nous l'avons déjà mentionné). La bijection $f : A \to B'$ se définit alors de manière simple :

1. $f(x) = x$ si x n'est pas dans C_∞
2. $f(x) = i(x)$ sinon

On laisse encore le lecteur avide de rigueur vérifier que cet ensemble existe bien (encore une fois via l'axiome de compréhension) et qu'il définit bien une bijection telle qu'on la voulait.

Il est important de remarquer que la démonstration précédente n'a pas fait intervenir l'axiome du choix. Ainsi le théorème de Cantor-Bernstein est vrai indépendamment de l'axiome du choix. Toutefois, souvent, il est commode d'utiliser certains de ses corollaires dans lesquels il intervient des surjections. Et le hic c'est que construire une injection à partir d'une surjection est quelque chose qui utilise l'axiome du choix. Je ne prétends rien démontrer mais moralement cela provient du fait que l'énoncé toute surjection ensembliste est "scindée" est équivalent à l'axiome du choix. Ainsi les deux énoncés suivants qui ressemblent beaucoup au théorème de Cantor-Bernstein, eux, utilisent l'axiome du choix :

1. Soient A et B deux ensembles tels qu'il existe une injection et une surjection de A dans B, alors il existe une bijection de A dans B.
2. Soient A et B deux ensembles tels qu'il existe une surjection de A dans B et une surjection de B dans A, alors il existe une bijection de A dans B.

Dénombrabilité de $\mathbb{Q}$

À partir du théorème de Cantor-Bernstein, il est plus ou moins aisé de déduire la dénombrabilité de $\mathbb{Q}$. Ce que l'on a à construire, c'est une bijection entre $\mathbb{N}$ et $\mathbb{Q}$. Il suffit donc pour cela de construire une injection de $\mathbb{N}$ dans $\mathbb{Q}$ et une injection de $\mathbb{Q}$ dans $\mathbb{N}$. L'injection de $\mathbb{N}$ dans $\mathbb{Q}$ est déjà toute trouvée. Il ne reste donc plus que l'injection de $\mathbb{Q}$ dans $\mathbb{N}$. Mais on se rappelle que construire une bijection entre $\mathbb{N}$ et $\mathbb{N}^2$ n'est pas quelque chose de monstrueusement difficile. Par exemple l'application $(n, m) \mapsto (2n+1) \cdot 2^m - 1$ convient. Il suffit donc finalement de trouver une injection de $\mathbb{Q}$ dans $\mathbb{N}^2$. Mais cela est possible et pas très difficile. Je vous laisse écrire une formule explicite qui convient...

On remarque si l'on mène cette démonstration jusqu'à terme qu'en fait, elle n'utilise pas l'axiome du choix. Ainsi $\mathbb{Q}$ est dénombrable même sans l'axiome du choix, ce qui est somme toute assez rassurant, et ce qui va nous permettre de faire plein d'autres choses aussi étrange que cela puisse paraître. Par exemple, voilà tout de suite une première application.

Produits d'ouverts dans $\mathbb{R}$

Soit I un ensemble et soit (U_i) une famille d'ouverts non vides de $\mathbb{R}$ (bien entendu, celui que l'on a défini dans la première partie). On va prouver sans utiliser l'axiome du choix que le produit des U_i est non vide. Pour ce faire, il va falloir être capable de définir un élément particulier sans chacun des U_i. C'est là qu'intervient $\mathbb{Q}$ ainsi que le fait qu'il soit dénombrable.

En effet fixons f une bijection entre $\mathbb{Q}$ et $\mathbb{N}$. L'ordre naturel sur $\mathbb{N}$ va se transporter via f en un certain ordre sur $\mathbb{Q}$. Ce nouvel ordre va rester un bon ordre, dans le sens où toute partie non vide de $\mathbb{Q}$ va admettre pour cet ordre un plus petit élément. Ainsi $\mathbb{Q}$ va admettre une fonction de choix : je parle ici de la fonction qui à une partie non vide de $\mathbb{Q}$ associe justement ce plus petit élément. On a déjà plus ou moins vu que cette fonction existe bien. Voilà, un bon point.

Voyons maintenant comment cela permet de résoudre notre problème. Notons par exemple g la fonction de choix que l'on vient de définir. Le fait que les U_i soient des ouverts de $\mathbb{R}$ prouve que ces U_i intersectent $\mathbb{Q}$ puisqu'il est dense dans $\mathbb{R}$. Je dis alors qu'un élément du produit des U_i est par exemple la fonction x définie par $x(i) = g(\mathbb{Q} \cap U_i)$, comme il est facile de le vérifier.

Bien entendu, cet exemple peut se généraliser abondamment. Tout d'abord au cas de $\mathbb{R}^n$. Il s'agit d'abord de prouver que $\mathbb{Q}^n$ est dénombrable mais cela se fait par récurrence. En effet, on commence par dire que, comme $\mathbb{Q}$ est dénombrable, $\mathbb{Q}^2$ est en bijection avec $\mathbb{N}^2$ et est donc dénombrable. Ainsi $\mathbb{Q}^3 = \mathbb{Q}^2 \times \mathbb{Q}$ est lui aussi en bijection avec $\mathbb{N}^2$ et donc dénombrable, et ainsi de suite. Le même raisonnement que celui fait précédemment prouve illico que l'on n'a pas besoin de l'axiome du choix pour construire un élément du produit des U_i où les U_i forment une famille d'ouverts non vides de $\mathbb{R}^n$ indexée par un ensemble I.

Le résultat important de ce paragraphe qu'il faut retenir, c'est qu'un ensemble dénombrable admet toujours une fonction de choix. Plus généralement tout ensemble qui admet un bon ordre admet également une fonction de choix. En fait, la réciproque est même vraie, c'est-à-dire qu'un ensemble admet une fonction de choix si et seulement s'il admet un bon ordre. Nous démontrerons ce résultat par la suite.

Constructions par récurrence

Avant de poursuivre, il devient nécessaire de faire un petit topo sur ce que l'on appelle les constructions par récurrence. Énonçons juste en fait un théorème qui va préciser tout cela.

Soient E un ensemble non vide et $\varphi : \mathbb{N} \times E \to E$ une fonction. On se donne également x un élément de E. Alors il existe une fonction $u : \mathbb{N} \to E$ telle que :

1. $u(0) = x$
2. $u(n+1) = \varphi(n, u(n))$

Autrement dit, il est possible de construire une fonction partant de $\mathbb{N}$ par récurrence. Je vous conseille d'aller regarder à nouveau l'énoncé de l'axiome du choix dépendant et de vous persuader intimement qu'il ne s'agit pas du tout de la même chose.

Bien sûr étant donné que nous n'avons toujours pas défini $\mathbb{N}$, il ne nous est pour l'instant pas possible de prouver quoi que ce soit. Admettons cela momentanément, admettons aussi que ce résultat n'utilise pas l'axiome du choix, une preuve de tout cela sera plus ou moins fournie au paragraphe 4.4.3.

Théorème de Baire

Une autre application de la dénombrabilité est le fait que le théorème de Baire sur un espace métrique complet séparable n'utilise aucune forme de l'axiome du choix. La démonstration que l'on donne classiquement et qui marche sans hypothèse de séparabilité, elle, utilise l'axiome du choix dépendant. Nous allons simplement l'adapter un peu dans ce qui suit.

Rappelons peut-être avant de commencer la définition de "séparable" et l'énoncé du théorème de Baire. Un espace topologique X est dit *séparable* s'il existe une partie de X à la fois dense et dénombrable. Par exemple $\mathbb{R}$ est séparable, et ce même sans l'axiome du choix, parce que l'on vient de voir de $\mathbb{Q}$ est dénombrable et dense dans $\mathbb{R}$. De même $\mathbb{R}^n$ est séparable.

Le théorème de Baire dit que si X est un espace métrique complet et si (U_n) est une famille d'ouverts denses indexée par $\mathbb{N}$, alors l'intersection des U_n est encore dense.

Montrons donc ce théorème sans utiliser l'axiome du choix. On part donc d'un espace métrique X que l'on suppose complet et séparable. On fixe A une partie dense et dénombrable de X. Comme A est dénombrable, il existe une fonction de choix sur A. Fixons-en une que l'on notera f. On considère en outre une famille (U_n) indexée par $\mathbb{N}$ d'ouverts denses de X. Il s'agit de montrer que l'intersection des U_n que l'on va noter U est dense dans X. Soit pour cela un élément x de X et un réel ε strictement positif. Il s'agit de construire un élément y dans U qui soit tel que $d(x,y) < \varepsilon$, d désignant la distance sur X. Pour cela on va construire par récurrence une suite V_n d'ouverts de X inclus dans la boule de centre x et de rayon ε, V_n étant inclus dans l'intersection des (U_k) pour $k < n$ et de diamètre inférieur à $\frac{\varepsilon}{n}$. Il s'agit donc pour cela de définir une fonction φ qui à un couple (n, V) associe un ouvert V'. Comment fait-on cela ?

On part donc d'un couple (n, V). V étant un ouvert de X, il intersecte l'ouvert dense U_n. Cette intersection est encore un ouvert et donc elle intersecte à son tour A. Notons disons B l'intersection de V avec U_{n+1} et avec A, ce que l'on vient de dire c'est que B est non vide. En particulier l'élément $f(B)$ est bien défini. D'autre part comme l'intersection $(U_n \cap V)$ est un ouvert, l'ensemble des $\eta > 0$, $\eta < \frac{\varepsilon}{n}$ tels que la boule de centre $f(B)$ et de rayon η soit incluse dans $(U_n \cap V)$ est non vide et majoré et donc admet une borne supérieure. Appelons s cette borne supérieure. L'ouvert V' que j'associe au couple (n, V) est alors la boule ouverte de centre $f(B)$ et de rayon $\frac{s}{2}$.

Le lecteur pourra alors vérifier par lui-même que si l'on choisit pour V_0 la boule ouverte de centre x et de rayon ε, la suite construire par le théorème du paragraphe précédent vérifie bien les conditions que l'on voulait.

Maintenant il est assez simple de conclure. Pour tout n de $\mathbb{N}$, l'intersection de V_n et de A est non vide. Je définis une suite (y_n) en posant $y_n = f(V_n \cap A)$. Je dis qu'il est alors immédiat que (y_n) est une suite de Cauchy et que sa limite fournit un y tel qu'on le désirait.

Complétude de $\mathbb{R}^n$

Afin de prouver que le théorème de Baire a une quelconque utilité, nous allons montrer que $\mathbb{R}^n$, muni de la norme infinie disons (il est encore vrai que toutes les normes sur $\mathbb{R}^n$ sont équivalentes sans l'axiome du choix mais passons) est complet et ce encore indépendamment de l'axiome du choix. Bien entendu, il suffit de le faire pour $\mathbb{R}$, ensuite on conclut simplement par récurrence.

Rappelons que l'on avait décrit $\mathbb{R}$ comme étant l'ensemble des suites de Cauchy à valeurs dans $\mathbb{Q}$ quotienté par la relation d'équivalence disant que deux suites sont équivalentes si et seulement si leur différence converge vers 0. Considérons (x_n) une suite de Cauchy de réels. Il s'agit de construire un réel ℓ, limite de la suite (x_n). Par définition, ce réel est simplement une suite de Cauchy de rationnels (ℓ_n). Nous aurons besoin pour cela d'une fonction de choix sur $\mathbb{Q}$. Comme nous l'avons déjà maintenant souvent dit, une telle fonction existe même sans l'axiome du choix, simplement par dénombrabilité de $\mathbb{Q}$. Notons f une telle fonction de choix.

On considère n un entier, c'est-à-dire un élément de $\mathbb{N}$. On définit alors ℓ_n comme l'image par f de l'intersection non vide de $[x_n - \frac{1}{n}, x_n]$ avec $\mathbb{Q}$. Il est alors facile de vérifier que la suite (ℓ_n) est de Cauchy donc définit un réel et d'autre part que la différence $\ell_n - x_n$ converge vers 0 et que donc le réel défini est bien la limite de la suite (x_n).

4.4 Étude des bons ordres

Les quelques exemples précédents ont, je l'espère, montré l'importance des ensembles bien ordonnés pour se passer de l'axiome du choix. Nous allons par la suite étudier ceux-ci un peu plus en détail.

4.4.1 Présentation intrinsèque

On commence par regarder la classe des bons ordres, c'est-à-dire des couples $(E, \leqslant)$ où $\leqslant$ est une relation de bon ordre sur E. Il n'est pas très difficile de se convaincre qu'il n'existe aucun ensemble dont les éléments sont précisément tous ces couples, c'est la raison pour laquelle nous préférons employer le terme de "classe".

Soient $(E, \leqslant)$ et $(F, \leqslant)$ (il y a ici un abus de notation, les deux relations d'ordre ne sont pas du tout les mêmes en général) deux bons ordres. On dit qu'ils sont isomorphismes s'il existe une bijection $f : E \to F$, telle que :

$$\forall x \in E,\ \forall y \in E,\ (x \leqslant y) \Rightarrow (f(x) \leqslant f(y))$$

(f vérifiant cette formule est dite tout simplement croissante). On notera par la suite $E \sim F$ pour dire que les bons ordres $(E, \leqslant)$ et $(F, \leqslant)$ sont isomorphes.

En fait, la classe des bons ordres peut être munie d'une "relation" de pré-ordre. Si $(E, \leqslant)$ et $(F, \leqslant)$ sont deux bons ordres, on dit que E est plus petit que F, et on note $E \leqslant F$, si E est isomorphe à un segment initial de F, un *segment initial* de F étant un sous-ensemble F' de F tel que si x appartient à F' tout élément inférieur à x lui appartient également.

Il est assez simple de vérifier que cette relation est réflexive et transitive. C'est donc un pré-ordre. Que se passe-t-il si E et F sont deux bons ordres tels que $E \leqslant F$ et $F \leqslant E$? E est alors isomorphe à un segment initial de lui-même, disons E'. Montrons que cette bijection, disons f, ne peut être que l'identité de E, et donc du coup qu'en fait $E = E'$. Supposons que ce ne soit pas le cas, alors il existe un plus petit

élément x de E tel que $f(x) \neq x$. Mais alors, si $y < x$, on a $f(y) = y < x$. Ainsi, $f(x) > x$, puisque f est bijective. On en déduit par croissance que si $y \geqslant x$, alors $f(y) > x$. Ceci prouve que x n'est pas atteint et pourtant $f(x) > x$ l'est manifestement, on aboutit ainsi à une contradiction. On en déduit que $E = E'$ et donc que E et F étaient en fait isomorphes. Finalement, la "relation" de pré-ordre que l'on vient de définir induit une "relation" d'ordre sur les classes d'isomorphismes de bons ordres. Les guillemets sont là pour garder en mémoire que l'"ensemble" des bons ordres ou des classes d'équivalence de bons ordres n'en est justement pas un, et donc que cela n'est pas à prendre dans un sens formel.

Cette "relation" d'ordre est même un bon ordre dans le sens où si les (E_i) sont des ensembles bien ordonnés, alors il existe un j tel que E_j soit plus petit que tous les autres. Disons rapidement comment l'on prouve cela. On choisit un ensemble quelconque parmi les E_i, disons E, et on regarde la réunion des segments initiaux de E qui sont plus petits que tous les E_i. On montre ensuite que cet ensemble est isomorphe en tant qu'ensemble bien ordonné à l'un des E_j et qu'il est plus petit que tous les E_i.

En particulier, cette "relation" d'ordre est totale. Cela veut dire qu'étant donné deux bons ordres E et F, on a soit $E \leqslant F$, soit $F \leqslant E$.

4.4.2 Les ordinaux

Ce que l'on va appeler un ordinal, c'est un représentant particulier de chacune des classes que l'on vient de définir. Mais comment choisir un tel représentant ? Ce que l'on constate, c'est que si E est un ensemble bien ordonné, l'ensemble de ses segments initiaux stricts (ie différents de E) muni de l'inclusion forme également un ensemble bien ordonné qui est en fait isomorphe à E (en effet étant donné un élément x de E, l'ensemble S_x des éléments de E strictement plus petits que x forme un segment initial et réciproquement étant donné un segment initial strict S de E, l'ensemble $E \backslash S$ est non vide et admet donc un plus petit élément x, il est alors facile de voir que $S = S_x$). On pense donc à remplacer E par l'ensemble de ses segments initiaux stricts, chacun de ces segments initiaux est un bon ordre on lui applique alors la même transformation et ainsi de suite... et de fait ça marche. Voyons comment ça marche sur les premiers bons ordres.

Commençons par l'ensemble vide. Il est muni d'un unique ordre, l'ordre vide, qui a toutes les propriétés requises pour être un bon ordre. Il est même tout seul dans sa classe d'équivalence, c'est donc nécessairement lui qu'il faut choisir. Il est même facile de voir qu'il s'agit du plus petit ordinal, on le note 0.

Prenons maintenant un ensemble E à un unique élément, disons $E = \{x\}$. E encore est muni d'un unique ordre qui encore est un bon ordre. E admet un unique segment initial strict qui est l'ensemble vide. Le représentant que l'on va choisir dans la classe de E sera donc le singleton $\{0\} = \{\emptyset\}$. C'est lui le deuxième plus petit ordinal, on le note 1.

Si maintenant E a deux éléments, $E = \{x, y\}$, et est muni de la relation de bon ordre définie par $x < y$, les segments initiaux de E sont $\emptyset$ et $\{x\}$. On remplace ensuite chacun de ces segments initiaux par leur représentant. Ici donc le représentant choisi dans la classe de E sera $\{0, 1\} = \{\emptyset, \{\emptyset\}\}$. Et voici le troisième plus petit ordinal, on le note 2.

Et on continue ainsi...

L'ordinal n serait alors l'ensemble $\{0, 1, \ldots, n-1\}$ sur lequel on a mis le bon ordre auquel on pense. De façon plus générale, un ordinal n'est autre que l'ensemble des ordinaux plus petits que lui.

Ce qu'il y a d'intéressant, c'est que les opérations classiques que l'on peut imaginer sur les classes d'équivalence de bons ordres se transposent très simplement sur les ordinaux.

Tout d'abord, si E est un ensemble bien ordonné d'ordinal α, il est légitime de s'intéresser à la classe venant juste après celle de E, ie formellement à la plus petite classe qui soit strictement supérieure à celle

de E. Il lui correspond un ordinal β. Il n'est pas bien difficile de voir que d'après la construction que l'on a fait, l'ordinal β s'exprime simplement par $\beta = \alpha \cup \{\alpha\}$. β est alors appelé l'ordinal successeur de α. Un ordinal qui est le successeur d'un autre est appelé un *ordinal successeur*. Un ordinal non successeur et non nul est appelé un *ordinal limite*.

Prenons maintenant une famille (E_i) de bons ordres indexée par un *ensemble* I. Notons α_i l'ordinal de E_i et intéressons-nous au plus petit bon ordre qui majore simultanément tous les E_i, ce que l'on pourrait appeler la borne supérieure des E_i. Notons E ce bon ordre. L'ordinal de E est là encore assez facile à décrire, il s'agit simplement de la réunion des α_i comme il est encore assez facile de s'en convaincre.

Remarquez que pour l'instant nous n'avons donné aucune définition rigoureuse. En effet, étant donné un ensemble, on est à ce stade plus ou moins incapable de dire s'il s'agit d'un ordinal ou si ce n'est pas le cas. Cependant, il existe bien une formule qui permet de faire cela. Plus précisément α est un ordinal s'il vérifie les deux conditions suivantes :

1. *(transitivité)* $\forall x \forall y((x \in y) \text{ et } (y \in \alpha)) \Rightarrow (x \in \alpha)$
2. la relation d'appartenance entre les éléments de α constitue une relation de bon ordre strict

Une chose d'important et assez facile à prouver est qu'il n'existe pas d'ensemble ayant précisément tous les ordinaux pour éléments. Une façon de le voir est de remarquer qu'un tel ensemble serait lui-même un ordinal, et donc serait un élément de lui-même... ce qui n'est pas possible au vu de la définition.

4.4.3 Construction de $\mathbb{N}$

On est maintenant en mesure de construire cet ensemble $\mathbb{N}$ dont on n'arrête pas de parler depuis si longtemps. L'axiome de l'infini que nous n'avons pas encore utilisé assure l'existence d'un ordinal non nul et non successeur. Nous n'allons pas démontrer cela, le lecteur soucieux pourra le faire par lui-même.

En particulier, d'après les propriétés des ordinaux, il existe un plus petit ordinal non nul et non successeur. C'est cet ensemble que l'on appelle $\mathbb{N}$, ou plus souvent ω. Il s'agit précisément de l'ensemble des ordinaux finis, un *ordinal fini* étant par définition un ordinal successeur ou nul et tel que tous les ordinaux strictement plus petits que lui soient également successeurs ou nuls. Ces ordinaux finis sont la traduction dans notre modèle de ZF des entiers naturels.

Maintenant sur $\mathbb{N}$, et d'ailleurs plus généralement sur les ordinaux on peut construire des opérations, à savoir l'addition et la multiplication. Commençons par construire l'addition. Prenons α et β deux ordinaux. Prenons A (resp. B) un ensemble bien ordonné d'ordinal α (resp. β). Sur l'union disjointe de A et de B, on peut mettre un bon ordre naturel : dit avec les mains, on met d'abord les éléments de A que l'on classe comme ils le sont déjà puis on rajoute derrière les éléments de B sans encore toucher à l'ordre. Ce bon ordre là est donné par un ordinal, c'est celui-ci que l'on définit comme étant la somme de α et de β et que l'on note $\alpha + \beta$.

Il faut faire attention à ce que cette opération ne possède pas toutes les propriétés que l'on souhaiterait. Cette addition par exemple n'est pas commutative (par exemple $\omega + 1$ est le successeur de ω – et plus généralement $\alpha + 1$ est toujours le successeur de α – mais $1 + \omega$ est ω). Toutefois, l'associativité, elle, reste valable. Toutefois également, si l'on se restreint aux ordinaux finis, cette opération fournit une application de $\mathbb{N}$ dans $\mathbb{N}$, l'addition, qui elle est bien commutative.

Voyons maintenant la multiplication. Comme précédemment on part de deux ensembles bien ordonnés A et B d'ordinal respectif α et β. On regarde ce coup-ci le produit $A \times B$ que l'on munit de l'ordre lexicographique en donnant priorité aux éléments de B. Autrement dit, le couple (a, b) sera strictement plus petit que le couple (a', b') si $b < b'$ ou si $b = b'$ et $a < a'$. Ceci fournit un bon ordre sur le produit $A \times B$. Il lui correspond un ordinal, c'est le produit $\alpha \cdot \beta$.

Là encore, il faut faire attention au fait que la multiplication n'est pas commutative. Elle est distributive sur l'addition simplement d'un seul côté... on laisse en exercice au lecteur le soin de trouver lequel :-). Toutefois encore si l'on se restreint aux ordinaux finis, on obtient une application de $\mathbb{N}$ dans $\mathbb{N}$ qui a les bonnes propriétés de la multiplication que l'on manie depuis notre plus tendre enfance.

Les propriétés générales de ces opérations se démontrent grâce au principe d'induction que l'on détaillera dans le paragraphe suivant. Les propriétés valables seulement pour les ordinaux finis se démontrent, elles, grâce au principe de récurrence (qui est un cas particulier du principe d'induction) que nous énonçons tout de suite.

Soit $F(x)$ une formule possédant une variable libre. Si $F(0)$ est vraie et si pour tout ordinal fini n, $F(n)$ implique $F(n+1)$, alors la formule $\forall n \in \mathbb{N}$, $F(n)$ est également vraie.

Une application plus ou moins directe et encore laissée au lecteur de ce principe de récurrence est la démonstration de la propriété énoncée dans le paragraphe 4.3.5.

4.4.4 Principe d'induction

Le principe d'induction dit la chose suivante. Soit $F(x)$ une formule à une variable libre. On suppose que :

$$\forall \alpha \text{ ordinal } (\forall \beta \text{ ordinal } < \alpha,\ F(\beta)) \Rightarrow F(\alpha)$$

Alors on en déduit que $\forall \alpha$ ordinal $F(\alpha)$

La démonstration est la suivante. Supposons que la conclusion soit fausse. Alors il existe au moins un ordinal α tel que $F(\alpha)$ soit fausse. Considérons le plus petit tel α. Par définition tous les $F(\beta)$ pour $\beta < \alpha$ sont vraies, mais alors $F(\alpha)$ est vraie grâce à l'hypothèse. D'où la contradiction et le théorème.

On remarquera qu'il n'est pas nécessaire de faire une hypothèse supplémentaire d'initialisation dans ce théorème, cette initialisation étant impliquée par l'hypothèse en prenant $\alpha = 0$.

On pourra aussi remarquer que ce principe d'induction implique le principe de récurrence énoncé précédemment. Toutefois, il est peut-être encore plus simple, afin de prouver le principe de récurrence, d'adapter le raisonnement donné ci-dessus.

4.4.5 Retour sur les équivalents de l'axiome du choix

Les énoncés équivalents à l'axiome du choix auxquels nous allons nous intéresser ici sont le lemme de Zorn, le théorème de Zermelo. Les énoncés de ces propriétés ont été donnés et plus ou moins commentés dans le paragraphe 4.3.4. Nous nous proposons ici de donner des indications sur la preuve de l'équivalence de toutes ces propriétés en utilisant la puissance des ordinaux.

Théorème de Zermelo

Prouvons dans un premier temps que l'axiome du choix implique le théorème de Zermelo. Prenons donc E un ensemble quelconque. On cherche à construire un bon ordre sur E. Rappelons-nous que par hypothèse, on dispose d'une fonction de choix sur E, disons $f : \mathcal{P}(E)\backslash\{\emptyset\} \to E$. On va définir notre bon ordre par induction sur les ordinaux. Plus précisément, on va définir pour tout ordinal α, une partie E_α de E munie d'un bon ordre et ce de telle façon que si $\beta < \alpha$, E_β soit inclus dans E_α et le restriction du bon ordre sur E_α à E_β coïncide avec le bon ordre sur E_β. D'après le principe d'induction, pour faire cela, il suffit de dire comment construire E_α à partir des E_β, $\beta < \alpha$.

C'est assez simple en fait. On regarde E' défini comme la réunion de ces E_β. Avec les hypothèses faites, E' est muni d'un bon ordre. On regarde maintenant l'ensemble $E\backslash E'$. S'il est vide, on pose $E_\alpha = E'$. Sinon on regarde l'élément $x = f(E\backslash E')$ qui bien sûr n'appartient pas à E' et on met sur l'union $E' \cup \{x\}$ un bon ordre en disant que x est plus grand que tout le monde. Cela convient.

Il faut ensuite se persuader qu'il existe un α tel que $E_\alpha = E$. On remarque pour cela que si ce n'est pas le cas, par construction E_β est strictement inclus dans E_α pour $\beta < \alpha$. Mais cela n'est pas possible... on aurait ainsi une injection de la classe des ordinaux dans un ensemble E, ce qui prouverait que la classe des ordinaux est un ensemble, ce qui est faux.

La réciproque, quant à elle est toute simple. Étant donné un bon ordre sur E, on construit une fonction de choix en associant à une partie non vide de E son plus petit élément.

On remarquera que l'on a démontré ici un peu plus que l'équivalence entre l'axiome du choix et le théorème de Zermelo. On a prouvé qu'un ensemble E admet une fonction de choix si et seulement s'il admet un bon ordre.

Lemme de Zorn

Prouver le lemme de Zorn à partir de l'axiome du choix se fait encore avec les ordinaux. Nous n'allons en fait pas détailler cette démonstration, les idées qui interviennent étant essentiellement celles décrites dans le paragraphe précédent.

Voyons la réciproque. On montre ici la deuxième forme de l'axiome du choix, celle avec les produits. Soit donc I un ensemble non vide et (X_i) une famille d'ensembles non vides indexée par I. On considère l'ensemble des fonctions f définies sur une partie J de I et telles que pour tout élément i de J, $f(i)$ appartienne à X_i. Ces fonctions sont ordonnées par inclusion. Il n'est pas bien dur de voir que cet ensemble est inductif, une chaîne admettant naturellement pour majorant l'union des éléments qui la constituent. Le lemme de Zorn fournit alors un élément maximal, c'est un élément du produit des X_i qui est donc non vide.

4.4.6 D'autres applications

E est-il en bijection avec $2E$?

Disons tout d'abord que $2E$ est par définition le produit $2 \times E$, ou encore $\{0,1\} \times E$. Regardons tout d'abord le cas où E peut être muni d'un bon ordre (ou ce qui revient au même d'une fonction de choix). En fait on peut même regarder le plus petit bon ordre que l'on peut obtenir ainsi. Cet ordinal désigne ce que l'on appelle communément le cardinal de E.

Il y a une définition disons intrinsèque d'un cardinal. Il s'agit d'un ordinal qui n'est en bijection avec aucun ordinal strictement plus petit. Il est immédiat de se convaincre que l'ordinal associé ci-dessus est bien un cardinal et même que tout cardinal est l'"associé" d'un certain ensemble (par exemple lui-même). Tout ça pour dire que pour prouver le résultat lorsque E admet un bon ordre, on peut supposer que E est un cardinal que l'on va appeler κ.

Une dernière chose à savoir sur les cardinaux, c'est que ceux-ci sont bien ordonnés. C'est évident car la classe des cardinaux forme une sous classe de la classe des ordinaux qui est bien ordonnée. Remarquez que ceci n'utilise pas l'axiome du choix et n'est pourtant pas du tout en contradiction avec le fait que le lemme de trichotomie l'utilise. On rappelle en effet que l'on n'a pas associé un cardinal à tout ensemble, mais simplement aux ensembles qui peuvent être munis d'un bon ordre.

En particulier le principe d'induction s'applique encore sur les cardinaux. Plus précisément pour montrer que κ est en bijection avec $2 \times \kappa$ pour tout cardinal κ, il suffit de prouver qu'étant donné κ un cardinal, κ est en bijection avec $2 \times \kappa$ sous l'hypothèse que pour tout cardinal $\kappa' < \kappa$, on a κ' en bijection avec $2 \times \kappa'$. Mais bien sûr, on ne va pas pouvoir montrer cela puisqu'il est clair que ce n'est pas vrai si κ est un cardinal fini non nul. Un *cardinal fini* est par définition un élément de $\mathbb{N}$ (on pourra se convaincre que tout élément de $\mathbb{N}$ est un cardinal successeur et que la réciproque est même vraie). Un

cardinal qui n'est pas fini sera dit *infini*. Dans le paragraphe suivant, nous allons montrer par induction sur les cardinaux infinis que $2 \times \kappa$ est toujours en bijection avec κ.

Allons-y. On va construire une injection de $2 \times \kappa$ dans κ par induction sur l'ordinal $\alpha \leqslant \kappa$, le théorème de Cantor-Bernstein permettra alors de conclure. Cela signifie que l'on va construire pour tout ordinal $\alpha \leqslant \kappa$ une injection de $2 \times \alpha$ dans κ, ces injections étant compatibles dans un sens évident.

Si $\alpha = 0$, il n'y a rien à construire. Supposons maintenant que $\alpha = \beta + 1$ est un ordinal successeur. Par hypothèse d'induction on a une injection $f : 2 \times \beta \to \kappa$. Si le cardinal de β est infini, $2 \times \beta$ est en bijection avec β par la première hypothèse d'induction et $\beta < \kappa$ (car $\alpha \leqslant \kappa$) n'est pas en bijection avec κ puisque κ est un cardinal. D'autre part, si le cardinal de β est fini, celui de $2 \times \beta$ l'est également (ce que l'on peut montrer indépendamment par récurrence) et donc il n'est pas non plus en bijection avec κ. Dans tous les cas, la fonction f ne peut être surjective. Considérons le plus petit élément de κ qui n'est pas dans l'image de f, appelons le x. On peut prolonger f en posant $f(0, \beta) = x$. Pour les mêmes raisons que précédemment, f ainsi prolongée n'est toujours pas surjective. Appelons y le plus petit élément de κ qui n'est pas dans son image et prolongeons encore f en posant $f(1, \beta) = y$. On obtient ainsi une injection de $2 \times \alpha$ dans κ, ce qui est précisément ce que l'on voulait.

Maintenant si α est un ordinal limite, il suffit de prendre pour f la réunion de toutes les fonctions f construites pour les ordinaux $\alpha < \beta$. Celle-ci convient.

Ainsi exhiber une bijection entre E et $2E$ peut se faire sans l'axiome du choix dès que E peut être muni d'un bon ordre. Nous n'allons pas le prouver mais dans le cas général, l'axiome du choix est requis...

E est-il en bijection avec E^2 ?

Là encore, on va commencer par traiter le cas où E est un ensemble qui admet un bon ordre. Comme précédemment, on se ramène au cas où E est un cardinal κ infini et comme précédemment on peut supposer que le résultat est démontré pour tout cardinal κ' infini strictement inférieur à κ. Il s'agit ce coup-ci de construire une injection de κ^2 dans κ, ce que l'on fait par induction sur l'ordinal $\alpha \leqslant \kappa$.

Il s'agit donc, vous l'auriez deviné, de construire une injection de α^2 dans κ. Supposons dans un premier temps que α soit un ordinal limite, alors comme précédemment la réunion des fonctions précédemment construites convient. Supposons donc maintenant que α soit un ordinal successeur, par exemple $\alpha = \beta + 1$. Comme $\alpha \leqslant \kappa$, on a $\beta < \kappa$ et du coup $\alpha < \kappa$. On dispose d'une injection $f : \beta^2 \to \kappa$ et il s'agit donc de la prolonger en lui attribuant des valeurs sur l'ensemble $(\alpha^2) \backslash (\beta^2)$. Mais cet ensemble peut être muni d'un bon ordre. Il suffit par exemple de le voir comme l'union disjointe $(\{\alpha\} \times \alpha) \cup (\alpha \times \{\alpha\}) \cup (\{(\alpha, \alpha)\})$ que l'on munit d'un bon ordre en décrétant que les éléments de la première composante sont plus petits que ceux de la deuxième, eux mêmes plus petits que ceux de la troisième. Comme précédemment f n'est pas surjective et même encore par un argument de cardinalité (que nous laissons au lecteur), κ privé de l'image de f est un ensemble bien ordonné de cardinal κ. Ainsi l'union disjointe précédente est isomorphe à un segment initial de κ privé de l'image de f. Ceci permet de prolonger f tel qu'on le désirait.

Là encore si E est un ensemble quelconque, ceci n'est plus vrai sans l'axiome du choix. Un peu plus fort même, le fait que E soit en bijection avec E^2 pour tout ensemble E infini est un énoncé équivalent à l'axiome du choix. Nous n'allons pas démontrer cette dernière affirmation non plus.

Clôture algébrique

La question ici est la suivante. Soit K un corps. Peut-on construire une clôture algébrique de K sans l'axiome du choix ? Ça ne paraît pas évident, en tout cas la démonstration classique utilise le lemme de Krull qui est connu pour être une conséquence de l'axiome du choix. Voyons tout de même ce que l'on peut faire.

Bien entendu, au vu des exemples précédents, on va commencer par supposer que K peut être muni d'un bon ordre. Ce que l'on doit faire, c'est ajouter à K les racines de tous les polynômes (irréductibles) sur K. On commence donc par lister tous les polynômes à coefficients dans K. Cet ensemble peut être muni d'un bon ordre en disant par exemple que l'on commence à ordonner ces polynômes en regardant les degrés puis qu'à l'intérieur d'un même degré on utilise l'ordre lexicographique. Notons par exemple α l'ordinal associé à ce bon ordre.

Ce que l'on va faire c'est construire par induction sur l'ordinal $\beta \leqslant \alpha$, des corps K_β extensions compatibles de K qui vont être munis d'un bon ordre et qui seront tels que tous les polynômes indexés par un ordinal $\leqslant \beta$ auront au moins une racine dans K_β. Le corps K_α ainsi construit sera une clôture algébrique de K.

Commençons par construire K_0. Il s'agit d'ajouter à K une racine du polynôme P_0. Pour faire cela, on commence par décomposer P_0 en produits de polynômes irréductibles et on choisit un de ces facteurs. Bien entendu, on ne choisit pas n'importe lequel, on prend par exemple celui qui est le plus petit pour le bon ordre défini sur l'ensemble des polynômes à coefficients dans K. Si P désigne ce polynôme irréductible, on prend pour K_0 le corps $K[X]/P$. Il ne reste plus qu'à mettre un bon ordre sur K_0 mais tout élément de K_0 peut être vu comme un polynôme de degré inférieur au degré de P, l'ordre lexicographique peut donc être utilisé.

Et en fait, on applique exactement la même construction pour passer de K_β à $K_{\beta+1}$. Si β est un ordinal limite, on commence par regarder la limite inductive des $K_{\beta'}$ pour $\beta' < \beta$ et on applique la construction précédente à cette limite inductive. Cela fonctionne.

On vient donc de construire une clôture algébrique de K et on a même un petit bonus : dès que K est fini, cette clôture algébrique est dénombrable, si K est infini, elle a le même cardinal que celui de K. Qu'en est-il de l'unicité ? Voyons cela. Prenons donc L une clôture algébrique de K et essayons de construire un isomorphisme entre K_α et L (en gardant les notations précédentes). Cet isomorphisme va se construire par induction sur l'ordinal $\beta \leqslant \alpha$. Il s'agit donc simplement à chaque étape de choisir dans L une racine du polynôme P. Aïe, mais nous n'avons rien supposé sur L, il n'admet pas forcément de fonction de choix. On laisse le lecteur écrire proprement la démonstration que sous l'hypothèse que L est bien ordonnable alors il existe une bijection entre K_α et L.

Toutefois cela n'est pas vrai en général. Il existe des modèles de ZF dans lesquels le corps des rationnels $\mathbb{Q}$ admet une clôture algébrique qui n'est pas dénombrable. De fait, elle ne sera pas isomorphe à la clôture algébrique de $\mathbb{Q}$ donnée par la construction précédente. D'après ce que l'on vient de dire, il s'agira là d'un ensemble n'admettant pas de fonction de choix...

Finalement, on peut signaler que si A est une clôture algébrique de $\mathbb{Q}$, il est toujours vrai que A est réunion dénombrable d'ensembles finis, à savoir l'ensemble des racines d'un polynôme à coefficients rationnels donné. Notamment, une réunion dénombrable d'ensembles finis n'est pas forcément dénombrable, comme nous allons le redire juste en dessous. :-)

4.4.7 Quelque désillusion

Nous espérons vous avoir plus ou moins convaincu dans ce qui précède que les bons ordres sont quelque chose d'intimement lié à l'axiome du choix et que souvent quand on en dispose il est possible de faire nombre de constructions sans utiliser justement l'axiome du choix.

Toutefois il y a des écueils à ce principe. Nous allons citer un unique exemple mais qui vaut son pesant d'or. Sans l'axiome du choix, il n'est pas vrai qu'une union dénombrable d'ensembles dénombrables est forcément dénombrable. Pour pouvoir utiliser la magie des bons ordres, il faudrait soit mettre simultanément un bon ordre sur chaque ensemble dénombrable (et dit comme cela ceci requiert manifestement

l'axiome du choix) ou à la limite mettre un bon ordre sur l'union mais justement a priori on ne sait pas que celle ci est dénombrable.

Peut-être, allez-vous me dire : "Mais non, notons par exemple U_n les ensembles dénombrables dont on veut prendre l'union. Ben, pour tout n, U_n est en bijection avec $\mathbb{N}$, donc l'union des U_n s'injecte dans $\mathbb{N}^2$ et Cantor-Bernstein permet de conclure". Eh ben, non, ce raisonnement est faux car pour construire l'injection de l'union des U_n dans $\mathbb{N}^2$, il faut disposer simultanément de toutes les bijections $U_n \to \mathbb{N}$ et cela requiert l'axiome du choix, dénombrable seulement certes mais quand même.

Si vous êtes encore sceptique, essayez de formaliser proprement cette démonstration, vous verrez qu'elle bogue à un moment.

4.5 Conclusion

L'axiome du choix, dans sa plus grande généralité, est aujourd'hui largement accepté dans le monde mathématique. Il est à la base de nombreux résultats classiques et fondamentaux que l'on ne peut pas prétendre remettre en cause.

Toutefois, c'est aussi quand même lui qui affirme l'existence de "monstres" dirons-nous. C'est lui qui permet de construire une partie de $\mathbb{R}$ non mesurable. Un résultat du même gabarit encore plus spectaculaire est sans doute le paradoxe de Banach-Tarski. Il dit que si U et V sont deux parties bornées de $\mathbb{R}^3$ d'intérieur non vide, alors on peut trouver un entier n, une partition $\{U_1, ..., U_n\}$ de U, une partition $\{V_1, ..., V_n\}$ de V et des isométries σ_i de $\mathbb{R}^3$ qui envoient précisément l'ensemble U_i sur l'ensemble V_i. Autrement dit, partant d'une orange, il est possible de la découper en un nombre fini de parties et de reconstituer une boule de la taille du soleil en déplaçant et en recomposant ces parties...

Il serait peut-être finalement intéressant de parler d'autres axiomes plus ou moins répandus dans le monde mathématique. L'hypothèse du continu est sans doute la plus médiatisée. Elle dit qu'un sous-ensemble de $\mathbb{R}$ est soit fini, soit dénombrable, soit en bijection avec $\mathbb{R}$. Cet énoncé aussi est indécidable dans ZF et même dans ZFC... on peut donc choisir de le rajouter à la liste ou pas. Il semble que la tendance actuelle soit de ne pas le rajouter, de le remplacer plutôt par d'autres axiomes moins évidents à décrire mais qui reflètent mieux ce que l'on aimerait voir. Nous n'allons cependant pas détailler ces axiomes.

Pour finir, j'aimerais parler de l'axiome de détermination. Commençons par prendre une partie A de l'intervalle $[0, 1]$. Prenons également deux joueurs et faisons les jouer au jeu suivant. Le premier joueur choisit un chiffre en base 2, c'est-à-dire soit 0, soit 1. C'est le premier chiffre après la virgule de l'écriture binaire d'un nombre. Le deuxième joueur choisit un second chiffre, ce sera le deuxième chiffre... et ainsi de suite jusqu'à la fin des temps. Le premier joueur gagne si le nombre écrit au final est dans la partie A, perd sinon. Vous pourrez vous amuser à montrer par exemple que si A est un intervalle, il y a toujours un joueur qui a une stratégie gagnante. Un peu plus dur est de montrer que si $A = \mathbb{Q} \cap [0, 1]$, le deuxième joueur a une stratégie gagnante. On peut même montrer que si A est un borélien, alors un des deux joueurs a une stratégie gagnante. L'axiome de détermination dit que pour toute partie de $[0, 1]$, un de deux joueurs a une stratégie gagnante. C'est bien joli tout ça, mais cet axiome contredit l'axiome du choix. En effet, via l'axiome du choix, on peut construire une partie A de $[0, 1]$ pour laquelle aucun de deux joueurs n'a de stratégie gagnante... Cet axiome a cependant des conséquences assez intéressantes comme par exemple le fait que toute partie de $\mathbb{R}$ devient mesurable.

Que faut-il prendre comme axiome alors ? L'axiome du choix ? L'axiome de détermination ? Encore autre chose, comme celui qui dit que tout ensemble doit être constructible ? Vaste question... L'axiome du choix a l'air de très bien s'imposer aujourd'hui, et les raisons de cela sont vraiment importantes, mais qui sait ?

Chapitre 5

Un cours d'arithmétique

L'association Animath (`http://www.animath.fr`) a pour but de repérer des élèves de lycée brillants, et de les faire travailler soit en leur faisant découvrir des mathématiques qui ne leur sont pas enseignés à l'école, soit en les entraînant à résoudre des exercices de type Olympiades. Voici un cours d'arithmétique que j'ai rédigé dans ce cadre.

Sommaire

Dans tout ce cours :

- $\mathbb{N}$ désignera l'ensemble des entiers naturels : $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$
- $\mathbb{N}^\star$ désignera l'ensemble des entiers naturels non nuls : $\mathbb{N}^\star = \{1, 2, 3, \ldots\}$
- $\mathbb{Z}$ désignera l'ensemble des entiers relatifs : $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- $\mathbb{Z}^\star$ désignera l'ensemble des entiers relatifs non nuls : $\mathbb{Z}^\star = \{\ldots, -3, -2, -1, 1, 2, 3, \ldots\}$

5.1 Quand on ne regarde que le dernier chiffre...

5.1.1 Qu'est-ce que $\mathbb{Z}/10\mathbb{Z}$?

Commençons par introduire les notations suivantes :

- $\dot{0}$ sera un entier naturel quelconque se terminant par 0
- $\dot{1}$ sera un entier naturel quelconque se terminant par 1

$$\vdots$$

- $\dot{9}$ sera un entier naturel quelconque se terminant par 9

Remarquons que la définition précédente n'a rien de rigoureux. Il aurait mieux fallu définir par exemple $\dot{0}$ comme l'ensemble des nombres se terminant par 0 plutôt que comme l'un quelconque d'entre eux, mais cela ne changera rien par la suite et c'est sans doute plus simple de voir les choses de cette façon.

L'ensemble $\mathbb{Z}/10\mathbb{Z}$ est alors par définition :

$$\mathbb{Z}/10\mathbb{Z} = \left\{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5}, \dot{6}, \dot{7}, \dot{8}, \dot{9}\right\}$$

Il s'agit donc d'un ensemble fini comportant 10 éléments.

5.1.2 Opérations dans $\mathbb{Z}/10\mathbb{Z}$

Ce que l'on sait depuis que l'on sait effectuer des opérations mais qu'il est remarquable de constater ici, c'est que pour calculer le dernier chiffre d'une somme ou d'un produit, il suffit de connaître les derniers chiffres des nombres que l'on additionne ou multiple.

Cela permet de voir que l'on peut en fait additionner et multiplier directement les éléments de $\mathbb{Z}/10\mathbb{Z}$. Par exemple supposons que l'on veuille multiplier $\dot{3}$ par $\dot{7}$. On choisit alors un nombre se terminant par 3, par exemple 13, un autre se terminant par 7 par exemple 47. On multiplie 13 et 47 entre eux, on trouve 611 et on ne garde que le dernier chiffre. Bien entendu ce dernier chiffre ne dépend pas des représentants que l'on a choisi pour faire le calcul. Ainsi il est légitime de poser :

$$\dot{3} \times \dot{7} = \dot{1}$$

Bien entendu, pour faire ce calcul, il aurait été plus rusé de choisir les représentations 3 et 7 plutôt que 13 et 47. Enfin, bon, ça tombe sous le sens.

Dressons les tables d'addition et de multiplication de $\mathbb{Z}/10\mathbb{Z}$. On trouve :

$+$	$\dot{\mathbf{0}}$	$\dot{\mathbf{1}}$	$\dot{\mathbf{2}}$	$\dot{\mathbf{3}}$	$\dot{\mathbf{4}}$	$\dot{\mathbf{5}}$	$\dot{\mathbf{6}}$	$\dot{\mathbf{7}}$	$\dot{\mathbf{8}}$	$\dot{\mathbf{9}}$
$\dot{\mathbf{0}}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$
$\dot{\mathbf{1}}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{0}$
$\dot{\mathbf{2}}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{0}$	$\dot{1}$
$\dot{\mathbf{3}}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{0}$	$\dot{1}$	$\dot{2}$
$\dot{\mathbf{4}}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{\mathbf{5}}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$\dot{\mathbf{6}}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$
$\dot{\mathbf{7}}$	$\dot{7}$	$\dot{8}$	$\dot{9}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$
$\dot{\mathbf{8}}$	$\dot{8}$	$\dot{9}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$
$\dot{\mathbf{9}}$	$\dot{9}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$

$\times$	$\dot{\mathbf{0}}$	$\dot{\mathbf{1}}$	$\dot{\mathbf{2}}$	$\dot{\mathbf{3}}$	$\dot{\mathbf{4}}$	$\dot{\mathbf{5}}$	$\dot{\mathbf{6}}$	$\dot{\mathbf{7}}$	$\dot{\mathbf{8}}$	$\dot{\mathbf{9}}$
$\dot{\mathbf{0}}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{\mathbf{1}}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$	$\dot{7}$	$\dot{8}$	$\dot{9}$
$\dot{\mathbf{2}}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{6}$	$\dot{8}$	$\dot{0}$	$\dot{2}$	$\dot{4}$	$\dot{6}$	$\dot{8}$
$\dot{\mathbf{3}}$	$\dot{0}$	$\dot{3}$	$\dot{6}$	$\dot{9}$	$\dot{2}$	$\dot{5}$	$\dot{8}$	$\dot{1}$	$\dot{4}$	$\dot{7}$
$\dot{\mathbf{4}}$	$\dot{0}$	$\dot{4}$	$\dot{8}$	$\dot{2}$	$\dot{6}$	$\dot{0}$	$\dot{4}$	$\dot{8}$	$\dot{2}$	$\dot{6}$
$\dot{\mathbf{5}}$	$\dot{0}$	$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{0}$	$\dot{5}$	$\dot{0}$	$\dot{5}$
$\dot{\mathbf{6}}$	$\dot{0}$	$\dot{6}$	$\dot{2}$	$\dot{8}$	$\dot{4}$	$\dot{0}$	$\dot{6}$	$\dot{2}$	$\dot{8}$	$\dot{4}$
$\dot{\mathbf{7}}$	$\dot{0}$	$\dot{7}$	$\dot{4}$	$\dot{1}$	$\dot{8}$	$\dot{5}$	$\dot{2}$	$\dot{9}$	$\dot{6}$	$\dot{3}$
$\dot{\mathbf{8}}$	$\dot{0}$	$\dot{8}$	$\dot{6}$	$\dot{4}$	$\dot{2}$	$\dot{0}$	$\dot{8}$	$\dot{6}$	$\dot{4}$	$\dot{2}$
$\dot{\mathbf{9}}$	$\dot{0}$	$\dot{9}$	$\dot{8}$	$\dot{7}$	$\dot{6}$	$\dot{5}$	$\dot{4}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

On constate sur les tables précédentes que, bien évidemment, ajouter $\dot{0}$ ou multiplier par $\dot{1}$ ne change pas le résultat. En outre, multiplier par $\dot{0}$ fournit toujours un résultat égal à $\dot{0}$.

5.1.3 Équations dans $\mathbb{Z}/10\mathbb{Z}$

Il arrive très souvent que des problèmes d'arithmétique se réduisent à la résolution d'équation par exemple dans $\mathbb{Z}/10\mathbb{Z}$. Nous allons voir comment l'on procède pour résoudre ces équations.

$\dot{x} + \dot{a} = \dot{b}$

Le résultat important à remarquer ici, et que l'on peut par exemple voir sur les tables précédentes, est que pour tout élément $\dot{a} \in \mathbb{Z}/10\mathbb{Z}$, il existe un élément $\dot{a}' \in \mathbb{Z}/10\mathbb{Z}$ tel que $\dot{a} + \dot{a}' = \dot{0}$. Un tel $\dot{a}'$ est unique et s'appelle l'*opposé* de $\dot{a}$.

Ainsi résoudre l'équation de départ est quelque chose de simple, il suffit d'ajouter $\dot{a}'$ des deux côtés de l'égalité. On obtient :

$$\dot{x} = \dot{b} + \dot{a}'$$

C'est l'unique solution.

$\dot{a}\dot{x} = \dot{b}$

Là encore, il nous faudrait trouver un élément $\dot{a}'$ tel que le produit $\dot{a} \times \dot{a}'$ soit égal à $\dot{1}$. On multiplierait alors par $\dot{a}'$ des deux côtés et on aurait une expression pour $\dot{x}$. Un tel $\dot{a}'$ s'appelle l'*inverse* de $\dot{a}$.

Toutefois, comme on peut le constater sur les tables, il n'est pas vrai que tout élément admet un inverse. $\dot{2}$ par exemple n'en admet pas. Mais cela se conçoit très bien : prenons un entier naturel se terminant par 2, ce nombre est pair et tous ces multiples seront donc pairs. Ainsi il n'est pas possible en le multipliant par un autre nombre d'obtenir un entier se terminant par 1 qui serait alors impair.

Un élément qui admet un inverse est qualifié d'*inversible*. Il est facile de faire la liste des inversibles de $\mathbb{Z}/10\mathbb{Z}$, il s'agit de $\dot{1}$, $\dot{3}$, $\dot{7}$ et $\dot{9}$.

Ainsi pour résoudre l'équation $\dot{3}\dot{x} = \dot{2}$ par exemple, il suffit de multiplier par $\dot{7}$ des deux côtés. Cela n'est plus valable pour l'équation $\dot{2}\dot{x} = \dot{3}$ qui, elle, n'a pas de solution. En revanche, l'équation $\dot{4}\dot{x} = \dot{2}$ admet deux solutions qui sont $\dot{3}$ et $\dot{8}$.

5.2 10 n'est-il pas un peu arbitraire ?

5.2.1 Division euclidienne

Théorème 5.2.1.1. *Soient a et b deux entiers relatifs, on suppose $b \neq 0$. Alors il existe un* unique *couple d'entiers (q, r) tels que*
i) $a = bq + r$
ii) $0 \leqslant r < |b|$

Trouver le couple (q, r) du théorème est ce que l'on appelle *effectuer la division euclidienne de a par b*. q s'appelle le *quotient* de cette division euclidienne et r le *reste*.

Pour effectuer une division euclidienne, on fait par exemple comme l'on a appris dans les petites classes. Il faut faire attention cependant lorsque des nombres négatifs interviennent. Par exemple, la division euclidienne de -17 par -4 s'écrit :

$$-17 = (-4) \times (-5) + 3$$

et non pas :

$$-17 = (-4) \times (-4) - 1$$

En effet il faut bien se rappeler que l'on impose que le reste soit positif (et strictement plus petit que $|b|$).

5.2.2 Décomposition en base n

On fixe dans ce chapitre et dans le suivant un entier $n \geqslant 2$.

Théorème 5.2.2.1. *Soit a un entier naturel. Il existe une* unique *suite $(a_i)_{i\geqslant 0}$ d'entiers telle que :*
i) (a_i) est nulle à partir d'un certain rang
ii) pour tout i, $0 \leqslant a_i < n$
iii) $a = a_0 + a_1 n + a_2 n^2 + \ldots + a_i n^i + \ldots$

On remarque dans un tout premier temps que la dernière somme écrite est en réalité finie puisque la suite (a_i) est nulle à partir d'un certain moment. La suite (a_i) est appelée la *décomposition en base n* de l'entier a.

Pour démontrer ce théorème, il s'agit simplement de faire des divisions euclidiennes. Plus précisément la dernière condition nous dit que a_0 *doit* être le reste de la division euclidienne de a par n, le quotient de cette division sera $a_1 + a_2 n + \ldots + a_i n^{i-1} + \ldots$.

Pour déterminer la décomposition de a en base n, on commence donc par effectuer la division euclidienne de a par n. Le reste fournit alors l'élément a_0. Quant au quotient, sa décomposition en base n va fournir les autres termes de la suite. On décompose donc ce quotient en base n et pour cela on effectue la division euclidienne de celui-ci par n. Le reste de cette division va en fait fournir a_1 et on continue ensuite avec le nouveau quotient obtenu.

Pour prouver finalement le théorème, il s'agit de voir que cela s'arrête en un nombre fini de divisions euclidiennes, c'est-à-dire qu'au bout d'un moment on tombe sur un quotient nul. Mais si le quotient n'est pas nul, il va décroître strictement puisque l'on divise par un nombre plus grand ou égal à 2. On conclut alors en disant que toute suite strictement décroissante d'entiers naturels s'arrête forcément.

Présentons les calculs sur un exemple. Supposons que l'on veuille déterminer la décomposition en base 7 de 125487. On effectue alors successivement les divisions euclidiennes :

$$\begin{aligned}
125487 &= 7 \times 17926 + 5 \\
17926 &= 7 \times 2560 + 6 \\
2560 &= 7 \times 365 + 5 \\
365 &= 7 \times 52 + 1 \\
52 &= 7 \times 7 + 3 \\
7 &= 7 \times 1 + 0 \\
1 &= 7 \times 0 + 1
\end{aligned}$$

On voit ainsi que :

$$125487 = 5 + 6 \cdot 7 + 5 \cdot 7^2 + 1 \cdot 7^3 + 3 \cdot 7^4 + 0 \cdot 7^5 + 1 \cdot 7^6$$

On écrit parfois cela sous la forme $125487 = \underline{1031565}_7$.

5.2.3 Présentation de $\mathbb{Z}/n\mathbb{Z}$

Il s'agit exactement de la même chose que celle qui a été présentée dans la première partie sauf que l'on remplace 10 par un entier $n \geqslant 2$ quelconque.

Plus précisément si a est un chiffre de la base n, c'est-à-dire un entier compris entre 0 et $n-1$, on note $\dot{a}$ un entier naturel naturel quelconque se terminant par a en base n. D'après ce que l'on a dit précédemment, il s'agit donc d'un entier dont le reste de la division euclidienne par n est précisément a[1]. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est alors :

$$\mathbb{Z}/n\mathbb{Z} = \left\{\dot{0}, \dot{1}, \ldots, \overline{n-1}\right\}$$

Là encore sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$, on peut définir une addition et une multiplication : pour calculer le dernier chiffre d'une somme ou d'un produit, on n'a encore besoin que des derniers chiffres des nombres que l'on souhaite additionner ou multiplier.

5.2.4 Congruences

On dit que deux entiers naturels a et b sont congrus modulo n s'ils se terminent par le chiffre lorsqu'ils sont écrits en base n. On peut généraliser aux entiers relatifs en disant que deux entiers relatifs a et b sont congrus modulo n s'ils ont même reste dans la division euclidienne par n. En fait, on préfère classiquement prendre la définition suivante peut-être moins visuelle mais qui a l'avantage non négligeable de ne pas utiliser de notions compliquées et qui est ainsi plus facilement maniable :

Définition 5.2.4.1. *Soient a et b deux entiers relatifs. On dit que a et b sont* congrus *modulo n (et on note $a \equiv b \pmod{n}$) si n divise la différence $a - b$.*

Les propriétés qui disent que le dernier chiffre d'une somme ou d'un produit se calcule simplement en utilisant les derniers chiffres des termes ou des facteurs se retraduisent directement en termes de congruence. Plus précisément, on a la propriété suivante :

Théorème 5.2.4.2. *Si a, a', b et b' sont des entiers relatifs tels que $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, alors :*

$$a + b \equiv a' + b' \pmod{n}$$

$$ab \equiv a'b' \pmod{n}$$

Nous allons démontrer ce théorème. Par hypothèse n divise $a - a'$ et $b - b'$, il divise donc la somme $(a - a') + (b - b') = (a + b) - (a' + b')$, ce qui signifie exactement que :

$$a + b \equiv a' + b' \pmod{n}$$

Pour la multiplication, on écrit $a' = a + kn$ et $b' = b + ln$. Ainsi :

$$a'b' = ab + n\,(kb + al + knl)$$

et donc finalement :

$$ab \equiv a'b' \pmod{n}$$

[1] Cela permet d'ailleurs de donner un sens précis et agréable à ce qu'est le dernier chiffre d'un entier négatif.

5.3 Équations dans $\mathbb{Z}/n\mathbb{Z}$

5.3.1 $\dot{x} + \dot{a} = \dot{b}$

Comme dans le cas $n = 10$, il est facile de constater que tout nombre admet un opposé. Pour cela, il suffit de prouver que si a est un entier, relatif, il existe toujours a' tel que $a + a' \equiv 0 \pmod{n}$. Bien entendu, il suffit de prendre $a' = -a$.

Cela signifie que l'on peut passer les éléments de l'autre côté de l'égalité en changeant le signe bien sûr, comme on le fait classiquement pour résoudre ces équations.

5.3.2 $\dot{a}\dot{x} = \dot{b}$

Ici, déjà dans le cas $n = 10$, on a vu que ce n'était pas toujours possible de *diviser*. Nous allons dans ce chapitre donner un critère qui explique lorsque l'on a le droit de diviser et qui explique ce que l'on a quand même le droit de faire si ce n'est pas le cas. Pour cela, nous aurons besoin de faire quelques rappels sur le plus grand diviseur commun (PGCD).

Notion de PGCD

Définition 5.3.2.1. *Soient a et b deux entiers non tous les deux nuls. Le* PGCD *de a et b (noté* $\text{PGCD}\,(a, b)$*) le plus grand des diviseurs commun à a et à b.*

Remarquons qu'il n'y a pas de problèmes avec cette définition : l'ensemble des entiers divisant à la fois a et b est fini, il en existe bien donc un plus grand. Remarquons également la chose suivante. Si $d = \text{PGCD}\,(a, b)$, on a toujours l'équivalence suivante :

$$x \text{ divise } d \quad \Leftrightarrow \quad x \text{ divise } a \text{ et } x \text{ divise } b$$

Une autre façon de présenter le PGCD de a et de b, si $b \neq 0$ disons, est de dire qu'il s'agit du plus grand entier par lequel on peut simplifier la fraction $\frac{a}{b}$. En particulier, dire que cette fraction est irréductible c'est exactement dire que $\text{PGCD}\,(a, b) = 1$. On dit dans ce cas que les entiers a et b sont *premiers entre eux.*

Une chose intéressante est que le calcul du PGCD peut se faire simplement et de façon systématique. Pour cela, on applique ce que l'on appelle couramment l'*algorithme d'Euclide.* On commence par écrire a et b l'un à côté de l'autre en mettant le plus grand des deux à gauche[2]. On effectue ensuite la division euclidienne du dernier nombre écrit avec celui qui le précède et on inscrit le reste de cette division à droite du dernier nombre. On continue ainsi jusqu'à obtenir un reste nul. Le PGCD cherché est alors le dernier nombre non nul écrit.

Voyons peut-être un exemple. Supposons que l'on veuille calculer $\text{PGCD}\,(1848, 804)$. On écrit donc :

$$1848 \quad 804 \quad 240 \quad 84 \quad 72 \quad 12 \quad 0$$

En effet, le reste de la division euclidienne de 1848 par 804 est 240, celui de la division euclidienne de 804 par 240 est 84 et ainsi de suite. On déduit de cela que le PGCD cherché est 12.

Une démonstration du fait que cet algorithme retrouve effectivement le PGCD et même un petit complément sont fournis dans l'exercice 2.

[2] Si $a = b$, le PGCD cherché est cette valeur commune.

Cas où a est premier avec n

Théorème 5.3.2.2. *$\dot{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si a et n sont premiers entre eux.*

Nous n'allons pas prouver complètement ce théorème, donnons toutefois quelques idées. Notons $d = \text{PGCD}\,(a, n)$ et supposons dans un premier temps que $d \neq 1$. Dans ce cas tout multiple de a sera encore un multiple de d mais être un multiple de d, comme d divise n, se traduit en base n simplement en disant que le dernier chiffre reste parmi les chiffres multiples de d. On voit bien alors que 1 ne pourra jamais être dernier chiffre, et donc que $\dot{a}$ n'est pas inversible dans $\mathbb{Z}/n\mathbb{Z}$.

La réciproque est un peu plus compliquée, il s'agit en fait d'une application directe du théorème de Bézout. Celui-ci est énoncé et démontré dans l'exercice 2. Cet exercice fournit même un moyen de calculer effectivement l'inverse.

Ce résultat a pour conséquence directe la chose suivante :

Théorème 5.3.2.3 (Lemme de Gauss). *Soient a, b et c trois entiers. On suppose que a divise le produit bc et que a et b sont premiers entre eux. Alors a divise c.*

En effet plaçons nous dans $\mathbb{Z}/a\mathbb{Z}$ (on peut bien entendu supposer $a \geqslant 2$). L'hypothèse nous dit que $\dot{b}\dot{c} = \dot{0}$ et que $\dot{b}$ est inversible. En multipliant par son inverse, on obtient directement $\dot{c} = \dot{0}$ et donc la conclusion voulue.

Une remarque importante à faire est que si p est un nombre premier, les entiers $1, \ldots, p-1$ sont tous premiers avec p. Ainsi tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible. Autrement dit, dans $\mathbb{Z}/p\mathbb{Z}$ quand p est premier, les choses se passent un peu comme dans $\mathbb{R}$: pour diviser, il s'agit juste de faire attention à ce que le nombre par lequel on divise soit non nul.

Attention, cela n'est plus vrai si p n'est pas premier : on a vu par exemple de $\dot{2}$ n'est pas inversible dans $\mathbb{Z}/10\mathbb{Z}$.

Voici par exemple une table des inverses de $\mathbb{Z}/7\mathbb{Z}$:

$\mathbf{a}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6}$
$\mathbf{a}^{-1}$	$\times$	$\dot{1}$	$\dot{4}$	$\dot{5}$	$\dot{2}$	$\dot{3}$	$\dot{6}$

Cas général

On rappelle que l'on a à résoudre l'équation :

$$ax = b \pmod{n}$$

Notons $d = \text{PGCD}\,(a, n)$ et supposons $d \neq 1$. On remarque dans un premier temps que si b n'est pas un multiple de d, l'équation n'a pas de solutions.
Si maintenant b lui aussi est un multiple de d, l'équation se réécrit sous la forme :

$$\left(\frac{a}{d}\right) x = \frac{b}{d} \pmod{\frac{n}{d}}$$

Mais ce coup-ci les quantités $\frac{a}{d}$ et $\frac{n}{d}$ sont premières entre elles, et donc on peut inverser $\frac{a}{d}$ modulo $\frac{n}{d}$ comme on l'a vu dans le cas précédent. Il est important de noter ici que les solutions sont définies modulo $\frac{n}{d}$, en particulier si l'on veut vraiment résoudre l'équation dans $\mathbb{Z}/n\mathbb{Z}$, on aura d solutions.

Mais prenons plutôt un exemple sans doute plus parlant. Disons que l'on veuille résoudre dans $\mathbb{Z}/10\mathbb{Z}$, l'équation $\dot{4}\dot{x} = \dot{2}$. 4 et 10 ne sont pas premiers entre eux, leur PGCD est 2. Comme 2 est un multiple de 2, on sait déjà qu'il va y avoir des solutions et même deux solutions.

Pour les trouver, on divise on divise notre équation par 2, et il faut donc résoudre dans $\mathbb{Z}/5\mathbb{Z}$, la nouvelle équation $\dot{2}\dot{x} = \dot{1}$. $\dot{2}$ admet bien un inverse dans $\mathbb{Z}/5\mathbb{Z}$, c'est $\dot{3}$. On multiplie donc notre équation par $\dot{3}$ et on obtient :

$$\dot{x} = \dot{3}$$

dans $\mathbb{Z}/5\mathbb{Z}$. Les solutions dans $\mathbb{Z}/10\mathbb{Z}$ sont donc $\dot{3}$ et $\dot{8}$.

5.3.3 $\dot{a}^x = \dot{b}$

Puissances successives de $\dot{a}$

Posons par exemple $u_k = \dot{a}^k$ pour tout entier naturel k. On obtient une suite à valeurs dans l'ensemble fini $\mathbb{Z}/n\mathbb{Z}$. Ainsi il va exister deux entiers i et j tels que $u_i = u_j$ et disons $i < j$. Mais u_{k+1} se calcule seulement à partir de u_k, simplement en multipliant par $\dot{a}$ et donc on en déduit que $u_{i+1} = u_{j+1}$, puis $u_{i+2} = u_{j+2}$ et ainsi de suite.

Cela prouve en fait que la suite (u_k) va être périodique de période $j - i$ au moins à partir du rang i.

Toutefois, il n'est pas vrai en général que cette suite est périodique à partir du rang 0. Plus exactement, il est facile de calculer $u_0 = \dot{1}$. Si la suite était périodique à partir du rang 0, il existe un entier $k > 0$ tel que $u_k = 1$. Mais alors $\dot{a} \cdot \dot{a}^{k-1} = \dot{1}$ et donc $\dot{a}$ serait inversible. Ainsi si $\dot{a}$ n'est pas inversible, notre suite n'est pas périodique dès le commencement.

Déterminer le rang à partir duquel la suite devient périodique et la plus courte période est un problème en général difficile. Nous allons, dans le paragraphe suivant, essayer de donner quelque élément de réponse lorsque $\dot{a}$ est inversible.

Cas où a est premier avec n

Lorsque a est premier avec n (ou encore lorsque $\dot{a}$ est inversible), la suite définie précédemment est en fait périodique à partir du rang 0.

Il n'est en fait pas difficile de voir cela. On sait déjà qu'il existe des entiers $i < j$ tels que :

$$\dot{a}^i = \dot{a}^j$$

Notons maintenant $\dot{a}'$ un inverse de $\dot{a}$, c'est-à-dire un élément de $\mathbb{Z}/n\mathbb{Z}$ tel que $\dot{a}\dot{a}' = \dot{1}$. En multipliant l'égalité précédente par $(\dot{a}')^i$, il vient :

$$\dot{a}^{j-i} = \dot{1}$$

ce qui prouve bien ce que l'on veut.

Fonction indicatrice d'Euler

Calculer la période n'est vraiment pas quelque chose de facile. Par contre, il n'est pas très difficile de déteminer un nombre k tel que $\dot{a}^k = \dot{1}$, le problème étant que ce n'est pas forcément le plus petit.

Nous allons pour cela définir une fonction φ qui s'appelle la *fonction indicatrice* d'Euler. Si $n \geqslant 2$ est un entier, $\varphi(n)$ désigne le nombre d'entiers naturels inférieurs à n et premiers avec n. Il s'agit donc d'après ce que l'on a vu précédemment du cardinal de l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Théorème 5.3.3.1. *Soit $\dot{a}$ un inversible de $\mathbb{Z}/n\mathbb{Z}$, alors :*

$$\dot{a}^{\varphi(n)} = \dot{1}$$

On peut reformuler le théorème précédent simplement en termes de congruences :

Théorème 5.3.3.2. *Soit a et n deux entiers premiers entre eux. Alors :*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

On insiste bien sur le fait que l'hypothèse de relative primalité est primordiale, cela est totalement faux sinon.

Nous n'allons pas prouver ce théorème : cela n'est pas bien difficile lorsque l'on connait un peu de théorie des groupes, il n'est pas d'ailleurs bien difficile non plus de refaire le peu de théorie des groupes qui nous manque pour arriver à cette conclusion mais cela n'entre pas dans le cadre de ce cours.

Un cas particulier intéressant du théorème précédent est quand même celui où $n = p$ est un nombre premier. Dans ce cas, on a vu que tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ étaient en fait inversibles. Le théorème nous dit donc que si $\dot{a} \in \mathbb{Z}/p\mathbb{Z}$ est tel que $\dot{a} \neq \dot{0}$, alors $\dot{a}^{\varphi(p)} = \dot{1}$. Mais $\varphi(p)$ est par définition le nombre d'inversibles de $\mathbb{Z}/p\mathbb{Z}$. Comme seul $\dot{0}$ n'est pas inversible, on a $\varphi(p) = p-1$. Ainsi $\dot{a}^{p-1} = \dot{1}$. Mais cela n'est vrai que si $\dot{a} \neq \dot{0}$. Pour ne pas avoir à distinguer ce cas particulier, il est usuel de multiplier l'égalité précédente par $\dot{a}$ qui donc deviendra vraie même si $\dot{a}$ est nul. On vient donc de prouver le théorème suivant :

Théorème 5.3.3.3 (Petit théorème de Fermat). *Soit p un nombre premier. Pour tout $\dot{a} \in \mathbb{Z}/p\mathbb{Z}$, on a l'égalité :*

$$\dot{a}^p = \dot{a}$$

On peut bien entendu énoncer le même théorème avec des congruences. Il devient :

Théorème 5.3.3.4 (Petit théorème de Fermat). *Soit p un nombre premier. Pour tout entier a, on a la congruence :*

$$a^p \equiv a \pmod{p}$$

Ce dernier résultat peut en fait se démontrer de façon relativement simple. Sans prétendre faire une preuve complète, nous donnons ici quelques éléments pour y aboutir. Le premier point est de vérifier que si p est premier et si k est un entier compris au sens large entre 1 et $p-1$, alors le nombre :

$$C_p^k = \frac{p(p-1)\dots(p-k+1)}{k(k-1)\dots 1}$$

est un multiple de p.

On utilise ensuite la formule du binôme de Newton qui dit :

$$(x+y)^p = \sum_{k=0}^{p} C_p^k x^k y^{n-k}$$

On déduit de ces deux remarques que pour tous entiers x et y, on a la congruence :

$$(x+y)^p \equiv x^p + y^p \pmod{p}$$

Par récurrence ensuite, on prouve que si $x_1, \dots, x_n$ sont des entiers, on a de façon analogue la congruence :

$$(x_1 + \dots + x_n)^p = x_1^p + \dots + x_n^p \pmod{p}$$

On applique ensuite ce résultat avec $n = a$ et $x_1 = \dots = x_a = 1$.

Formule pour $\varphi(n)$

Théorème 5.3.3.5. *Si la décomposition en facteurs premiers de l'entier n est :*

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$$

alors $\varphi(n)$ peut se calculer à l'aide de la formule suivante :

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_r}\right)$$

La preuve de ce théorème fait l'objet de l'exercice 3.

5.3.4 $\dot{a}\dot{x}^2 + \dot{b}\dot{x} + \dot{c} = 0$

Dans $\mathbb{Z}/p\mathbb{Z}$, p premier impair

On utilise pour résoudre la méthode classique, celle du discriminant. Plus précisément, on écrit successivement les étapes suivantes :

$$\begin{aligned}
\dot{a}\dot{x}^2 + \dot{b}\dot{x} + \dot{c} &= 0\\
\dot{a}\left(\dot{x}^2 + \frac{\dot{b}}{\dot{a}}\dot{x} + \frac{\dot{c}}{\dot{a}}\right) &= 0\\
\dot{a}\left(\dot{x} + \frac{\dot{b}}{\dot{2}\dot{a}}\right)^2 - \frac{\dot{b}^2}{\dot{4}\dot{a}} + \frac{\dot{c}}{\dot{a}} &= 0\\
\left(\dot{x} + \frac{\dot{b}}{\dot{2}\dot{a}}\right)^2 &= \frac{\dot{\Delta}}{\dot{4}\dot{a}^2}
\end{aligned}$$

où $\dot{\Delta} = \dot{b}^2 - \dot{4}\dot{a}\dot{c}$.

Bien entendu, les divisions par $\dot{2}$, $\dot{4}$ et $\dot{a}$ correspondent respectivement aux multiplications par les inverses de ces nombres. C'est pour cela qu'il est important de supposer que p est impair dans un premier temps. On ne voit pas encore bien où intervient de façon cruciale le fait que p soit premier, il aurait pour l'instant seulement fallu qu'il soit premier avec a. Mais cela vient.

Il s'agit maintenant de déterminer une racine carrée de $\dot{\Delta}$, c'est-à-dire un élément $\dot{\delta} \in \mathbb{Z}/p\mathbb{Z}$ tel que $\dot{\delta}^2 = \dot{\Delta}$. Il existe un critère pour savoir dans un premier temps si un tel élément existe et le calculer effectivement par la suite. Cela est présenté dans l'exercice 4. Supposons qu'on ait trouvé un tel élément et continuons la question.

L'équation devient :

$$\begin{aligned}
\left(\dot{x} + \frac{\dot{b}}{\dot{2}\dot{a}}\right)^2 &= \left(\frac{\dot{\delta}}{\dot{2}\dot{a}}\right)^2\\
\left(\dot{x} + \frac{\dot{b}+\dot{\delta}}{\dot{2}\dot{a}}\right)\left(\dot{x} + \frac{\dot{b}-\dot{\delta}}{\dot{2}\dot{a}}\right) &= 0
\end{aligned}$$

On est donc arrivé à un produit nul, la question est de savoir si l'on peut en déduire que l'un des facteurs est nul. La réponse est *oui* mais cela bien parce que l'on a supposé p premier (penser par exemple que dans $\mathbb{Z}/10\mathbb{Z}$, $\dot{2}\cdot\dot{5} = \dot{0}$). En effet, supposons que le premier facteur soit non nul, alors il est inversible et on trouve que le deuxième facteur est nul après avoir multiplié par l'inverse en question.

Dans $\mathbb{Z}/n\mathbb{Z}$, c'est plus compliqué

C'est en effet plus compliqué, et je ne connais pas de méthode générale pour résoudre l'équation. Déjà calculer une racine carrée est du même ordre de complexité que déterminer la décomposition en facteurs premiers de n. Mais même une fois cela fait, cela ne résout pas du tout le problème.

Une approche peut-être pas trop mauvaise est la suivante. Supposons que l'on connaisse la décomposition en facteurs premiers de n, disons $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Il est alors bon de commencer par chercher les solutions dans les $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ et de recoller les morceaux grâce à ce que l'on appelle le lemme chinois et qui est présenté dans l'exercice 3.

5.4 Exercices corrigés

Exercice 1

Énoncer et prouver le critère de divisibilité par 9.

Solution :

Le critère de divisibilité par 9 dit que le nombre x est divisible par 9 si et seulement si la somme des chiffres de x est divisible par 9.

Nous allons prouver cela. Notons, si a est un entier $S(a)$ la somme des chiffres de a. Cela veut dire que si a s'écrit :

$$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_n \cdot 10^n$$

alors

$$S(a) = a_0 + a_1 + a_2 + \ldots + a_n$$

On remarque alors que comme $10 \equiv 1 \pmod 9$, on a toujours la congruence :

$$S(a) \equiv a \pmod 9$$

On déduit de cela directement le critère annoncé.

Exercice 2

a) Soient a et b deux entiers, on suppose $b \neq 0$. On effectue la division euclidienne de a par b pour obtenir $a = bq + r$ où $r < |b|$. Montrer que dans ces conditions :

$$\text{PGCD}(a, b) = \text{PGCD}(b, r)$$

En déduire que l'algorithme d'Euclide présenté dans le cours calcule bien ce que l'on souhaite.

b) On modifie un peu l'algorithme d'Euclide. On prend toujours a et b deux entiers, on suppose $a > b > 0$. On presente maintenant les calculs dans un tableau que l'on complète de la façon suivante :

a	1	0
b	0	1
$\vdots$	$\vdots$	$\vdots$
r_{n-2}	u_{n-2}	v_{n-2}
r_{n-1}	u_{n-1}	v_{n-1}
r_n	$u_n = u_{n-2} - q_n u_{n-1}$	$v_n = v_{n-2} - q_n v_{n-1}$
$\vdots$	$\vdots$	$\vdots$

où q_n et r_n désignent respectivement le quotient et le reste de la division euclidienne de r_{n-2} par r_{n-1}.

Montrer que pour tout n, $r_n = au_n + bv_n$. En déduire le théorème suivant :

Théorème 5.4.0.1 (Théorème de Bézout). *Soit $d = \text{PGCD}(a, b)$. Alors il existe des entiers u et v tels que $au + bv = d$.*

Solution :

a) Nous allons en fait prouver que les diviseurs communs à a et b sont exactement les mêmes que les diviseurs communs à b et r. Prenons pour cela dans un premier temps d un diviseur commun à a et b, alors d divise bien entendu b et $r = a - bq$. Réciproquement si d divise à la fois b et r, il divise b et $a = bq + r$. Cela prouve l'égalité :

$$\text{PGCD}(a, b) = \text{PGCD}(b, r)$$

Il reste deux choses à faire pour prouver que l'algorithme fonctionne correctement, c'est d'une part prouver que $\text{PGCD}(0, x) = x$ pour tout entier strictement positif x et d'autre part prouver que l'on va bien tomber sur un reste nul au bout d'un nombre fini d'étapes.

Pour la première chose, il suffit de remarquer si tout nombre est un diviseur de 0 (car 0 est bien multiple de tout nombre). Ainsi par définition $\text{PGCD}(0, x)$ est le plus grand diviseur de x, c'est donc bien x.

La deuxième chose n'est pas difficile non plus, il suffit de remarquer que la suite des nombres que l'on écrit est strictement décroissante. Elle doit donc s'arrêter un jour.

Remarque : On peut en fait donner de bonnes majorations sur le nombre de divisions euclidiennes qu'il va falloir faire avant de trouver le PGCD recherché. On peut montrer par exemple que si (F_n) désigne la suite de Fibonacci définie par :

$$F_0 = 0 \quad ; \quad F_1 = 1 \quad ; \quad F_{n+2} = F_{n+1} + F_n$$

alors le nombre de divisions euclidiennes à faire est plus petit que le plus petit entier n tel que $F_{n-1} \geqslant \min\{a, b\}$

b) On prouve cela par récurrence. Pour les deux premières étapes, on vérifie directement que la relation est vraie. Il suffit donc de montrer l'hérédité, c'est-à-dire que sous les hypothèses $r_{n-2} = au_{n-2} + bv_{n-2}$ et $r_{n-1} = au_{n-1} + bv_{n-1}$, on a $r_n = au_n + bv_n$.

Rappelons pour cela que l'on a les égalités :

$$\begin{aligned} r_{n-2} &= q_n r_{n-1} + r_n \\ u_n &= u_{n-2} - q_n u_{n-1} \\ v_n &= v_{n-2} - q_n v_{n-1} \end{aligned}$$

On calcule donc :

$$\begin{aligned} au_n + bv_n &= a\left(u_{n-2} - q_n u_{n-1}\right) + b\left(v_{n-2} - q_n v_{n-1}\right) \\ &= \left(au_{n-2} + bv_{n-2}\right) - q_n\left(au_{n-1} + bv_{n-1}\right) \\ &= r_{n-2} - q_n r_{n-1} = r_n \end{aligned}$$

ce qui permet de conclure.

En regardant l'étape précédent le premier reste nul, on déduit de l'égalité précédente le théorème de Bézout.

Remarque : Cela permet lorsque a est premier avec n de calculer un inverse de $\dot{a}$ dans $\mathbb{Z}/n\mathbb{Z}$. Plus précisément avec la méthode précédente, on détermine u et v tels que $au+vn=1$, l'inverse de $\dot{a}$ est alors $\dot{u}$.

Exercice 3

On considère dans cet exercice deux entiers n et m supérieurs ou égaux à 2 et premiers entre eux. On définit l'application :

$$f : \left(\begin{array}{ccc} \mathbb{Z}/nm\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ \\ \dot{x} & \mapsto & (\dot{x}, \dot{x}) \end{array} \right)$$

a) Comprendre ce qu'est cette application. La décrire explicitement dans le cas $n = 2$ et $m = 5$.
b) Prouver le théorème suivant :

Théorème 5.4.0.2 (Lemme chinois). *L'application f est une bijection.*

c) Montrer qu'un élément $\dot{x} \in \mathbb{Z}/nm\mathbb{Z}$ est inversible si et seulement si $f(\dot{x})$ est un couple constitué de deux éléments inversibles.
d) Si φ désigne la fonction indicatrice d'Euler, et p est un nombre premier, calculer $\varphi\left(p^k\right)$ pour tout entier naturel k. En déduire la formule qui calcule $\varphi(n)$ donnée dans le cours.

Solution :

a) Ce qu'il est important de constater c'est qu'un élément de $\mathbb{Z}/nm\mathbb{Z}$ définit un élément de $\mathbb{Z}/n\mathbb{Z}$ (et un de $\mathbb{Z}/m\mathbb{Z}$). Autrement dit, il faut voir que si x et y sont deux entiers qui se terminent par le même chiffre en base mn alors ils se terminent aussi par le même chiffre en base n. Avec des congruences, cela signifie que si la différence $x - y$ est un multiple de mn alors c'est également un multiple de n, ce qui est alors clair.

Dans le cas $n = 2$ et $m = 5$, l'application précédente est :

$$\begin{aligned}
\dot{0} &\mapsto (\dot{0}, \dot{0}) \\
\dot{1} &\mapsto (\dot{1}, \dot{1}) \\
\dot{2} &\mapsto (\dot{0}, \dot{2}) \\
\dot{3} &\mapsto (\dot{1}, \dot{3}) \\
\dot{4} &\mapsto (\dot{0}, \dot{4}) \\
\dot{5} &\mapsto (\dot{1}, \dot{0}) \\
\dot{6} &\mapsto (\dot{0}, \dot{1}) \\
\dot{7} &\mapsto (\dot{1}, \dot{2}) \\
\dot{8} &\mapsto (\dot{0}, \dot{3}) \\
\dot{9} &\mapsto (\dot{1}, \dot{4})
\end{aligned}$$

b) Dire est l'application f est bijective signifie que tout élément de l'ensemble d'arrivée a un et un unique antécédent. Il n'est pas anodin de constater que pour montrer cela il suffit de prouver que tout élément de l'ensemble d'arrivée a au plus un antécédent, on pourra alors conclure en disant que les ensembles de départ et d'arrivée ont même cardinal.

Prenons donc $(\dot{x}, \dot{y})$ dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et supposons qu'il possède deux antécédents $\dot{a}$ et $\dot{b}$. Cela signifie que $\dot{a} = \dot{b} = \dot{x}$ dans $\mathbb{Z}/n\mathbb{Z}$ et que $\dot{a} = \dot{b} = \dot{x}$ dans $\mathbb{Z}/m\mathbb{Z}$. Avec des congruences, cela se dit :

$$a \equiv b \pmod{n}$$

$$a \equiv b \pmod{m}$$

La différence $b - a$ est donc divisible par n et m et puis par leur produit puisque ces deux nombres sont premiers entre eux. Finalement $a \equiv b \pmod{mn}$, et donc $\dot{a} = \dot{b}$ dans $\mathbb{Z}/mn\mathbb{Z}$. On a bien montré ainsi que le couple $(\dot{x}, \dot{y})$ a au plus un antécédent.

c) Si $\dot{x}$ est inversible dans $\mathbb{Z}/nm\mathbb{Z}$, il existe $\dot{x}' \in \mathbb{Z}/nm\mathbb{Z}$ tels que $\dot{x}\dot{x}' = \dot{1}$. Mais cette dernière égalité est encore vraie dans $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$. Le couple associé à $\dot{x}$ est donc constitué de deux éléments inversibles.

Réciproquement, prenons un couple $(\dot{x}, \dot{y})$ dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ tel que $\dot{x}$ soit inversible dans $\mathbb{Z}/n\mathbb{Z}$ et $\dot{y}$ soit inversible dans $\mathbb{Z}/m\mathbb{Z}$. Il existe donc $\dot{x}' \in \mathbb{Z}/n\mathbb{Z}$ et $\dot{y}' \in \mathbb{Z}/m\mathbb{Z}$ tels que $\dot{x}\dot{x}' = \dot{1}$ et $\dot{y}\dot{y}' = \dot{1}$, la première égalité ayant lieu dans $\mathbb{Z}/n\mathbb{Z}$ et la seconde dans $\mathbb{Z}/m\mathbb{Z}$.

Maintenant les couples $(\dot{x}, \dot{y})$ et $(\dot{x}', \dot{y}')$ ont un unique antécédent et le produit de ces antécédants vaut $\dot{1}$ dans $\mathbb{Z}/mn\mathbb{Z}$. Cela prouve la réciproque.

d) $\varphi\left(p^k\right)$ est le nombre d'entiers compris entre 1 et $p^k - 1$ qui sont premiers avec p^k. Mais être premier avec p^k signifie simplement ne pas être multiple de p. Ainsi :

$$\varphi\left(p^k\right) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

D'autre part la question c) prouve que si n et m sont premiers entre eux, on a la relation :

$$\varphi(nm) = \varphi(n)\,\varphi(m)$$

Ainsi si la décomposition de n en facteurs premiers est $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, on a :

$$\varphi(n) = \varphi\left(p_1^{\alpha_1}\right) \dots \varphi\left(p_r^{\alpha_r}\right) = n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right)$$

Exercice 4

Dans cet exercice, on considère p un nombre premier impair. On considère également $\dot{x}$ un élément non nul de $\mathbb{Z}/p\mathbb{Z}$. Le but est de donner un moyen calculatoire pour déterminer une racine carrée de $\dot{x}$ dans $\mathbb{Z}/p\mathbb{Z}$.

On admet la chose suivante. Il existe un élément $\dot{\alpha} \in \mathbb{Z}/p\mathbb{Z}$ tel que les puissances successives de $\dot{\alpha}$ atteignent tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$. Autrement dit, il existe un entier α tel que pour tout chiffre non nul de la base p, il existe un exposant n tel que α^n se termine par le chiffre en question.

a) Montrer que $\dot{x}$ admet une racine carrée si et seulement si $\dot{x}^{\frac{p-1}{2}} = \dot{1}$.

On suppose à partir de maintenant que $\dot{x}$ admet une racine carrée dans $\mathbb{Z}/p\mathbb{Z}$. On choisit un élément $\dot{a} \in \mathbb{Z}/p\mathbb{Z}$. On calcule $\dot{a}^2$: s'il vaut $\dot{x}$, on a trouvé une racine carrée, sinon on développe formellement l'expression $\left(a + \sqrt{\dot{x}}\right)^{\frac{p-1}{2}}$. On obtient ainsi des éléments de $\mathbb{Z}/p\mathbb{Z}$, $\dot{b}$ et $\dot{c}$ vérifiant :

$$\left(\dot{a} + \sqrt{\dot{x}}\right)^{\frac{p-1}{2}} = \dot{b} + \dot{c}\sqrt{\dot{x}}$$

b) Montrer que si $\dot{b}$ est nul, alors $\dot{c}$ ne l'est pas et son inverse fournit une racine carrée de $\dot{x}$.

c) Montrer qu'il existe au moins $\frac{p-1}{2}$ choix de $\dot{a}$ pour lesquels cette méthode réussit effectivement.

Solution :

a) Le fait qu'il existe un tel élément $\dot{\alpha}$ prouve que l'ensemble $\mathbb{Z}/p\mathbb{Z}$ est précisément :

$$\mathbb{Z}/p\mathbb{Z} = \left\{\dot{0}, \dot{1}, \dot{\alpha}, \dot{\alpha}^2, \ldots, \dot{\alpha}^{p-2}\right\}$$

cela étant principalement dû au fait que les puissances successives de l'inversible $\dot{\alpha}$ prennent toutes les valeurs possibles et donc que l'ordre de $\dot{\alpha}$ est exactement $p-1$. (On sait par ailleurs que cet ordre est inférieur à $p-1$ par exemple en utilisant le petit théorème de Fermat).

Maintenant, comme $\dot{x}$ est non nul, il va exister un entier n tel que $\dot{x} = \dot{\alpha}^n$. Il est alors immédiat de voir que $\dot{x}$ est un carré si et seulement si la congruence suivante admet une solution en k :

$$2k \equiv n \pmod{p-1}$$

$p-1$ est pair, donc cette congruence admet une solution si et seulement si n est pair.

D'autre part, on a :

$$\dot{x}^{\frac{p-1}{2}} = \dot{\alpha}^{n\frac{p-1}{2}}$$

Cette quantité vaut $\dot{1}$ si et seulement si l'exposant est un multiple de $p-1$ et donc si et seulement si n est pair. En regroupant les deux résultats précédents, on obtient la conclusion attendue.

b) Il faut bien comprendre dans cette question ce que sont $\dot{b}$ et $\dot{c}$. « Développer formellement » signifie que l'on développe sans se préoccuper ce que peut être $\sqrt{\dot{x}}$, on utilise juste le fait qu'il vérifie la relation :

$$\left(\sqrt{\dot{x}}\right)^2 = \dot{x}$$

Par exemple, on aura :

$$\begin{aligned}\left(\dot{1} + \sqrt{\dot{x}}\right)^2 &= \left(\dot{1} + \sqrt{\dot{x}}\right)\left(\dot{1} + \sqrt{\dot{x}}\right) \\ &= \dot{1} + \sqrt{\dot{x}} + \sqrt{\dot{x}} + \left(\sqrt{\dot{x}}\right)^2 \\ &= (\dot{1} + \dot{x}) + \dot{2}\sqrt{\dot{x}}\end{aligned}$$

Mais maintenant si $\dot{y}$ est véritablement une racine carrée de $\dot{x}$, c'est-à-dire un élément de $\mathbb{Z}/p\mathbb{Z}$ vérifiant $\dot{y}^2 = \dot{x}$, on va bien entendu avoir :

$$(\dot{a} + \dot{y})^{\frac{p-1}{2}} = \dot{b} + \dot{c}\dot{y}$$

et donc si $\dot{b} = 0$, on aura :

$$(\dot{a} + \dot{y})^{\frac{p-1}{2}} = \dot{c}\dot{y}$$

En élevant cette dernière égalité au carré, on trouve :

$$\dot{1} = (\dot{a} + \dot{y})^{p-1} = \dot{c}^2\dot{y}^2 = \dot{c}^2\dot{x}$$

Cette dernière égalité prouve que $\dot{c}$ est inversible (d'inverse $\dot{c}\dot{x}$) et que si $\dot{c}'$ désigne un inverse de $\dot{c}$, on a $\dot{c}'^2 = \dot{x}$, et donc on a bien déterminé une racine carrée de $\dot{x}$.

Remarque : Cette méthode fournit un moyen pratique de déterminer une racine carrée de $\dot{x}$ dans $\mathbb{Z}/p\mathbb{Z}$ en supposant qu'on ait suffisamment de chance pour tomber sur un $\dot{a}$ qui soit tel que $\dot{b} = 0$. On pourrait croire que l'élévation à la puissance $p-1$ est un calcul compliqué mais en fait non.

Voyons comment on procède sur un exemple. Prenons $p = 2003$ et $\dot{x} = \dot{3}$. On commence par calculer $\frac{p-1}{2} = 1001$. Il s'agit dans un premier temps de calculer explicitement $\dot{3}^{1001}$. Pour cela, on procède de la façon suivante. On commence par écrire :

$$\dot{3}^{1001} = \dot{3} \cdot \left(\dot{3}^{500}\right)^2$$

Il ne s'agit donc maintenant plus que de calculer $\dot{2}^{500}$. On procède de même et on écrit successivement les lignes :

$$\begin{aligned}
\dot{3}^{500} &= \left(\dot{3}^{250}\right)^2 \\
\dot{3}^{250} &= \left(\dot{3}^{125}\right)^2 \\
\dot{3}^{125} &= \dot{3} \cdot \left(\dot{3}^{62}\right)^2 \\
\dot{3}^{62} &= \left(\dot{3}^{31}\right)^2 \\
\dot{3}^{31} &= \dot{3} \cdot \left(\dot{3}^{15}\right)^2 \\
\dot{3}^{15} &= \dot{3} \cdot \left(\dot{3}^{7}\right)^2 \\
\dot{3}^{7} &= \dot{3} \cdot \left(\dot{3}^{3}\right)^2 \\
\dot{3}^{3} &= \dot{3} \cdot \left(\dot{3}\right)^2
\end{aligned}$$

On est maintenant capable d'effectuer le calcul :

$$\begin{aligned}
\dot{3}^{3} &= \dot{3} \cdot \left(\dot{3}\right)^2 = \overline{27} \\
\dot{3}^{7} &= \dot{3} \cdot \left(\dot{3}^{3}\right)^2 = \overline{184} \\
\dot{3}^{15} &= \dot{3} \cdot \left(\dot{3}^{7}\right)^2 = \overline{1418} \\
\dot{3}^{31} &= \dot{3} \cdot \left(\dot{3}^{15}\right)^2 = \overline{1139} \\
\dot{3}^{62} &= \left(\dot{3}^{31}\right)^2 = \overline{1380} \\
\dot{3}^{125} &= \dot{3} \cdot \left(\dot{3}^{62}\right)^2 = \overline{644} \\
\dot{3}^{250} &= \left(\dot{3}^{125}\right)^2 = \overline{115} \\
\dot{3}^{500} &= \left(\dot{3}^{250}\right)^2 = \overline{1207} \\
\dot{3}^{1001} &= \dot{3} \cdot \left(\dot{3}^{500}\right)^2 = \dot{1}
\end{aligned}$$

On en déduit ainsi que $\dot{3}$ est bien un carré dans $\mathbb{Z}/2003\mathbb{Z}$. Pour en déterminer une racine carrée, on choisit maintenant un $\dot{a}$ quelconque, par exemple $\dot{a} = \dot{3}$. On calcule comme précédemment :

$$\left(\dot{3} + \sqrt{\dot{3}}\right)^{1001} = \overline{1207} \cdot \sqrt{\dot{3}}$$

D'après ce que l'on vient de prouver, une racine carrée de $\dot{3}$ est un inverse de $\overline{1}207$. On le détermine grâce à l'algorithme d'Euclide. On trouve ainsi que :

$$\overline{385}^2 = \dot{3}$$

d) On rappelle que $\dot{b}$ et $\dot{c}$ sont définis par la relation suivante :

$$\left(\dot{a} + \sqrt{\dot{x}}\right)^{\frac{p-1}{2}} = \dot{b} + \dot{c}\sqrt{\dot{x}}$$

On voit facilement, par exemple en regardant comment les calculs se passent, que l'on a également la relation :

$$\left(\dot{a} - \sqrt{\dot{x}}\right)^{\frac{p-1}{2}} = \dot{b} - \dot{c}\sqrt{\dot{x}}$$

En sommant ces deux égalités, on obtient une expression de $\dot{b}$:

$$\dot{2}\dot{b} = (\dot{a} + \dot{y})^{\frac{p-1}{2}} + (\dot{a} - \dot{y})^{\frac{p-1}{2}}$$

où $\dot{y}$ est une racine carrée de $\dot{x}$ dans $\mathbb{Z}/p\mathbb{Z}$. Comme on a choisi p impair, $\dot{2}$ est inversible. En particulier $\dot{b} = \dot{0}$ si et seulement si :

$$\left(\frac{\dot{a} + \dot{y}}{\dot{a} - \dot{y}}\right)^{\frac{p-1}{2}} = 1$$

cette expression a bien un sens puisque l'on choisit $\dot{a} \neq \dot{y}$, étant donné que l'on a pris de vérifier avant de commencer les calculer que $\dot{a}^2 \neq \dot{x}$.

Il ne reste alors plus qu'à dire que la fonction $\dot{a} \mapsto \frac{\dot{a}+\dot{y}}{\dot{a}-\dot{y}}$ réalise une bijection de $(\mathbb{Z}/p\mathbb{Z}) \setminus \{\dot{y}, -\dot{y}\}$ dans $(\mathbb{Z}/p\mathbb{Z}) \setminus \{\dot{0}, \dot{1}\}$ et à remarquer qu'il y a exactement $\frac{p-1}{2}$ carrés non nuls dans $\mathbb{Z}/p\mathbb{Z}$.

Chapitre 6

Sujets de réflexion

Toujours dans le cadre de Animath (cf Chapitre 5), j'ai rédigé plusieurs sujets servant à faire réfléchir les élèves sur des thèmes variés et pas forcément simples, pouvant d'ailleurs facilement intéresser des étudiants ayant passés depuis longtemps le lycée.

Sommaire

6.1 Les équations algébriques

Une équation n'est en fait rien d'autre qu'une égalité entre deux membres. Souvent, dans les problèmes, l'on veut déterminer une certaine quantité et l'énoncé se traduit simplement par une égalité qui fait intervenir la quantité inconnue. Comme le fait de nommer les choses permet souvent de mieux les étudier, ce que l'on fait, c'est que l'on donne un certain nom à notre inconnu, le plus souvent on l'appelle x. On obtient ainsi une égalité que doit vérifier x, une équation comme on dit. Bien sûr, il y a des équations de toutes sortes. Il y a les affines, c'est-à-dire celles qui sont de la forme $ax + b = 0$. Il y a les équations de degré 2, celles de degré 3, etc. Mais il y en a encore tout un tas d'autres, notamment celles de la forme $a^x = b$, ou encore $\cos(5x + 1) = 3^{x^2} - 2x$. Résoudre une équation, c'est trouver *tous* les nombres x qui vérifient l'égalité de départ. Ce que l'on appelle *équation algébrique*, c'est une équation pouvant se mettre sous la forme $a_n x^n + \ldots + a_0 = 0$, où les a_i sont des nombres réels. Ce sont en fait les équations d'un certain degré. Je vais donner par la suite des méthodes pour résoudre les équations algébriques de degré allant de 1 à 4.

6.1.1 Le premier degré

Il n'y a pas grand chose à dire... Enfin si, mais tu dois déjà le savoir. Les équations du premier degré sont celles qui peuvent se mettre sous la forme $ax + b = 0$. Il y a une unique solution qui est $x = \frac{-b}{a}$. Je signale toutefois qu'il faut faire attention au cas particulier où $a = 0$. Dans ce cas, l'expression donné juste au-dessus n'a aucun sens, car est-il encore utile de le rappeler, il est interdit de diviser par 0. Mais dans ce cas, résoudre l'équation est encore plus simple. En effet, si $b = 0$, tout x est solution et si $b \neq 0$, il n'y a aucune solution.

6.1.2 Le second degré

L'équation générale se met ici sous la forme $ax^2 + bx + c = 0$. Bien entendu, l'on peut supposer que $a \neq 0$, car sinon l'équation serait en fait de degré 1 et donc releverait du paragraphe précédent. Regardons comment l'on peut faire pour résoudre.

Tout d'abord je dis que quitte à diviser par a (que l'on vient de supposer non nul, je tiens à le préciser), on peut supposer que $a = 1$. Bon, qu'est-ce que ça veut dire que cette phrase barbare ? Je vais l'expliquer. On a au début à résoudre l'équation $ax^2 + bx + c = 0$. Si l'on divise cette égalité par a (supposé différent de 0), on obtient $x^2 + \frac{b}{a}x + \frac{c}{a} = 0$. Il s'agit d'une équation de la forme précédente, à la différence près que désormais il n'y a plus de coefficient devant x^2, ou ce qui revient au même, que désormais le coefficient devant x^2 vaut 1. Ainsi si l'on sait résoudre les équations du second degré qui sont telles que le coefficient devant le terme en x^2 est 1, on saura résoudre toutes les équations du second degré puisque l'on vient de voir qu'en fait toutes ces équations se ramènent à ce cas particulier. On peut donc se restreindre à l'étude des équations du second degré qui sont telles que $a = 1$ et c'est ce que nous allons faire par la suite.

Question 6.1.1. *Montrer que quitte à poser $x' = x + \frac{b}{2}$, on peut supposer que $b = 0$.*

Question 6.1.2. *Résoudre finalement l'équation simplifiée qui est $x^2 + c = 0$. On fera attention à distinguer les cas $c < 0$, $c = 0$ et $c > 0$.*

En fait, dans la pratique, on présente les calculs de la façon suivante. On cherche à résoudre $ax^2 + bx + c = 0$. Pour cela, on calcule ce que l'on appelle le *discriminant* de l'équation qui est ici $\Delta = b^2 - 4ac$. La nature des solutions dépend alors du signe de Δ.

Question 6.1.3. *Montrer que si $\Delta < 0$, l'équation n'admet pas de solutions. Montrer que si $\Delta = 0$, l'équation admet une unique solution qui est $\frac{-b}{2a}$. Montrer que si $\Delta > 0$, l'équation admet deux solutions qui sont $\frac{-b-\sqrt{\Delta}}{2a}$ et $\frac{-b+\sqrt{\Delta}}{2a}$.*

Question 6.1.4. *On considère le système d'équations :*

$$\begin{cases} x+y=S \\ xy=P \end{cases}$$

où S et P sont des nombres donnés. Expliquer pourquoi résoudre ce système revient en fait exactement à résoudre l'équation en t, $t^2-St+P=0$. On fera bien attention à n'oublier aucun cas.

6.1.3 Le troisième degré

L'équation à résoudre ici est $ax^3+bx^2+cx+d=0$. Comme précedemment, on va supposer $a \neq 0$, car sinon l'équation serait en fait de degré 2 et relèverait du paragraphe précédent.

Question 6.1.5. *Montrer que quitte à diviser par a puis à poser $x'=x+\frac{b}{3}$, on peut supposer que $a=1$ et que $b=0$.*

Ainsi, l'équation qu'il nous faut résoudre devient $x^3+cx+d=0$, ce qui est quand même a priori plus simple. L'idée pour faire cela est de chercher x sous la forme $p+q$, en espérant que ceci donne suffisamment de liberté pour pouvoir imposer au moins une autre condition sur p et q et obtenir un problème plus simple. En substituant $p+q$ à x, l'équation devient :

$$p^3+q^3+(p+q)(3pq+c)+d=0$$

Question 6.1.6. *Le vérifier.*

La condition supplémentaire que l'on aimerait imposer sur p et q est $3pq+c=0$. On obtient ainsi le système suivant dont une solution va nous donner une solution de notre équation de départ.

$$\begin{cases} 3pq=-c \\ p^3+q^3=-d \end{cases}$$

Question 6.1.7. *En s'inspirant de la question 6.1.4, résoudre le système précédent. Montrer que si $\frac{d^2}{4}+\frac{c^3}{27} \geqslant 0$, on obtient effectivement par cette méthode une solution à l'équation $x^3+cx+d=0$.*

On peut montrer que si $\frac{d^2}{4}+\frac{c^3}{27}>0$, alors la solution que l'on a trouvé précédemment est en fait l'unique solution de l'équation. Il suffit pour cela d'étudier la fonction f définie par $f(x)=x^3+cx+d$. Dans le cas où $\frac{d^2}{4}+\frac{c^3}{27}=0$, l'étude de la fonction montre qu'il y a en fait deux solutions, celle donnée par la méthode précédente qui est $-2\sqrt{\frac{-c}{3}}=-2\sqrt[3]{\frac{d}{2}}$ (c est ici forcément un nombre négatif) et une autre qui est $\sqrt{\frac{-c}{3}}=\sqrt[3]{\frac{d}{2}}$. (Ces deux solutions n'en sont en fait qu'une dans le cas très particulier où $c=d=0$). Le dernier cas qui est $\frac{d^2}{4}+\frac{c^3}{27}<0$ est beaucoup plus frustrant. On peut montrer encore en étudiant la fonction f qu'il y a trois solutions mais la méthode précédente n'en fournit aucune. En fait, ce que l'on aimerait faire, c'est donner un sens aux racines carrées de nombres négatifs. Ceci se résout par l'introduction des nombres complexes qui ont d'ailleurs été développés à l'origine précisément pour résoudre ce genre d'équations, mais nous n'allons pas détailler leur étude ici. Sache toutefois que combinée à la puissance des nombres complexes, la méthode précédente permet de résoudre au moins en théorie toutes les équations algébriques du troisième degré.

Question 6.1.8. *Vérifier que la méthode proposée est impuissante face à l'équation $x^3-2x+1=0$. Vérifier pourtant que 1, $\frac{-1-\sqrt{5}}{2}$ et $\frac{-1+\sqrt{5}}{2}$ sont trois solutions. En fait, ce sont les seules.*

6.1.4 Le quatrième degré

L'équation à résoudre ici est $ax^4 + bx^3 + cx^2 + dx + e = 0$ et comme d'habitude on va supposer que $a \neq 0$.

Question 6.1.9. *Montrer que quitte à diviser par a puis à faire un changement de variable que l'on précisera, on peut supposer que $a = 1$ et $b = 0$.*

L'équation à résoudre devient alors $x^4 + cx^2 + dx + e = 0$. Pour faire cela, on introduit un paramètre t (que l'on va choisir judicieusement par la suite) et l'on réécrit l'équation sous la forme suivante :

$$\left(x^2 + t\right)^2 - \left[(2t - c)\, x^2 - dx + \left(t^2 - e\right)\right] = 0$$

Question 6.1.10. *Vérifier que l'équation est bien équivalente à l'égalité écrite ci-dessus.*

On aimerait en fait que la partie entre crochets de l'expression précédente puisse s'écrire comme un carré car dans ce cas, on saurait factoriser notre expression et l'on n'aurait plus qu'à résoudre deux équations de degré 2, ce que l'on sait théoriquement déjà faire.

Question 6.1.11. *Vérifier que si t est tel que $4\,(2t - c)\left(t^2 - e\right) = d^2 \neq 0$, alors on a :*

$$(2t - c)\, x^2 - dx + \left(t^2 - e\right) = (2t - c)\left(x - \frac{d}{4t - 2c}\right)^2$$

Conclure pour le cas $d \neq 0$ (attention au signe de $2t - c$).

Question 6.1.12. *Résoudre l'équation dans le cas $d = 0$. On pourra poser $X = x^2$.*

6.1.5 Et après...

De jolies méthodes générales de ce genre n'existent plus pour les degrés supérieurs à 5... La phrase précédente est volontairement floue car il est difficile d'expliquer précisément ce que l'on sait à ce propos sans rentrer dans des détails trop techniques et donc je ne vais pas le faire. (Si tu le souhaites, je pourrais faire une feuille d'exercices de ce genre pour t'expliquer ce que j'entends par " De telles méthodes n'existent pas" et peut-être même te le faire démontrer mais bon...)

Enfin, cela ne veut pas dire que l'on est totalement impuissant face à des équations de degré supérieur. Je vais expliquer dans la suite comment on peut espérer les aborder.

Donc on s'attaque à l'équation $a_n x^n + \ldots + a_0 = 0$, n n'étant pas forcément supérieur à 5 : tout ce que je vais dire s'applique à un n quelconque et souvent il est préférable d'utiliser les méthodes que je vais décrire par la suite que les méthodes générales qui sont en général un peu lourdes. On peut supposer comme toujours que $a_n \neq 0$. On va poser $P(x) = a_n x^n + \ldots + a_0$. L'idée fondamentale est que si l'on a trouvé une solution, disons a vérifiant donc $P(a) = 0$, on est ramené à un problème plus simple qui est celui de résoudre une équation de degré $n - 1$. On verra plus loin comment on fait pour trouver un tel a (en général c'est par chance...), pour l'instant supposons que l'on dispose d'une solution a et voyons comment on réussit à faire baisser le degré de 1.

Question 6.1.13. *Montrer que pour tout entier k et tout réel y, on dispose de la factorisation suivante :*

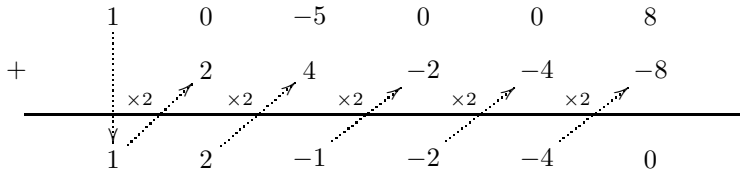
$$x^k - y^k = (x - y)\left(x^{k-1} + yx^{k-2} + y^2x^{k-1} + \ldots + y^{k-2}x + y^{k-1}\right)$$

En déduire que $P(x) - P(y)$ s'écrit $(x - y)\, Q_y(x)$ où Q_y est une expression de degré $n - 1$ en x. En particulier comme a est solution de $P(x) = 0$, on peut écrire :

$$P(x) = (x - a)\, Q_a(x)$$

Question 6.1.14. *En déduire qu'une équation de degré n a au plus n solutions. En particulier cela démontre l'affirmation de la question 6.1.8.*

Il ne reste plus qu'à donner une méthode effective pour calculer le polynôme Q_a. Présentons-la sur un exemple. Prenons $P(x) = x^5 - 5x^3 + 8$, l'équation à résoudre est donc $x^5 - 5x^3 + 8 = 0$. On remarque que 2 est une solution. On présente en fait les calculs dans le tableau qui suit. Sur la première ligne, on écrit les coefficients qui apparaissent dans notre équation dans l'ordre (ie du degré le plus élevé au degré 0) en n'oubliant pas les zéros éventuels. On abaisse alors le premier coefficient sur la troisième ligne. On multiplie le nombre que l'on vient de recopier par a (ici par 2) et on écrit le résultat sur la case immédiatement en haut à droite. On somme les deux nombres écrits dans la deuxième colonne et on reporte le résultat dans la troisième ligne... et on continue ainsi.



Le zéro tout en bas à droite correspond en fait à la valeur de $P(2)$. Ainsi si un jour, après application de cette méthode de calcul, on ne trouve pas un zéro en bas à droite, c'est qu'il y a en fait un erreur quelque part. Un autre point remarquable, c'est qu'il est souvent beaucoup plus rapide de calculer la valeur de P en un certain réel a en utilisant cette méthode qu'en calculant bêtement. Ainsi si l'on veut trouver une solution en testant un peu au hasard, ce n'est pas une mauvaise idée de choisir des nombres a et de leur faire subir le sort que l'on vient de décrire. Si l'on ne trouve pas un zéro en bas à droite, c'est que l'on avait pas fait un choix judicieux. Sinon, c'est que l'on est effectivement tombé sur une solution et on a déjà la décomposition.

À propos, je n'ai toujours pas dit comment on retrouvait la factorisation dans notre tableau. C'est en fait tout simple : les nombres qui apparaissent sur la dernière ligne à l'exception du dernier sont les coefficients rangés dans le bon ordre de Q_a. Autrement dit, dans notre cas particulier, on a :

$$P(x) = (x-2)\left(x^4 + 2x^3 - x^2 - 2x - 4\right)$$

et on est ramené à résoudre une équation de degré 4.

Question 6.1.15. *Montrer que la méthode expliquée ci-dessus fonctionne bien.*

Voyons maintenant comment l'on arrive à trouver des solutions particulières. Il n'y a en fait pas de méthodes générales et souvent il faut y aller au petit bonheur la chance. Toutefois, si l'on cherche des solutions rationnelles et que l'équation que l'on cherche à résoudre est à coefficients entiers, il y a quand même moyen d'en éliminer pas mal. Plus précisément, revenons à notre situation de départ, c'est-à-dire dans celle où l'on cherche à résoudre $a_n x^n + ... + a_0 = 0$. On a déjà vu que l'on pouvait supposer $a_n \neq 0$. En fait, on peut aussi supposer $a_0 \neq 0$, car sinon 0 est une solution évidente et l'on factorise par x tant que c'est possible. Nous supposerons en outre dans la suite de ce paragraphe que tous les a_i sont des entiers.

Question 6.1.16. *Montrer que si $\frac{p}{q}$ est une solution écrite sous forme irréductible (c'est-à-dire que p et q sont premiers entre eux), alors p est un diviseur de a_0 et q est un diviseur de a_n. (On pourra utiliser le lemme de Gauss qui dit que si un nombre a divise un produit bc et que a et b sont premiers entre eux, alors a divise c).*

Ainsi si une fraction $\frac{p}{q}$ est telle que p ne divise pas a_0 *ou* q ne divise pas a_n, elle n'a aucune chance d'être solution de l'équation. Ceci réduit donc à un nombre fini (et en général petit) le nombre de tests à faire pour trouver une solution rationnelle si elle existe. Notons en particulier que si $a_n = 1$, alors les solutions rationnelles sont en fait entières et elles se comptent parmi les diviseurs de a_0 et que si $a_n = a_0 = 1$, la seule solution rationnelle possible est 1.

6.1.6 Les équations réciproques

Il y a un type d'équations bien particulier sur lequelles on arrive à faire des manipulations intéressantes. Il s'agit des *équations réciproques*. Ce sont celles qui sont de la forme $a_n x^n + \ldots + a_0 = 0$ où $a_n = a_0 \neq 0$, $a_{n-1} = a_1$, $a_{n-2} = a_2$, etc. Je ne vais pas expliquer la théorie de façon générale mais juste la présenter sur un exemple. Prenons l'équation :

$$x^6 - 2x^5 + 3x^4 - 3x^3 + 3x^2 - 2x + 1 = 0$$

La méthode consiste d'abord à tout diviser par x^3, on obtient :

$$x^3 - 2x^2 + 3x - 3 + \frac{3}{x} - \frac{2}{x^2} + \frac{1}{x^3} = 0$$

Question 6.1.17. *Pourquoi le fait de diviser par x^3 ne change pas les solutions dans ce cas particulier ? Et qu'en est-il dans le cas général ?*

On pose ensuite $X = x + \frac{1}{x}$. La structure de l'équation de départ permet de prouver que X vérifie une certaine équation algébrique de degré plus petit.

Question 6.1.18. *Montrer que dans ce cas, l'équation vérifiée par X est $X^3 - 2X^2 + 1 = 0$. Expliquer comment on arrive à trouver cette équation dans le cas général.*

Question 6.1.19. *Essayer d'appliquer la méthode générale des équations de degré 3 pour résoudre l'équation vérifiée par X.*

C'est laborieux, hein. Et puis en plus, si je ne me suis pas trompé, tu devrais tomber dans le cas où justement cette méthode ne fonctionne pas. Enfin c'est pas grave, on va s'en sortir quand même. Pour cela, on cherche une solution particulière, commençons par les rationnelles. D'après ce que l'on a dit précédemment, la seule solution rationnelle possible est 1. Il faut essayer...

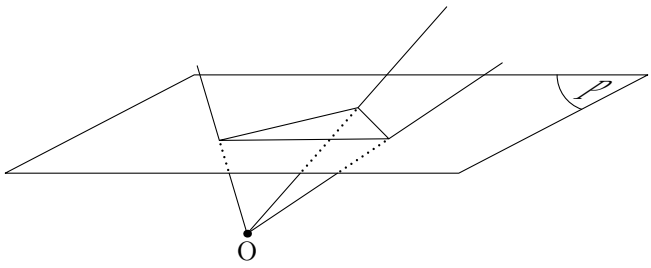
Question 6.1.20. *Vérifier que 1 est effectivement solution. Résoudre l'équation en X. En déduire les solutions de l'équation de départ.*

6.2 Le plan projectif

L'art de la géométrie réside très souvent dans les transformations du plan. Celles-ci permettent de transformer une figure en une autre où les choses deviennent plus simples à comprendre et à étudier. Toutefois si l'on veut espérer transporter certains informations que l'on a obtenu en étudiant la figure simplifiée à la figure d'origine, il va falloir que ces transformations conservent certains choses, c'est que l'on appelle un invariant. Les isométries sont par exemple les transformations qui conservent les distances, les similitudes sont celles qui conservent les rapports de distance, etc. Ce que l'on aimerait, nous, c'est trouver des transformations qui conservent l'alignement, ou ce qui revient au même qui conservent les droites. Mais si l'on conserve les droites, on va conserver les droites parallèles car deux droites qui ne se rencontraient pas avant transformation ne vont pas se couper miraculeusement après et donc notre transformation va aussi forcément conserver les directions. Et ça, ça ne nous plaît pas car ça ne donne pas assez de liberté pour modifier la figure comme on le voudrait. L'idée consiste alors à "éliminer" les droites parallèles et pour faire cela, on aimerait voir le plan dans quelque chose de plus gros où justement ces droites parallèles vont se couper. C'est cela le *plan projectif* et ce qui va nous intéresser, ça va être les transformations de ce plan projectif qui conservent l'alignement.

6.2.1 Description du plan projectif

Le plus simple et le plus naturel pour définir le plan projectif est sans doute de commencer par plonger le plan de façon intelligente dans l'espace ambiant. Considérons donc un plan P dans l'espace et un point O qui n'appartient pas à P. Un point M du plan P va alors être représenté dans l'espace par toute la droite (OM). Le sous-ensemble de P formé des deux points M et M' va alors naturellement être représenté par la réunion des droites (OM) et (OM'). Un cercle dans P sera représente par la réunion de toutes les droites reliant O à un point du cercle, ce qui est un cône. Et ainsi de suite.



Prenons maintenant deux points A et B dans P et voyons par quoi par être représentée la droite (AB). Ce sera bien entendu la réunion des droites reliant O à un point de (AB) et on obtient ainsi le plan (OAB). En fait, non. On obtient seulement presque tout le plan, on obtient tout le plan à l'exception de la droite D qui est parallèle à (AB) et qui passe par O, cette droite n'intersectant pas le plan P. C'est un peu décevant, on aurait préféré de loin obtenir tout le plan. C'est tellement décevant que l'on décide d'ajouter cette droite manquante et on décide même qu'elle correspond à un nouveau point de la droite (AB), celui qui est au bout. Au bout ? Puis quel bout, d'abord ? Ben, les deux en fait. En effet, si l'on choisit des points M de plus en plus loin sur la droite (AB), la droite (OM) va se rapprocher de la droite D et ce indépendamment du sens dans lequel on s'éloigne. Il est donc légitime de dire que D correspond à un nouveau point qui est au bout de cette droite ou même plus précisément qui relie les deux bouts de cette droite. C'est ce que l'on appelle un *point à l'infini*.

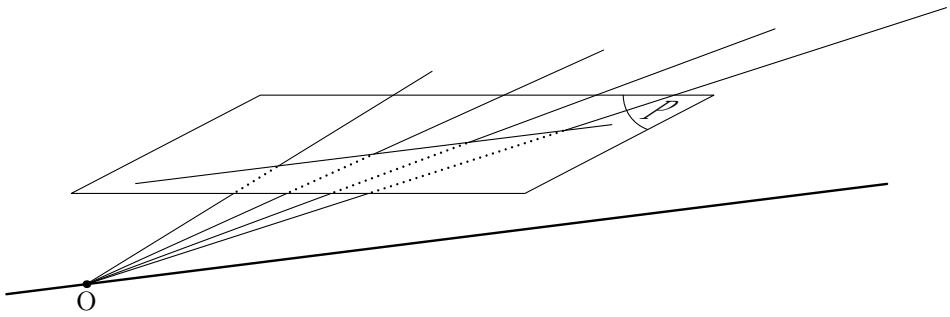


Illustration d'un point à l'infini

On complète ainsi le plan P en rajoutant des points à l'infini au bout de toutes les droites. Regardons si par hasard un point à l'infini ne peut pas être au bout de plusieurs droites à la fois. Ben en fait, si. Parce que vu dans l'espace ambiant, un point à l'infini ce n'est pas un truc comme ça qui tombe du ciel, que l'on décide d'ajouter arbitrairement. Un point à l'infini vu dans l'espace ambiant, c'est juste une droite parallèle à une certaine droite du plan P. Autrement dit, c'est juste une droite parallèle au plan P. Et si on prend M un point à l'infini, il va être au bout de toutes les droites de P qui vont être parallèles à la droite qui représente M dans l'espace ambiant. Une autre façon de dire cela est de voir un point à

l'infini comme une direction et alors un point à l'infini est au bout d'une droite si et seulement si cette droite a la bonne direction.

On vient de voir que si l'on considère deux droites parallèles de P, le point à l'infini qui est à leur bout est en fait le même. Une autre façon de dire cela est de dire que nos deux droites parallèles s'intersectent en fait et précisément en ce point à l'infini. Plus généralement, considérons deux droites quelconques mais distinctes du plan P. Elles vont être représentés dans l'espace par deux plans distincts passant par O. Bien entendu leur intersubsection sera représentée par l'intersubsection de ces deux plans. Mais l'intersubsection de deux tels plans est toujours une droite (*Pourquoi ?*) et donc vu dans le plan (auquel on a rajouté les points à l'infini) l'intersubsection de nos deux droites sera toujours un et un unique point. Ce point sera un vrai point du plan si la droite qui le représente n'est pas parallèle à P ou encore si les deux droites que l'on intersecte se coupe réellement dans P. Ce point sera un point à l'infini dans le cas contraire, c'est-à-dire lorsque la droite qui le représente est parallèle au plan P ou encore lorsque les droites que l'on cherche à intersecter sont parallèles.

On vient de voir que toute droite de notre plan P complété est représentée par un certain plan passant par le point O. Le contraire est-il vrai ? Autrement dit, tout plan passant par O correspond-il à une certaine droite de P muni de ses points à l'infini ? C'est clairement le cas pour tous les plans qui ne sont pas parallèles à P, la droite qu'il représente étant tout simplement l'intersubsection de ce plan avec P. Mais qu'en est-il du plan passant par O qui est parallèle à P ? Par définition ce plan contient toutes les droites parallèles au plan P. Ces droites, comme on l'a dit, sont précisément celles qui correspondent aux points à l'infini. Donc vu dans le plan P complété avec les points à l'infini, le plan parallèle à P passant par O est l'ensemble des points à l'infini. Et comme il s'agit d'un plan, il est légitime de dire que l'ensemble des points à l'infini forme une droite, qui s'appelle sans grande surprise *droite à l'infini*.

Donc récapitulons. On vient de décrire un plan auquel on a rajouté des points à l'infini, un pour chaque direction, tous ces points étant alignés sur une certaine droite qui est la droite à l'infini. C'est ce truc bizarre que l'on appelle *plan projectif*. Une bonne façon de le voir est réellement de se le représenter dans l'espace comme nous venons de le faire pour le décrire. D'après ce que l'on a dit, se donner une figure (c'est-à-dire un ensemble de points) dans le plan projectif, c'est exactement se donner une figure de l'espace qui s'écrit comme réunion de droites passant par O, c'est-à-dire une figure de l'espace qui est stable par les homothéties de centre O, ou encore une figure de l'espace qui est telle que dès qu'elle contient un point M, elle contient toute la droite (OM). Avec cette description, on n'a plus de problème sur la façon a priori non intuitive d'interpréter les points à l'infini, puisqu'ainsi il s'agit de droites comme les autres.

6.2.2 Les homographies

Considérons maintenant une certaine figure F dans le plan projectif. Nous avons vu que l'on pouvait voir F dans l'espace comme un ensemble stable par les homothéties de centre O. À ce sous-ensemble de l'espace ambiant, que l'on va appeler F^s, on peut faire subir des transformations. On va ainsi obtenir un nouvel ensemble qui va correspondre à une nouvelle figure dans le plan projectif. Déjà il faut que notre transformation soit telle que la figure associée à F^s possède encore les propriétés requises, c'est-à-dire la stabilité par les homothéties de centre O. Cela revient simplement à imposer que notre transformation envoie une droite passant par O sur une droite passant par O. Mais ce que l'on aimerait également, comme on l'a dit, c'est que notre transformation conserve l'alignement, c'est-à-dire les droites, dans le plan projectif. Mais les droites du plan projectif sont les plans passant par O de l'espace ambiant. Ainsi il va falloir imposer en outre que notre transformation conserve les plans passant par O (ce qui implique d'ailleurs qu'elle conserve les droites passant par O – *Pourquoi ?*).

En fait, on va se restreindre juste à un certain type de transformations vérifiant ces conditions, plus précisément aux transformations de l'espace qui laissent fixe le point O et qui sont des *isométries*, c'est-à-dire qui conserve les distances.

Question 6.2.1. *Montrer qu'une isométrie laissant fixe O envoie un plan passant par O sur un plan passant par O. Montrer qu'elle envoie un plan ne passant pas par O sur un plan ne passant pas par O. En déduire que l'on a des résultats analogues pour les droites.*

Ce sont ces transformations du plan projectif associées à ces transformations particulières de l'espace que l'on va appeler dans ce document *homographies*[1].

Parmi ces transformations, il y en a qui vont laisser stable le plan P et d'autres non. Il est facile de voir que celles qui laissent stables le plan P vont envoyer les vrais points sur d'autres vrais points et les points à l'infini sur d'autres points à l'infini. En fait, de telles transformations vont être simplement des isométries du plan P et ce ne sont pas elles qui vont modifier la figure en profondeur. Par exemple, le fait que les vrais points et les points à l'infini ne soient pas permutés veut exactement dire que les droites qui étaient sécantes vont le rester, tout comme les droites qui étaient parallèles.

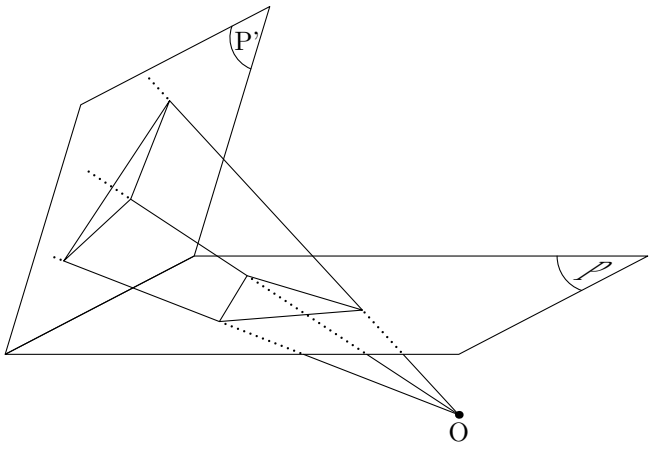
Par contre, les isométries laissant fixe O qui ne stabilisent pas le plan P, elles, sont beaucoup plus intéressantes. En effet, notons P' l'image réciproque de P par une telle isométrie que l'on va appeler f. P' est par définition l'ensemble des points qui sont envoyés par f dans P.

Question 6.2.2. *Montrer que P' est un plan.*

Appelons P_O (resp. P'_O), le plan parallèle à P (resp. P') passant par O.

Question 6.2.3. *Montrer que si deux plans sont parallèles, leurs images par f sont encore parallèles. En déduire que f applique P'_O sur P_O.*

Ceci veut exactement dire que la figure transformée est en fait F^s vu dans le plan projectif défini par P' et O. En particulier, ses vrais points s'obtiennent en regardant l'intersubsection de F^s et de P' et ses points à l'infini correspondent aux droites du plan P'_O qui sont contenues dans F^s.



[1]Normalement, une homographie est quelque chose de plus général. Plus précisément il s'agit d'une transformation du plan projectif qui est associée non pas à une isométrie mais à une bijection linéaire (terme que je ne vais pas expliquer) de l'espace ambiant. Mais en fait, pour les applications, cela revient en gros au même.

6.2.3 Envoyons des points à l'infini

Comment utilise-t-on pratiquement les homographies ? Ce qu'il faut voir, c'est que si l'on a deux droites sécantes et que l'on arrive à trouver une homographie qui envoie le point d'intersubsection de ces deux droites sur un point à l'infini, dans la figure que l'on va obtenir les deux droites en question vont devenir parallèles et c'est bien plus sympathique. Bien sûr cela vaut aussi pour trois droites concourrantes. Si l'on arrive à trouver une homographie qui envoie le point d'intersubsection de ces trois droites sur un point à l'infini, elles vont devenir parallèles et donc les questions de concourrance vont pouvoir de temps en temps se ramener à des questions de parallélisme qui sont a priori plus simples à traiter.

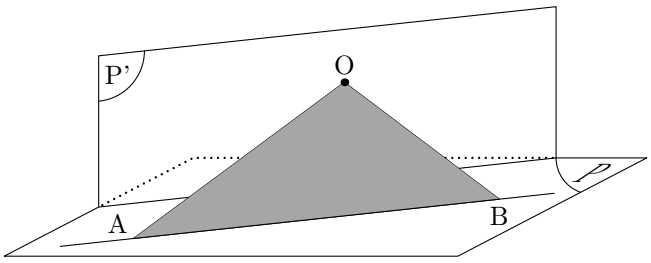
Mais voyons comment l'on peut trouver une homographie qui envoie un point donné M du plan projectif sur un point à l'infini. Supposons qu'une telle homographie existe et notons f l'isométrie de l'espace qui lui est associée. Notons également comme tout à l'heure P' l'image réciproque de P par f. On a vu que les points qui allaient être envoyés à l'infini étaient ceux qui étaient représentés par des droites contenues dans le plan P'_O, plan parallèle à P' et passant par O. Et nous, ce que l'on veut c'est que le point M soit envoyé à l'infini, c'est-à-dire exactement que la droite (OM) appartienne à ce fameux plan P'_O. Finalement, pour construire notre homographie, il suffit d'exhiber une transformation linéaire qui envoie un certain plan parallèle à la droite (OM) sur P.

En fait, on va prouver beaucoup mieux, on va prouver qu'étant donné un plan P'_O quelconque passant par O, on peut trouver une isométrie f de l'espace laissant fixe O et un plan P' parallèle à P'_O et ne passant pas par O, le tout tel que f envoie P' sur P. L'idée pour arriver à un tel résultat est de considérer le plan bissecteur des plan P'_O et P que l'on peut supposer sécants. Le problème c'est que ce plan ne passe pas forcément par O, et même en fait il n'y passe jamais. Mais qu'à cela ne tienne, on translate notre plan P'_O de façon à ce qu'il reste toujours parallèle à lui-même et ce jusqu'à ce que le nouvel plan bissecteur passe par O. On considère alors la réflexion par rapport à ce dernier plan qui fait bien ce que l'on veut.

Question 6.2.4. *Rédiger proprement cette démonstration.*

Ainsi l'on a prouvé qu'étant donné A un point quelconque de notre plan projectif, on pouvait trouver une homographie qui envoyait A sur un point à l'infini. Mais en fait, on a prouvé mieux que cela. Le résultat plus fort que l'on vient de démontrer implique qu'étant donnés deux points quelconques, que l'on va supposer distincts, A et B de notre plan projectif, on peut trouver une homographie envoyant A et B sur des points à l'infini, la droite (AB) étant alors naturellement envoyée sur la droite à l'infini.

Question 6.2.5. *Pourquoi une telle chose ?*

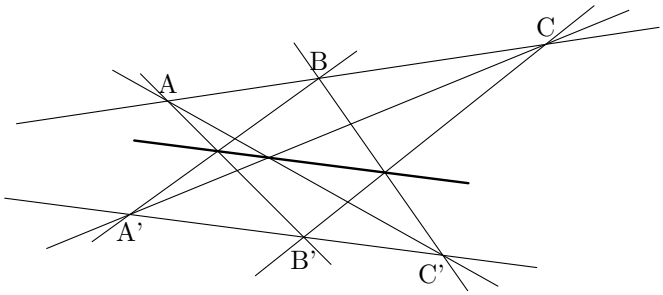


La droite (AB) envoyée à l'infini...

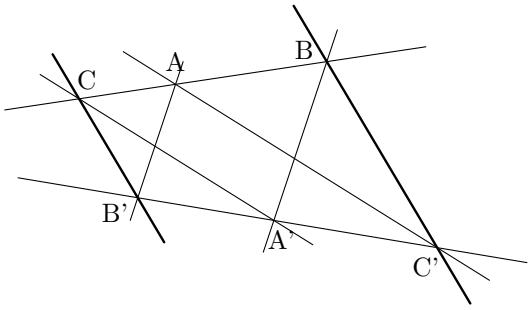
6.2.4 Avec des parallèles, c'est plus simple...

Comment utilise-t-on le résultat précédent en pratique ? Supposons que l'on dispose d'une figure un peu compliquée sur laquelle on nous demande de démontrer un alignement ou la concourrance de certains droites. Ce que l'on vient de voir, c'est que l'on est tout en fait en droit de choisir A et B deux points quelconques de la figure et de les envoyer à l'infini. Cela signifie concrètement que l'on a le droit de décréter que pour tous les points M de la droite (AB), les droites qui se coupaient alors en M sont désormais parallèles, bien entendu les anciens parallélismes ne vont pas être conservés mais en général ce n'est pas trop grave car lorsque l'on est réduit à faire ce genre de choses, c'est que l'on n'a pas de parallélisme. Ce qu'il y a de bien, c'est que cela n'altère ni les alignements, ni les concourrances, et donc par exemple montrer un certain alignement va revenir à montrer le même alignement sur la figure simplifiée avec plein de parallèles.

Donnons un exemple. Supposons que l'on veuille démontrer le théorème suivant connu sous le nom de théorème de Pappus : si deux triplets de points alignés (A, B, C) et (A', B', C') sont situés sur deux droites distinctes, alors les trois points d'intersubsection de (AB') et $(A'B)$, (AC') et $(A'C)$, (BC') et $(B'C)$ sont alignés.



Fixons des notations : appelons a le point d'intersubsection de (BC') et $(B'C)$, b celui de (AC') et $(A'C)$ et c celui de (AB') et $(A'B)$. Il s'agit de montrer comme on l'a dit que a, b et c sont alignés. L'idée est alors d'utiliser une homographie qui va considérablement simplifier la figure. Décidons par exemple d'envoyer les points b et c à l'infini. La figure se redessine alors de la façon suivante :



En effet, les droites (AC') et $(A'C)$ sont désormais parallèles puisqu'elles se coupent au point a qui est à l'infini. Il en est de même des droites (AB') et $(A'B)$. Et ce qu'il faut prouver c'est que le point d'intersubsection des droites (BC') et $(B'C)$ se situe sur la droite (bc). Mais b et c étant tous les deux à l'infini, la droite (bc) est la droite à l'infini et donc ce qu'il faut voir c'est que les droites (BC') et $(B'C)$ s'intersectent à l'infini, c'est-à-dire qu'elles sont parallèles.

Question 6.2.6. *En utilisant le théorème de Thalès, finir la démonstration du théorème de Pappus.*

Question 6.2.7. *Montrer en utilisant une méthode analogue le théorème de Desargues. Soient ABC et $A'B'C'$ deux triangles tels que les droites (AA'), (BB') et (CC') soient concourrantes. Alors les trois points d'intersubsection de (AB) et $(A'B')$, (AC) et $(A'C')$, (BC) et $(B'C')$ sont alignés.*

6.2.5 Le birapport

Il est assez évident que les homographies ne conservent pas les distances quand on les regarde dans le plan. En effet, il est tout à fait possible d'envoyer des points à l'infini et donc de transformer des distances finies en distances infinies. Les rapports de distance non plus ne sont pas conservés. En effet supposons par exemple que notre figure soit simplement constituée de deux points A et B et de leur milieu I. Considérons un point quelconque M en dehors de la droite (AB). On a vu que l'on pouvait trouver une homographie envoyant B et M à l'infini. L'ensemble des points qui vont être envoyés à l'infini sera la droite (BM) et donc les points A et I vont rester de vrais points. On voit ici que le rapport $\frac{AI}{BI}$ n'est pas conservé.

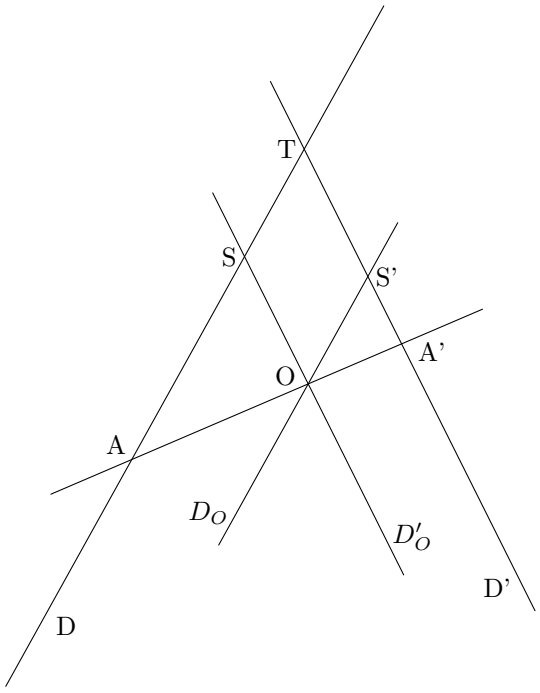
Toutefois, il y a quand même une quantité qui est conservée par les homographies, c'est ce que l'on appelle le birapport. Étant donné quatre points A, B, C, D distincts et *alignés*, on définit leur *birapport* comme le quotient suivant :

$$[A, B, C, D] = \frac{\bar{AC} \cdot \bar{BD}}{\bar{BC} \cdot \bar{AD}}$$

où $\bar{AB}$ désigne la distance algébrique de A à B. Cela signifie que l'on choisit arbitrairement un sens sur la droite qui passe par A, B, C et D et que l'on compte les distances positivement dans ce sens et négativement dans l'autre. Le birapport de quatre points ne dépend pas du sens que l'on choisit pour orienter notre droite (*Pourquoi ?*).

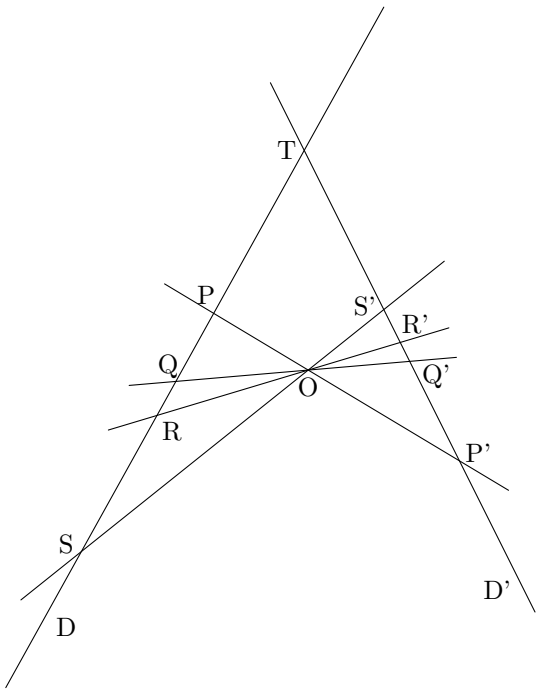
Il y a encore un problème à discuter. Il s'agit du cas où l'un des quatre points se trouve à l'infini (il ne peut pas y en avoir deux, car il n'y a qu'un seul point à l'infini sur une droite et que l'on a supposé que nos quatre points étaient distincts). Si le point à l'infini est A, les deux quantités $\bar{AC}$ et $\bar{AD}$ sont infinies et on convient de les simplifier le birapport étant alors simplement $\frac{\bar{BD}}{\bar{BC}}$. De même pour les autres points.

Pour prouver que le birapport est invariant par homographie, on commence par étudier le problème suivant. On considère deux droites sécantes D et D', et on appelle T leur point d'intersubsection. On considère également un point O extérieur à ces deux droites. On trace ensuite la parallèle à D (resp. D') passant par O que l'on appelle D_O (resp. D'_O). On note S le point d'intersubsection de D et de D'_O et S' celui de D' et de D_O. On choisit maintenant A un point quelconque de D et on appelle A' l'intersubsection de la droite (AO) avec la droite D'.



Question 6.2.8. *Montrer que l'on a la relation* $\bar{AS} \cdot \bar{A'S'} = \bar{ST} \cdot \bar{S'T}$.

La deuxième étape consiste à considérer le dessin plus complexe suivant. On se donne encore nos deux droites D et D' que l'on suppose toujours sécantes et se coupant en T. On se donne en outre quatre points distincts P, Q, R et S sur D. On note P' l'intersubsection de la droite (PO) avec la droite D' et on définit de même les points Q', R' et S'.

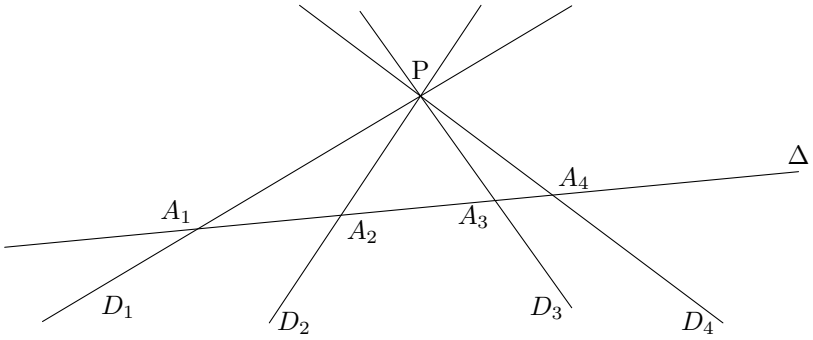


Question 6.2.9. *Montrer qu'ici le birapport est conservé, c'est-à-dire que l'on a l'égalité :*

$$\frac{\bar{PR} \cdot \bar{QS}}{\bar{QR} \cdot \bar{PS}} = \frac{\bar{P'R'} \cdot \bar{Q'S'}}{\bar{Q'R'} \cdot \bar{P'S'}}$$

Question 6.2.10. *En déduire que le birapport est conservé par les homographies.*

On peut définir également le birapport de quatre droites concourrantes (éventuellement en un point à l'infini, auquel cas, il s'agit de quatre droites parallèles). Cela est fort simple. On se donne donc D_1, D_2, D_3 et D_4 quatre droites concourrantes en un certain point P. Et on considère une droite quelconque qui ne passe pas par P, disons Δ. Δ va intersecter nos droites en quatre points (encore éventuellement à l'infini) que l'on note A_1, A_2, A_3, A_4 comme le montre le dessin ci-dessous.



Question 6.2.11. *Montrer que le birapport $[A_1, A_2, A_3, A_4]$ ne dépend du choix de la droite Δ et qu'il est donné par le quotient :*

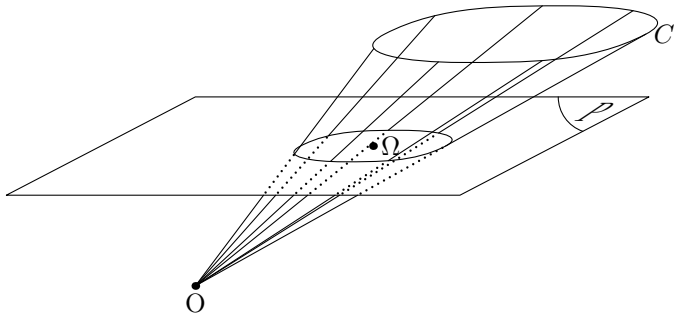
$$[A_1, A_2, A_3, A_4] = \frac{\sin \widehat{A_1PA_3} \cdot \sin \widehat{A_2PA_4}}{\sin \widehat{A_2PA_3} \cdot \sin \widehat{A_1PA_4}}$$

C'est cette quantité que l'on appelle le *birapport* des quatre droites concourrantes D_1, D_2, D_3 et D_4 et on la note $[D_1, D_2, D_3, D_4]$.

Question 6.2.12. *Montrer que le birapport de quatre droites est invariant par homographie.*

6.2.6 Les coniques

On a vu que les homographies conservaient l'alignement, c'est-à-dire qu'une homographie transforme une droite en une droite. On est en droit de se demander à quoi va ressembler l'image d'un cercle par une homographie. Bien entendu, comme ni les distances, ni les rapports de distance ne sont conservés, il n'y aucune raison a priori pour qu'un cercle soit tranformé en un autre cercle, et effectivement ce n'est pas le cas. Mais voyons déjà par quoi est représenté un cercle dans l'espace ambiant.



C'est ce que l'on appelle un *cône*. Notons-le $\mathcal{C}$. Comme on l'a vu, l'image de notre cercle de départ par l'homographie qui correspond à l'isométrie f de l'espace, n'est autre que l'intersubsection de notre cône par le plan P' image réciproque de P par f. Ainsi étudier les images possibles de notre cercle par une homographie revient à étudier les intersubsections de $\mathcal{C}$ par des plans P' image de P par une isométrie de l'espace laissant fixe O (*Pourquoi ?*). Mais on a vu également qu'un tel plan pouvait prendre toutes les directions possibles, au sens où si l'on se donne un plan P' quelconque de l'espace, il va exister un tel plan parallèle à P', disons P''. Mais si P' ne passe pas par O, P'' va être l'image de P' par une homothétie de centre O et donc les intersubsections respectives de $\mathcal{C}$ avec P' et P'' vont aussi pouvoir se déduire l'une de l'autre par une homothétie. Tout ça pour dire que si l'on ne s'intéresse qu'à la "forme" de l'image de notre cercle, on peut étudier de façon plus générale l'intersubsection de $\mathcal{C}$ par un plan ne passant pas par O sans se soucier du fait qu'il soit ou non image de P par une isométrie de l'espace laissant fixe O. Ces intersubsections sont ce que l'on appelle des *coniques*.

Question 6.2.13. *Se convaincre qu'une figure du plan projectif est une conique si et seulement si il existe une homographie qui l'envoie sur un cercle. Montrer que l'image d'une conique par une homographie est encore une conique.*

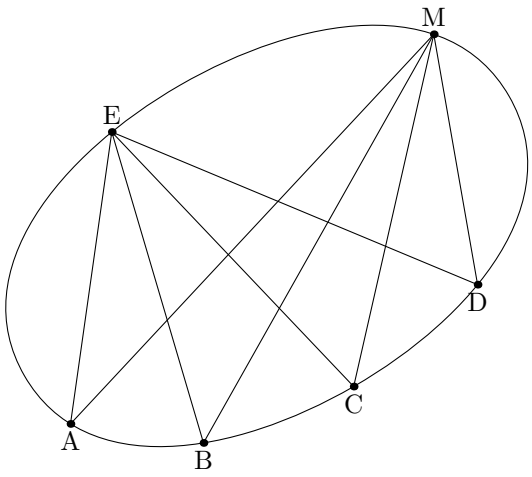
Il y a trois sortes de coniques, qui correspondent à des inclinaisons plus ou moins importantes pour le plan de coupe. Le cas limite est celui de la *parabole*, il correspond à un plan de coupe parallèle à une droite (OM) pour un certain point M placé sur le cercle de départ. Les plans moins inclinés correspondent à ce que l'on appelle des *ellipses*, les plans plus inclinés à ce que l'on appelle des *hyperboles*.

Question 6.2.14. *Donner l'allure d'une ellipse, d'une parabole et d'une hyperbole. Ne pas oublier de décrire les points à l'infini.*

Il existe plein d'autres présentations des ellipses. Il y a la présentation analytique qui consiste simplement à dire qu'une conique est l'ensemble des points du plan (projectif) de coordonnées (x, y) tels que $P(x, y) = 0$ où P est un polynôme de degré 2 en les deux variables x et y. Bien entendu, on est capable au vu des coefficients de dire si l'on a affaire à une ellipse, une parabole ou une hyperbole mais la condition n'est pas quelque chose qui peut se voir directement. Une autre présentation possible est la suivante. On se donne une droite D dans le plan projectif et un point F n'appartenant pas à D. On se donne aussi e un réel strictement positif. On s'intéresse à l'ensemble des points M tels que le quotient $\frac{MF}{MD} = e$, où MD désigne la distance du point M à la droite D. Ce que l'on montre c'est que cet ensemble est une conique et que toute conique peut être obtenue ainsi, et ce d'au plus deux façons, les deux façons lorsqu'il y en a effectivement deux se déduisant l'une de l'autre par une symétrie. Là le type de la conique se lit directement sur e. Si $e < 1$ on a affaire à une ellipse, si $e = 1$ c'est une parabole et si $e > 1$, c'est une hyperbole. Donnons un peu de terminologie. F s'appelle un *foyer* de la conique, D la *directrice* associée à ce foyer et e est l'*excentricité*. Contrairement à ce que l'on pourrait croire, il n'est pas évident de construire, à partir d'un cône et d'un plan coupant ce cône, le foyer de la conique intersubsection du cône et du plan. En particulier, il est faux que le foyer est donné par la droite $(O\Omega)$ et que la directrice est donnée par le plan parallèle à P passant par O, avec les notations précédentes.

Il existe finalement une autre description des coniques qui rentre plus dans notre contexte ici et donc nous allons la présenter. Soit $\mathcal{C}$ une conique dans le plan projectif. On considère cinq points A, B, C, D et E deux à deux distincts sur $\mathcal{C}$.

Question 6.2.15 (Théorème de Chasles). *Montrer qu'un point M du plan projectif appartient à la conique $\mathcal{C}$ si et seulement si* $[(EA), (EB), (EC), (ED)] = [(MA), (MB), (MC), (MD)]$.



Question 6.2.16. *En déduire que par cinq points du plan projectif, il passe au plus une conique. Existe-t-il toujours une telle conique ?*

6.3 Les ordinaux

6.3.1 Ensembles dénombrables

On dit qu'un ensemble E est *dénombrable* s'il peut être mis en bijection avec $\mathbb{N}$, l'ensemble des entiers naturels. Cela signifie qu'il existe une fonction $f : \mathbb{N} \to E$ [2] telle que tout élément de E a un et un seul antécédent par f. Autrement dit, E est dénombrable si on est capable de numéroter tous ses éléments, c'est-à-dire de dire qu'un tel est le zéroième, un tel le premier, un tel le deuxième, etc. et ce sans en oublier aucun. Donnons tout de suite des exemples.

Le plus simple est sans doute $\mathbb{N}$ qui est dénombrable. En effet, il est facile de numéroter les entiers. On dit tout simplement que 0 est le zéroième, 1 le premier, plus généralement n le n-ième. La fonction qui correspond à cela est simplement l'identité, c'est-à-dire la fonction $\mathbb{N} \to \mathbb{N}$ qui à un entier associe lui-même. Bien entendu, elle est bijective.

Considérons désormais une partie infinie A de $\mathbb{N}$. Là encore, on peut numéroter les éléments de A. On dit par exemple que le plus petit est le zéroième, que le deuxième plus petit est le premier, ainsi de suite.

Question 6.3.1. *Construire rigoureusement par récurrence cette fonction $\mathbb{N} \to A$ et prouver qu'elle est bijective.*

On en déduit qu'un ensemble E est dénombrable si et seulement s'il est infini et l'on peut trouver une fonction $f : \mathbb{N} \to E$ *surjective* (ie tout élément de E a au moins un antécédent, mais pas forcément un unique). En effet, si l'on a construit une telle fonction, on peut considérer le sous-ensemble A de $\mathbb{N}$ formé des entiers x tels que pour tout $x' < x$, $f(x') \neq f(x)$. La fonction f restreinte à A, que l'on notera $f_{|A}$, est alors bijective (*Pourquoi ?*). D'autre part A est infini donc d'après ce que l'on vient de faire il existe une bijection $g : \mathbb{N} \to A$. La fonction $f_{|A} \circ g$ réalise alors une bijection de $\mathbb{N}$ dans E (*Pourquoi ?*).

Question 6.3.2. *Montrer en utilisant ce qui précéde qu'une partie d'un ensemble dénombrable est soit finie, soit dénombrable (on dit souvent* au plus dénombrable*).*

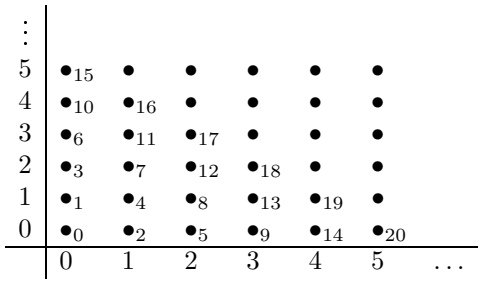
[2] On remarquera qu'une fonction de $\mathbb{N}$ dans E n'est autre qu'une suite à valeurs de $\mathbb{N}$. En effet, noter $f(n)$ ou f_n (ou u_n) revient moralement au même.

L'ensemble $\mathbb{Z}$ des nombres relatifs est dénombrable. Une façon d'énumérer les éléments de $\mathbb{Z}$ est par exemple $0, 1, -1, 2, -2, 3, -3$, etc. La fonction considérée ici est la fonction de $\mathbb{N}$ dans $\mathbb{Z}$ qui à un nombre pair $2n$ associe $-n$ et qui à un nombre impair $2n+1$ associe $n+1$. Je prétends qu'elle est bijective.

Question 6.3.3. *Le vérifier.*

L'ensemble $\mathbb{N}^2$ est dénombrable. Une façon de numéroter ses éléments est décrite par le dessin de la page suivante.

(Je te conseille de t'amuser à chercher avant de regarder la solution. C'est assez instructif je trouve).



On déduit de cette propriété des conséquences qui vont nous permettre de montrer plus rapidement que certains ensembles sont dénombrables.

La première est que si A et B sont deux ensembles dénombrables, il en est de même de leur produit cartésien $A \times B$. Pour voir cela, considérons $f_A : \mathbb{N} \to A$, $f_B : \mathbb{N} \to B$ deux bijections. Elles existent puisque A et B sont dénombrables. On regarde alors la fonction f définie par :

$$f : \left(\begin{array}{ccc} \mathbb{N}^2 & \to & A \times B \\ (n,m) & \mapsto & (f_A(n), f_B(m)) \end{array} \right)$$

Il s'agit d'une bijection de $\mathbb{N}^2$ dans $A \times B$. Si maintenant l'on prend $g : \mathbb{N} \to \mathbb{N}^2$ une bijection, la composée $f \circ g$ sera une bijection de $\mathbb{N}$ dans $A \times B$ et donc $A \times B$ sera dénombrable.

Question 6.3.4. *Rédiger proprement la démonstration précédente. En déduire par récurrence que si $A_1, \ldots, A_n$ sont des ensembles dénombrables, alors leur produit $A_1 \times \cdots \times A_n$ l'est aussi.*

Une autre conséquence est que si l'on se donne pour tout entier $n \in \mathbb{N}$, un ensemble dénombrable A_n, alors la réunion des A_n notée $\cup_{n\in\mathbb{N}} A_n$ (c'est-à-dire l'ensemble des éléments qui appartiennent au moins à un des A_n) est encore dénombrable. Je tiens à remarquer que cette propriété n'est pas la même que celle énoncée précédemment pour les produits. En effet pour les produits, on se cantonnait à des produits finis[3] au sens où le nombre de termes qui apparaissent dans le produit était fini, aussi grand qu'on le souhaitait certes mais fini. Ici, on prend la réunion d'une infinité d'ensembles, ce n'est pas la même chose. Je tiens également à remarquer que le fait que les ensembles A_n soit indicés par les entiers naturels est très importants. De fait, il n'est pas vrai qu'une réunion quelconque d'ensembles dénombrables l'est encore.

Question 6.3.5. *Bien comprendre les deux remarques qui précèdent. Ne pas hésiter à poser des questions si nécessaire.*

Esquissons à présent la démonstration de la propriété énoncée. Pour tout entier n, il existe une bijection $\mathbb{N} \to A_n$, notons-la f_n. Définissons l'application f suivante :

$$f : \left(\begin{array}{ccc} \mathbb{N}^2 & \to & \cup_{n\in\mathbb{N}} A_n \\ (n,m) & \mapsto & f_n(m) \end{array} \right)$$

[3]Il est possible de parler de produits infinis mais déjà les définir n'est pas quelque chose de si simple. Nous n'en parlerons pas ici de toute façon.

Cette application n'est en général pas bijective. Par contre, elle est toujours surjective et sa composée avec une bijection $\mathbb{N} \to \mathbb{N}^2$ l'est également. Autrement dit, on vient de construire une surjection de $\mathbb{N}$ dans $\cup_{n\in N} A_n$, et on a vu que cela suffisait à entraîner que $\cup_{n\in\mathbb{N}} A_n$ est un ensemble dénombrable.

Ces deux propriétés permettent de montrer que bien des ensembles sont dénombrables. Par exemple $\mathbb{N} \times \ldots \times \mathbb{N}$ (n fois), que l'on note souvent $\mathbb{N}^n$ est dénombrable. $\mathbb{Z}^n$ l'est également. L'ensemble des rationnels $\mathbb{Q}$ est également dénombrable. En effet, on peut écrire $\mathbb{Q}$ comme la réunion des $\frac{1}{q}\mathbb{Z}$ pour q parcourant $\mathbb{N}^\star$ où $\frac{1}{q}\mathbb{Z}$ est l'ensemble des rationnels de la forme $\frac{p}{q}$ pour p entier relatif. Comme les $\mathbb{Z}$ est dénombrable, les $\frac{1}{q}\mathbb{Z}$ le sont également (*Pourquoi ?*), et finalement par la propriété précédente, leur réunion $\mathbb{Q}$ est dénombrable.

Question 6.3.6. *Montrer de même que l'ensemble des suites à valeurs entières qui sont périodiques à partir d'un certain rang est dénombrable.*

Réfléchis un instant à ce que cela signifie. Cela signifie précisément que l'on a un moyen de numéroter les suites à valeurs entières qui sont périodiques à partir d'un certain rang, c'est-à-dire que l'on peut dire que celle-ci est la zéroième, celle-là la première et ainsi de suite et ce sans en omettre une seule. N'est-ce pas impressionnant ?

Jusqu'à présent, on a cité plein d'ensembles dénombrables mais il existe également des ensembles qui ne le sont pas. Un des premiers exemples est $\mathbb{R}$, l'ensemble des nombres réels. En fait, nous allons montrer quelque chose de plus fort nous allons montrer que l'intervalle $[0, 1]$ n'est pas dénombrable[4]. Pour arriver à nos fins, nous allons faire ce que l'on appelle un raisonnement par l'absurde, c'est-à-dire que nous allons supposer que l'intervalle $[0, 1]$ est dénombrable et aboutir à une contradiction. Cela signifiera donc que notre hypothèse de départ était fausse. Supposons donc que $[0, 1]$ soit un ensemble dénombrable. L'ensemble $[0, 1[$ le serait également. Considérons donc une bijection $f : \mathbb{N} \to [0, 1[$. Les nombres de $[0, 1[$ s'écrivent sous la forme $0, a_1a_2a_3...$ où a_i est la i-ième décimale de notre réel, c'est un entier compris entre 0 et 9. De façon analogue, on développe tous les nombres réels suivants :

$$\begin{array}{lcccccccc}
f(1) & = & 0, & a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & \ldots \\
f(2) & = & 0, & a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & \ldots \\
f(3) & = & 0, & a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & \ldots \\
f(4) & = & 0, & a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & a_{4,5} & \ldots \\
f(5) & = & 0, & a_{5,1} & a_{5,2} & a_{5,3} & a_{5,4} & a_{5,5} & \ldots \\
\vdots & & & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}$$

N'oublions pas que l'on veut arriver à une contradiction et que nous avons supposé f bijective. Ce que l'on peut faire c'est donc construire un réel compris entre 0 et 1 qui ne soit l'image d'aucun entier par f. Autrement dit, on peut construire réel x compris entre 0 et 1 qui soit différent de $f(1)$, différent de $f(2)$, etc. Écrivons x sous la forme $0, x_1x_2x_3...$ et essayons de voir comment l'on peut choisir les x_i pour que x satisfasse ce que l'on veut. Mais pour que x soit différent de $f(1)$, il suffit qu'une décimale de x diffère que la décimale correspondante de $f(1)$. Par exemple si l'on choisit $x_1 \neq a_{1,1}$ on sera sûr que $x \neq f(1)$. Mais l'on peut continuer ainsi : en choisissant $x_2 \neq a_{2,2}$, on aura la garantie que $x \neq f(2)$. Finalement si l'on choisit pour tout entier n, un entier x_n compris entre 0 et 9 qui est différent de $a_{n,n}$, le réel x obtenu va être différent de tous les $f(n)$, ce qui veut dire qu'il n'aura pas d'antécédent par f... et là voilà notre contradiction.

Question 6.3.7. *Soient a et b deux réels tels que $a < b$. Construire une bijection entre l'intervalle $[a, b]$ et l'intervalle $[0, 1]$. En déduire que l'intervalle $[a, b]$ n'est pas dénombrable.*

[4] C'est plus fort car nous avons vu qu'un sous-ensemble d'un ensemble dénombrable l'est encore. Ceci prouve qu'un sur-ensemble d'un ensemble non dénombrable ne l'est pas non plus.

6.3.2 Ensembles totalement ordonnés

Soit E un ensemble. Munir E d'un *ordre total*, c'est être capable de dire étant donnés deux éléments distincts quelconques de E, disons x et y, si $x < y$ ou si $x > y$ et ce de façon exclusive. On impose quand même le fait que si $x < y$ et $y < z$ alors $x < z$. Bien entendu, les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sont naturellement munis d'ordres totaux. Mais on peut imaginer des ordres totaux sur d'autres ensembles, même des ensembles dont les éléments ne sont pas des nombres. Par exemple, l'ensemble des mots français est muni d'une structure d'ordre total, tout simplement en disant qu'un certain mot est plus petit qu'un autre s'il est placé avant dans le dictionnaire. On pourra écrire par exemple (un $>$ cinq) ou encore (abeille $<$ abracadabra). Bien sûr, si le mot X est placé avant le mot Y dans le dictionnaire et que le mot Y est placé avant le mot Z, X sera alors avant Z, ce qui bien la propriété que l'on a à vérifier.

Considérons donc E un ensemble totalement ordonné. On dit que E admet un *plus grand élément* x si pour tout élément $y \in E$, on a $y \leqslant x$. On dit qu'une partie $A \subset E$ admet un plus grand élément, s'il existe dans A un élément x plus grand ou égal à tous les éléments de A. Par exemple, il est facile de voir que ni $\mathbb{N}$, ni $\mathbb{Z}$, ni $\mathbb{Q}$, ni $\mathbb{R}$ n'admet de plus grand élément. Par contre, l'ensemble des mots français lui en admet un : il s'agit bien sûr du dernier mot du dictionnaire. On définit de même ce qu'est un *plus petit élément*. Là encore $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ n'admettent pas de plus petit élément et le premier mot du dictionnaire est un plus petit élément de l'ensemble des mots français. Par contre, ce coup-ci, $\mathbb{N}$ admet un plus petit élément qui est 0. En fait, comme on l'a déjà plus ou moins utilisé tout à l'heure, toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

On considère toujours un ensemble totalement ordonné E et on prend maintenant en outre une partie non vide A de E. On définit maintenant la partie $A^{\geqslant}$ de E qui consiste en l'ensemble des éléments $x \in E$ qui sont plus grand ou égaux que *tous* les éléments de A. S'il existe, le plus petit élément de cet ensemble $A^{\geqslant}$ est ce que l'on appelle la *borne supérieure* de A. Prenons un exemple, l'intervalle $A =]0, 1[$. L'ensemble $A^{\geqslant}$ des majorants de A est alors l'intervalle $[1, \infty[$. Celui-ci admet un plus petit élément qui est 1 donc la borne supérieure de A existe et est 1. On définit de façon analogue la *borne inférieure* de A (*Comment ?*).

Question 6.3.8. *Montrer que si une partie $A \subset E$ admet un plus grand élément M, alors A admet une borne supérieure qui est précisément M. Montrer de même que si une partie $A \subset E$ admet un plus petit élément m, alors A admet une borne inférieure qui est m.*

Lorsqu'ils existent, le plus grand élément d'une partie $A \subset E$ se note $\max A$, le plus petit élément $\min A$, la borne supérieure $\sup A$ et la borne inférieure $\inf A$.

Une dernière définition. On considère toujours notre ensemble E totalement ordonné. Soit x un élément de E. On regarde l'ensemble X des éléments de E qui sont *strictement* plus grands que x. Si cet ensemble admet un plus petit élément, on dit que x admet un *successeur* et ce successeur est précisément le plus petit élément de l'ensemble X. Je le noterai par la suite $\mathrm{S}(x)$. Par exemple dans $\mathbb{N}$ et dans $\mathbb{Z}$, tout élément admet un successeur, le successeur de n étant $n + 1$. Dans l'ensemble des mots français, tout élément à l'exception du dernier, admet un successeur, le successeur d'un mot étant le mot venant juste après dans le dictionnaire. Par contre, dans $\mathbb{Q}$ et $\mathbb{R}$, aucun élément n'admet de successeurs. Montrons-le pour $\mathbb{R}$. Considérons donc un réel x, l'ensemble des réels strictement plus grands que x est précisément $]x, \infty[$ mais cet intervalle n'admet pas de plus petit élément (*Pourquoi ?*).

6.3.3 Les ordinaux dénombrables

Une bonne façon de caractériser $\mathbb{N}$ muni de son ordre est de dire qu'il s'agit du plus petit ensemble totalement ordonné admettant un plus petit élément et qui soit tel que tout élément admet un successeur. Ce que j'entends par là, c'est que si E est un autre ensemble admettant un plus petit élément et tel que tout élément de E admet un successeur alors on peut trouver une fonction strictement croissante $\mathbb{N} \to E$. Ceci est une définition rigoureuse et elle vaut ce qu'elle vaut mais il y a une façon beaucoup plus terre à

terre de voir les choses. En effet, essayons de contruire un ensemble E admettant un plus petit élément et tel que tout élément de E admet un successeur. Bon, comme on l'a dit et répété E admet un plus petit élément, appelons-le 0. Maintenant ce 0 admet un successeur qui est forcément strictement plus grand que 0, appelons-le 1. Mais ce 1 aussi admet un successeur, c'est 2, et ainsi de suite. Autrement dit l'ensemble E contient au moins les éléments 0, 1, 2, 3, etc. triés de la façon suivante :

$$0 < 1 < 2 < 3 < 4 < 5 < \dots$$

et donc il est légitime de dire que $\mathbb{N}$ est le plus petit ensemble ayant ces propriétés.

On a maintenant envie de s'intéresser au plus petit ensemble E totalement ordonné admettant un plus petit élément, qui soit tel que tout élément admet un successeur et qui soit tel, aussi, que toute partie de E admet une borne supérieure. Du coup, manifestement $\mathbb{N}$ est trop petit : la partie formée de tous les entiers (ou de tous les entiers pairs) n'admet pas de borne supérieure car aucun entier n'est plus grand que tous les entiers ou autrement dit étant donné un entier, on peut toujours en trouver un plus grand. Si l'on veut continuer notre construction, il va donc falloir rajouter un élément qui va être la borne supérieure de tous les entiers et que l'on va appeler ω (lire `omega`). Mais maintenant, il lui faut un successeur et on ne l'a pas. Qu'à cela ne tienne, rajoutons-le et appelons-le $\omega + 1$. De fait, on va être obligé de rajouter $\omega + 2$, $\omega + 3$, etc. Mais là encore, ça ne va pas suffir : l'ensemble de tous les "nombres" que l'on a ajoutés jusqu'à présent ne va pas avoir de borne supérieure... On commence à voir qu'il y a un problème ici, on a peut-être en fait été trop gourmand. En effet, on ne voit pas trop comment cette construction pourrait s'arrêter, même au bout d'un temps vachement long. De façon plus précise, supposons que l'on ait réussi à fourrer dans un ensemble E tous les éléments construits ainsi, c'est-à-dire que l'on ait réussi à construire un ensemble E vérifiant les conditions que l'on s'est données. Alors cet ensemble devra admettre une borne supérieure (puisque c'est lui-même une partie de E). Cette borne supérieure sera alors forcément un plus grand élément (*Pourquoi ?*). Mais il ne peut pas y avoir de plus grand élément puisque tout élément possède un successeur qui est strictement plus grand que lui. Cela prouve qu'un tel ensemble n'existe pas.

Mais en fait, ce n'était pas si mal parti. Le problème c'est que l'on a supposé de trop de bornes supérieures existaient. Il faudrait se limiter à assurer l'existence de bornes supérieures que pour certaines parties de E, typiquement celles qui ne risquent pas d'aller à l'"infini", typiquement celles qui ne sont pas trop grandes. Un moyen d'y arriver est de se limiter aux parties dénombrables. Autrement dit, maintenant on chercher un ensemble E qui admet un plus petit élément, qui est tel que tout élément admet un successeur et qui est tel que tout partie $A \subset E$ dénombrable admet une borne supérieure.

Question 6.3.9. *En s'inspirant de la démonstration précédente, prouver que si un tel ensemble existe, il est forcément non dénombrable.*

Bon, maintenant que l'on a un peu affaibli nos hypothèses, reprenons notre construction et voyons ce qu'elle donne. On a dit que forcément tous les entiers doivent appartenir à un ensemble vérifiant de telles propriétés. Mais maintenant l'ensemble de tous les entiers, ie $\{0, 1, 2, \dots\}$ est dénombrable et donc il doit admettre une borne supérieure. Autrement dit, on va être obligé de rajouter ω et donc de rajouter $\omega + 1$, $\omega + 2$, etc. Mais alors l'ensemble $\{\omega, \omega + 1, \omega + 2, \dots\}$ qui est dénombrable ne va pas admettre de borne supérieure. Ben, rajoutons-là et appelons-là $\omega 2$. Mais ça n'arrange pas les choses. Il nous faut encore ajouter $\omega 2 + 1$, $\omega 2 + 2$, $\omega 2 + 3$, etc. et puis la borne supérieure de l'ensemble $\{\omega 2, \omega 2 + 1, \omega 2 + 2, \dots\}$ que l'on va appeler $\omega 3$. Et ça continue, on aura ainsi $\omega 3$, $\omega 4$, etc. Voici pour l'instant les éléments que l'on a

construit :

$$\begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & 5 & \dots \\ \omega & \omega+1 & \omega+2 & \omega+3 & \omega+4 & \omega+5 & \dots \\ \omega 2 & \omega 2+1 & \omega 2+2 & \omega 2+3 & \omega 2+4 & \omega 2+5 & \dots \\ \omega 3 & \omega 3+1 & \omega 3+2 & \omega 3+3 & \omega 3+4 & \omega 3+5 & \dots \\ \omega 4 & \omega 4+1 & \omega 4+2 & \omega 4+3 & \omega 4+4 & \omega 4+5 & \dots \\ \omega 5 & \omega 5+1 & \omega 5+2 & \omega 5+3 & \omega 5+4 & \omega 5+5 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \end{array}$$

Est-ce que c'est bon ? Peut-on s'arrêter ? Ben non, l'ensemble $\{0, \omega, \omega 2, \omega 3, \omega 4, \dots\}$ est tout ce qu'il y a de plus dénombrable mais il n'admet pas de borne supérieure. Il faut la rajouter et naturellement on va l'appeler $\omega\omega$ ou encore ω^2. C'est reparti : il faut encore rajouter le successeur de ω^2 que l'on va appeler ω^2+1, puis le successeur de ω^2+1 qui est ω^2+2, et ainsi de suite, et puis leur borne supérieure qui va être $\omega^2+\omega$, puis le successeur de celui-ci $\omega^2+\omega+1$, puis le successeur de ce dernier $\omega^2+\omega+2$, et leur borne supérieure $\omega^2+\omega 2$, et puis bientôt $\omega^2+\omega 3$, $\omega^2+\omega 4$, $\omega^2+\omega 5$, etc. et leur borne supérieure que l'on nomera $\omega^2+\omega^2$, soit $\omega^2 2$. Mais on peut encore continuer : on va construire ainsi $\omega^2 3$, $\omega^2 4$, etc. et l'ensemble $\{\omega^2, \omega^2 2, \omega^2 3, \dots\}$ est dénombrable et donc on doit lui fournir une borne supérieure. Soit, appelons-là $\omega^2\omega$, ou plus simplement ω^3. On n'est toujours pas au bout de nos peines. Il va y avoir ω^3+1, ω^3+2 et donc $\omega^3+\omega$, et puis $\omega^3+\omega 2$, $\omega^3+\omega 3$, et ainsi on va arriver à $\omega^3+\omega^2$, puis à $\omega^3+\omega^2 2$, à $\omega^3+\omega^2 3$, et donc rapidement à $\omega^3+\omega^3=\omega^3 2$. C'est toujours pas fini : il va arriver $\omega^3 3$ puis $\omega^3 4$ et puis sans grande surprise $\omega^3\omega=\omega^4$. Puis ω^5, ω^6, etc. Et là encore l'ensemble $\{\omega, \omega^2, \omega^3, \omega^4, \dots\}$ est tout ce qu'il y a de plus dénombrable et il exige donc une borne supérieure. Appelons-là ω^ω, ça s'impose. C'est fini ? Et non, toujours pas : ω^ω n'a pas de successeur. Ah oui, ben rajoutons-le, c'est $\omega^\omega+1$. Ainsi on va devoir rajouter $\omega^\omega+\omega$, puis $\omega^\omega+\omega^2$, puis $\omega^\omega+\omega^3$, etc. et ensuite leur borne supérieure qui sera $\omega^\omega+\omega^\omega=\omega^\omega 2$. On ne va pas tarder à arriver à $\omega^\omega\omega$ que l'on peut noter $\omega^{\omega+1}$. Mais lui n'a toujours pas du successeur et en brulant des étapes, on va devoir construire $\omega^{\omega+2}$, puis $\omega^{\omega 2}$, puis ω^{ω^2}, puis ω^{ω^ω}, puis $\omega^{\omega^{\omega^\omega}}$, etc. Et c'est toujours pas fini car l'ensemble $\left\{\omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \dots\right\}$ est dénombrable et n'admet pour l'instant pas de borne supérieure. Tiens, on a peut-être un petit problème de notation ce coup-ci. Enfin, c'est pas très grave, appelons-la ε_0 (lire `epsilon zéro`) cette borne supérieure. Mais là encore ça continue... Il va y avoir ε_0+1, etc, etc... et un de ces jours $\varepsilon_0^{\varepsilon_0}$, puis $\varepsilon_0^{\varepsilon_0^{\varepsilon_0}}$ et ainsi de suite et là encore il nous manque une borne supérieure... Qu'à cela ne tienne, ajoutons-là, on n'est plus à ça près et appelons-là ε_1. Mais on va avoir le même problème avec ε_1, il va falloir créer ε_2, puis ε_3, puis dans un avenir proche ε_ω, et tant qu'on y est, $\varepsilon_{\varepsilon_0}$, $\varepsilon_{\varepsilon_{\varepsilon_0}}$, etc. et encore leur borne supérieure que l'on nomme ce coup-ci ζ_0 (lire `zêta zéro`) . Puis bientôt ζ_1, ζ_2, ζ_ω, ζ_{ζ_0}, $\zeta_{\zeta_{\zeta_0}}$, et on commence vraiment à désespérer à arriver un jour au bout. Mais j'y pense : en faisant ces constructions, on obtient toujours des ensembles dénombrables (*Pourquoi ?*) et on a vu que si E existait il était forcément non dénombrable donc en fait on n'arrivera jamais à tous les attraper de cette façon. Il faut donc trouver un autre moyen d'appréhender le problème et c'est ce que nous allons faire.

6.3.4 Les bons ordres

Commençons par une définition. On dit qu'un ensemble est *bien ordonné* si toutes ses parties non vides admettent un plus petit élément. On a déjà vu un exemple d'ensemble bien ordonné, c'est $\mathbb{N}$. En fait, il y en a plein d'autres, comme nous allons le voir bientôt. Déjà, on peut dire :

Question 6.3.10. *Montrer par récurrence sur le cardinal que tout ensemble fini totalement ordonné est bien ordonné.*

Une caractérisation utile des bons ordres est la suivante. Considérons E un ensemble totalement ordonné. Alors E est bien ordonné si et seulement s'il n'existe pas de suites (infinies) d'éléments strictement décroissantes.

Question 6.3.11. *Le montrer.*

Question 6.3.12. *Montrer que si E est bien ordonné, tout élément de E sauf le plus grand élément de E s'il existe admet un successeur. Montrer que si E est bien ordonné, toute partie $A \subset E$ qui est majorée admet une borne supérieure.*

Rappelons la définition de l'ensemble que l'on cherche. Il s'agit du plus petit ensemble totalement ordonné E qui admet un plus petit élément, tel que tout élément de E admet un successeur et toute partie dénombrable de E admet une borne supérieure. Rappelons également que pour l'instant, on a vu que E était forcément non dénombrable. Nous allons adopter à present un nouvelle démarche : au lieu d'essayer de contruire E petit à petit, ce qui on l'a vu donne une idée assez précise de ce à quoi va ressembler E mais ne permet d'arriver à le construire entièrement, on va supposer qu'un tel ensemble E existe et regarder quelles propriétés il devrait vérifier.

Pour cela pour tout élément $\alpha \in E$, on va noter E_α l'ensemble des éléments de E strictement plus petits que α.

Question 6.3.13. *Montrer que le sous-ensemble de E formé des éléments α tels que E_α est dénombrable vérifie les conditions imposées à E et qu'il est plus petit que E. En déduire que pour tout $\alpha \in E$, E_α est dénombrable. Montrer, en utilisant ce précédent résultat, que E_α est bien ordonné et en déduire qu'il en est de même de E.*

On vient de voir quelque chose d'intéressant. À tout élément $\alpha \in E$, on peut associer un ensemble dénombrable bien ordonné qui n'est autre que E_α. Il serait donc peut-être pas mal de définir E comme l'ensemble des ensembles dénombrables munis d'un bon ordre[5]. Mais pour faire cela, il faudrait vérifier que si on prend un ensemble dénombrable bien ordonné, on peut le retrouver dans E et ce de façon unique, et vérifier également que si l'on prend deux ensembles dénombrables bien ordonnés différents, ils correspondent à deux éléments différents de E.

Commençons par exemple par essayer de montrer la première condition. Prenons donc X un ensemble dénombrable bien ordonné et il s'agit de le voir dans E, c'est-à-dire de trouver un $\alpha \in E$ tel que X soit E_α dans un sens à préciser. Mais bien entendu, X ne pourra être précisément E_α, car par exemple si l'on décide de prendre pour X l'ensemble des mots français et que l'on décide d'appeler les éléments de E en commençant par les entiers puis ω, puis ε_0, comme on l'a fait précédemment, on ne voit pas trop comment on pourrait retrouver les mots du dictionnaire dans E. Mais cela n'est en fait qu'une question de notation. Ce que l'on cherche, c'est en fait une bijection $f : X \to E_\alpha$, pour un certain α, qui respecte l'ordre c'est-à-dire qui est strictement croissante. Ceci est juste la façon mathématique de dire que les éléments n'ont en fait le même nom, f ne faisant qu'expliquer comment les noms se transportent de X à E.

Voyons comment l'on peut construire cette application. Il faut forcément envoyer le plus petit élément de X, disons x_0 sur le plus petit élément de E, disons 0 (*Pourquoi ?*) donc on commence ainsi. Puis il va falloir envoyer le successeur de x_0, disons x_1, sur le successeur de 0 qui est 1. Et ainsi de suite, il va falloir envoyer x_2 sur 2, x_3 sur 3 et la borne supérieure des x_n, disons x_ω, sur la borne supérieure des entiers qui est ω... et on continue ainsi. Mais, on a vu tout à l'heure que c'était désespéré. Mais ce qui était désespéré, c'était juste le fait d'arriver à épuiser E et la raison était qu'il n'est pas dénombrable, mais là c'est X que l'on veut épuiser et celui-ci est dénombrable donc il y a encore des chances que cela marche. En fait, cela marche très bien. L'idée pour le montrer est de considérer l'ensemble D des éléments de x sur lequel on peut définir f par un tel procédé. On vient de voir que tous les entiers, ainsi que ω sont dans D et ce que l'on veut prouver c'est qu'en fait $D = X$. Supposons que ce ne soit pas le cas, alors $X \backslash D$ (X auquel

[5] En fait, un tel ensemble n'existe pas mais comme on n'aura pas à le considérer, ça ne va pas nous gêner.

on a retiré les éléments de D) est non vide et donc il admet un plus petit élément, disons x. Autrement dit, x est le plus petit élément sur lequel f n'est pas défini. Mais alors, D est forcément l'ensemble des éléments de X strictement plus petits que x et D est dénombrable (car inclus dans X) dont il admet une borne supérieure disons x'.

Question 6.3.14. *Montrer que soit $x = x'$, soit x est le successeur de x' et que dans ce deux cas, on peut prolonger la fonction f à x. En déduire que f peut être définie sur tout X et qu'ainsi il existe un unique $\alpha \in E$ tel que $f : X \to E_\alpha$ soit une bijection strictement croissante.*

Le raisonnement que l'on vient de présenter est une vaste généralisation des raisonnements par récurrence classiques, c'est que l'on appelle la *récurrence transfinie*.

Le deuxième point qu'il nous fallait montrer que si l'on se donne deux ensembles bien ordonnés différents, ils correspondent à deux éléments de E qui sont différents. Mais comme on l'a déjà expliqué, cela ne peut pas être vrai, à cause de fait que l'on peut renommer les éléments. Ce que l'on peut faire, c'est choisir parmi tous les ensembles bien ordonnées qui correspondent à un même α un qui serait plus beau que les autres, un que l'on pourrait facilement distinguer. Autrement dit, donnons-nous un ensemble X dénombrable et bien ordonné et ce qu'il nous faut c'est trouver un moyen bien défini, et qui ne dépende que de l'ordre, d'appeler les éléments de X. Bien entendu, on pourrait appeler le plus petit 0, son successeur, s'il existe, 1, etc. Puis la borne supérieure de tous ces éléments, si elle existe, ω, et continuer ainsi. Mais c'est pas fameux car on a vu tout à l'heure qu'au bout d'un moment, on commençait à avoir des problèmes de notation : on a introduit ε_0 puis ζ_0 mais ça risque de continuer longtemps et l'on ne va pas pouvoir donner indéfiniment un nom (*Pourquoi ?*). Il faut donc trouver autre chose.

L'idée est de considérer comme tout à l'heure pour tout élément $x \in X$ l'ensemble X_x des éléments de x strictement plus petits que x et de remplacer systématiquement x par E_x au niveau de l'appelation. Voilà ce que cela donne pour le bon ordre $\mathbb{N}$. L'ensemble $\mathbb{N}_0$ des nombres entiers strictement négatifs est l'ensemble vide. Autrement à partir de maintenant, 0 va s'appeler $\emptyset$. L'ensemble $\mathbb{N}_1$ est tout simplement le singleton $\{0\}$ et donc à partir de maintenant 1 va s'appeler $\{\emptyset\}$. Continuons : 2 va s'appeler $\{\emptyset, \{\emptyset\}\}$, 3 va s'appeler $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, et ainsi de suite. On trouve bien ici un moyen *canonique* d'appeler les éléments, il est par contre un peu lourd et on voit pourquoi il n'est pas utiliser dans la pratique. À titre d'exemple, essaie d'écrire explicitement le nombre 15 dans ce langage et admire. Une dernière chose à voir est comment s'écrit la relation d'ordre dans notre nouveau langage. Mais c'est en fait tout simple, car dire que $x \leqslant y$ signifie simplement que $E_x \subset E_y$ et donc après renomination, $x \leqslant y$ va se dire $x \subset y$.

Question 6.3.15. *Montrer qu'après renomination, $x < y$ se dit simplement $x \in y$. Montrer qu'après renomination, le successeur de x est, s'il existe, simplement l'élément $x \cup \{x\}$. Montrer qu'après renomination la borne supérieure d'une sous-ensemble $A \subset X$ (forcément dénombrable) est, si elle existe, la réunion des ensembles x, x décrivant A.*

L'ensemble obtenu après renomination est ce que l'on appelle un *ordinal dénombrable*.

Ce que l'on aimerait maintenant c'est caractériser les ordinaux dénombrables parmi les ensembles dénombrables bien ordonnés. En fait, il n'est pas difficile de voir qu'un ensemble dénombrable bien ordonné est un ordinal (dénombrable) si et seulement si la relation d'ordre sur l'ensemble est donnée par l'appartenance. Ainsi l'on peut définir un ordinal dénombrable comme étant tout simplement un ensemble dénombrable sur lequel la relation d'appartenance est une relation d'ordre total qui fait de notre ensemble un bon ordre. On montre ensuite que l'ensemble des ordinaux dénombrables est effectivement un ensemble et que c'est exactement le E que l'on recherchait. Je passe les détails. Cet ensemble n'est pas en général noté E mais plutôt $\aleph_1$ (lire `aleph un`).

Cette construction est bien jolie et se généralise très bien d'ailleurs aux ordinaux qui ne sont pas forcément dénombrables (mais nous n'allons pas détailler ce point) mais il faut dire ce qui est, elle n'est pas très intuitive. Une bonne façon à mon avis de se représenter $\aleph_1$ est la description que j'ai esquissé

au début avec mes ω, mes ω^2, mes ω^ω, mais ε_0 et tout ça... bien qu'il faille se rappeler que l'on obtient ainsi que des approximations de $\aleph_1$ mais souvent dans la pratique on n'a pas besoin d'aller exhiber des ordinaux aussi grands. Il est quand même très utile de se rappeler également qu'un élément de $\aleph_1$ est un ensemble dénombrable muni d'une structure de bon ordre et que réciproquement à tout ensemble X dénombrable bien ordonné, il correspond un et un unique élément de $\aleph_1$, que l'on appelle l'*ordinal* de X.

6.3.5 Opérations sur les ordinaux dénombrables

Comme pour les entiers, on peut effectuer des opérations sur les ordinaux dénombrables. Il y a principalement l'addition, la multiplication et l'élévation à la puissance, ce que l'on appelle l'exponentiation. Ces opérations sont définies, comme pour les entiers, par récurrence mais pour pouvoir atteindre tous les éléments de $\aleph_1$, il va être nécessaire de faire une récurrence transfinie.

L'addition

Voyons comme cela marche pour l'addition. On choisit α un ordinal dénombrable. Et maintenant pour tout $\beta \in \aleph_1$, on veut définit $\alpha + \beta$. Bien entendu, on va poser $\alpha + 0 = \alpha$ et on va définir $\alpha + 1$ comme étant le successeur de α, $\alpha + 2$ comme étant le successeur de $\alpha + 1$ et ainsi de suite. Pour justifier ce "ainsi de suite" il va être nécessaire de distinguer deux types d'ordinaux[6] : les ordinaux qui sont des successeurs que l'on appelle *ordinaux successeurs* et les autres que l'on appelle *ordinaux limites*. Avec cette définition 0 serait un ordinal limite, mais en général on préfère l'exclure et lui donner un statut particulier. L'ordinal 1 est successeur puisque c'est par définition le successeur de 0. L'ordinal 2 aussi est successeur. Par contre l'ordinal ω lui n'est pas successeur comme on le voit facilement, c'est le plus petit ordinal limite. Maintenant, on est en mesure de donner la définition de l'addition. On pose $\alpha + 0 = \alpha$. Si β est un ordinal successeur, alors il s'écrit $\beta = \beta' + 1$ et on définit $\alpha + \beta$ comme le successeur de $\alpha + \beta'$. Si β est un ordinal limite, alors on regarde l'ensemble des ordinaux qui s'écrivent sous la forme $\alpha + \beta'$ pour un certain $\beta' < \beta$ (ie $\beta' \in \beta$). On obtient ainsi un ensemble dénombrable qui admet par définition une borne supérieure. C'est cette borne supérieure que l'on définit comme étant égale à $\alpha + \beta$.

Question 6.3.16. *Montrer que cela définit bien $\alpha + \beta$ pour tout ordinal dénombrable β. (On pourra raisonner par l'absurde et considérer le plus petit β tel que $\alpha + \beta$ ne soit pas défini et aboutir à une contradiction).*

Essayons de faire quelques calculs. Examinons dans un premier temps le cas où $\alpha = 0$. $0 + 0 = 0$ par définition. Comme 1 est le successeur de 0, $0 + 1$ est défini comme étant le successeur de $0 + 0 = 0$, donc $0 + 1 = 1$. Par récurrence, on montre que pour tout entier n, $0 + n = n$. On est maintenant en mesure de déterminer $0 + \omega$. C'est par définition la borne supérieure de tous les $0 + n = n$ pour $n < \omega$, ie n entier. Finalement $0 + \omega = \omega$. On va montrer par récurrence transfinie que pour tout $\alpha \in \aleph_1$, $0 + \alpha = \alpha$. Supposons que ce ne soit pas le cas et considérons le plus petit ordinal dénombrable (qui existe bien car $\aleph_1$ est bien ordonné) α tel que $0 + \alpha \neq \alpha$. Il y a alors deux cas. Si α est successeur, on peut écrire $\alpha = \alpha' + 1$ pour un certain α' forcément strictement plus petit que α. $0 + \alpha$ est alors défini comme étant le successeur de $0 + \alpha'$. Mais $0 + \alpha' = \alpha'$ car $\alpha' < \alpha$ et donc $0 + \alpha$ est le successeur de α', c'est-à-dire α, ce qui est contradictoire. Si maintenant α est limite, il s'agit de regarder l'ensemble des ordinaux se mettant sous la forme $0 + \alpha'$ pour $\alpha' < \alpha$. Mais si $\alpha' < \alpha$, $0 + \alpha' = \alpha'$ et donc cet ensemble est précisément l'ensemble des ordinaux dénombrables strictement plus petit que α (qui n'est autre que α lui-même rappelons-le) et sa borne supérieure est α. Donc $0 + \alpha = \alpha$, ce qui est encore une contradiction. Finalement, on en déduit que pour tout $\alpha \in \aleph_1$, on a $0 + \alpha = \alpha$. C'est bien.

Tiens, qu-est-ce que cette opération donne pour les ordinaux qui sont aussi des entiers. En fait, les choses se passent bien. Plus précisément :

[6] En fait, ce n'est pas nécessaire. On peut définir l'addition en disant que $\alpha + 0 = \alpha$ et si $\beta \neq 0$, $\alpha + \beta$ est la borne supérieure de l'ensemble des ordinaux qui s'écrivent comme le successeur de $\alpha + \beta'$ pour un certain $\beta' < \beta$. Cependant je trouve que l'on voit moins bien comment les choses se passent avec cette présentation.

Question 6.3.17. *Soit a et b deux entiers. Montrer par récurrence sur b que la somme $a+b$ où a et b sont vus comme des ordinaux dénombrables est précisément l'entier $a+b$.*

Continuons à faire nos calculs. $\omega+1$ est par définition le successeur de ω et donc ce que l'on avait tout à l'heure appelé innocemment $\omega+1$... quelle chance ! Quid de $1+\omega$? Voyons cela. ω est un ordinal limite, $1+\omega$ est alors défini comme la borne supérieure des $1+n$ pour $n<\omega$, c'est-à-dire n entier. Cette borne supérieure est précisément ω et donc $1+\omega=\omega$. En particulier $1+\omega\neq\omega+1$. En langage barbare, on dit que l'addition que l'on vient de définir n'est pas commutative. Par contre, elle est associative, au sens où si α, β et γ sont trois ordinaux dénombrables, on a toujours $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$ et donc en général, on le note simplement $\alpha+\beta+\gamma$ sans parenthèses.

Question 6.3.18. *Montrer l'associativité en utilisant une récurrence transfinie sur γ.*

On peut en fait décrire la somme que l'on vient de définir en termes de bons ordres. Prenons α et β deux ordinaux dénombrables. Considérons maintenant A (resp. B) un ensemble dénombrable totalement ordonné d'ordinal α (resp. β). On a vu que l'on pouvoir choisir pour A l'ensemble des ordinaux dénombrables strictement plus petits que α qui est d'ailleurs précisément α, mais je préfère lui donner un nom différent. Bien entendu, la même remarque est valable pour β. Une fois cela fait, on peut considérer l'ensemble C qui est ce que l'on appelle l'*union disjointe* de A et de B. Cela signifie qu'un élément de C est soit de la forme $(0,a)$ pour $a\in A$ soit de la forme $(1,b)$ pour $b\in B$. On peut munir cet ensemble C d'un ordre total que l'on appelle l'*ordre lexicographique* (qui correspond exactement à l'ordre du dictionnaire) en disant que $(n,x)<(n',x')$ si $n<n'$ ou si $n=n'$ et $x<x'$. Ceci correspond exactement à mettre tous les éléments de la forme $(0,a)$ en premier en les triant dans le même ordre que dans A et puis ensuite à mettre ceux de la forme $(1,b)$ en gardant ici le même ordre que dans B. Pour l'analogie avec le classement du dictionnaire, on met d'abord les mots qui commencent par 0 que l'on trie comme on sait faire, puis ceux qui commencent par 1.

Question 6.3.19. *Montrer C est un ensemble dénombrable et que l'ordre que l'on vient de définir fait de C un ensemble bien ordonné.*

On en déduit que C est en correspondance avec un unique ordinal dénombrable, c'est ce que l'on a appelé l'ordinal de C. Notons γ cet ordinal.

Question 6.3.20. *Montrer par récurrence transfinie que $\alpha+\beta=\gamma$.*

La multiplication

La multiplication se définit de façon très similaire. On se donne α un ordinal dénombrable et on veut définir par récurrence transfinie, l'ordinal $\alpha\cdot\beta$ pour tout $\beta\in\aleph_1$. Si $\beta=0$, on pose $\alpha\cdot 0=0$. Si β est successeur, $\beta=\beta'+1$ et on pose $\alpha\cdot\beta=\alpha\cdot\beta'+\alpha$ où l'addition est celle qui a été définie précédemment. Si β est limite, on définit $\alpha\cdot\beta$ comme la borne supérieure des ordinaux dénombrables se mettant sous la forme $\alpha\cdot\beta'$ pour $\beta'<\beta$.

Question 6.3.21. *Montrer par récurrence que si a et b sont des entiers, le produit $a\cdot b$ que l'on vient de définir correspond au produit classique ab sur les entiers.*

Montrer par récurrence transfinie que pour tout $\alpha\in\aleph_1$, $\alpha\cdot 0=0\cdot\alpha=0$ et $\alpha\cdot 1=1\cdot\alpha=\alpha$. Montrer par récurrence transfinie que pour tous $\alpha,\beta,\gamma\in\aleph_1$, on a $(\alpha\cdot\beta)\cdot\gamma=\alpha\cdot(\beta\cdot\gamma)$ et $\alpha\cdot(\beta+\gamma)=(\alpha\cdot\beta)+(\alpha\cdot\gamma)$. Montrer par contre, que l'on n'a pas nécessairement $\alpha\cdot\beta=\beta\cdot\alpha$ ni $(\alpha+\beta)\cdot\gamma=(\alpha\cdot\gamma)+(\beta\cdot\gamma)$.

Là encore, on a une description en termes d'ensembles dénombrables bien ordonnés. Choisissons α et β deux ordinaux dénombrables et A (resp. B) un ensemble bien ordonné d'ordinal α (resp. β). On peut mettre sur le produit $B\times A$ (attention, on inverse l'ordre) l'ordre lexicographique.

Question 6.3.22. *Montrer que $B\times A$ muni de cet ordre est bien ordonné et qu'il définit ainsi un ordinal γ qui n'est autre que $(\alpha\cdot\beta)$.*

L'exponentiation

L'exponentiation, elle aussi se définit de façon très analogue. Soit $\alpha \in \aleph_1$. On pose $\alpha^0 = 1$. Si β est un ordinal dénombrable successeur, on a $\beta = \beta' + 1$ et on pose $\alpha^\beta = \alpha^{\beta'} \cdot \alpha$. Si β est un ordinal limite, on regarde l'ensemble des ordinaux $\alpha^{\beta'}$ où β' parcourt les ordinaux strictement plus petits que β. On définit alors α^β comme la borne supérieure de cet ensemble.

Question 6.3.23. *Regarder si les propriétés que l'on peut penser vraies le sont effectivement. Calculer* 2^ω, 2^{ω^ω}, 2^{ε_0}.

La description avec les ensembles bien ordonnées est ici un peu plus difficile à donner mais nous n'avons peur de rien. Prenons donc α et β deux ordinaux dénombrables et A et B deux ensembles bien ordonnés d'ordinal respectif α et β. On considère maintenant C l'ensemble des fonctions f de B dans A qui sont telles que le sous-ensemble de B formé des éléments b tels que $f(b) \neq a_0$ (où a_0 est le plus élément de A) soit fini. Sur C, on peut mettre un bon ordre qui est le suivant. Prenons f et g deux fonctions distinctes de C. Dire qu'elles sont distinctes, c'est exactement dire que l'ensemble des $b' \in B$ tels que $f(b') \neq g(b')$ est non vide. D'autre part, d'après les hypothèses faites sur f et g, cet ensemble est fini donc il admet un plus grand élément, disons b. On va dire que $f < g$ si $f(b) < g(b)$ et que $f > g$ dans le cas contraire.

Question 6.3.24. *Montrer que C muni de cet ordre est un ensemble bien ordonné et que l'ordinal de C est précisément α^β.*

Question 6.3.25. *Reprendre le papier sur les jeux de Nim en supposant que le nombre d'anneaux initialement dans les piquets n'est plus un entier mais un ordinal dénombrable quelconque et qu'un coup autorisé ne consiste plus à prendre un certain nombre d'anneaux dans un certain piquet, mais à choisir pour un piquet donné, un ordinal strictement plus petit que celui qui lui était affecté. Montrer que* tous *les résultats annoncés se généralisent directement.*

6.3.6 D'autres opérations peut-être plus sympathiques

Prenons deux ordinaux dénombrables α et β et deux ensembles dénombrables bien ordonnés A et B d'ordinal respectif α et β. Désignons par C l'union disjointe de A et de B. On a mis tout à l'heure un bon ordre sur C en disant que les éléments de A devaient être plus petits que ceux de B mais c'est un peu arbitraire comme choix. Ce qui serait plus équitable serait de regarder tous les bons ordres que l'on peut mettre sur C qui ne contredisent ni l'ordre de A, ni celui de B. Pour chacun de ces bons ordres, on obtient un ordinal et ensuite on peut considérer la borne supérieure de tous les ordinaux que l'on a obtenus ainsi (dont on peut montrer l'existence car l'ensemble considéré est en fait dénombrable). C'est cette dernière que l'on définit comme étant la somme $\alpha \oplus \beta$. On peut faire de même pour le produit. On considère l'ensemble $A \times B$ et on regarde tous les bons ordres que l'on peut y mettre qui sont compatibles avec les ordres de A et de B. Pour chacun, on obtient un ordinal et on considère la borne supérieure de tous ces ordinaux, c'est un nouvel ordinal et c'est celui que l'on appelle $\alpha \otimes \beta$.

On définit ainsi une nouvelle addition et une nouvelle multiplication sur $\aleph_1$ qui a de bien plus jolies propriétés et notamment :

$$\begin{array}{rclcrcl} \alpha \oplus \beta & = & \beta \oplus \alpha & & (\alpha \oplus \beta) \oplus \gamma & = & \alpha \oplus (\beta \oplus \gamma) \\ \alpha \otimes \beta & = & \beta \otimes \alpha & & (\alpha \otimes \beta) \otimes \gamma & = & \alpha \otimes (\beta \otimes \gamma) \end{array}$$

$$\alpha \otimes (\beta \oplus \gamma) = (\alpha \otimes \beta) \oplus (\alpha \otimes \gamma) \qquad (\alpha \oplus \beta) \otimes \gamma = (\alpha \otimes \gamma) \oplus (\beta \otimes \gamma)$$

On obtient ainsi une sorte de prolongement des nombres entiers munis de leurs opérations. À partir de cela, on peut recréer le nombres relatifs qui sont associés à ces nouveaux nombres entiers, puis les

rationnels, puis les réels... Il faut aussi voir qu'il n'existe pas que des ordinaux dénombrables, il existe aussi d'autres ordinaux que l'on construit à peu près de la même manière que celle présentée ici. Et sur ces ordinaux, on peut également mettre des opérations de ce genre, ce qui donne encore plus d'entiers, encore plus de rationnels, encore plus de réels.

6.4 Les jeux de Nim

Le principe du jeu est le suivant. Le plateau de jeu se présente sous la forme d'un certain nombre de piquets plantés dans un morceau de bois. Ces piquets sont destinés à recevoir des petits anneaux. Au début de la partie, on met un certain nombre d'anneaux autour de chacun des piquets, pas forcément le même nombre pour chaque piquet. Chacun son tour, chacun des deux joueurs choisit un piquet et y retire le nombre d'anneaux qu'il souhaite. Le jeu se termine lorsque tous les anneaux ont été retirés, le gagnant étant celui qui a pris le dernier anneau.

Donnons un exemple. Supposons qu'il y ait quatre piquets et qu'au début de la partie, le premier piquet est entouré d'un unique anneau, le second de trois anneaux, le troisième de cinq et le quatrième de sept. Par la suite, on notera cette position par le quadruplet $(1, 3, 5, 7)$. C'est au premier joueur, disons Paul, de jouer. Il choisit le dernier piquet et décide d'y retirer trois anneaux de sorte que l'on arrive dans la position $(1, 3, 5, 4)$. Son adversaire, Pierre, enlève alors les trois anneaux du deuxième piquet. La position est $(1, 0, 5, 4)$. Paul prend alors trois anneaux autour du troisième piquet. La position est $(1, 0, 2, 4)$. Pierre réfléchit et retire un unique anneau du dernier piquet... on arrive dans la position $(1, 0, 2, 3)$. Paul se sent mal, il prend quand même l'anneau restant dans la premier piquet, ce à quoi Pierre répond en enlevant un anneau du dernier piquet. On arrive dans la position $(0, 0, 2, 2)$. Paul abandonne. *Vois-tu pourquoi ?*

Avant de commencer à étudier en détail ce jeu, fixons un peu de vocabulaire. Un *jeu de Nim à n piquets* sera un jeu de Nim dont le plateau de jeu comporte n piquets. Une position est dite *gagnante* si quand un certain joueur arrive dans celle-ci (et donc après avoir joué), il a une stratégie pour finir la partie et la gagner, c'est-à-dire que quelles que soient les réactions de son adversaire, il sait quoi faire pour gagner la partie. La position $(0, \ldots, 0)$ est gagnante car un joueur qui arrive dans cette position a déjà gagné la partie. Si la position initiale d'une partie est gagnante, le deuxième joueur a une stratégie pour gagner. *Pourquoi ?*

Question 6.4.1 (Un peu de logique). *Montrer que si la position initiale d'une partie n'est pas gagnante, alors c'est le premier joueur qui a une stratégie pour gagner.*

Ceci prouve en particulier que si les joueurs savent bien jouer, l'issue de la partie est en fait simplement déterminée par la position initiale. C'est pourquoi, nous allons étudier les positions gagnantes.

6.4.1 Étude des positions gagnantes

Question 6.4.2. *Déterminer toutes les positions gagnantes pour un jeu de Nim à un seul piquet.*

Question 6.4.3. *Montrer qu'une position P est gagnante si et seulement si aucune des positions qui peuvent être atteintes à partir de P en un seul coup n'est gagnante.*

Plaçons-nous alors un instant dans le cas du jeu de Nim à deux piquets. La propriété énoncée dans la question précédente va nous permettre de déterminer facilement toutes les positions gagnantes.

En effet, représentons les positions par le tableau qui suit. Une gros point indique que la position en question est gagnante et une croix qu'elle me l'est pas. Une case non remplie bien entendu indique que l'on ne sait pas (encore) ce qu'il en est. Pour l'instant, on a :

	0	1	2	3	4	5	6
0	•						
1							
2							
3							
4							
5							
6							

On remarque que sur ce tableau les positions qui peuvent être atteintes en un coup à partir de la position P sont exactement celles qui se trouvent soit à gauche, soit en dessus de P. Ainsi la proposition de la question 6.4.3 peut se redire de la façon suivante : une case contient un point si et seulement si toutes les cases qui sont à sa gauche *et* toutes les cases qui sont au-dessus contiennent des croix. Cela implique en particulier que dès qu'une case contient un point, toutes les cases qui sont à sa droite et toutes les cases qui sont en-dessous doivent contenir une croix. Ainsi on peut déjà compléter le tableau de la façon suivante :

	0	1	2	3	4	5	6
0	•	×	×	×	×	×	×
1	×						
2	×						
3	×						
4	×						
5	×						
6	×						

Regardons maintenant la case $(1,1)$. Les cases qui sont à sa gauche et les cases qui sont en dessus contiennent toutes des croix. Ainsi cette case doit contenir un point et on peut continuer la construction du tableau :

	0	1	2	3	4	5	6
0	•	×	×	×	×	×	×
1	×	•	×	×	×	×	×
2	×	×					
3	×	×					
4	×	×					
5	×	×					
6	×	×					

Question 6.4.4. *Montrer rigoureusement à l'aide d'une récurrence que les positions gagnantes sont exactement celles de la forme* (n,n)*. Donner pour une telle position, la stratégie que doit suivre le deuxième joueur pour gagner. Donner pour une position qui n'est pas gagnante, la stratégie que doit suivre le premier joueur pour gagner.*

Question 6.4.5. *Regarder comment cette méthode se généralise pour des jeux de Nim à* n *piquets. Montrer que pour un jeu de Nim à quatre piquets, la position* $(1,3,5,7)$ *est gagnante (et donc que Paul aurait pu abandonner la partie dès le début).*

Si tu es arrivé au bout de la question précédente, tu as dû pouvoir constater que cette méthode théorique n'est pas très facile à mettre en pratique. Nous nous proposons par la suite de donner une méthode de calcul plus simple pour déterminer si une position donnée est gagnante ou non.

6.4.2 Une loi bizarre sur les entiers naturels

Étant donnés deux entiers natuerls x et y, on définit l'entier $x\#y$ comme étant le plus petit entier qui ne se met ni sous la forme $x'\#y$ où x' est un entier naturel strictement plus petit que x, ni sous la forme $x\#y'$ où y' est un entier naturel strictement plus petit que y. Bon, c'est la définition... ça ne paraît vraiment pas simple ni pratique mais essayons quand même de faire des choses avec.

Calculons dans un premier temps $0\#0$. Il s'agit de regarder l'ensemble des entiers qui s'écrivent soit sous la forme $x'\#0$ avec $x' < 0$, soit sous la forme $0\#y'$ avec $y' < 0$. Mais des entiers naturels strictement négatifs, il n'y en a pas et donc quelle que soit la définition de $\#$, l'ensemble que l'on regarde est vide. Le plus petit entier qui n'appartient pas à cet ensemble est donc 0. On a donc calculé $0\#0 = 0$.

Voyons maintenant $0\#1$. L'ensemble à considérer est cette fois $\{0\#0\} = \{0\}$. Le plus petit entier n'étant pas dans cet ensemble est 1. On a donc $0\#1 = 1$. De même, on montre que $1\#0 = 1$.

Question 6.4.6. *Montrer par récurrence que pour tout entier x, $x\#0 = 0\#x = x$.*

Question 6.4.7. *Montrer que pour tous entiers x et y, $x\#y = y\#x$.*

Voyons désormais comment on peut présenter les calculs pour attraper $x\#y$ pour tous x et y de façon relativement simple. Ben encore sous forme de tableau. On a pour l'instant établi cela (bien entendu, l'entier qui est à l'intersubsection de la x-ième ligne et de la y-ième colonne est $x\#y$) :

#	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1						
2	2						
3	3						
4	4						
5	5						
6	6						

La définition dit exactement que l'entier qui doit être écrit dans la case de coordonnées (x, y) est le plus petit entier qui ne se situe pas dans une case à gauche de la case (x, y) ou dans une case au-dessus de la case (x, y). Ainsi, on a $1\#1 = 0$, puis $1\#2 = 3$, $1\#3 = 2$, etc.

Question 6.4.8. *Finir de remplir le tableau...*

On voit que cette construction ressemble en fait beaucoup à ce que l'on faisait tout à l'heure pour résoudre les jeux de Nim. En fait :

Question 6.4.9. *Montrer par récurrence que la position (x, y) est gagnante si et seulement si $x\#y = 0$.*

L'intêret de cette description est qu'elle s'adapte plus facilement pour les jeux de Nim à n piquets. Commençons par trois piquets. On définit la fonction f qui va associer un entier naturel à un triplet d'entiers naturels (qui va correspondre à la position dont on veut savoir si elle est gagnante ou pas) par la propriété suivante : étant donnés x, y et z trois entiers naturels, $f(x, y, z)$ est le plus petit entier naturel qui ne peut se mettre ni sous la forme $f(x', y, z)$ avec $x' < x$, ni sous la forme $f(x, y', z)$ avec $y' < y$, ni sous la forme $f(x, y, z')$ avec $z' < z$.

Question 6.4.10. *Montrer que la fonction f ainsi définie est unique et que la position (x, y, z) est gagnante si et seulement si $f(x, y, z) = 0$.*

Question 6.4.11. *Montrer que les fonctions* $(x,y,z) \mapsto (x\#y)\,\#z$ *et* $(x,y,z) \mapsto x\#\,(y\#z)$ *vérifient la propriété définissant* f*. En déduire que pour tous entiers naturels* x*,* y *et* z *:*

$$f\,(x,y,z) = (x\#y)\,\#z = x\#\,(y\#z)$$

Question 6.4.12. *Généraliser la construction précédente et montrer que la position* $(x_1,\ldots,x_n)$ *d'un jeu de Nim à* n *piquets est gagnante si et seulement si* $x_1\#\ldots\#x_n = 0$*.*

6.4.3 Digression sur la base 2

Tu as sûrement déjà dû remarquer que par exemple :

$$1548 = 1\cdot 1000 + 5\cdot 100 + 4\cdot 10 + 8 = 1\cdot 10^3 + 5\cdot 10^2 + 4\cdot 10^1 + 8\cdot 10^0$$

$$217 = 2\cdot 100 + 1\cdot 10 + 7 = 2\cdot 10^2 + 1\cdot 10^1 + 7\cdot 10^0$$

où $10^n = 10\cdot\ldots\cdot 10$ (n fois) et où par convention $10^0 = 1$.

On peut représenter cette propriété par le tableau suivant :

	10^4	10^3	10^2	10^1	10^0
1548		1	5	4	8
217			2	1	7

Mais le choix de 10 est en fait totalement arbitraire, pourquoi n'a-t-on pas pris un autre nombre ? Sûrement parce que l'on a dix doigts mais il y a pas de raisons mathématiques. En effet, quelque soit le nombre entier $b > 1$, on peut décomposer tout nombre sur les puissances de b comme on vient de le faire avec 10 avec des chiffres qui sont des entiers compris entre 0 et $b-1$. Nous allons regarder en détail le cas $b = 2$ et donc il n'y a que deux chiffres qui sont 0 et 1. Voyons ce que cela donne pour nos deux nombres :

	2^{11}	2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
	2048	1024	512	256	128	64	32	16	8	4	2	1
1548		1	1	0	0	0	0	0	1	1	0	0
217					1	1	0	1	1	0	0	1

Question 6.4.13. *Pourquoi est-ce vraiment cela ? Écrire la décomposition dans le tableau de* 483 *et* 3754*.*

Question 6.4.14. *Montrer que pour tout nombre entier* x*, il existe un unique* n *tel que* $2^n \leqslant x < 2^{n+1}$*. En déduire, grâce à une récurrence, que tout nombre se décompose dans le tableau précédent. Montrer qu'il s'y décompose de façon unique.*

Une façon plus économique de noter la décomposition est la suivante. Par exemple, on écrira $1548 = \overline{11000001100}$ et $217 = \overline{11011001}$. Ceci est *l'écriture en base* 2 des nombres 1548 et 217.

On remarque que l'addition et la multiplication se posent en base 2 comme on a l'habitude de la faire avec des nombres écrits en base 10, il y a juste moins de tables à apprendre. Une seule chose à laquelle il faut faire attention est que l'équivalent de $1+1=2$ en base 2 est $\overline{1}+\overline{1} = \overline{10}$ et donc lorsque l'on a à ajouter $\overline{1}$ et $\overline{1}$, il faut penser à poser $\overline{0}$ et à retenir $\overline{1}$.

Question 6.4.15. *Calculer en base* 2 *et en base* 10 *le produit de* 1548 *par* 217 *et vérifier que l'on trouve deux fois le même résultat.*

On peut faire une autre opération amusante, que l'on appelle souvent le *ou exclusif* sur les entiers en regardant leur écriture en base 2. Considérons x et y deux entiers naturels. À ces deux nombres, on associe l'entier $z = x \$ y$ défini par : le n-ième chiffre (en partant de la droite) de z est 1 si et seulement si le n-ième chiffre (en partant par la droite) de x est 1 ou le n-ième chiffre (en partant par la droite) de y est 1 mais pas les deux. Une autre façon de dire cela est de dire que le n-ième chiffre (en partant par la droite) de z est 1 si et seulement si le n-ième chiffre (en partant par la droite) de x est différent du n-ième chiffre (en partant par la droite) de y. Par exemple, calculons $1548 \$ 217$:

$$\begin{array}{rr} & 11000001100 \\ \$ & 11011001 \\ \hline & 11011010101 \end{array}$$

on obtient $1548 \$ 217 = 1749$.

Question 6.4.16. *Montrer que pour tout entier naturel x, $0 \$ x = x \$ 0 = x$ et que $x \$ x = 0$. Montrer que pour tous entiers naturels x et y, $x \$ y = y \$ x$. Montrer que pour tous entiers naturels x, y et z, $(x \$ y) \$ z = x \$ (y \$ z)$.*

6.4.4 Quand les lois bizarres se rencontrent

Je sais que tu vas être troublé mais en fait les deux lois étranges que l'on vient de définir sur les entiers naturels sont exactement les mêmes. Ce que je veux dire, c'est que pour tous les entiers x et y, on a $x\#y = x \$ y$. Ceci fournit donc un moyen assez simple de calculer $x\#y$, ce qui permet de reconnaître les positions gagnantes de façon relativement simple. Mais essayons de voir pourquoi ce que je raconte est vrai.

En fait, pour voir cela, il suffit de démontrer que la loi $\$$ vérifie la même propriété que celle qui définit la loi $\#$. Autrement dit, il suffit de montrer que pour tous entiers naturels x et y, $x \$ y$ est le plus petit entier qui ne peut se mettre ni sous la forme $x' \$ y$ avec $x' < x$, ni sous la forme $x \$ y'$ avec $y' < y$. Introduisons des notations. Appellons A_1 l'ensemble des entiers de la forme $x' \$ y$ pour $x' < x$ et A_2 l'ensemble des entiers de la forme $x \$ y'$ pour $y' < y$. Posons $A = A_1 \cup A_2$. Avec ces conventions, il s'agit de voir que le plus petit entier n'appartenant pas à A est $x \$ y$.

Question 6.4.17. *Montrer que si $x' \$ y = x \$ y$, alors $x' = x$. De même prouver que si $x \$ y' = x \$ y$, alors $y' = y$. En déduire que $x \$ y \notin A$.*

Question 6.4.18. *Soit a un entier naturel strictement plus petit que $x \$ y$. En regardant le premier chiffre qui est différent dans l'écriture en base 2 de $x \$ y$ et de a, montrer que l'on a soit $a \$ x < y$, soit $a \$ y < x$. En déduire que $a \in A$. Conclure.*

Question 6.4.19. *Retrouver de façon simple que la position $(1, 3, 5, 7)$ du jeu de Nim à quatre piquets est gagnante.*

6.4.5 Les jeux de Nim de dimension supérieure

On peut formuler différemment le jeu de Nim que nous venons d'étudier. Le plateau de jeu se présente alors comme une suite infinie de trous qui vont être amenés à recevoir des billes. Ces trous sont numérotés, ie il y a le premier, le deuxième, etc. et ces trous sont rangés de gauche à droite par ordre croissant. Au début de la partie, un certain nombre de trous (fini) contient des billes, les autres trous sont vides. Lorsqu'un joueur joue, il choisit un trou contenant une bille, enlève cette bille, choisit ensuite un autre trou plus à gauche et y dépose la bille qu'il vient de prendre si celui-ci est vide alors que si celui-ci est

plein, il prend la bille qui est dedans et retire les deux billes qu'il a prises du jeu. Un joueur gagne quand son adversaire ne peut plus jouer (c'est-à-dire lorsqu'il ne reste plus de billes, ou qu'une seule bille dans le premier trou).

Question 6.4.20. *Expliquer pourquoi ce jeu est équivalent au jeu de Nim tel qu'on l'a décrit précédemment.*

L'intêret de cette présentation un peu moins visuelle est qu'elle se généralise en dimension supérieure de façon assez simple. Je vais juste présenter ici ce qu'il en est en dimension 2. Le jeu se joue toujours à deux. Le plateau de jeu est alors un quart de plan, disons le quart supérieur-droit, où il y a des trous à tous les points de coordonnées entières. Au début de la partie, certains de ces trous (un nombre fini) contiennent des billes, les autres sont vides. Lorsqu'un joueur joue, il choisit un trou contenant une bille, disons que c'est celui de coordonnée (x, y). Il enlève cette bille. Il choisit ensuite une case située à gauche et en dessous de la case dans laquelle il vient de prendre la bille. Si l'on note (x', y') les coordonnées de cette case, la condition de position se traduit par le fait que $x' < x$ et $y' < y$. Pour chacune des cases (x', y'), (x', y) et (x, y'), il inverse l'état de la case... autrement dit, il enlève la bille présente si la case était pleine ou en ajoute une si elle était vide. Un joueur gagne lorsque son adversaire ne peut plus jouer.

Question 6.4.21. *Montrer qu'une partie d'un tel jeu se termine nécessairement.*

Pour étudier ce nouveau jeu, il a été introduit une autre loi, $@$, sur les entiers naturels. Elle est définie de la façon suivante. Étant donnés deux entiers naturels x et y, $x@y$ est défini comme étant le plus petit entier naturel qui ne peut pas s'écrire sous la forme $(x'@y) \# (x'@y') \# (x@y')$ pour $x' < x$ et $y' < y$. Cette loi a des propriétés étonnantes. Notamment, elle est telle que $(\mathbb{N}, \#, @)$ est un corps de caractéristique 2 et même le plus petit corps de caractéristique 2 sur lequel tous les équations de degré 2 ont des solutions. Bon, je ne pense pas que cela te parle beaucoup mais je tenais à le dire...

Quatrième partie

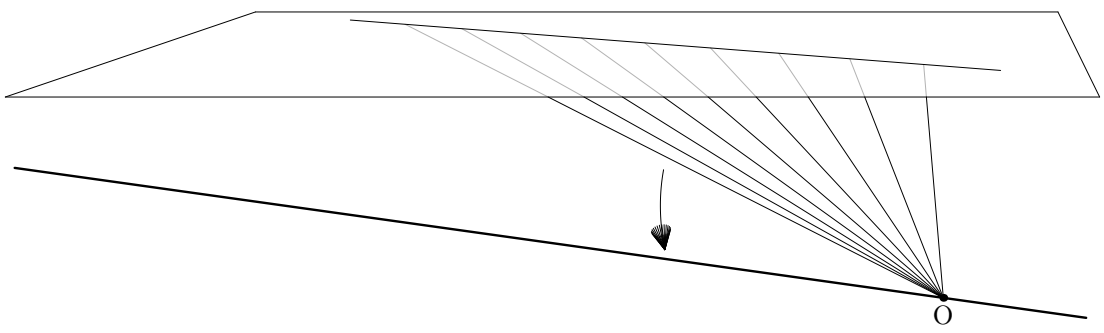
Informatique

Chapitre 7

Un package 3D pour Métapost

J'ai développé ce package après mettre rendu compte après avoir tapé le sujet de réflexion sur le **Plan projectif** (cf paragraphe 6.2) que peu de logiciels étaient disponibles pour insérer des figures en 3D dans un document.

Sommaire



`3d.mp` est un ensemble de macros permettant de créer de façon relativement simple des figures en trois dimensions avec MetaPost. En particulier, comme nous allons le voir, il s'occupe tout seul de dessiner différemment les arêtes cachées et permet de changer d'angle de vue par une simple commande.

7.1 Comment utiliser ce package ?

Pour utiliser les macros définies dans ce package, il suffit d'inclure dans vos fichiers MetaPost le fichier `3d.mp` au moyen de la commande suivante :

```
input 3d.mp;
```

Signalons tout de suite qu'afin d'éviter les risques de conflits, les noms des variables globales utilisées ainsi que ceux des macros définies[1] commencent tous par le préfixe `td`.

7.2 Deux moyens de se repérer dans l'espace

7.2.1 Le type `td_coords`

`3d.mp` définit un nouveau type de variable qui porte le nom de `td_coords`[2]. Celui-ci consiste en des triplets de `numeric` que l'on peut additionner et multiplier par des scalaires. Il est possible d'accéder aux composantes d'un `td_coords` via les fonctions `td_x`, `td_y` et `td_z`. Pour ses propres besoins, le package `3d.mp` définit quelques opérations sur les variables de ce nouveau type. Il est peut-être utile de les présenter :

- `td_pdtscal(u,v)` : retourne le produit scalaire de `u` et `v`
- `td_pdtvect(u,v)` : retourne le produit vectoriel de `u` par `v`
- `td_norme(u)` : retourne la norme du vecteur `u`
- `td_unite(u)` : retourne le vecteur unitaire qui a la même direction et le même sens que `u`
- `td_projnorm(u,n)` : retourne le projeté du vecteur `u` sur un plan normal au vecteur `n`

7.2.2 Repérage des plans

Un plan P de l'espace est repéré par trois variables de type `td_coords` que l'on désignera par la suite par les lettres `i`, `j` et `o` qui correspondent respectivement à deux vecteurs qui forment une base de notre plan P et un point O qui appartient à P.

Un point de P pourra être repéré simplement par la donnée d'une variable de type `pair` une fois connu le plan P. On dispose ainsi d'un second moyen pour repérer les points de l'espace : un point M de l'espace est repéré par trois variables de type `td_coords` et une variable de type `pair`, les trois premières variables servant à déterminer un plan P auquel M appartient et la dernière servant à préciser où se situe M sur ce plan.

Le fichier `3d.mp` possède une macro permettant de déterminer la *position absolue* d'un point M à partir de la donnée des quatre variables décrites précédemment. Il s'agit de la fonction `td_ddtotd` qui prend pour argument dans l'ordre `i`, `j`, `o` puis `u` où `u` est la variable de type `pair` qui sert à repérer la position de M dans la plan.

Il existe ici aussi quelques macros permettant d'effectuer des opérations sur les vecteurs lorsqu'ils sont repérés de la façon précédente. Il s'agit de :

- `td_projdir(i,j,o,m)` donne les coordonnées dans le plan défini par `i`, `j` et `o` du projeté orthogonal du point de position absolu `m` dans ce plan

[1] Liste consultable en annexe.

[2] Il s'agit en fait simplement d'une redéfinition du type `color`.

– `td_pcentdir(i,j,o,c,m)` donne les coordonnées dans le plan défini par `i`, `j` et `o` de l'image du point de position absolue `m` par la projection de centre le point défini par `c` sur le plan évoqué précédemment

7.3 Fonctions de base

7.3.1 Segments

L'appel de la fonction `td_ligneabs(a,b)` permet de tracer un segment reliant la point de position absolue `a` à celui de position absolue `b`. Pour illustrer cela regardons le code suivant qui dessine les douze arêtes d'un cube :

```
td_beginfig(1);
  td_ech:=3cm;
  td_coords A,B,C,D,E,F,G,H;
  A:=(0,0,0); B:=(0,1,0); C:=(1,1,0); D:=(1,0,0);
  E:=(0,0,1); F:=(0,1,1); G:=(1,1,1); H:=(1,0,1);
  td_ligneabs(A,B); td_ligneabs(B,C); td_ligneabs(C,D); td_ligneabs(D,A);
  td_ligneabs(E,F); td_ligneabs(F,G); td_ligneabs(G,H); td_ligneabs(H,E);
  td_ligneabs(A,E); td_ligneabs(B,F); td_ligneabs(C,G); td_ligneabs(D,H);
td_endfig;
```

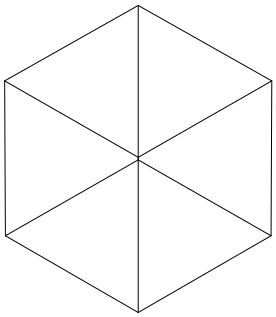


Figure 1

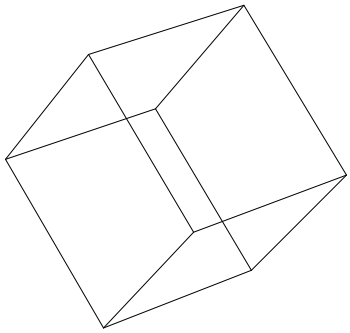


Figure 2

Le résultat produit est celui de la figure 1. Il est nécessaire de faire quelques commentaires. Tout d'abord l'emploi des macros habituelles `beginfig` et `endfig` a été remplacé par `td_beginfig` et `td_endfig`. Elles fonctionnent de la même manière à l'exception qu'elles font certaines choses en plus comme la mise à jour de certaines variables globales dont se servent les autres macros du package. Il est également important de noter que les macros appelées pour faire des dessins comme `td_ligneabs` ne dessinent en fait pas réellement sur le fichier PostScript final mais plutôt dans deux variables globales de type `picture` répondant au nom de `td_aretes` et `td_aretescachees` et c'est seulement à l'appel de la macro `td_endfig` que celles-ci sont effectivement dessinées. Il est toutefois possible de récupérer le dessin déjà constitué par l'intermédiaire de la macro `td_image` qui retourne ce-dit dessin.

Une autre remarque est l'apparition de la variable globale `td_ech`. Il s'agit simplement d'une variable de type `numeric` qui représente la longueur des vecteurs unitaires.

On remarquera que malheureusement il est nécessaire de déclarer toutes les variables de type `td_coords` qui apparaissent. En effet, si cela n'est pas fait, MetaPost va croire bêtement qu'il s'agit de variables de type `pair` et va produire une erreur.

Il est assez souvent commode d'utiliser le raccourci

```
td_ligneabs(A,B,C,D,A);
```

qui est équivalent à

```
td_ligneabs(A,B); td_ligneabs(B,C); td_ligneabs(C,D); td_ligneabs(D,A);
```

Ainsi le code que nous avons fourni peut-être un peu raccourci, devenant ainsi même plus lisible.

Il existe une autre façon de tracer des segments qui utilise le repérage relatif des points dans l'espace. Elle se concrétise via la commande `td_ligne(i,j,o,m1,m2,...)` qui permet de tracer les segments M_iM_{i+1} où les `m.i` sont des variables de type `pair` qui correspondent aux coordonnées des points M_i dans le plan repéré par `i`, `j` et `o`. Il est également possible d'utiliser la macro `td_ligne_(m1,m2,...)` qui utilise les variables globales `td_i_enc`, `td_j_enc` et `td_o_enc` pour savoir dans quel plan les segments doivent être tracés. Par défaut, `td_i_enc` est initialisé à `(1,0,0)`, `td_j_enc` à `(0,1,0)` et `td_o_enc` à `(0,0,0)`, mais bien entendu il est possible de les changer. Toutefois, un appel à `td_beginfig` rendra à ces variables leur valeur d'origine.

7.3.2 Changer d'angle de vue

Le résultat de la figure 1 n'est pas extraordinaire. En effet, l'on n'arrive pas à distinguer grand chose tant les arêtes sont les unes sur les autres. Pour palier à cela, il faudrait regarder le cube depuis un autre endroit. Ceci peut se faire à l'aide de la commande `td_anglevue(oeil,direction,angle)`. `oeil` est une variable de type `td_coords` qui correspond à la position de l'œil qui regarde la figure. `direction` est également une variable de type `td_coords` qui correspond à un vecteur. La direction de celui-ci fournit la direction du regard alors que sa norme fournit le facteur d'échelle avec lequel l'œil est capable de voir. Quant à `angle`, il s'agit d'une variable de type `numeric` qui correpond à l'angle (exprimé en degré) duquel est tourné l'œil. Un angle de 0 degré correspond à un œil dont le bas est dirigé vers les z négatifs.

Par exemple, la figure 2 est obtenue simplement en rajoutant au début du code présenté précedemment la ligne

```
td_anglevue((-10,-8,-3),(10,7,2),30);
```

Il est important de noter que la fonction `td_anglevue` modifie des variables globales qui sont ensuite réutilisées par les macros de dessin telles `td_ligneabs`. Il est donc fortement conseillé de faire appel à la macro `td_anglevue` (et de même par exemple de définir la valeur de `td_ech`) avant de commencer à dessiner quoi que ce soit. Par défaut la position de l'œil est mise à `(-60,-60,60)`, la direction du regard est à `(50,50,-50)` et l'angle de l'œil est de 0 degré. Cela correspond plus ou moins à une perspective isométrique.

Finalement, il est peut-être mieux de placer l'œil suffisamment loin de la figure pour ne pas trop altérer les droites parallèles, cela pouvant paraître choquant au premier abord.

7.3.3 Courbes

Il est possible de tracer des courbes pourvu que celles-ci soient contenues dans un plan. Ceci se fait simplement par l'appel de la fonction `td_courbe(i,j,o,p)`. Les `td_coords` `i`, `j` et `o` servent à préciser le plan dans lequel la courbe doit être tracée, alors que le `path` `p` est précisément la courbe à tracer. Là encore, il y a la macro `td_courbe_(p)` qui trace le `path` `p` dans le plan courant défini par les variables globales `td_i_enc`, `td_j_enc` et `td_o_enc`. Par exemple, la commande

```
td_courbe_(fullcircle scaled 5);
```

trace un cercle de diamètre 5 et de centre l'origine du repère dans le plan horizontal (si l'on n'a rien redéfini).

Voici un code permettant de dessiner une figure ressemblant à une sphère :

```
td_beginfig(3);
  td_anglevue((0,50,0),(0,-200,0),85);
  td_precision:=50;
  td_option(withcolor 0.6white);

  for t=0 step 5 until 360:
    td_j_enc:=(0,cosd(t),sind(t));
    td_courbe_(fullcircle);
  endfor
td_endfig;
```

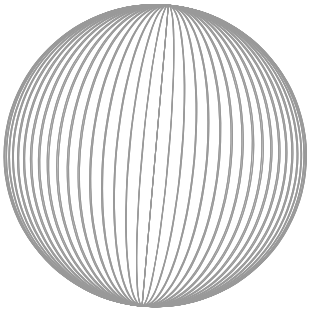


Figure 3

Là encore, il nous faut faire quelques commentaires. Tout d'abord, on remarque l'apparition de la variable globale `td_precision`. Celle-ci indique le nombre de points qui vont être considérés lors du tracé d'une courbe. Par défaut, elle vaut 500 mais ici il a été préférable de la réduire étant donné que le nombre de courbes à tracer n'est pas petit. Une grande précision fait rapidement augmenter le temps de calcul et la taille du fichier produit.

Il y a ensuite l'appel à la macro `td_option`. Ceci permet de définir avec quel style on souhaite faire les tracés ultérieurs. On notera qu'il est inutile de faire des appels à `pickup` ou à `drawoptions`, ceci n'affectant que le comportement de la macro `draw` qui n'est point utilisée dans le package `3d.mp`.

7.3.4 Flèches

Il existe tout un tas de macros pour dessiner des flèches soit au bout de segments, soit au bout de courbes. La liste exhaustive est la suivante :

- `td_ligneflecheabs`
- `td_lignefleche`
- `td_lignefleche_`
- `td_ligneflecheiabs`
- `td_ligneflechei`
- `td_ligneflechei_`
- `td_ligneflechesabs`
- `td_lignefleches`
- `td_lignefleches_`
- `td_courbefleche`
- `td_courbeflechei`
- `td_courbefleches`

Les fonctions précises de ces macros s'intuitent très facilement. Il suffit pour cela de savoir que `fleche` permet d'ajouter une flèche au bout, `flechei` une flèche au début et `fleches` une au bout et une au début.

Des variables globales permettent de contrôler la taille et l'allure des flèches. Il s'agit de `tdfleche_long` qui renferme la longueur *longitudinale* de la flèche, de `tdfleche_norm` qui renferme la longueur *normale* de la flèche et finalement de `tdfleche_nb` qui donne le nombre de petits segments qui partent du sommet et qui vont former la flèche[3]. Par défaut `tdfleche_long` est initialisé à 0.6, `tdfleche_norm` à 0.2 et `tdfleche_nb` à 25. Un appel à `td_beginfig` reinitialise les valeurs de ces constantes.

Et voici un joli trièdre direct :

[3]On remarquera en particulier que le design des flèches en trois dimensions n'a rien à voir avec celui des flèches en deux dimensions... Il ne faut pas mélanger les torchons et les serviettes, voyons !

```
td_beginfig(4);
  td_coords O,I,J,K;
  O:=(0,0,0); I:=(1,0,0);
  J:=(0,1,0); K:=(0,0,1);
  td_ligneflechesabs(4I,O,4J);
  td_ligneflecheabs(O,4K);
td_endfig;
```

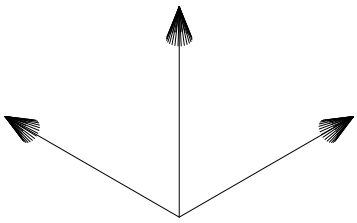


Figure 4

7.4 Surfaces

Un certain nombre de surfaces *planes* peuvent être définies. L'intêret de définir une surface, plutôt que de tracer les arêtes qui constituent son bord, est que l'ordinateur saura par la suite que la partie qui se trouve à l'intérieur de ces arêtes est composée de matière. Ainsi les tracés qui seront cachés à l'œil par cette matière vont être dessinés de façon différente. Mais voyons tout de suite comment cela fonctionne.

7.4.1 Surfaces rectangulaires, plans

Le premier type de surface que l'on peut définir sont les surfaces rectangulaires. Ceci se fait grâce à la commande `td_nouveauplan(i,j,o,m,M)`. Les premiers paramètres `i`, `j` et `o` permettent de désigner le plan de travail. `m` correspond aux coordonnées dans le plan précédent du point inférieur gauche du rectangle tandis que `M` correspond aux coordonnées du point supérieur droit. En réalité chaque surface est repérée par un entier qui lui est affecté lors de sa création. Ainsi l'appel à la fonction précédente retourne une valeur de type `numeric` qui est le numéro de la surface créée. On n'a souvent que faire de cette valeur mais afin d'éviter une erreur de compilation, il est bon d'utiliser la tournure suivante :

```
whatever=td_nouveauplan(i,j,o,m,M);
```

Il existe également la fonction `td_nouveauplan_` qui utilise les valeurs de `td_i_enc`, `td_j_enc` et `td_o_enc` pour se repérer.

Il est bien entendu également possible de dessiner ces surfaces. C'est en fait fort simple : pour dessiner la surface repérée par le numéro `i`, il suffit d'entrer la commande

```
td_surface(i);
```

Un appel à `td_surfaces` dessinera toutes les surfaces définies.

Regardons le code qui suit.

```
td_beginfig(5);
  td_anglevue((60,-30,30),(-30,15,-15),0);
  td_ech:=0.5cm;

  td_coords O,I,J,K;
  O:=(0,0,0); I:=(1,0,0); J:=(0,1,0); K:=(0,0,1);
  whatever=td_nouveauplan(I,J,O,(0,0),(10,10));
  whatever=td_nouveauplan(J,K,O,(0,0),(10,10));
  td_surfaces;
  for i=1 upto 9: td_ligneabs((-8,i,12),(12,5,-5)); endfor
td_endfig;
```

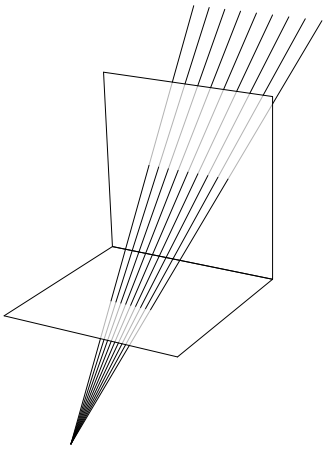


Figure 5

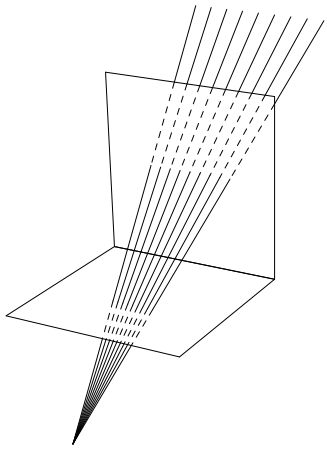


Figure 6

Il produit le dessin de la figure 5. On voit que par défaut les arêtes cachées sont tracées en gris clair. Il est cependant tout à fait possible de modifier ce comportement. Ceci se fait grâce à la commande `td_cachees`. Par exemple la figure 6 a été obtenu en rajoutant simplement au début du code précédent la ligne

```
td_cachees(dashed evenly scaled 0.8);
```

Il est aussi possible de masquer totalement les arêtes cachées grâce à la commande

```
td_cachees(withcolor background);
```

ou encore mieux (car dans ce cas les arêtes ne sont pas du tout dessinées) en utilisant les macros

```
td_masquees;
td_nonmasquees;
```

Il faut noter qu'un appel à `td_beginfig` redonne le style par défaut aux arêtes cachées.

7.4.2 Surfaces polygonales

Les surfaces polygonales planes se définissent avec `td_nouvellesurf(i,j,o,m1,m2,...)`. Là encore, `i`, `j` et `o` servent à définir le plan dans lequel la surface va vivre tandis que les `m.i` correspondent aux coordonnées dans ce plan des sommets du polygone délimitant notre surface. Là encore, l'appel à cette fonction retourne une valeur qui correspond au numéro de la surface et si l'on ne veut pas le garder l'utilisation de `whatever` est un bon compromis. Là encore, on peut utiliser la macro `td_nouvellesurf_` qui permet de se dispenser de la donnée de `i`, `j` et `o`.

Le comportement de ces macros n'est pas du tout garanti dans les cas suivants (NDLR : remarquez que la réciproque n'est pas énoncée...) :
- la surface définie a une aire nulle
- la surface définie n'est pas un polygone convexe
- les sommets de ce polygone ne sont pas donnés dans l'ordre

On peut par exemple reprendre l'exemple précédent en tronquant quelque peu le plan vertical :

```
td_beginfig(7);
  td_anglevue((60,-30,30),(-30,15,-15),0);
  td_ech:=0.5cm; td_masquees;
  td_coords O,I,J,K;
  O:=(0,0,0); I:=(1,0,0);
  J:=(0,1,0); K:=(0,0,1);
  whatever=td_nouveauplan(I,J,O,(0,0),(10,10));
  whatever=td_nouvellesurf(J,K,O,
           (0,0),(10,0),(10,10));
  td_surfaces;
  for i=1 upto 9:
    td_ligneabs((-8,i,12),(12,5,-5));
  endfor
td_endfig;
```

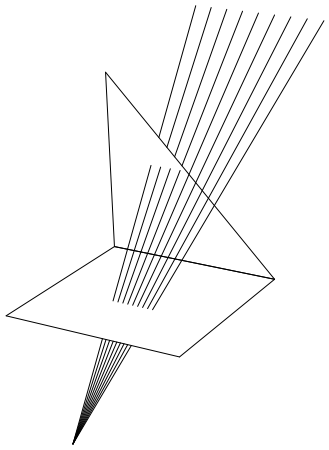


Figure 7

On peut aussi définir des surfaces polygonales en donnant les sommets en position absolue. La syntaxe est alors `td_nouvellesurfabs(m1,m2,...)` où les `m.i` sont ce coup-ci des `td_coords`. Cependant, il n'est pas possible de faire n'importe quoi, la surface définie doit être plane. Si les points `m.i` ne sont pas coplanaires, ceux-ci seront projetés sur le plan défini par les premiers points.

Notez à ce propos qu'il n'existe aucune macro permettant de calculer les `i`, `j` et `o` définissant un certain plan lorsque celui-ci est donné par exemple par un point et une normale ou par trois points non alignés... Mais il ne tient qu'à vous de les créer. On peut par exemple écrire :

```
def normtodir(expr i,j,n) =
  save u; td_coords u; u:=td_unite(n);
  if (td_x(u)=0) and (td_y(u)=0): j:=(0,1,0); else:
    j:=td_unite(td_projnorm((0,0,-1),u));
  fi
  i:=td_unite(td_pdtvect(u,j));
enddef;

def pointstodir(expr i,j,o,a,b) =
  i:=td_unite(a-o);
  j:=td_unite(td_projnorm(b-o,i));
enddef;
```

Je ne sais pas trop s'il est mieux de faire les quelques tests qui s'imposent (comme vérifier que le vecteur `n` est non nul ou que les points `o`, `a` et `b` ne sont pas alignés) avant de faire le calcul proprement dit. Cela permettrait sans aucun doute d'avoir un message d'erreur un peu plus explicite lors de la compilation mais ralentirait sans doute aussi beaucoup le temps nécessaire à celle-là. L'attitude choisie dans toutes les macros du package `3d.mp` est de ne faire aucun test.

Mais revenons à nos moutons.

Donnons un exemple d'utilisation de la macro `td_nouvellesurfabs`. Elle peut servir à tracer de façon simple un cube plein, un résultat à comparer avec la figure 2.

```
td_beginfig(8);
  td_anglevue((-10,-8,-3),(10,7,2),30);
  td_ech:=4cm;
  td_coords A,B,C,D,E,F,G,H;
  A:=(0,0,0); B:=(0,1,0);
  C:=(1,1,0); D:=(1,0,0);
  E:=(0,0,1); F:=(0,1,1);
  G:=(1,1,1); H:=(1,0,1);
  whatever=td_nouvellesurfabs(A,B,C,D);
  whatever=td_nouvellesurfabs(E,F,G,H);
  whatever=td_nouvellesurfabs(A,B,F,E);
  whatever=td_nouvellesurfabs(B,C,G,F);
  whatever=td_nouvellesurfabs(C,D,H,G);
  whatever=td_nouvellesurfabs(D,A,E,H);
  td_surfaces;
td_endfig;
```

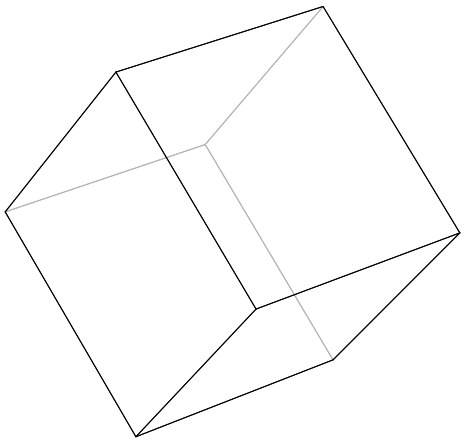
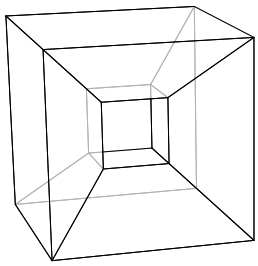


Figure 8

Et même des figures plus compliquées comme un cube troué :



obtenu par le code suivant :

```
td_beginfig(9);
  td_anglevue((20,-60,20),(-10,30,-10),0);
  td_ech:=0.6cm;

  td_coords A,B,C,D,E,F,G,H,Ap,Bp,Cp,Dp,Ep,Fp,Gp,Hp;
  A:=(0,0,0); B:=(0,9,0); C:=(9,9,0); D:=(9,0,0);
  E:=(0,0,9); F:=(0,9,9); G:=(9,9,9); H:=(9,0,9);
  Ap:=(3,3,3); Bp:=(3,6,3); Cp:=(6,6,3); Dp:=(6,3,3);
  Ep:=(3,3,6); Fp:=(3,6,6); Gp:=(6,6,6);  Hp:=(6,3,6);

  whatever=td_nouvellesurfabs(A,B,C,D);
  whatever=td_nouvellesurfabs(E,F,G,H);
  whatever=td_nouvellesurfabs(A,B,F,E);
  whatever=td_nouvellesurfabs(C,D,H,G);
  whatever=td_nouvellesurfabs(Ap,Bp,Cp,Dp);
  whatever=td_nouvellesurfabs(Ep,Fp,Gp,Hp);
  whatever=td_nouvellesurfabs(Ap,Bp,Fp,Ep);
  whatever=td_nouvellesurfabs(Cp,Dp,Hp,Gp);
```

```
  whatever=td_nouvellesurfabs(D,A,Ap,Dp);
  whatever=td_nouvellesurfabs(H,E,Ep,Hp);
  whatever=td_nouvellesurfabs(B,C,Cp,Bp);
  whatever=td_nouvellesurfabs(F,G,Gp,Fp);
  whatever=td_nouvellesurfabs(A,E,Ep,Ap);
  whatever=td_nouvellesurfabs(D,H,Hp,Dp);
  whatever=td_nouvellesurfabs(B,F,Fp,Bp);
  whatever=td_nouvellesurfabs(C,G,Gp,Cp);
  td_surfaces;
td_endfig;
```

7.4.3 Surfaces définies par une courbe

Finalement, il est possible de définir une surface par une courbe plane. La syntaxe pour faire cela est `td_nouvellesurfc(i,j,o,p)` où `i`, `j` et `o` sont comme d'habitude les `td_coords` qui servent à repérer le plan de travail et où `p` est la variable de type `path` définissant la courbe dans ce plan. Là encore, on peut utiliser la fonction `td_nouvellesurfc_(p)`. Là encore, le comportement de la macro n'est pas défini si la surface délimitée par la courbe est d'aire nulle ou n'est pas convexe.

Signalons qu'en fait une telle surface n'est autre qu'une surface polygonale avec un grand nombre de côtés. ce nombre est précisé dans la variable globale `tdsurf_precision` et vaut par défaut 100.

Un autre comportement particulier de ce genre de surfaces est à décrire. En effet, elles ne sont par défaut pas tracées par l'appel de la fonction `td_surfaces`. Ceci simplement parce qu'un polygône à 100 côtés c'est certes une bonne approximation de notre surface mais peut-être en fait pas suffisamment précise pour donner lieu à une jolie courbe régulière. En fait, le fait qu'un contour de surface soit tracé ou non par la commande `td_surfaces` est déterminé par le tableau global de booléens `tdsurf_dessin[]`. Par défaut une surface créée par l'intermédiaire de `td_nouvellesurfc` renseigne ce tableau en mettant un `false` à l'indice adéquat, tandis que les appels à `td_nouvellesurf` et `td_nouveauplan` positionne un `true` dans ce tableau. Ainsi un moyen de faire en sorte que `td_surfaces` dessine effectivement les surfaces définies à partir de courbe est de les déclarer par la commande

```
tdsurf_dessin(td_nouvellesurfc(i,j,o,p)):=true;
```

mais il est sans doute préférable de tracer la courbe par un moyen alternatif.

7.5 Autres fonctions

7.5.1 Projections orthogonale et centrale

On a déjà vu qu'il était défini des macros permettant de calculer l'image d'un vecteur dans une projection orthogonale ou une projection centrale. L'équivalent de ces macros existe également pour des courbes. Il s'agit de `td_projc(i,j,o,i',j',o',p)` et de `td_pcentc(i,j,o,i',j',o',c,p)`. `i`, `j` et `o` servent à repérer le plan dans lequel se trouve la courbe `p` avant d'être projeté. `i'`, `j'` et `o'` définissent le plan de projection, et dans le cas d'une projection centrale `c` est une variable de type `td_coords` donnant la position absolue du centre de la projection.

```
td_beginfig(10);
  td_anglevue((10,-100,30),(-2,60,-15),0);
  td_ech:=0.2cm;

  path p,q;
  td_coords i,j,u,A,O;
  i:=(1,0,0); j:=(0,1,0); u:=(1,0,1); A:=(45,5,-20); O:=(0,0,0);

  whatever=td_nouveauplan(i,j,O,(0,-5),(47,15));
  whatever=td_nouveauplan(u,j,O,(0,-5),(25,15));
  td_surfaces;

  p:=fullcircle scaled 5 shifted (30,5); td_courbe(i,j,O,p);
  q:=td_pcentc(i,j,O,u,j,O,A,p); td_courbe(u,j,O,q);

  for z=0 upto 40:
    td_ligneabs(A,td_ddtotd(u,j,O,point z/40*length(q) of q));
  endfor
td_endfig;
```

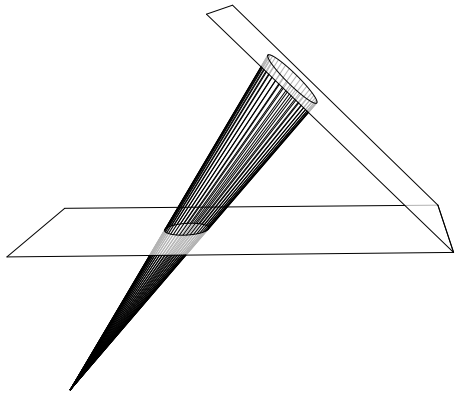


Figure 10

7.5.2 Insertion d'une image

Il est possible d'insérer une variable de type `picture` n'importe où sur la dessin. La commande pour faire cela est `td_insere(p,o)` où `o` est la position absolue du point qui va correspondre au centre de l'image `p` à insérer. L'image insérée ne subira aucune modification, elle sera juste posée à l'endroit demandé.

Une application de cela est sûrement la nomination des points ou des droites ou des plans d'une figure. En effet, placer la lettre "O" à l'origine se fait simplement par la commande suivante

```
td_insere(thelabel.bot("O",(0,0)),(0,0,0))
```

qui peut être raccourcie en

```
td_label.bot("O",(0,0,0));
```

Les macros `td_labels`, `td_dotlabel` et `td_dotlabels` sont également définies. Par exemple la figure 11 s'obtient simplement en rajoutant la ligne

```
td_dotlabels.rt(A);
```

à la fin du code précédent.

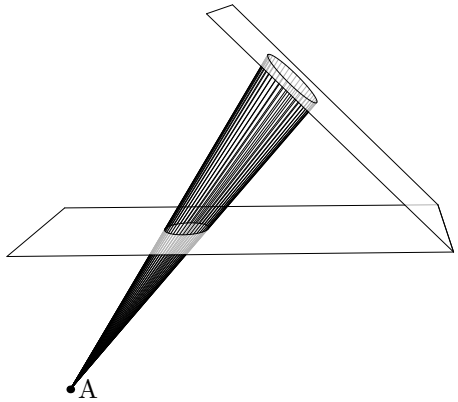


Figure 11

Ainsi ce sont bien les variables globales `laboff`, `labxf`, `labyf` et `dotlabeldiam` ou encore `defaultfont` et `defaultscale` qui sont utilisées et par conséquent ce sont bien elles qu'il faut mettre à jour. D'ailleurs ce serait peut-être bon de le faire ici.

7.6 Bogues

Il y en a sûrement plein... à chaque fois que je compile quelque chose j'en trouve un nouveau. N'hésitez surtout pas à me les signaler à <`caruso@clipper.ens.fr`>. Il y a aussi quelques manques : tout d'abord, je ne suis pas satisfait de la façon dont est gérée l'annotation. Ensuite, il serait bien de pouvoir travailler avec des surfaces pas forcément planes, et faire des opérations sur icelles comme l'intersection. Finalement (enfin non sûrement pas), les macros servant à tracer les courbes pourraient ne pas se contenter de prélever quelques points sur celles-ci mais se préoccuper en outre des tangentes en ces points, permettant ainsi d'avoir de plus belles courbes avec moins de calcul. Mais bon, complète qui voudra.

Sinon, également quelques trucs grotesques comme les noms de macros et des variables qui sont en français à l'exception de `td_beginfig`, `td_endfig`, `td_label` et ses dérivés, mais je n'ai pas envie de corriger ça maintenant.

Annexes

Liste des variables globales

Nom de la variable	Type
td_aretes	picture
td_aretescachees	picture
td_bas	td_coords
td_direction	td_coords
td_ech	numeric
td_i	td_coords
td_i_enc	td_coords
td_j	td_coords
td_j_enc	td_coords
td_masq	boolean
td_o_enc	td_coords
td_oeil	td_coords
td_options	text
td_pointilles	text
td_precision	td_coords
td_zero	numeric
tdfleche_long	numeric
tdfleche_nb	numeric
tdfleche_norm	numeric
tdsurf_dessin[]	boolean
tdsurf_i[]	td_coords
tdsurf_indice	numeric
tdsurf_j[]	td_coords
tdsurf_nb[]	numeric
tdsurf_o[]	td_coords
tdsurf_precision	numeric
tdsurf_sommets[][]	td_coords

Liste des macros

Nom de la macro	Type des arguments	Valeur de retour
td_anglevue	(td_coords,td_coords,numeric)	
td_beginfig	(numeric)	
td_cachees	(text)	
td_courbe	(td_coords,td_coords,td_coords,path)	
td_courbe_	(path)	
td_courbefleche	(td_coords,td_coords,td_coords,path)	
td_courbeflechei	(td_coords,td_coords,td_coords,path)	
td_courbefleches	(td_coords,td_coords,td_coords,path)	
td_ddtotd	(td_coords,td_coords,td_coords,pair)	td_coords
td_det	(pair,pair)	numeric
td_dotlabel	(string,td_coords)	
td_dotlabels	(string,...)	
td_endfig		
td_fleche	(td_coords,td_coords)	
td_image		picture

Nom de la macro	Type des arguments	Valeur de retour
td_init		
td_insere	(picture,td_coords)	
td_label	(string,td_coords)	
td_labels	(string,...)	
td_ligne	(td_coords,td_coords,td_coords,pair,...)	
td_ligne_	(pair,...)	
td_ligneabs	(td_coords,...)	
td_ligneabs__	(td_coords,td_coords)	
td_lignefleche	(td_coords,td_coords,td_coords,pair,...)	
td_lignefleche_	(pair,...)	
td_ligneflechei	(td_coords,td_coords,td_coords,pair...)	
td_ligneflechei_	(pair,...)	
td_ligneflecheiabs	(td_coords,...)	
td_lignefleches	(td_coords,td_coords,td_coords,pair,...)	
td_lignefleches_	(pair,...)	
td_ligneflechesabs	(td_coords,...)	
td_masquees		
td_memesigne	(numeric,numeric)	boolean
td_nonmasquees		
td_norme	(td_coords)	numeric
td_nouveauplan	(td_coords,td_coords,td_coords, td_coords,td_coords)	numeric
td_nouveauplan_	(td_coords,td_coords)	numeric
td_nouvellesurf	(td_coords,td_coords,td_coords,text)	numeric
td_nouvellesurf_	(td_coords,...)	numeric
td_nouvellesurfabs	(text)	numeric
td_nouvellesurfc	(td_coords,td_coords,td_coords,path)	numeric
td_nouvellesurfc_	(path)	numeric
td_option	(text)	
td_pcentc	(td_coords,td_coords,td_coords,td_coords, td_coords,td_coords,td_coords,path)	path
td_pcentdir	(td_coords,td_coords,td_coords, td_coords,td_coords)	pair
td_pdtscal	(td_coords,td_coords)	numeric
td_pdtvect	(td_coords,td_coords)	td_coords
td_plandroite	(td_coords,td_coords,td_coords, td_coords,td_coords)	numeric
td_projc	(td_coords,td_coords,td_coords, td_coords,td_coords,td_coords,path)	path
td_projdir	(td_coords,td_coords,td_coords)	pair
td_projnorm	(td_coords,td_coords)	td_coords
td_surface	(numeric)	
td_surfaces		
td_trace	(path)	
td_tracecache	(path)	
td_unite	(td_coords)	td_coords
td_visible	(td_coords,numeric)	boolean
td_x	(td_coords)	numeric
td_y	(td_coords)	numeric
td_z	(td_coords)	numeric

Code source du dessin de la page de garde

```
td_beginfig(0);
  td_ech:=0.7cm;
  td_anglevue((0,-50,20),(0,25,-5),0);

  td_coords i,j,k,O,P,A,B;
  i:=(1,0,0); j:=(0,1,0); k:=(0,0,1); P:=(0,0,10); O:=(0,0,0);

  whatever=td_nouveauplan(i,j,P,(-5,-8),(30,8));
  td_surfaces;

  A:=td_ddtotd(i,j,P,(-2,-4));
  B:=td_ddtotd(i,j,P,(25,6));
  td_ligneabs(A,B);

  for t=1 upto 9: td_ligneabs(O,A+(t/10)*(B-A)); endfor

  tdfleche_long:=1;
  tdfleche_norm:=0.4;
  td_courbefleche (td_unite(B-A),td_unite(td_projnorm(O-A,B-A)),O,
               subpath (7.52,7.95) of fullcircle scaled 25);

  td_dotlabels.bot(O);

  td_option(withpen pencircle scaled 1);
  td_ligneabs(-0.2*(B-A),(1.8)*(B-A));
td_endfig;
```

Chapitre 8

PrettyCurses

Curses est une librairie permettant de dessiner de jolis écrans en mode texte. Cette librairie est traduite en de nombreux langages, notamment en *C* ou en *perl*.

Toutefois les utilitaires sous *perl* permettant d'implémenter des objets un peu complexes, comme des zones de saisie ou des menus, n'offrent pas toutes les opportunités que l'on pourrait souhaiter. Ce package se propose d'implémenter quelques unes de ces fonctionnalités.

Sommaire

Introduction

Description

`PrettyCurses v1.0` est une librairie, fonctionnant sous `perl`, version `5.x`. Elle est une extension de la libraires `Curses` et implémente un certain nombre de widgets utilisés fréquemment.

Licence

Installation

Rien de particulier n'est prévu pour l'installation. Il suffit en fait de copier, en conservant l'arborescence, tous les fichiers `*.pm` distribués dans un répertoire que l'on aura pris soin de rajouter dans la variable globale `@INC` s'il n'y était pas déjà.

Les pages d'aide regroupés dans ce document sont incluses dans les fichiers source sous le format `pod`. La commande *pod2man(1)* permet de créer des pages directement lisibles par la commande *man(1)*.

Auteur

Je m'appelle Xavier Caruso. Vous pouvez m'écrire à l'adresse <`xavier.caruso@ens.fr`>.

Avertissement

Cette librairie a été écrite assez rapidement et n'a pas trop été testée. Il est donc fort probable qu'un nombre encore important de petites et moyennes erreurs subsistent. N'hésitez pas à me le signaler si vous en rencontrez.

J'ai bien quelques idées en tête pour poursuivre le développement ou améliorer certains points mais il est peu probable que je m'y intéresse rapidement.

Finalement, ce document regroupe les différentes pages d'aide écrite pour cette librairie. En espérant que cette dernière puisse vous être utile...

PrettyCurses

NOM

PrettyCurses

SYNOPSIS

```
use PrettyCurses;
```

DESCRIPTION

« `PrettyCurses` » est une librairie qui implémente principalement quelques widgets standard et qui en permet une gestion relativement simple et complète.

« `PrettyCurses` » introduit son propre type de variables pour les fenêtres. Il s'agit simplement d'un *Curses(3)* muni d'une donnée supplémentaire qui est la taille de la bordure. L'intérêt de cela est que les fonctions d'affichage n'écrivent pas par défaut sur cette bordure lorsque le texte est trop long pour tenir sur la fenêtre, ou que les barres de défilement s'affichent correctement.

Variables globales

« `PrettyCurses` » définit un nombre assez important de variables globales qui peuvent ensuite être appelées n'importe où dans le programme. Attention, « `PrettyCurses` » n'initialise pas ces variables, voir à ce propos *PrettyCurses::default(3)*.

Voici la liste des variables globales :

`$PC_stdscr`
: Fenêtre qui correspond à l'écran standard. Exceptionnellement, cette variable est initialisée lors de l'appel de la fonction `PC_initscr` et remise à jour lors de l'appel de la fonction `PC_init`.

`$PC_lower`
: Chaîne de caractères regroupant les lettres en minuscules.

`$PC_upper`
: Chaîne de caractères regroupant les lettres majuscules correspondant aux lettres minuscules précédentes.

`$PC_order`
: Chaîne de caractères expliquant par quelle lettre il faut remplacer les lettres précédentes lorsque l'on désire les classer. Par exemple si « `é` » de `$PC_lower` correspond à « `e` » de `$PC_order`, la fonction `PC_sort` classera les « `é` » avec les « `e` » et non à la fin comme le fait la fonction `sort` quand elle est mal configurée.

`$PC_re_lower`
: Expression régulière qui reconnaît une lettre en minuscule.

`$PC_re_upper`
: Expression régulière qui reconnaît une lettre en majuscule.

`$PC_re_letter`
: Expression régulière qui reconnaît une lettre soit en minuscule, soit en majuscule.

`$PC_re_space`
: Expression régulière qui reconnaît une espace ou un caractère équivalent.

`$PC_re_word`
: Expression regulière qui reconnaît une lettre (ou un caractère) d'un mot. Attention, c'est ainsi l'expression régulière `/$PC_re_word+/` qui reconnaît un mot.

`$PC_re_wordp`
: Expression regulière qui reconnaît une lettre (ou un caractère) d'un mot pouvant être une abréviation se terminant pour un point (e.g. `Av.`).

`@PC_spacebeforepunct = ( qr/$regexp1/ => $string1, ... )`
: Liste expliquant quel espacement il est nécessaire de mettre avant telle ponctuation. Attention, bien que cela se présente comme une table de hash, il s'agit bien d'une liste. Cela permet de garder un ordre dans les tests et donc de mettre des expressions régulières qui peuvent de recouper.

`@PC_spacebeforepunct = ( qr/$regexp1/ => $string1, ... )`
: Liste expliquant quel espacement il est nécessaire de mettre après telle ponctuation.

`$PC_openquotes`
: Chaîne de caractères définissant un guillemet ouvrant.

`$PC_closequotes`
: Chaîne de caractères définissant un guillemet fermant.

`$PC_prefix_cmdtex`
: Expression regulière qui reconnaît un caractère susceptible d'annoncer une commande LaTeX. Bien que toutes les commandes LaTeX sont introduites par un « \ », cette variable globale n'est pas inutile lorsqu'il est nécessaire de repérer des erreurs de saisie.

`@PC_cmdtex = ( /$regexp1/ => [ /$regexp1.1/ => $string1.1, ... ], ... )`
: Liste associant une référence sur une liste à une expression régulière censée reconnaître une certaine commande LaTeX. La liste dont il est question précédemment associe à une expression régulière censée reconnaître l'argument de la commande LaTeX dont il est question la chaîne de caractères par laquelle il va falloir remplacer cette commande. Ceci est notamment utile pour traiter les accents qui seraient tapés à la LaTeX dans les champs de texte.

`$PC_re_mathtex`
: Expression régulière reconnaissant une expression LaTeX valide en mode maths.

`$PC_re_tex`
: Expression régulière reconnaissant une expression LaTeX valide.

`$PC_directory_default`
: Format par défaut que doit utliser la librairie *PrettyCurses::directory(3)*.

`$PC_lengthline`
: Longueur par défaut d'une ligne.

`$PC_re0`, ..., `$PC_re9`
: Variables supplémentaires supposées contenir des expressions régulières devant être réutilisées.

Méthodes

Initialisation

`PC_initscr ();`
: Initialise *Curses(3)* et la variable globale `$PC_stdscr`. Cette fonction ne doit normalement être appelée qu'une unique fois au début du programme.

`PC_init ();`
: Met à jour la variable globale `$PC_stdscr` et détruit toutes les autres fenêtres qui ont été créées jusqu'alors.

Attendre un caractère

`$PC_win->PC_getch ();`
: Attend un caractère sur la fenêtre `$PC_win`. Cette fonction reconnaît les séquences de caractères que

l'on lui a dit de reconnaître, ce qui sert notamment à intercepter des touches comme SHIFT-LEFT ou CONTROL-F2.

`PC_getch_addsequences ( $sequence1 => $code1, ... );`
Définit les séquences de caractères passées en arguments. Par exemple, l'appel de la fonction `PC_getch_addsequences ( "^[[A" => "UP" );` permet de reconnaître une pression sur la touche <UP> et de renvoyer dans ce cas le code UP.

`$PC_win->PC_getch_add ( $key1, ... );`
Simule sur la fenêtre `$PC_win` la pression de la touche `$key1`, puis celle de la touche `$key2` et ainsi de suite.

`$PC_win->PC_getch_on_press ($code);`
Définit le code à exécuter lorsqu'une touche est pressée dans l'écran `$PC_win` ou un de ses fils (voir la fonction `derwin`). La touche pressée est passée en argument au code.

Fonctions usuelles de gestion d'une fênetre

`$PC_win->PC_getxy ();`
Renvoie la taille de la fenêtre `$PC_win` sous le format `($Y, $X)`.

`$PC_win->PC_derwin ($height_y, $height_x, $y, $x, $border, $write_on_border);`
Crée une nouvelle fenêtre. Les deux premiers arguments `$height_y` et `$height_x` fournissent la taille de cette nouvelle fenêtre. Les deux arguments suivants `$y` et `$x` donnent la position du coin supérieur gauche de la fênetre, position repérée par rapport à la fenêtre `$PC_win`. `$border` correspond à la taille de la bordure de la fenêtre en cours de création. `$write_on_border` est un booléen. S'il est positionné à une valeur définie et non nulle, la fenêtre nouvelle créée pourra empiéter sur la bordure de `$PC_win`. Finalement, cette fonction renvoie la fenêtre créée. Il se peut que les dimensions de celle-ci ne soient pas celles demandées si la place venait à manquer. Si encore pour faute de place, la fenêtre n'a pu être créée, la fonction renvoie un objet vide mais du bon type.

`$PC_win->PC_clear ();`
Efface tout ce qu'il y a écrit sur la fenêtre `$PC_win`.

`$PC_win->PC_border ();`
Dessine la bordure de la fenêtre `$PC_win`.

`$PC_win->PC_defilbar ($begin, $end, $buttom);`
Dessine une barre de défilement sur la bordure de la fenêtre `$PC_win`. Ne fait rien si cette fenêtre n'a pas de bordure. `$begin` et `$end` fournissent respectivement le numéro de la première ligne affichée et celui de la dernière ligne affichée. `$buttom`, quant à lui, donne le nombre total de lignes. Il est conseillé de faire d'abord appel à `PC_border` avant afin d'effacer l'ancienne barre de défilement s'il y avait.

`$PC_win->PC_addstr ($y, $x, $s, $write_on_border);`
Affiche sur la fenêtre `$PC_win`, à la position repérée par `$y` et `$x`, la chaîne de caractères `$s`. N'affiche pas les caractères qui débordent de la fenêtre. Le booléen `$write_on_border` précise s'il faut écrire sur la bordure ou s'il ne faut pas.

`$PC_win->PC_refresh ();`
Dessine effectivement les modifications qui ont été faites dans la fenêtre `$PC_win`.

`$PC_win->PC_delwin ();`
Supprime la fenêtre `$PC_win`. Attention, cela ne l'efface pas du tout de l'écran même après tous les appels à `$PC_refresh` possibles et imaginables; il est nécessaire de réécrire par dessus pour avoir cet effet.

Gestion des couleurs

« PrettyCurses » redéfinit également ce qu'est une couleur (trop fort ;-). Une couleur, disons $color, est une reférence sur une table de hash de la forme suivante :

```
$color = {   NOFOCUS_FORE     =>     ,
             NOFOCUS_BACK     =>     ,
             FOCUS_FORE       =>     ,
             FOCUS_BACK       =>          };
```

Les valeurs affectées dans cette table de hash sont des noms de couleurs, tout ce qu'il y a de plus classique (e.g. blue, white...). FORE et BACK correspondent respectivement à la couleur du texte et à la couleur de fond.

Les fonctions qui permettent de gérer tout cela sont les suivantes :

`PC_definecolors ( $name1 => $color1, ... );`
: Définit la couleur $name1 et lui assigne la valeur $color1 et ainsi de suite. Bien entendu, les $color doivent être des objets du type décrit précédemment.

`$PC_win->PC_colorset ($color, $focus);`
: Déclare que désormais toutes les modifications sur la fenêtre $PC_win seront faites avec la couleur $color. Si $focus est positionné à une valeur définie et non nulle, utilise les couleurs définies par FOCUS_*, sinon utilise les couleurs définies par NOFOCUS_*. Si une ou plusieurs couleurs ne sont pas définies, remplace icelle par la couleur correspondante de default.

Gestion du redimensionnement

« PrettyCurses » intercepte le signal WINCH émis lorsque la fenêtre en cours est redimentionné. Il simule alors la pression d'une touche fictive nommée WINCH que le programme devra intercepter et gérer correctement, principalement en appelant la fonction PC_init et en recréant et redessinant toutes les fenêtres.

PrettyCurses::default_french

NOM

PrettyCurses::default_french

SYNOPSIS

```
use PrettyCurses::default_french;
```

DESCRIPTION

Initialise les variables globales définies par *PrettyCurses(3)* en tenant plus ou moins compte des normes de la typographie française.

Définit en outre les séquences d'échappement classiques et les couleurs `default`, `fields` et `error`.

PrettyCurses::utils

NOM

PrettyCurses::utils

SYNOPSIS

```
use PrettyCurses::utils;

PC_upper ($text);
PC_lower ($text);
PC_truncate ($text, $length);

PC_compare ($a, $b);
PC_sort (@list);

PC_copy ($a);
PC_equal ($a, $b);

PC_addorder ($new, $old);
```

DESCRIPTION

Définit quelques fonctions parfois bien utiles. En voici la liste :

Gestion des chaînes de caractères

`PC_upper ($text);`
: Met en majuscules la chaîne de caractères `$text` en utilisant la correspondance donnée par les variables globales `$PC_lower` et `$PC_upper` et renvoie le résultat.

`PC_lower ($text);`
: Met en minuscules la chaîne de caractères `$text` en utilisant la correspondance donnée par les variables globales `$PC_lower` et `$PC_upper` et renvoie le résultat.

`PC_order ($text);`
: Renvoie ce qui permet de classer alphabétiquement la chaîne de caractères `$text` en utilisant la correspondance donnée par les variables globales `$PC_lower`, `$PC_upper` et `$PC_order`.

`PC_truncate ($text, $length);`
: Coupe le texte `$text` pour qu'il tienne sur des lignes de longueur `$length`. Les « `\n` » déja présents sont conservés. Si le paramètre `$length` n'est pas défini, la valeur utilisée est celle de la variable globale `$PC_lengthline`. Renvoie une référence sur la liste des lignes.

Fonctions de comparaison

`PC_compare ($a, $b);`
: Compare les chaînes de caractères `$a` et `$b` en utilisant l'ordre défini par la variable globale `$PC_order`. Renvoie `-1` si `$a` est plus petit que `$b`, `0` s'ils sont égaux et `1` si `$a` est plus grand que `$b`.

`PC_sort (@list);`
: Trie la liste `@list` en utilisant l'ordre défini par la variable globale `$PC_order` et renvoie la liste triée.

Gestion des structures complexes

`PC_copy ($a);`
: Renvoie une copie de l'objet `$a`. Attention, cette fonction ne fonctionne correctement que si l'objet `$a` ne contient récursivement que des références sur des `LIST` et sur des `HASH`.

`PC_equal ($a, $b);`
: Compare les objets `$a` et `$b`. Là encore, cette fonction ne fonctionne correctement que si les objets `$a` et `$b` ne font intervenir récursivement que des références sur des `LIST` et sur des `HASH`. Renvoie `1` si les objets sont égaux, `0` sinon.

Autre fonction

`PC_addorder ($new, $old);`
: Forme un ordre composé à mettre dans une table de hash `KEYS` (voir *PrettyCurses::Widgets(3)*) à partir de `$new` et de `$old`. L'ordre qui en résulte est de la forme `$new/$old`. Si toutefois `$old` était un ordre prioritaire, `$new` n'est pas ajouté.

PrettyCurses::Message

NOM

PrettyCurses::Message

SYNOPSIS

```
use PrettyCurses::Message;

PC_message ($PC_win, $param);
```

DESCRIPTION

Affiche un message sur la fenêtre `$PC_win`. Le message et son format sont fournis grâce à l'argument `$param`. Il s'agit d'une référence sur une table de hash dont le format est le suivant :

```
$param = {   HEIGHT_X         =>     ,
             MESSAGE_TEXT     =>     ,
             BUTTON_TEXT      =>     ,
             KEYS             =>          };
```

Détaillons ces paramètres.

`HEIGHT_X`
: Définit la taille horizontale de la fenêtre du message. Si ce paramètre n'est pas fourni, la taille prise par défaut correspond aux deux tiers de la largeur de la fenêtre `$PC_win`.

`MESSAGE_TEXT`
: Texte du message. Il peut s'agir soit d'une chaîne de caractères, soit d'une référence sur une liste. Dans le deuxième cas, tous les éléments de la liste sont affichés dans l'ordre, un saut de ligne est inséré entre chacun d'eux. Il est tout à fait possible de mettre des « `\n` » dans ces chaînes de caractères, ils seront interprétés comme des retours à la ligne. Finalement, il n'est pas nécessaire de faire attention à formater le texte pour qu'il ne dépasse pas en largeur de la fenêtre, ceci est fait automatiquement.

`BUTTON_TEXT`
: Texte qui doit apparaître sur le bouton au bas du message. La valeur par défaut est « `OK` ».

`KEYS` Voir la description générale de *PrettyCurses::Widgets(3)*.

PrettyCurses::Corrections

NOM

PrettyCurses::Corrections

SYNOPSIS

```
use PrettyCurses::Corrections;

PrettyCurses::Corrections::tex ($value);

PrettyCurses::Corrections::quotes ($value);
PrettyCurses::Corrections::punctuation ($value);

PrettyCurses::Corrections::caps ($value);
PrettyCurses::Corrections::small_caps ($value);
PrettyCurses::Corrections::transliteration ($value);

PrettyCurses::Corrections::telephone ($value);
```

DESCRIPTION

Ce package implémente un certain nombre de fonctions adhoc pour effectuer les corrections automatiques. Il est utilisé directement par *PrettyCurses::TextField(3)* et donc aussi indirectement par plusieurs autres packages.

L'argument `$value` doit être une référence sur une liste de références de listes de chaînes de caractères comme cela est détaillé dans *PrettyCurses::TextField(3)*. La valeur de retour de chacune de ces fonctions est un objet du même type. Il faut noter que justement cette structure permet de ne jamais perdre la valeur initiale et de proposer ensuite à l'utilisateur d'accepter ou de refuser la correction proposée.

Voici la liste des fonctions en question :

LaTeX

`PrettyCurses::Corrections::tex ($value);`

Oublie les anciennes corrections. Vérifie si la valeur passée est une expression LaTeX valide selon l'expression régulière de la variable globale `$PC_re_tex` et si c'est le cas, reconnaît les commandes LaTeX présentes dans la variable globale `@PC_cmdtex` et les remplace par les valeurs correspondantes.

Typographie

`PrettyCurses::Corrections::quotes ($value);`

Repère les guillemets et les remplace par le standard défini dans les variables globales `$PC_openquotes` et `$PC_closequotes`.

`PrettyCurses::Corrections::punctuation ($value);`

Corrige l'espacement autour des ponctuations.

Les fonctions précédentes n'ont pas toujours un comportement très à propos. Afin de limiter les dégats, il est conseillé de les appeler dans l'ordre dans lequel elles ont été présentées. C'est exactement ce que fait *PrettyCurses::TextField(3)* sur appel de la fonction `correct`.

Correction sur les mots

`PrettyCurses::Corrections::caps ($value);`
: Oublie les anciennes corrections. Écrit tous les mots en majuscules.

`PrettyCurses::Corrections::small_caps ($value);`
: Oublie les anciennes corrections. Écrit tous les mots en petites majuscules (ie écrit la première lettre en majuscules et les autres lettres en minuscules).

`PrettyCurses::Corrections::transliteration ($value, $tr, $punct);`
: L'argument `$tr` est une référence sur une liste qui met en correspondance des expressions régulières avec des chaînes de caractères. La fonction commence par oublier les anciennes corrections puis regarde si chacun des mots de `$value` est reconnu par les expressions régulières de la liste `$tr`. Si c'est le cas, la fonction remplace ce mot par la valeur qui est associée à cette expression régulière. Cette valeur peut contenir des `$1`, `$2`, etc. Ils seront interprétés correctement sauf s'ils sont protégés par des « \ ». Le booléen `$punct` précise s'il faut utiliser l'expression régulière `/$PC_word+/` pour reconnaître un mot (cas `$punct = 1`) ou s'il faut utiliser l'expression régulière `/$PC_wordp+/` (cas `$punct = 0`).

PrettyCurses::Widgets

NOM

PrettyCurses::Widgets

SYNOPSIS

```
use PrettyCurses::<widget>;

$w = PrettyCurses::<widget>->new ({
        X                   =>     ,
        Y                   =>     ,
        HEIGHT_X            =>     ,
        HEIGHT_Y            =>     ,
        VALUE               =>     ,
        KEYS                =>     ,
        READONLY            =>     ,
        UNDO                =>     ,
        CURRENT_LINE        =>     ,
        CURRENT_FIELD       =>     ,
        CURSOR_POS          =>     ,
        CORRECT             =>     ,
        COLOR               =>     ,
        COLOR_ERR           =>     ,
        DRAW_AFTER_EXECUTE  =>
});

$w->getParam ($name);
$w->setParam ( $name1 => $value1, ... );
$w->getValue ();
$w->setValue ($value);

$w->draw ($PC_win, $focus);
$w->execute ($PC_win);

$w->correct ($PC_win, $focus);

$w->undo ($PC_win, $focus);
$w->redo ($PC_win, $focus);
$w->save_position ($name);
$w->remove_position ($name);
$w->addinhistory ($name);
$w->clearhistory ();
```

DESCRIPTION

Cette page ne décrit pas à proprement parler un package, mais plutôt la syntaxe générale de tous les widgets proposés par *PrettyCurses(3)*. Bien que cela ne soit pas programmé comme ça, il est bon de voir cela comme une classe abstraite dont les widgets dérivent.

Les widgets en question sont `Button`, `Caption`, `ChechBox`, `Form`, `Menu`, `MultiFields`, `TextField` et `TextMemo`.

Créer une nouvelle instance d'un widget

Cela se fait grâce à la fonction `new` dont la syntaxe générale a été décrite précédemment. Nous allons décrire un par un ce à quoi correspondent les paramètres cités précédemment. Ceux-ci sont ceux qui sont censés être définis pour tous les widgets. Bien sûr, certains paramètres n'ont pas de sens pour certains widgets (e.g. `READONLY` pour un widget `Caption`) mais cela n'est pas grave. Moralement, ce que l'on a écrit impose que si un widget utilise un des paramètres donnés ci-dessus, il devra lui conférer le sens que l'on va décrire tout de suite.

Finalement, si un de ces paramètres n'est pas défini lors de l'appel de la fonction `new`, il est généralement positionné à une valeur par défaut. Toutefois, celle-ci dépend du widget dont on veut créer une instance. Les valeurs par défaut ne sont pas décrites ici mais dans les pages de mân spécifiques.

`X` et `Y`
: Décrivent la position du widget sur la fênetre sur laquelle il va être afficher.

`HEIGHT_X` et `HEIGHT_Y`
: Décrivent la taille du widget.

`VALUE`
: Valeur du widget.

`KEYS` Il s'agit d'une référence sur une table de hash qui précise le comportement à avoir lorsqu'une certaine touche, disons `$key`, a été enfoncée pendant l'exécution du widget. Si `$key` n'apparaît pas dans les clés de la table de hash, la touche est ignorée. Si au contraire, `$key` apparaît, il y a deux cas : soit la valeur qui lui est associée est une réfèrence sur un `CODE` et alors ce code est exécuté recevant comme paramètre une référence sur le widget en question et l'exécution se poursuit normalement, soit ce n'est pas le cas et alors l'exécution du widget s'arrête et renvoie la valeur associée. Si le widget, pour une raison quelconque, devait intercepter précisément la touche `$key`, alors cette interception est prioritaire sauf dans les deux cas suivants : la valeur associée est une référence sur un `CODE` ou ce n'est pas le cas et celle-ci débute par le caractère « / ». Il y a deux codes particuliers qui sont `ON_PRESS` et `ON_MODIFY`. Ils ne sont prioritaires sur aucune autre interception et sont exécutés respectivement lorsqu'une quelconque touche a été enfoncée et lorsque le widget a été modifié. Bien sûr, `ON_MODIFY` est prioritaire sur `ON_PRESS`.

`READONLY`
: Précise si le widget est modifiable (cas `READONLY => 0`) ou si ce n'est pas le cas (cas `READONLY => 1`).

`UNDO` Précise s'il faut retenir l'historique et si les touches `CONTROL_PGUP` et `CONTROL_PGDOWN` doivent respectivement annuler et refaire la dernière modification (cas `UNDO => 1`) ou si ce n'est pas nécessaire (cas `UNDO => 0`).

`CURRENT_LINE`
: Numéro de la ligne courante. Ce paramètre peut être interprété différemment selon les widgets, il est plus sûr de se reporter aux pages de mân spécifiques pour connaître son comportement exact.

`CURRENT_FIELD`
: Numéro du champ courant si le widget comprend plusieurs champs. Ce paramètre peut être interprété différemment selon les widgets, il est plus sûr de se reporter aux pages de mân spécifiques pour connaître son comportement exact.

`CURSOR_POS`
: Position du curseur. Ce paramètre peut être interprété différemment selon les widgets, il est plus sûr de se reporter aux pages de mân spécifiques pour connaître son comportement exact.

`CORRECT`
: Précise s'il faut faire les corrections automatiques lorsque la combinaison de touches `CONTROL-T` est enfoncée ou si ce n'est pas nécessaire.

`COLOR`
: Couleur avec laquelle devra être dessinée le widget.

`COLOR_ERR`
: Couleur avec laquelle seront dessinées les parties erronées du widget. Voir *PrettyCurses::TextField(3)* pour plus d'informations.

`DRAW_AFTER_EXECUTE`
: Précise s'il faut redessiner le widget après l'exécution (cas `DRAW_AFTER_EXECUTE => 1`) ou si ce n'est pas nécessaire (cas `DRAW_AFTER_EXECUTE => 0`).

Méthodes

Gestion des paramètres

`$w->getParam ($name);`
: Renvoie la valeur du paramètre `$name`.

`$w->setParam ( $name1 => $value1, ... );`
: Affecte la valeur `$value1` au paramètre `$name1` et ainsi de suite.

`$w->getValue ();`
: Renvoie la valeur du paramètre `VALUE`. Attention, cela n'est pas forcément équivalent à la commande `$w->getParam ('VALUE');`, parfois les paramètres de ce type étant stockés de façon spéciale. Pour plus d'informations, se reporter aux pages de mân spécifiques.

`$w->setValue ($value);`
: Met à jour la valeur du paramètre `VALUE`. Même remarque que précédemment.

Fonctions d'affichage

`$w->draw ($PC_win, $focus);`
: Dessine le widget `$w` sur la fenêtre `$PC_win` puis rend la main. Si `$focus` est positionné à une valeur définie et non nulle, dessine le widget comme si celui-ci avait le focus.

`$w->execute ($PC_win);`
: Lance l'exécution du widget `$w`. Comme expliqué précedemment, la table de hash définie par le paramètre `KEYS` détermine lorsque cette procédure termine et le code de retour renvoyé. Redessine le widget via la commande `$w->draw ($PC_win);` avant de rendre la main si le paramètre `DRAW_AFTER_EXECUTE` est positionné à `1`. Il est par exemple intéressant de positionner cette valeur à `0` lorsque les événements `ON_PRESS` ou `ON_MODIFY` sont interceptés.

Autres fonctions

`$w->correct ($PC_win, $focus);`
: Fait les corrections automatiques sur la valeur du widget `$w` (voir les pages de mân spécifiques et *PrettyCurses::Corrections(3)* pour plus d'informations). Si `$PC_win` est défini, redessine finalement le widget `$w` via la commande `$w->draw ($PC_win, $focus);`. Si le paramètre `CORRECT` est positionné à `1`, cette fonction est appelée automatiquement lorsque la combinaison de touches `CONTROL-T` est pressée.

`$w->undo ($PC_win, $focus);`
: Remonte d'un cran dans l'historique. Si `$PC_win` est défini, redessine finalement le widget `$w` via la commande `$w->draw ($PC_win, $focus);`. Si le paramètre `UNDO` est positionné à `1`, cette fonction est appelée automatiquement lorsque la combinaison de touches `CONTROL-PGUP` est pressée.

`$w->redo ($PC_win, $focus);`
: Descend d'un cran dans l'historique. Si `$PC_win` est défini, redessine finalement le widget `$w` via la

commande `$w->draw ($PC_win, $focus);`. Si le paramètre `UNDO` est positionné à `1`, cette fonction est appelée automatiquement lorsque la combinaison de touches `CONTROL-PGDOWN` est pressée.

`$w->save_position ($name);`
Sauvegarde la position actuelle sous le nom `$name`. Quelques noms sont utilisés par la librairie elle-même. Tous ceux-ci sont introduits par la chaîne de caractères « `__` ». Il est donc déconseillé d'utiliser des noms commençant par « `__` ».

`$w->unlock_position ($name);`
Supprime la position `$name`.

`$w->addinhistory ($name);`
Ajoute dans l'historique la position `$name`. Si aucun argument n'est passé, y ajoute la position actuelle. Si le paramètre `UNDO` est positionné à `1`, cette fonction est appelée automatiquement *avant* chaque modification du widget.

`$w->clearhistory ();`
Efface l'historique.

PrettyCurses::Caption

NOM

PrettyCurses::Caption

SYNOPSIS

```
use PrettyCurses::Caption;

$w = PrettyCurses::Caption->new ({
        X                   =>     0,
        Y                   =>     0,
        HEIGHT_X            =>     10,
        HEIGHT_X            =>     1,
        VALUE               =>     '',
        COLOR               =>     'default',
});

$w->getParam ($name);
$w->setParam ( $name1 => $value1, ... );
$w->getValue ();
$w->setValue ($value);

$w->draw ($PC_win);
```

DESCRIPTION

Ce package implémente un widget Caption (légende).

Paramètres

Pour les descriptions générales, se reporter à la page *PrettyCurses::Widgets(3)*. Les valeurs qui sont données ci-dessus sont celles qui sont passés par défaut si elles ne sont pas initialisées lors de l'appel de la fonction `new`.

Il faut signaler que le paramètre `VALUE` peut-être soit une référence sur une liste, soit une chaîne de caractères. Si c'est une référence sur une liste, chaque élément de la liste est dessinée et un retour à la ligne est insérée entre chacun d'eux. Finalement les caractères « `\n` » sont autorisés et sont compris naturellement comme des retours à la ligne.

Méthodes

Se reporter à la page *PrettyCurses::Widgets(3)*.

PrettyCurses::TextField

NOM

PrettyCurses::TextField

SYNOPSIS

```
use PrettyCurses::TextField;

$w = PrettyCurses::TextField->new ({
        X                   =>     0,
        Y                   =>     0,
        HEIGHT_X            =>     10,
        LENGTH              =>     0,
        VALUE               =>     [ ],
        KEYS                =>     { },
        READONLY            =>     0,
        UNDO                =>     1,
        CURSOR_POS          =>     0,
        CORRECT             =>     1,
        COLOR               =>     'fields',
        COLOR_ERR           =>     'error',
        DRAW_AFTER_EXECUTE  =>     1
});

$w->getParam ($name);
$w->setParam ( $name1 => $value1, ... );
$w->getValue ();
$w->setValue ($value);

$w->draw ($PC_win);
$w->execute ($PC_win);

$w->correct ($PC_win, $focus);

$w->undo ($PC_win, $focus);
$w->redo ($PC_win, $focus);
$w->save_position ($name);
$w->remove_position ($name);
$w->addinhistory ($name);
$w->clearhistory ();
```

DESCRIPTION

Ce package implémente un widget TextField (champ de texte).

Paramètres

Ici ne sont détaillés que les paramètres spécifiques au widget TextField. Pour les descriptions générales, se reporter à la page *PrettyCurses::Widgets(3)*. Les valeurs qui sont données ci-dessus sont celles qui sont passés par défaut si elles ne sont pas initialisées lors de l'appel de la fonction `new`.

`LENGTH`
: Définit le nombre maximal de caractères que peut contenir le champ. Si ce paramètre est positionné à `0`, aucune limite n'est fixée.

`VALUE`
: Voir le paragraphe suivant.

`CURSOR_POS`
: Position du curseur sur la ligne. Un nombre négatif indique que la position doit être comptée à partir de la fin du champ.

Description du paramètre VALUE

Ce paramètre contient la valeur du champ. Il est toutefois probablement nécessaire de préciser le format. Il s'agit d'une référence sur une liste, chaque élément de cette liste étant lui-même une référence sur une liste, cette dernière référence définissant une partie du champ de la manière suivante. Cette liste contient les chaînes de caractères susceptibles d'apparaître dans la valeur du champ, celle qui apparaît effectivement étant la première de la liste.

Cela sera peut-être plus clair sur un exemple. Si `VALUE` est positionné à :

```
[ [ "Bonjour", "Hello" ], [ " Xavier !" ] ]
```

la valeur du champ à cet instant sera « `Bonjour Xavier !` », mais il sera possible de passer rapidement à « `Hello Xavier !` » (grâce à la combinaison de touches `CONTROL-A`) ; `VALUE` sera alors positionné à :

```
[ [ "Hello", "Bonjour" ], [ " Xavier !" ] ]
```

de sorte qu'il est encore possible de revenir rapidement à l'ancienne valeur.

Les parties de champ pour lesquelles plusieurs possibilités sont offertes sont affichées avec la couleur définie par le paramètre `COLOR_ERR`, alors que les autres sont affichées avec la couleur définie par le paramètre `COLOR`.

Finalement, l'appel de la fonction `$w->setValue ($value);` affecte la valeur `[ [ $value ] ]` au paramètre `VALUE` tandis que la fonction `$w->getValue ();` renvoie la chaîne de caractères correspondante à la valeur courante. Pour être plus précis, il est nécessaire d'utiliser les fonctions `setParam` et `getParam`.

Méthodes

Se reporter à la page *PrettyCurses::Widgets(3)*.

Touches interceptées lors de l'exécution

`LEFT`, `RIGHT`, `HOME`, `END`
: Se déplace à l'endroit voulu dans le champ sauf si cela n'est pas possible auquel cas la touche n'est pas interceptée.

`SHIFT-LEFT`
: Se déplace au début du mot où la partie de champ courant. Si le curseur est déjà au début du champ, la touche n'est pas interceptée.

`SHIFT-RIGHT`
: Se déplace au début du mot suivant ou à la fin de la partie de champ courante. Si le curseur est déjà à la fin du champ, la touche n'est pas interceptée.

`DELETE`, `BACKSPACE`
: Efface le caractère attendu. Si cela n'est pas possible, la touche n'est pas interceptée. Ces touches ne sont de toute façon pas prises en compte si le paramètre `READONLY` est positionné à `1`.

`INSERT`
: Bascule entre le mode insertion et le mode remplacement.

`CONTROL-U`
: Efface tout le champ sauf si le champ est déjà vide auquel cas la touche n'est pas interceptée. Cette touche n'est de toute façon pas prise en compte si le paramètre `READONLY` est positionné à `1`.

`CONTROL-W`
: Efface le mot précédent. Cette touche n'est de toute façon pas prise en compte si le paramètre `READONLY` est positionné à `1`.

`CONTROL-A`
: Bascule la valeur effective de la partie de champ courante. Cette touche n'est de toute façon pas prise en compte si le paramètre `READONLY` est positionné à `1`.

`CONTROL-T`
: Applique les corrections automatiques. Cette touche n'est pas prise en compte si le paramètre `CORRECT` est positionné à `0` ou si le paramètre `READONLY` est positionné à `1`.

`CONTROL-PGUP`
: Remonte d'un cran dans l'historique. La touche n'est pas interceptée si on était déjà au début de l'historique. Cette touche est de toute façon ignorée si le paramètre `UNDO` est positionné à `0` ou si le paramètre `READONLY` est positionné à `1`.

`CONTROL-PGDOWN`
: Descend d'un cran dans l'historique. La touche n'est pas interceptée si on était déjà à la fin de l'historique. Cette touche est de toute façon ignorée si le paramètre `UNDO` est positionné à `0` ou si le paramètre `READONLY` est positionné à `1`.

PrettyCurses::TextMemo

NOM

PrettyCurses::TextMemo

SYNOPSIS

```
use PrettyCurses::TextMemo;

$w = PrettyCurses::TextMemo->new ({
        X                   =>     0,
        Y                   =>     0,
        HEIGHT_X            =>     10,
        HEIGHT_Y            =>     2,
        VALUE               =>     [ ],
        KEYS                =>     { },
        READONLY            =>     0,
        UNDO                =>     1,
        CURRENT_LINE        =>     0,
        CURSOR_POS          =>     0,
        CORRECT             =>     1,
        COLOR               =>     'fields',
        COLOR_ERR           =>     'error',
        DRAW_AFTER_EXECUTE  =>     1
});

$w->getParam ($name);
$w->setParam ( $name1 => $value1, ... );
$w->getValue ();
$w->setValue ($value);

$w->draw ($PC_win);
$w->execute ($PC_win);

$w->correct ($PC_win, $focus);

$w->undo ($PC_win, $focus);
$w->redo ($PC_win, $focus);
$w->save_position ($name);
$w->remove_position ($name);
$w->addinhistory ($name);
$w->clearhistory ();
```

DESCRIPTION

Ce package implémente un widget TextMemo. Il s'agit d'un champ de texte pouvant tenir sur un nombre arbitraire de lignes.

Paramètres

Ici ne sont détaillés que les paramètres spécifiques au widget TextMemo. Pour les descriptions générales, se reporter à la page *PrettyCurses::Widgets(3)*. Les valeurs qui sont données ci-dessus sont celles qui sont passés par défaut si elles ne sont pas initialisées lors de l'appel de la fonction `new`.

`VALUE`
: Référence sur une liste dont les éléments sont des objets de type celui du paramètre `VALUE` de *PrettyCurses::TextField(3)*. Bien sûr, chaque élément correspond à une ligne du champ. Comme dans *PrettyCurses::TextField(3)*, les fonctions `getValue` et `setValue` ont un comportement singulier. Ici, la fonction `getValue` renvoie juste une liste de chaînes de caractères et la fonction `setValue` prend une telle liste et l'affecte correctement au paramètre `VALUE`.

`CURRENT_LINE`
: Ligne sur laquelle se trouve le curseur. Si ce nombre est négatif, les lignes sont comptées à partir de la dernière.

`CURSOR_POS`
: Position du curseur sur la ligne déterminée par `CURRENT_LINE`. Si ce nombre est négatif, la position est comptée à partir de la fin de la ligne.

Méthodes

Se reporter à la page *PrettyCurses::Widgets(3)*.

Touches interceptées lors de l'exécution

Il faut noter que *PrettyCurses::TextMemo(3)* fait appel à *PrettyCurses::TextField(3)* pour gérer séparément chaque ligne de champ et que les interceptions de *PrettyCurses::TextField(3)* sont en général prioritaires. Expliquons cela en regardant par exemple le comportement de la touche `LEFT`. Si le curseur ne se trouve pas au début d'une ligne, c'est *PrettyCurses::TextField(3)* qui intercepte la touche et déplace simplement ce curseur vers la gauche. Sinon, c'est *PrettyCurses::TextMemo(3)* qui intercepte la touche et le curseur remonte à la ligne précédente si elle existe.

`LEFT` Déplace le curseur à la fin de la ligne précédente. Si le curseur était sur la première ligne, la touche n'est pas interceptée.

`RIGHT`
: Déplace le curseur au début de la ligne suivante. Si le curseur était sur la dernière ligne, la touche n'est pas interceptée.

`UP` Accède à la ligne précédente. Si le curseur était déjà positionné sur la première ligne, la touche n'est pas interceptée.

`DOWN` Accède à la ligne suivante. Si le curseur était déjà positionné sur la dernière ligne, la touche n'est pas interceptée.

`BACKSPACE`
: Réunit la ligne en cours avec la ligne précédente. Cette touche n'est pas prise en compte si le paramètre `READONLY` est positionné à `1`.

`DELETE`
: Réunit la ligne en cours avec la ligne suivante. Cette touche n'est pas prise en compte si le paramètre `READONLY` est positionné à `1`.

`ENTER`
: Sépare la ligne en cours en deux lignes. Cette touche n'est pas interceptée si le curseur est positionné sur la dernière ligne du champ et que celle-ci est vide. Cette touche n'est de toute façon pas prise en compte si le paramètre `READONLY` est positionné à `1`.

`CONTROL-U`
: Supprime la ligne en cours. Cette touche n'est pas prise en compte si le paramètre `READONLY` est positionné à `1`.

`CONTROL-T`
: Applique les corrections automatiques. Cette touche n'est pas prise en compte si le paramètre `CORRECT` est positionné à `0` ou si le paramètre `READONLY` est positionné à `1`. Il faut noter que les *PrettyCurses::TextField(3)* utilisés sont appelés avec le paramètre `CORRECT` positionné à `0` de sorte qu'ils ne peuvent pas intercepter cette touche.

`CONTROL-PGUP`
: Remonte d'un cran dans l'historique. La touche n'est pas interceptée si on était déjà au début de l'historique. Cette touche est de toute façon ignorée si le paramètre `UNDO` est positionné à `0` ou si le paramètre `READONLY` est positionné à `1`.

`CONTROL-PGDOWN`
: Descend d'un cran dans l'historique. La touche n'est pas interceptée si on était déjà à la fin de l'historique. Cette touche est de toute façon ignorée si le paramètre `UNDO` est positionné à `0` ou si le paramètre `READONLY` est positionné à `1`.

PrettyCurses::MultiFields

NOM

PrettyCurses::MultiFields

SYNOPSIS

```
$w = PrettyCurses::MultiFields->new ({
        X                   =>     0,
        Y                   =>     0,
        HEIGHT_X            =>     10,
        VALUE               =>     [ ],
        KEYS                =>     { },
        READONLY            =>     0,
        UNDO                =>     1,
        CURRENT_FIELD       =>     0,
        MAX_FIELDS          =>     0,
        CURSOR_POS          =>     0,
        CORRECT             =>     1,
        COLOR               =>     'fields',
        COLOR_ERR           =>     'error',
        SEPARATOR           =>     '/',
        COLOR_SEP           =>     'default',
        DRAW_AFTER_EXECUTE  =>     1
});

$w->getParam ($name);
$w->setParam ( $name1 => $value1, ... );
$w->getValue ();
$w->setValue ($value);

$w->draw ($PC_win);
$w->execute ($PC_win);

$w->correct ($PC_win, $focus);

$w->undo ($PC_win, $focus);
$w->redo ($PC_win, $focus);
$w->save_position ($name);
$w->remove_position ($name);
$w->addinhistory ($name);
$w->clearhistory ();
```

DESCRIPTION

Ce package implémente un widget MultiFields. Il s'agit d'une zone de texte pouvant contenir plusieurs champs à la suite. Ceci est notamment pratique pour faire saisir un chemin, chaque champ correspondra à un sous-répertoire.

Paramètres

Ici ne sont détaillés que les paramètres spécifiques au widget MultiFields. Pour les descriptions générales, se reporter à la page *PrettyCurses::Widgets(3)*. Les valeurs qui sont données ci-dessus sont celles qui sont passés par défaut si elles ne sont pas initialisées lors de l'appel de la fonction `new`.

`VALUE`
: Référence sur une liste dont les éléments sont des objets de type celui du paramètre `VALUE` de *PrettyCurses::TextField(3)*. Bien sûr, chaque élément correspond à un champ. Comme dans *PrettyCurses::TextField(3)*, les fonctions `getValue` et `setValue` ont un comportement singulier. Ici, la fonction `getValue` renvoie juste une liste de chaînes de caractères et la fonction `setValue` prend une telle liste et l'affecte correctement au paramètre `VALUE`.

`CURRENT_FIELD`
: Numéro du champ actif. Un nombre négatif précise que les champs sont comptés à partir du dernier.

`MAX_FIELDS`
: Nombre maximum de champs. Le nombre de champs n'est pas limité si ce paramètre est positionné à `0`. Toutefois, le nombre de champs est toujours limité par la taille du widget, en imposant à chaque champ de disposer d'au moins deux caractères.

`CURSOR_POS`
: Position du curseur sur le champ actif. Un nombre négatif précise que cette position doit être comptée à partir de la droite du champ.

`SEPARATOR`
: Chaîne de caractères à introduire pour séparer deux champs.

`COLOR_SEP`
: Couleur dans laquelle doit être dessinée la chaîne de caractères précédente.

Méthodes

Se reporter à la page *PrettyCurses::Widgets(3)*.

Touches interceptées lors de l'exécution

Il faut noter que *PrettyCurses::MultiFields(3)* fait appel à *PrettyCurses::TextField(3)* pour gérer séparément chaque ligne de champ et que les interceptions de *PrettyCurses::TextField(3)* sont en général prioritaires. Expliquons cela en regardant par exemple le comportement de la touche `LEFT`. Si le curseur ne se trouve pas au début d'une ligne, c'est *PrettyCurses::TextField(3)* qui intercepte la touche et déplace simplement ce curseur vers la gauche. Sinon, c'est *PrettyCurses::MultiFields(3)* qui intercepte la touche et le curseur est déplacé à la fin du champ précédent, le champ en cours est éventuellement supprimé s'il était vide.

`LEFT` ou `SHIFT-LEFT`
: Déplace le curseur à la fin du champ précédent. Efface le champ en cours si celui-ci était le dernier et vide et si le paramètre `READONLY` est positionné à `0`. La touche n'est pas interceptée si le champ actif était le premier.

`RIGHT` ou `SHIFT-RIGHT`
: Déplace le curseur au début du champ suivant. Si le champ en cours était le dernier, un nouveau champ est créé à moins que le nombre maximal de champs soit déjà atteint ou que le paramètre `READONLY` soit positionné à `0`. Dans ces derniers cas, la touche n'est pas interceptée.

`BACKSPACE`
: Regroupe le champ en cours avec le champ précédent. Cette touche n'est pas interceptée si le champ courant est le premier champ.

`DELETE`
: Regroupe le champ en cours avec le champ suivant. Cette touche n'est pas interceptée si le champ courant est le dernier champ.

`CONTROL-U`
: Efface tous les champs. Cette touche est ignorée si le paramètre `READONLY` est positionné à `1`.

`CONTROL-T`
: Applique les corrections automatiques. Cette touche n'est pas prise en compte si le paramètre `CORRECT` est positionné à `0` ou si le paramètre `READONLY` est positionné à `1`. Il faut noter que les *PrettyCurses::TextField(3)* utilisés sont appelés avec le paramètre `CORRECT` positionné à `0` de sorte qu'ils ne peuvent pas intercepter cette touche.

`CONTROL-PGUP`
: Remonte d'un cran dans l'historique. La touche n'est pas interceptée si on était déjà au début de l'historique. Cette touche est de toute façon ignorée si le paramètre `UNDO` est positionné à `0` ou si le paramètre `READONLY` est positionné à `1`.

`CONTROL-PGDOWN`
: Descend d'un cran dans l'historique. La touche n'est pas interceptée si on était déjà à la fin de l'historique. Cette touche est de toute façon ignorée si le paramètre `UNDO` est positionné à `0` ou si le paramètre `READONLY` est positionné à `1`.

PrettyCurses::Menu

NOM

PrettyCurses::Menu

SYNOPSIS

```
use PrettyCurses::Menu;

$w = PrettyCurses::Menu->new ({
        X                   =>     0,
        Y                   =>     0,
        HEIGHT_X            =>     10,
        HEIGHT_Y            =>     10,
        KEYS                =>     { },
        COLOR               =>     'default',
        BORDER              =>     1,
        DEFIL_BAR           =>     1,
        DRAW_AFTER_EXECUTE  =>     1,

        VALUE               =>     ,
        TREE                =>     [ ],
        ITEMS               =>     ,
        LENGTHS             =>     [ ],
        HEAD_LINE           =>     0,
        SELECTED_ITEM       =>     -1,
        COLORS              =>     [ ],
        MODE_SCROLL         =>     1,

        ENABLE_SEARCH       =>     1,
        CURRENT_FIELD       =>     -1,
        SEPARATOR           =>     '/',
        MAX_DEEP            =>     ,
        COLOR_FIELDS        =>     'fields',
        MODE_MODIFY         =>     1
});

$w->getParam ($name);
$w->setParam ( $name1 => $value1, ... );
$w->getValue ();

$w->draw ($PC_win, $focus);
$w->execute ($PC_win);
```

DESCRIPTION

Ce package implémente un widget menu qui offre des possibilités de sous-menus intégrés.

Chaque entrée du menu contient un certain nombre de champs fixé par la taille de la liste `LENGTHS`. C'est pour cette raison que les paramètres `CAPTION`, `LENGTHS` et `COLORS` sont des références sur des listes. Ceci alourdit certes la syntaxe parfois de façon inutile mais peut parfois être bien pratique.

Donnons tout de suite un exemple :

```
perl                                    rwx
|- librairies                           rwx
|  |- PrettyCurses.pm                   rw-
|  \- PrettyCurses                      rwx
|     |- Button.pm                      rw-
|     |- Caption.pm                     rw-
|     |- CheckBox.pm                    rw-
|     |- Corrections.pm                 rw-
|     |- default_french.pm              rw-
|     |- default.pm@                    rwx
|     |- directory.pm                   rw-
|     |- Form.pm                        rw-
|     |- Menu.pm                        rw-
|     |- Message.pm                     rw-
|     |- MultiFields.pm                 rw-
|     |- TextField.pm                   rw-
|     |- TextMemo.pm                    rw-
|     |- utils.pm                       rw-
|     \- Widgets.pm                     rw-
\- myprog.pl                            rw-
```

Ce menu est donc formé de deux champs : le premier correspond au nom du fichier et le deuxième aux droits que l'utilisateur a sur ce fichier. Ici `LENGTHS` pourra par exemple être initialisé à `[70, 3]`.

Fonction de recherche

Ce menu dispose en outre d'une fonction de recherche. Celle-ci est materialisée principalement par des champs de recherche, un par champ constituant une entrée. L'ensemble des valeurs de ces champs est appelé valeur de recherche.

Il est nécessaire de savoir lorsqu'une certaine valeur de recherche reconnaît une certaine entrée. Reprenons peut-être l'exemple précédent pour expliquer les choses. Chaque champ de recherche correspond à un champ du menu. Le premier est un *PrettyCurses::MultiFields(3)* dont chaque partie correspond à une sous-branche du menu. Les autres sont des *PrettyCurses::TextField(3)*. Pour qu'un certain texte soit reconnu par un champ de recherche, il faut que celui-ci commence par la valeur de ce champ. Par exemple, la valeur de recherche :

```
pe/lib/pretty/text
```

permet d'accéder aux entrées

```
perl/librairies/PrettyCurses/TextField.pm      rw-
perl/librairies/PrettyCurses/TextMemo.pm       rw-
```

Il est à noter que la différence minuscules / majuscules n'est pas prise en compte. Plus exactement, les recherches se font en tenant compte de la variable globale `$PC_order`.

La valeur de recherche

```
pe/lib/pretty/text                      rwx
```

n'aurait, quant à elle, reconnu aucune entrée.

Les champs de recherche peuvent contenir des jokers :

`?` Reconnaît n'importe quel caractère.

`*` Reconnaît n'importe quelle chaîne de caractères.

`$` Indique une fin de champ.

`[...]`
Propose une alternative. Par exemple `[abc]` reconnaît soit un `a`, soit un `b`, soit un `c`.

Pour le premier champ, il y a un dernier caractère spécial. La séquence « `**` » reconnaît un nombre arbitraire de menus intermédiaires. Ainsi, la valeur de recherche :

```
**/*.pm$
```

reconnaît toutes les entrées se terminant par `.pm`.

Finalement, il est possible d'introduire ces caractères sans leur donner le sens précis précédent en les protégeant par des « \ ».

Paramètres

Ici ne sont détaillés que les paramètres spécifiques au widget Menu. Pour les paramètres généraux, se reporter à *PrettyCurses::Widgets(3)*. Les valeurs qui sont données au début de cette page sont celles qui sont passés par défaut si elles ne sont pas initialisées lors de l'appel de la fonction `new`.

`BORDER`
Définit la taille de la bordure. S'il vaut `0`, aucune bordure n'est dessinée et les modes `SCROLL` et `MODIFY` ne sont pas affichés dans la barre d'état.

`DEFIL_BAR`
Précise si une barre de défilement doit être affichée (cas `DEFIL_BAR => 1`) ou si ce n'est pas nécessaire (cas `DEFIL_BAR => 0`). Celle-ci n'est de toute façon pas affichée s'il n'y a pas de bordure.

`TREE` Voir le paragraphe suivant.

`ITEMS`
Ce paramètre est un champ système ; il est donc tout à fait déconseillé d'y accéder directement, surtout en écriture. Il est créé automatiquement après une mise à jour des paramètres et est mis à jour dynamiquement lors de l'exécution du widget. Il contient la liste des entrées affichées sur l'écran auxquelles ont été ajoutées quelques pointeurs nécessaires à un déplacement efficace.

`LENGTHS`
Longueur des champs d'une entrée. Attention, on rappelle qu'il s'agit d'une référence sur une liste comme cela a été expliqué précédemment.

`HEAD_LINE`
Numéro de la première entrée affichée.

`SELECTED_ITEM`
Numéro de l'entrée sélectionnée. Il vaut `-1` si aucune entrée n'est sélectionnée.

`COLORS`
Couleur par défaut d'une entrée. Là encore, il s'agit d'une référence sur une liste.

`MODE_SCROLL`
Active (cas `MODE_SCROLL => 1`) ou désactive (cas `MODE_SCROLL => 0`) le mode `SCROLL`. Voir plus loin pour plus d'informations.

`ENABLE_SEARCH`
Précise s'il faut afficher les champs de recherche (cas `ENABLE_SEARCH => 1`) ou si ce n'est pas nécessaire (cas `ENABLE_SEARCH > 0`).

`CURRENT_FIELD`
Numéro du champ de recheche ayant le focus. S'il vaut `-1`, aucun de ces champs n'a le focus.

`MAX_DEEP`
Nombre maximal de ramifications autorisées dans le premier champ de recheche. S'il vaut `1`, le mode `SCROLL` n'est pas pris en considération.

COLOR_FIELD
: Couleur utilisée pour les champs de recherche.

MODE_MODIFY
: Active (cas `MODE_MODIFY => 1`) ou désactive (cas `MODE_MODIFY => 0`) le mode `MODIFY`. Il précise si les modifications faites dans le menu doivent se répercuter dans les champs de recherche et réciproquement. Voir plus loin pour plus d'informations.

Description du paramètre TREE

Il s'agit d'une référence sur la liste des entrées proposées dans le menu. Chaque entrée, disons `$item`, est une référence sur une table de hash devant respecter le format suivant :

```
$item =  {   CAPTION          =>     ,
             RETURN_VALUE     =>     ,
             COLORS           =>     ,
             SHOW_CHILDREN    =>     ,
             CHILDREN         =>     ,
             ARGV             =>     ,
             DYNAMIC          =>          };
```

CAPTION
: Intitulé de `$item`. Attention, on rappelle qu'il s'agit d'une référence sur une liste comme cela a été expliqué précédemment.

RETURN_VALUE
: Valeur à laquelle est positionné le paramètre global `VALUE` lorsque l'entrée en question est sélectionnée.

COLORS
: Couleur de `$item`. Là encore, il s'agit d'une référence sur une liste. Si une couleur n'est pas définie, la couleur correspondante dans la table référencée par le paramètre `COLORS` est utilisée.

SHOW_CHILDREN
: Précise s'il faut afficher les sous-menus disponibles dans cette entrée (cas `SHOW_CHILDREN => 1`) ou si ce n'est pas nécessaire (cas `SHOW_CHILDREN => 0`).

CHILDREN
: Deux cas sont possibles. 1) référence sur un objet de même type que `TREE` décrivant les entrées du sous-menu auquel on accède après avoir sélectionné `$item`. 2) référence sur un `CODE` dont la valeur de retour est comme décrit dans le cas précédent.

ARGV
: Référence sur la liste des arguments passée au code pointé par `CHILDREN`. Ce paramètre est ignoré dans le cas où `CHILDREN` ne contient pas une référence sur un `CODE`.

DYNAMIC
: Précise, dans le cas où `CHILDREN` contient une référence sur un `CODE`, si celui-ci doit être exécuté à chaque fois lorsqu'on désire accéder au sous-menu en question (cas `DYNAMIC => 1`) ou s'il n'est nécessaire d'exécuter le code que la première fois (cas `DYNAMIC => 0`).

Méthodes

Se reporter à la page *PrettyCurses::Widgets(3)*.

Touches interceptées lors de l'exécution

UP
: Sélectionne l'entrée précédente de même niveau.

`DOWN` Sélectionne l'entrée suivante de même niveau.

`PGUP` Sélectionne une entrée de même niveau suffisamment haute pour faire défiler l'écran

`PGDOWN`
Sélectionne une entrée de même niveau suffisamment basse pour faire défiler l'écran

`LEFT` Remonte au menu de niveau précédent. Efface le sous-menu fils si le mode `SCROLL` est actif.

`SHIFT-LEFT`
Remonte au menu de niveau précédent mais efface le sous-menu fils si le mode `SCROLL` est inactif.

`RIGHT`
Entre dans le sous-menu de l'entrée sélectionné s'il existe.

`ENTER`
Détaille le sous-menu de l'entrée sélectionné sans toutefois y entrer. La touche n'est pas interceptée s'il n'existe pas de tel sous-menu.

`DELETE`
Efface le sous-menu de l'entrée sélectionné au cas où il aurait été affiché.

`+` Détaille récursivement l'entrée selectionnée. Si aucune entrée n'est sélectionnée détaille récursivement tout l'arbre.

`-` Ordonne récursivement aux sous-menus du l'entrée selectionnée de ne plus afficher leurs sous-menus. Si aucune entrée n'est sélectionnée, ordonne cela à tous les sous-menus de l'arbre.

`CONTROL-UP`
Sélectionne l'entrée précédente la plus proche reconnue par la valeur de recherche en cours. Cette touche n'est pas interceptée si le paramètre `ENABLE_SEARCH` est positionné à `0`.

`CONTROL-DOWN`
Sélectionne l'entrée suivante la plus proche reconnue par la valeur de recherche en cours. Cette touche n'est pas interceptée si le paramètre `ENABLE_SEARCH` est positionné à `0`.

`CONTROL-END`
Retire le focus de tous les champs de recherche. Cette touche n'est pas interceptée si le paramètre `ENABLE_SEARCH` est positionné à `0`.

`CONTROL-U`
Efface la valeur de recherche actuelle. Le comportement global de `CONTROL-U` est donc le suivant. Si le champ en cours n'est pas vide, la valeur de ce champ est effacée. Si ce champ fait partie du premier champ de recherche et que celui-ci est vide, c'est ce premier champ de recherche tout entier qui est effacé s'il n'est pas vide. Si finalement cette touche est pressée sur un champ de recherche vide, c'est tous les champs de recherche qui sont simultanément effacés. Pour plus d'explications, consulter les pages *PrettyCurses::Widgets(3)*, *PrettyCurses::TextField(3)* et *PrettyCurses::MultiFields(3)*.

`M` ou `ALT-M`
Bascule le mode `MODIFY`.

`S` ou `ALT-S`
Bascule le mode `SCROLL`.

PrettyCurses::directory

NOM

PrettyCurses::directory

SYNOPSIS

```
use PrettyCurses::directory;

$d = PrettyCurses::directory->new ({
        CAPTION             =>     [ "__NAME()" ],
        RETURN_VALUE        =>     [ "__FULLPATH()" ],
        COLORS              =>     [ ],
        SHOW_CHILDREN       =>     0,
        DYNAMIC             =>     0,

        CODE                =>     "__NAME()",
        re_CODE             =>     qr/^[^\.]/,
        MAX_DEEP_SYMLINK    =>     5,

        HASH                =>     { }
});

$d->default ();

$d->getParam ($name);
$d->setParam ( $name1 => $value1, ... );
$d->setHash ( $name1 => $value1, ... );

$d->maketree ($dir);
```

DESCRIPTION

Ce package permet de construire un objet pouvant servir de paramètre `TREE` d'un *PrettyCurses::Menu(3)* dénotant toute l'arborescence d'un certain répertoire.

Pour cela, il est d'abord nécessaire de définir un format via la fonction `new`. L'appel de la fonction `maketree` crée alors l'objet souhaité.

Créer un nouveau format

Ceci se fait donc par l'intermédiaire de la fonction `new` dont la syntaxe a été détaillé précédemment. Les valeurs qui ont été assignées aux différents paramètres correspondent aux valeurs assignées par défaut. Si aucun argument n'est fourni lors de l'appel de la fonction `new`, ce sont ceux de la variable globale `$PC_directory_default` qui sont utilisés.

Mais détaillons tout de suite ce que sont ces paramètres.

`CAPTION`, `RETURN_VALUE`, `COLORS`, `SHOW_CHILDREN`, `DYNAMIC`
: Correspondent aux paramètres analogues d'un objet de type `TREE` (voir *PrettyCurses::Menu(3)*). Ils peuvent contenir des codes spéciaux qui seront détaillés dans le paragraphe suivant.

`CODE`, `re_CODE`
: `CODE` est un champ de caractères quelconque pouvant inclure lui aussi les codes spéciaux du paragraphe suivant. Un fichier est ajouté à l'objet qui va être créé si et seulement si l'expression régulière `re_CODE` reconnaît son `CODE`.

`MAX_DEEP_SYMLINK`
: Profondeur maximale pour suivre les liens symboliques.

`HASH` Référence sur une table de hash servant aux codes spéciaux précédents.

Description des codes spéciaux

Les codes spéciaux sont :

`__NAME()`
: Ce code est remplacé par le nom du fichier.

`__FULLPATH()`
: Ce code est remplacé par le chemin complet du fichier.

`__TYPE()`
: Ce code est remplacé par le type du fichier. Les types reconnus sont « `file` », « `directory` », « `FIFO` », « `socket` », « `block` » et « `character` ». Si le fichier est un lien symbolique le type est précédé de la chaîne de caractères « `symlink/` ».

`__READABLE()`
: Ce code est remplacé par « `r` » si l'utilisateur peut lire le fichier en question, par « - » si ce n'est pas le cas.

`__WRITABLE()`
: Ce code est remplacé par « `w` » si l'utilisateur peut modifier le fichier en question, par « - » si ce n'est pas le cas.

`__EXECUTABLE()`
: Ce code est remplacé par « `r` » si l'utilisateur peut exécuter le fichier en question, par « - » si ce n'est pas le cas.

Si une chaîne de caractères, disons `$code`, apparaît entre les parenthèses précédentes, les choses se passent de la façon suivante. C'est là qu'intervient le paramètre global `HASH`. Il est nécessaire de décrire sa structure. Il s'agit d'une référence sur une table de hash, disons `$hash` ayant la structure suivante :

```
$hash = { $code1 => [ qr/$regexp1.1/ => $string1.1, ... ],
          $code2 => [ qr/$regexp2.1/ => $string2.1, ... ],
          ...
        };
```

Dans le cas précédent, donc, on regarde si `$code` apparaît comme clé dans la table de hash `$hash`. Si ce n'est pas le cas, le comportement est le même que s'il n'y avait rien entre parenthèses. Si par contre, c'est le cas, on regarde dans l'ordre si la valeur qui devait être remplacée est reconnu par l'une des expressions régulières associées au code `$code`. Si ce n'est pas le cas, le comportement est encore celui décrit précédemment. Si par contre c'est le cas, le code spécial est remplacée par la valeur correspondante.

Les `$string` peuvent contenir des `$1`, `$2`, etc. Ils auront le comportement souhaité sauf s'ils sont protégés par des « \ ». Attention, les `$string` doivent vraiment être des chaînes de caractères ; il n'est par exemple pas question de définir ainsi une couleur par sa table de hash.

Finalement, il est possible de protéger ces codes spéciaux par des « \ ».

Méthodes

`$d->default ();`
Réinitialise les paramètres à ceux de la variable globale `$PC_directory_default`.

`$d->getParam ($name);`
Renvoie la valeur du paramètre `$name`.

`$d->setParam ( $name1 => $value1, ... );`
Affecte la valeur `$value1` au paramètre `$name1` et ainsi de suite.

`$d->setHash ( $code1 => [ qr/$regexp1.1/ => $string1.1, ... ], ...);`
Affecte à la clé `$code1` de la table de hash référencée par le paramètre `HASH` la valeur correspondante, et ainsi de suite.

`$d->maketree ($dir);`
Renvoie un objet de type `TREE` qui décrit l'arborescence du répertoire `$dir`.

PrettyCurses::CheckBox

NOM

PrettyCurses::CheckBox

SYNOPSIS

```
use PrettyCurses::CheckBox;

$w = PrettyCurses::CheckBox->new ({
        X                   =>     0,
        Y                   =>     0,
        VALUE               =>     0,
        KEYS                =>     { },
        READONLY            =>     0,
        UNDO                =>     1,
        COLOR               =>     'fields',
        DRAW_AFTER_EXECUTE  =>     1
});

$w->getParam ($name);
$w->setParam ( $name1 => $value1, ... );
$w->getValue ();
$w->setValue ($value);

$w->draw ($PC_win, $focus);
$w->execute ($PC_win);

$w->undo ($PC_win, $focus);
$w->redo ($PC_win, $focus);
$w->save_position ($name);
$w->remove_position ($name);
$w->addinhistory ($name);
$w->clearhistory ();
```

DESCRIPTION

Ce package implémente un widget CheckBox (case à cocher). Seulement la case est gérée par ce package. Pour rajouter une légende, se reporter à *PrettyCurses::Caption(3)* ou encore à *PrettyCurses::Form(3)*.

Paramètres

Pour les paramètres généraux, se reporter à la page *PrettyCurses::Widgets(3)*. Les valeurs qui sont données ci-dessus sont celles qui sont passés par défaut si elles ne sont pas initialisées lors de l'appel de la fonction `new`.

Le paramètre `VALUE` est positionné à `1` lorsque la case est cochée et à `0` si elle ne l'est pas.

Méthodes

Se reporter à la page *PrettyCurses::Widgets(3)*.

Touches interceptées lors de l'exécution

`SPACE`
: Coche ou décoche la case.

`CONTROL-PGUP`
: Remonte d'un cran dans l'historique. La touche n'est pas interceptée si on était déjà au début de l'historique. Cette touche est de toute façon ignorée si le paramètre `UNDO` est positionné à `0`.

`CONTROL-PGDOWN`
: Descend d'un cran dans l'historique. La touche n'est pas interceptée si on était déjà à la fin de l'historique. Cette touche est de toute façon ignorée si le paramètre `UNDO` est positionné à `0`.

PrettyCurses::Button

NOM

PrettyCurses::Button

SYNOPSIS

```
use PrettyCurses::Button;

$w = PrettyCurses::Button->new ({
        X                   =>     0,
        Y                   =>     0,
        HEIGHT_X            =>     length (CAPTION) + 4,
        HEIGHT_Y            =>     1,
        CAPTION             =>     'OK',
        KEYS                =>     { },
        COLOR               =>     'default',
        DRAW_AFTER_EXECUTE  =>     1
});

$w->getParam ($name);
$w->setParam ( $name1 => $value1, ... );

$w->draw ($PC_win, $focus);
$w->execute ($PC_win);
```

DESCRIPTION

Ce package implémente un widget Button (bouton).

Paramètres

Pour les paramètres généraux, se reporter à la page *PrettyCurses::Widgets(3)*. Les valeurs qui sont données ci-dessus sont celles qui sont passés par défaut si elles ne sont pas initialisées lors de l'appel de la fonction `new`.

Le paramètre `CAPTION` correspond au texte noté sur le bouton.

Méthodes

Se reporter à la page *PrettyCurses::Widgets(3)*.

Touches interceptées lors de l'exécution

`ENTER`
: Arrête l'exécution du widget en renvoie le code « `/BUTTONPRESS` » suivi de la valeur du paramètre `CAPTION`. Si le paramètre `KEYS` précisait qu'il fallait intercepter la touche `ENTER`, cette interception est prioritaire.

PrettyCurses::Form

NOM

PrettyCurses::Form

SYNOPSIS

```
use PrettyCurses::Form;

$w = PrettyCurses::Form->new ({
        X                   =>     0,
        Y                   =>     0,
        HEIGHT_X            =>     10,
        HEIGHT_Y            =>     10,
        KEYS                =>     { },
        READONLY            =>     0,
        UNDO                =>     0,
        CORRECT             =>     1,
        COLOR               =>     'default',
        CLEAR               =>     1,
        BORDER              =>     1,
        DEFIL_BAR           =>     1,
        DRAW_BEFORE_EXECUTE =>     0,
        DRAW_AFTER_EXECUTE  =>     0,

        HEAD_LINE           =>     0,
        CURRENT             =>     '__first',

        EMPTYLINES_BEFORE   =>     0,
        X_FIELDS            =>     ,
        HEIGHT_X_FIELDS     =>     ,
        HEIGHT_Y_FIELDS     =>     1,
        VALUE               =>     ,
        EXECUTE             =>     1,
        UNDO_FIELDS         =>     ,
        CORRECT_FIELDS      =>     ,
        COLOR_FIELDS        =>     ,
        COLOR_ERR           =>     ,
        DAE_FIELDS          =>     ,
        CAPTION_Xrel        =>     0,
        CAPTION_Yrel        =>     0,
        CAPTION_COLOR       =>     'default',

        RECURSIVE           =>     2
});

$w->getParam ($name);
$w->setParam ( $name1 => $value1, ... );
$w->getField ($field_name);
$w->setField ($field_name, { $name1 => $value1, ... });
$w->getWidget ($field_name);
```

```
$w->getFields ();
$w->getValues ();

$w->append ($field1, ...);
$w->add_before ($field_name, $field1, ...);
$w->add_after ($field_name, $field1, ...);
$w->delete ($field_name);

$w->draw ($PC_win, $focus);
$w->execute ($PC_win);

$w->correct ($PC_win, $focus);

$w->undo ($PC_win, $focus);
$w->redo ($PC_win, $focus);
$w->save_position ($name);
$w->remove_position ($name);
$w->addinhistory ($name);
$w->clearhistory ();
```

DESCRIPTION

Ce package implémente un widget Form. Il s'agit d'un formulaire pouvant contenir nombre d'autres widgets qui sont donc gérés ici.

Paramètres

Ici ne sont détaillés que les paramètres spécifiques au widget Menu. Pour les descriptions générales, se reporter à la page *PrettyCurses::Widgets(3)*. Les valeurs qui sont données ci-dessus sont celles qui sont passés par défaut si elles ne sont pas initialisées lors de l'appel de la fonction `new`.

`CLEAR`
: Précise s'il faut effacer l'ancien formulaire dessiné avant d'en dessiner un nouveau via la commande `draw`. Il peut être utile de positionner ce paramètre à `0` si l'on fait beaucoup d'appels à la fonction `draw` afin que l'écran ne *clignote* pas trop.

`BORDER`
: Précise la taille de la bordure. Si ce paramètre est positionné à `0`, aucune bordure n'est dessinée.

`DEFIL_BAR`
: Précise s'il faut dessiner une barre de défilement (cas `DEFIL_BAR => 1`) ou si ce n'est pas nécessaire (cas `DEFIL_BAR => 0`). Si aucune bordure n'est dessinée, la barre de défilement est de toute façon ignorée.

`DRAW_BEFORE_EXECUTE`
: Précise s'il faut redessiner le formulaire avant l'exécution (cas `DRAW_BEFORE_EXECUTE => 1`) ou si ce n'est pas nécessaire (cas `DRAW_BEFORE_EXECUTE => 0`).

`HEAD_LINE`
: Numéro de la première ligne affichée à l'écran.

`CURRENT`
: Nom du champ courant.

`RECURSIVE`
: Stipule si les paramètres globaux doivent être passés automatiquement aux divers champs. Si `RECURSIVE` est positionné à `0`, la fonction `setField` (détaillée plus loin) n'est jamais appelée

automatiquement. S'il est positionné à `1`, la fonction `setField` est appelée automatiquement sur tous les champs nouvellement créés. S'il est positionné à `2`, la fonction `setField` est de plus appelée après sur tous les champs après chaque appel à la fonction `setParam`. S'il est positionné à une valeur négative via la commande `setParam`, aucun appel à `setField` n'est fait lors de ce positionnement, mais le signe est supprimé de sorte que les appels suivants pourront tenir compte de la valeur affectée.

Les autres paramètres ne se rapportent pas à proprement parler au formulaire. Ils sont simplement passés par défaut aux divers champs que le formulaire va contenir.

Format des champs du formulaire

Les champs du formulaires sont stockées dans une liste doublement chaînée (implémentée au moins d'une table de hash). Cette liste contient deux éléments particuliers qui sont « `__first` » et « `__last` » qui sont situés respectivement avant le premier champ et après le dernier. Les autres éléments de cette liste sont des tables de hash qui doivent obéir au format suivant :

```
$field = {   NAME                =>     ,
             EMPTYLINES_BEFORE   =>     ,
             WIDGET              =>     ,
             X_FIELDS            =>     ,
             HEIGHT_X_FIELDS     =>     ,
             HEIGHT_Y_FIELDS     =>     ,
             VALUE               =>     ,
             EXECUTE             =>     ,
             READONLY            =>     ,
             UNDO_FIELDS         =>     ,
             CORRECT_FIELDS      =>     ,
             COLOR_FIELDS        =>     ,
             COLOR_ERR           =>     ,
             DAE_FIELDS          =>     ,
             CAPTION             =>     ,
             CAPTION_Xrel        =>     ,
             CAPTION_Yrel        =>     ,
             CAPTION_COLOR       =>          };
```

Les valeurs par défaut données à ces paramètres sont celles des paramètres globaux correspondant s'ils existent.

`NAME` Nom du champ. Si aucun nom n'est passé, un nom sera attribué automatiquement. Il peut être parfois utile de ne pas s'encombrer de noms mais ce n'est pas forcément une bonne idée.

`EMPTYLINES_BEFORE`
Nombre de lignes à sauter avant d'afficher le champ en question. Ce nombre peut très bien être négatif.

`WIDGET`
Widget implémentant le champ en question. Il n'est demandé au dit widget que de connaître les paramètres et les méthodes présentés dans *PrettyCurses::Widgets*.

`X_FIELDS`
Position horizontale du champ. Ce nombre peut être négatif auquel cas la position est comptée à partir du bord droit du formulaire.

`HEIGHT_X_FIELDS`
Taille horizontale du champ. Ce nombre peut-être négatif auquel cas le champ occupera toute la largeur du formulaire sauf le nombre de caractères précisé.

`HEIGHT_Y_FIELDS`
: Taille verticale du champ. Ce nombre peut-être négatif auquel cas le champ occupera toute la hauteur du formulaire sauf le nombre de ligne précisé.

`VALUE`
: Valeur du champ. Cette valeur est passée au widget via la commande `setValue`. Ainsi, si par exemple le widget est un *PrettyCurses::TextField(3)*, elle devra être renseignée à `" Bonjour "` et non à `[ [ "Bonjour" ] ]`. Voir *PrettyCurses::TextField(3)* pour plus d'informations.

`EXECUTE`
: Précise si ce widget doit être exécuté (cas `EXECUTE => 1`) ou si on doit simplement y passer dessus (cas `EXECUTE => 0`).

`READONLY`
: Précise si le champ doit être en lecture seule (cas `READONLY => 1`) ou si ce n'est pas le cas (cas `READONLY => 0`). Si le paramètre global `READONLY` est positionné à `1`, le champ sera de toute façon en lecture seule.

`UNDO_FIELDS`
: Précise si le champ doit retenir son historique et gérer les combinaisons de touches `CONTROL-PGUP` et `CONTROL-PGDOWN` (cas `UNDO_FIELDS => 1`) ou si ce n'est pas nécessaire (cas `UNDO_FIELDS => 0`). Si le paramètre global `UNDO` est positionné à `1`, ce paramètre sera affecté de la valeur `0` quoi qu'il arrive. Il est conseillé, pour des question de légèreté, de laisser les widgets gérer leur propre histoirique et de désactiver cette option pour le formulaire.

`CORRECT_FIELDS`
: Précise si le champ doit intercepter la combinaison de touches `CONTROL-T` afin de faire les corrections automatiques (cas `CORRECT_FIELDS => 1`) ou si ce n'est pas nécessaire (cas `CORRECT_FIELDS => 0`).

`COLOR_FIELDS`
: Couleur du champ.

`COLOR_ERR`
: Couleur que le champ doit utiliser pour les erreurs. Voir *PrettyCurses::TextField(3)*.

`DAE_FIELDS`
: Les initiales « `DAE` » signifient « `DRAW_AFTER_EXECUTE` ». Ce paramètre précise si le champ doit être redessiné après avoir été executé (cas `DAE_FIELDS => 1`) ou si ce n'est pas nécessaire (cas `DAE_FIELDS => 0`). Le champ courant n'est jamais redessiné si un événement `ON_PRESS` ou `ON_MODIFY` est intercepté.

`CAPTION`
: Texte de légende servant à introduire le champ.

`CAPTION_Xrel` et `CAPTION_Yrel`
: Position du texte précédent comptée relativement par rapport à la position du champ.

`CAPTION_COLOR`
: Couleur qu'il faut utiliser pour écrire le texte précédent.

Méthodes

Ici ne sont détaillés que les méthodes spécifiques au widget Menu. Pour les descriptions générales, se reporter à la page *PrettyCurses::Widgets(3)*.

Gestion des paramètres

`$w->getField ($field_name, $name);`
: Renvoie la valeur du paramètre `$name` du champ nommé `$field_name`. Renvoie `undef` si le champ `$field_name` n'existe pas.

`$w->setField ($field_name, { $name1 => $value1, ... });`
Met à jour la table de hash du champ `$field_name`.

`$w->getWidget ($field_name);`
Renvoie le widget du champ `$field_name`.

Gestion des champs

`$w->getFields ();`
Renvoie la liste des champs présents sur le formulaire dans l'ordre.

`$w->getValues ();`
Renvoie une liste qui associe à chaque nom de champ sa valeur, cette valeur étant récupérée via la commande `getValue`. La format de la liste renvoyée est `($name1, $value1, $name2, $value2, ...)`.

`$w->append ($field1, ...);`
Ajoute les champs `$field1`, `$field2`, etc. à la fin. Les arguments `$field` doivent être des tables de hash respectant le format décrit au chapitre précédent.

`$w->add_before ($field_name, $field1, ...);`
Ajoute les champs `$field1`, `$field2`, etc. juste avant le champ nommé `$field_name`. Ne fait rien si le champ `$field_name` n'existe pas. Les arguments `$field` doivent être des tables de hash respectant le format décrit au chapitre précédent.

`$w->add_after ($field_name, $field1, ...);`
Ajoute les champs `$field1`, `$field2`, etc. juste après le champ nommé `$field_name`. Ne fait rien si le champ `$field_name` n'existe pas. Les arguments `$field` doivent être des tables de hash respectant le format décrit au chapitre précédent.

`$w->delete ($field_name);`
Supprime le champ nommé `$field_name` du formulaire. Ne teste pas si malencontreusement le champ courant donné par le paramètre global `CURRENT` était précisément celui-ci.

Touches interceptées lors de l'exécution

Bien entendu, *PrettyCurses::Menu(3)* fait appel à chacun des widgets proposés. Il est donc très fréquent que le widget appelé intercepte la touche sans que *PrettyCurses::Menu(3)* soit au courant. Normalement, tout est fait correctement pour que le comportement attendu soit celui qui se passe réellement.

`LEFT` Se déplace à la fin du champ précédent. Si le focus était déjà donné au premier champ, la touche n'est pas interceptée.

`UP` Se déplace au début du champ précédent. Si le focus était déjà donné au premier champ, la touche n'est pas interceptée.

`RIGHT`, `DOWN`, `TAB`, `ENTER`
Se déplace au début du champ suivant. Si le focus était déjà sur le dernier champ, la touche n'est pas interceptée.

`PGUP` Se déplace au début d'un champ précédent suffisamment loin pour faire défiler l'écran.

`PGDOWN`
Se déplace au début d'un champ suivant suffisamment loin pour faire défiler l'écran.

`DOUBLE CONTROL-T`
Fait les corrections automatiques sur tous les champs du formulaire pour lesquels le paramètre `CORRECT_FIELDS` est positionné à `1`. La touche `DOUBLE CONTROL-T` s'obtient en double-appuyant (comme double-cliquant mais au clavier) sur la combinaison de touches `CONTROL-T`. La touche est de toute façon ignorée si le paramètre `READONLY` est positionné à `1`.

`CONTROL-PGUP`
: Remonte d'un cran dans l'historique. La touche n'est pas interceptée si on était déjà au début de l'historique. Cette touche est de toute façon ignorée si le paramètre `UNDO` est positionné à `0` ou si le paramètre `READONLY` est positionné à `1`.

`CONTROL-PGDOWN`
: Descend d'un cran dans l'historique. La touche n'est pas interceptée si on était déjà à la fin de l'historique. Cette touche est de toute façon ignorée si le paramètre `UNDO` est positionné à `0` ou si le paramètre `READONLY` est positionné à `1`.

Table des matières