L'ÉQUATION AUX S-UNITÉS

Rapport final de PSC
Diego Izquierdo - MAT 01

30 avril 2020

Khalil Bendriss, Paul Boisseau, Adam David, Félix Rebotier, Louis Rustenholz

TABLE DES MATIÈRES

INTRODUCTION

La pensée peut être munie d'objets abstraits qui l'incarnent, la cristallisent, et prennent leur propre vie, se libérant du flux continu et tumultueux des idées. Dans cette naissance du raisonnement, les nombres sont des compagnons rencontrés tôt. Les nombres – entiers tout d'abord – ne sont pas seulement des objets élémentaires du monde mathématique : ils sont également fondamentaux.

La théorie des nombres fournit des problèmes qui, si leur énoncé est remarquablement simple, ont tenu en échec des générations de mathématiciens, pendant plusieurs siècles. C'est que les structures qui vivent dans les nombres sont riches et complexes : en les étudiant sous le prisme de théories mathématiques variées, on y découvre des connexions profondes qui deviennent idées fécondes.

Ce livre n'a aucunement la prétention d'offrir une visite guidée exhaustive de cet univers. On va plutôt s'y balader et choisir sur la carte – au milieu de territoires inconnus – un objectif qui nous permettra d'autant mieux explorer. Au cours de notre voyage, on aura ainsi l'occasion d'étudier la géométrie des nombres, d'observer les symétries de structures algébriques qui s'y cachent, ou de relâcher notre regard pour s'éclipser dans un monde analytique plus lisse.

Notre objectif final, ce point bien localisé sur la carte, a un nom : *l'équation aux S-unités*.

Cadre et objectifs du voyage

Ce voyage mathématique a lieu dans le cadre du Projet Scientifique Collectif (PSC), proposé par l'École polytechnique aux élèves de deuxième année du cycle ingénieur. Nous sommes ainsi 5 à nous y être lancés, guidés et soutenus par notre tuteur, Diego Izquierdo.

L'objectif de cet ouvrage est multiple.

Le premier objectif, qui guide la structure du texte, est la démonstration d'un résultat puissant pour l'étude des équations diophantiennes : la finitude de l'équation aux S-unités. Plus précisément, on s'intéresse à la preuve proposée en 1996 par Beukers et Schlickewei, qu'on placera dans son contexte scientifique et dont on présentera l'intérêt dans la suite de cette introduction.

Notre deuxième objectif a été, en restituant l'ensemble de nos recherches dans un unique texte, de permettre au lecteur d'étudier ce théorème et sa preuve en limitant autant que possible les lectures annexes. En effet, la compréhension de l'article de Beukers et Schlickewei présuppose la connaissance de notions et résultats qui, s'ils sont bien sûr traités dans la littérature, ne sont généralement abordés que dans des cours de niveau M2, voire souvent connus des seuls spécialistes. Notre ambition a donc été de construire un parcours cohérent, permettant au lecteur dès le niveau de L3, voire L2, de comprendre et se construire une intuition du théorème et du monde mathématique qui le soutient. Pour cela, il nous a fallu reconstruire de nombreux résultats intermédiaires, réinterpréter et adapter des démonstrations, etc. : construire une démarche et son intuition.

Notre troisième objectif concerne les utilisations de ce document : sa quasi-totalité présente des mondes mathématiques qui prennent sens bien au-delà de l'étude de l'équation aux S-unités. Nous avons nous-mêmes tiré énormément partie de nombreux mémoires mis à disposition par leur auteurs, quand bien même ce que nous y cherchions ne représentait qu'une fraction du texte – souvent pas son objectif final. Nous espérons ainsi que cet ouvrage saura trouver des lecteurs pour lesquels il sera un apport dans leurs propres recherches.

Contexte scientifique : le monde diophantien

La question scientifique centrale, qui fait naître les théories développées dans ce document, est la suivante : comment d'étudier les équations – polynomiales – à solutions entières ? On parle d'*équations diophantiennes*.

S'il peut sembler plus naturel de chercher les solutions de ces équations dans les entiers, qui sont a priori des objets plus simples que les réels par exemple, cette restriction rend en fait le problème beaucoup plus difficile – on pourra aussi dire que c'est ce qui en fait le charme.

Au-delà du charme, pourquoi chercher des solutions entières ? C'est le naturel qui revient : en logistique, et donc en optimisation opérationnelle, on travaille souvent *in fine* avec une quantité entière d'objets. De ce fait, ces problèmes sont généralement très difficiles ! En informatique, l'univers est fini et discret : il faut le comprendre pour aborder la cryptographie, la compression et la correction automatique de signaux, ou quantité d'autres domaines. Plus généralement, on peut se contenter de dire que les nombres entiers sont fondamentaux et réapparaissent naturellement lors de l'étude de nombreux objets.

On peut aborder un point de vue géométrique sur cette question : étudier les solutions entières d'équations polynomiales, c'est *étudier les points entiers de variétés algébriques*.

Les question sont alors les suivantes. Est-ce qu'il y a des points entiers ? Est-ce qu'il y en a beaucoup ? À quelle densité ? Un nombre fini ? Y a-t-il une structure sur ces points, algébrique ou géométrique ?

C'est la morale moderne du monde diophantien, nourri de géométrie algébrique : les propriétés arithmétiques sont contrôlées par des propriétés géométriques !

Historiquement,

- Pendant plusieurs siècles, seules quelques équations particulières ont pu être traitées, laborieusement, souvent de façon ad-hoc et au cas par cas.
- Une prise de recul permet néanmoins de construire de puissants outils et stratégies au XVIIème et XVIIIème siècle.

  Au XVIIème Fermat introduit quelques grands problèmes (l'équation de Pell-Fermat sur laquelle on reviendra plusieurs fois, ou la dernière conjecture de Fermat qui n'est devenue le théorème de Fermat-Wiles que trois siècles plus tard en 1994), et propose des démonstrations par descente infinie – certaines erronées – de divers résultats sur des équations particulières.

  Le siècle suivant, Euler, Lagrange, Legendre et Gauss font partie de ceux qui développent la profondeur théorique du domaine. Par exemple, de premiers travaux en théorie analytique des nombres sont entrepris, et la loi de réciprocité quadratique est démontrée.

- Le XIXème siècle apporte un enrichissement considérable de la théorie des nombres. Pour ne retenir qu'un nom, évoquons celui de Dirichlet : on le retrouvera de nombreuses fois dans ce livre, par exemple aux chapitre 3 où on parlera de l'arithmétique des idéaux, qui permet de généraliser la notion de décomposition en facteurs premiers à des anneaux qui n'en admettent pas, ou quand on montrera au chapitre 4 le *théorème des unités de Dirichlet*, profond résultat de théorie algébrique des nombres.
- Grâce à cette nouvelle profondeur, le début du XXème siècle conçoit enfin les premiers outils généraux pour aborder les équations diophantiennes. On voit ainsi apparaître la théorie des hauteurs (introduite aux chapitre 5 et 6), qui mesure la complexité algébrique de solutions d'équations diophantiennes, ou des méthodes dues à Axel Thue qui s'appuient sur l'approximation diophantienne mais qu'on n'aborde pas ici.

  C'est en 1909 que Thue démontre un théorème qui sera peu à peu amélioré pour aboutir en 1996 au résultat de Beukers et Schlickewei qu'on étudie ici.

  On en reparlera un peu plus tard, mais on peut déjà dire ceci : il s'agit, enfin, d'un résultat de finitude non trivial qui peut s'appliquer à une large classe d'équations.
- En 1983 Gerd Faltings démontre un résultat majeur, très profond, qui lui vaudra la médaille Fields en 1986. Quand on dit que « les propriétés arithmétiques sont contrôlées par des propriétés géométriques », ont fait largement référence à ça.

  On cite ce théorème de façon informelle. Il est la démonstration d'une conjecture émise par Louis Mordell en 1922, qui avait par ailleurs démontré en 1920 un théorème qu'on va citer par la même occasion.

> **Théorème 1** (Théorème de Faltings)**.** *Considérons une courbe algébrique C définie, pour un polynôme $P \in \mathbb{Q}[X, Y]$, par l'équation*
>
> $$(C) \ : \quad P(x, y) = 0.$$
>
> *On cherche à caractériser le nombre X de points de C à coordonnées rationnelles.*
> ***Le nombre de solutions dépend du genre de** C (qui correspond intuitivement à son nombre de trous).*
>
> - *Si le genre vaut 0, alors $X = 0$ ou $X = \infty$.*
> - *Si le genre vaut 1, alors $X = 0$ ou C est une courbe elliptique. Dans ce deuxième cas, Mordell a montré en 1920 que l'on pouvait munir les points rationnels de C d'une structure de groupe abélien de type fini.*
> - *Si le genre est plus grand ou égal à 2, alors $X < \infty$. C'est le point démontré par Faltings.*

- Le théorème de Faltings est très puissant, mais il n'est absolument pas explicite. En particulier, dans le cas de finitude, on n'a aucune borne sur la densité de solutions, voire sur le nombre de solutions. Un domaine de recherche actuel très actif consiste à *expliciter Faltings*, de façon à pouvoir par exemple s'en servir dans des algorithmes ou dans des

raisonnements numériques. C'est là qu'intervient l'équation aux S-unités : elle fournit un angle d'attaque intéressant, puisque le théorème de finitude associé est au contraire très explicite.

Avant d'enfin énoncer le théorème de l'équation aux S-unités, présentons rapidement quelques classes d'équations diophantiennes particulières qu'il est intéressant d'étudier.

- On en reparlera plus tard, mais les grandes équations historiques ont bien sûr un intérêt illustratif. Citons l'équation de Pell-Fermat, sur laquelle on reviendra. Il s'agit de considérer $n \in \mathbb{N}$ qui n'est pas un carré parfait, $m \in \mathbb{Z}^*$, et d'étudier les solutions $x, y \in \mathbb{Z}$ de
$$x^2 - ny^2 = m.$$
- Le théorème de Mordell (énoncé plus haut) s'applique aux courbes elliptiques, et participe à leur conférer un intérêt particulier.
  Elles apparaissent à la fois dans un nombre croissant d'applications informatiques et dans des questions profondes de mathématiques pures. Elles apparaissent par exemple dans la conjecture de Shimura-Taniyama-Weil, en lien avec des « courbes modulaires » : la démonstration de cette conjecture a permis de démontrer le théorème de Fermat-Wiles. On peut également citer la conjecture de Birch et Swinnerton-Dyer, un des sept problèmes du millénaire (à ce jour seule la conjecture de Poincaré a été résolue par Grigori Perelman), qui s'énonce en reliant avec elles des objets analytiques.
  Informellement, elles sont décrites par les équations de la forme suivante, où $f \in \mathbb{Q}[X]$ est un polynôme unitaire de degré 3 :
$$y^2 = f(x).$$
- Nous venons de le dire, le théorème de Mordell s'applique aux courbes elliptiques : elles sont de genre 1. Pour voir plus large que cette contrainte, on peut s'intéresser aux courbes *hyperelliptiques*, définies par les équations de la forme suivante, où $f \in \mathbb{Q}[X]$:
$$y^2 = f(x).$$
  Le genre de la courbe est alors contrôlé par le degré de f.

Le théorème

Le décor étant placé, passons enfin à l'énoncé du théorème dont la démonstration est l'objectif final de ce livre.

On parlera de son histoire dans la partie suivante, puis on présentera quelques applications (qui ne seront pas étudiées dans ce texte).

On va maintenant présenter l'équation aux S-unités dans le contexte de $\mathbb{Z}$, puis dans un contexte plus général, puis montrer sur un cas élémentaire non trivial que ses solutions sont en nombre fini. Remarquez la simplicité de cette équation : c'est ce qui explique que de nombreux problèmes diophantiens s'y ramènent.

• Un premier cadre pour l'équation : $\mathbb{Z}_S$

Dans $\mathbb{Z}$, l'équation aux S-unités peut s'énoncer de la manière suivante.
Étant donné S un ensemble fini de nombres premiers, on se demande si l'équation

$$x + y = z$$

admet un nombre fini de solutions $(x, y, z) \in \mathbb{Z}^3$ telle que x, y, z sont deux à deux premiers entre eux et ont tous leurs facteurs premiers dans S.

On peut d'ores et déjà réécrire cette équation en posant $S = \{p_1, ..., p_s\}$ et $\mathbb{Z}_S$ l'anneau $\mathbb{Z}[p_1^{-1}, ..., p_s^{-1}]$. L'équation aux S-unités devient alors

$$x + y = 1,$$

où $x, y \in \mathbb{Z}_S^\times$, l'ensemble des éléments inversibles de $\mathbb{Z}_S$, qui peut-être ici explicité :

$$\mathbb{Z}_S^\times = \left\{ \pm\, p_1^{r_1} ... p_s^{r_s} \;\middle|\; p_i \in S,\, r_i \in \mathbb{Z} \right\}.$$

Avec cette formulation, on dispose du théorème suivant, démontré par le mathématicien d'origine allemande Kurt Mahler en 1933 [1].

Théorème 2 (Mahler, 1933)**.** *Soit $S = \{p_1, ..., p_s\}$ un ensemble de nombres premiers distincts. L'équation d'inconnues $x, y \in \mathbb{Z}_S^\times$*

$$x + y = 1$$

admet un nombre fini de solutions.

Mahler propose déjà en 1933 une borne du nombre de solutions, mais elle est très mauvaise et apporte peu d'informations.

Il est possible de considérer ce résultat sur des structures plus générales.

• Le cadre général de $\mathcal{O}_{K,S}$

Dans la première expression de l'équation, on travaillait dans $\mathbb{Z}_S$ qui était un sous-anneau de $\mathbb{Q}$. L'idée est maintenant de voir ce qui se passe pour des corps plus gros, mais qui ont toujours des propriétés assez agréables pour qu'on puisse y formuler le problème.

On verra dans le rapport que ce cadre naturel est celui des corps de nombres, c'est-à-dire des extensions finies de $\mathbb{Q}$.

Dans le cas de K un corps de nombres, on verra que c'est l'anneau des entiers algébriques de K, noté $\mathcal{O}_K$, qui joue un rôle analogue à $\mathbb{Z}$ en préservant certaines propriétés, par exemple une certaine notion de primalité. La reformulation est alors la suivante.

Définition 0.0.1. Soient K un corps de nombres et $S = \{a_1, ..., a_s\} \subset \mathcal{O}_K$ un ensemble fini. On définit $\mathcal{O}_{K,S}$ par

$$\mathcal{O}_{K,S} = \mathcal{O}_K[a_1^{-1}, ..., a_s^{-1}].$$

Ainsi, si on note $\langle S \rangle$ la partie multiplicative engendrée par S, c'est à dire l'ensemble des produits d'éléments de S, on a

$$\mathcal{O}_{K,S}^\times = \left\{ \frac{a}{b} \,\middle|\, a, b \in \langle S \rangle \right\}.$$

$\mathcal{O}_{K,S}^\times$ est donc en quelque sorte « K^* restreint à $\langle S \rangle$ ».

De façon analogue au cas entier, on a le résultat suivant, démontré en 1996 par Beukers et Schlickewei [2].

Théorème 3 (Beukers et Schlickewei, 1996)**.** *Soit K un corps de nombres. Soit $S \subset \mathcal{O}_K$ un ensemble fini. L'équation d'inconnues $x, y \in \mathcal{O}_{K,S}^\times$*

$$x + y = 1$$

admet un nombre fini de solutions.

De plus, ce nombre de solutions est borné par 2^{16r+8}, où r est le rang sans torsion de $\mathcal{O}_{K,S}^\times$ en tant que groupe abélien de type fini, et est donné par le théorème des S-unités de Dirichlet (théorème 12 de ce texte).

En fait, comme on le verra au dernier chapitre, le résultat montré par Beukers et Schlickewei est plus général et ne s'applique pas qu'à $\mathcal{O}_{K,S}^\times$, bien que cet exemple en soit la motivation.

• Un cas élémentaire

Avant d'aller plus loin, regardons ce qu'il se passe dans le cas non trivial le plus simple. Plaçons-nous dans le cadre de la première formulation : $K = \mathbb{Q}$ et $\mathcal{O}_K = \mathbb{Z}$. Prenons $S = \{2, 3\}$. On a donc l'expression

$$\mathbb{Z}_S^\times = \{\pm 2^r 3^s \,|\, r, s \in \mathbb{Z}\}.$$

Autrement dit, résoudre l'équation

$$x + y = 1 \quad \text{où } x, y \in \mathbb{Z}_S^\times$$

revient à trouver deux couples (r_1, s_1) et (r_2, s_2) de $\mathbb{Z}^2$ tels que

$$\pm 2^{r_1} 3^{s_1} \pm 2^{r_2} 3^{s_2} = 1.$$

On voit d'abord que cela revient à résoudre l'équation

$$2^r - 3^s = \pm 1 \quad \text{où } r, s \in \mathbb{N}. \tag{1}$$

En effet, si on a une solution avec des exposants strictement négatifs, on peut nettoyer les expressions et évaluer modulo 2 ou 3 soit pour conclure à une absurdité, soit pour se ramener au cas entier. Enfin, si on a uniquement des puissances positives, une évaluation modulo 2 ou 3 permet encore de conclure qu'on est dans le cas (1). On épargne au lecteur ces détails. Passons à la résolution de l'équation.

On distingue le cas 1 ou -1.

Premier cas

$$2^r - 3^s = 1 \quad \text{où } r, s \in \mathbb{N}.$$

- Si $r = 0$, il n'y a pas de solution.
- Si $r = 1$, l'unique solution est $s = 0$.
- Si $r = 2$, l'unique solution est $s = 1$.
- Si $r \geq 3$, on remarque que $2^r \equiv 0[8]$. En raisonnant sur la parité de s on remarque que $3^{2k} \equiv 1[8]$ et $3^{2k+1} \equiv 3[8]$. On ne peut donc pas avoir $2^r - 3^s = 1$.

Second cas

$$2^r - 3^s = -1 \quad \text{où } r, s \in \mathbb{N}.$$

- Si $r = 0$, pas de solution.
- Si $r = 1$, l'unique solution est $s = 1$.
- Si $r = 2$, pas de solution.
- Si $r \geq 3$, on distingue à nouveau selon les valeurs de s.
  - Si s est impair, alors $3^s \equiv 3[4]$ et $2^r - 3^s \equiv -3 = 1[4]$: pas de solution.
  - Si $s = 4k$ alors $3^s - 1 \equiv 0[5]$ et $3^s - 1$ n'est pas une puissance de 2 : pas de solution.
  - Si $s = 4k + 2$ alors $3^s - 1 \equiv 8[16]$ et on ne peut pas avoir $3^s - 1 = 2^r$ puisque $r \geq 3$.

Ainsi on a bien un nombre fini de solutions, et le théorème de Malher est vérifié. On voit bien à travers cet exemple que des stratégies « ad-hoc » vont parfois permettre de résoudre les cas particuliers, mais sûrement pas d'obtenir un résultat général.

Cela représente bien la situation des équations diophantienne, et explique pourquoi les résultats au sujet de ces équations ont été aussi tardifs (majoritairement au XIXème et XXème siècle), alors qu'elles sont étudiées depuis l'Antiquité.

Histoire du problème

Historiquement, le problème de l'équation aux S-unités est issu de la théorie de l'approximation diophantienne : à quel point peut-on bien approcher des irrationnels, éventuellement algébriques, par des rationnels ? Autrement dit, comment mesurer le « degré d'irrationalité » des nombres ?

Ces résultats sont rapidement appliqués à l'étude des des points entiers d'équations fournies par des *formes binaires*.

Le problème est ensuite réduit en une équation qui en cristallise l'essence : c'est l'*équation aux S-unités*.

• Approximation diophantienne et théorème de Thue-Mahler-Roth

Pour les besoins de l'exposé, introduisons la notion de *degré d'irrationalité* d'un réel.

Définition 0.0.2. Soit $\alpha \in \mathbb{R}$. On appelle *degré d'irrationalité* de α la quantité

$$\beta(\alpha) = \sup\left\{\beta \in \mathbb{R}_+ \,\middle|\, \left|\alpha - \frac{p}{q}\right| \leq q^{-\beta} \text{ admet un nombre infini de solutions en } p, q \in \mathbb{Z} \text{ où } p \wedge q = 1\right\}.$$

Ainsi, de façon peut-être surprenante, un nombre « très irrationnel » est un nombre qui peut être très bien approché par des rationnels.

- Cette question a été étudiée dès le XIXème siècle par Dirichlet. Grâce à sa méthode des tiroirs, il démontre que les nombres rationnels sont *très mal approchés* par d'autres rationnels
$$\forall x \in \mathbb{Q}\ \beta(x) = 1,$$
alors que pour les irrationels, on a
$$\forall \alpha \in \mathbb{R} \setminus \mathbb{Q}\ \beta(\alpha) \geq 2.$$
- Dans les années 1840, Liouville démontre que pour tout ζ algébrique de degré n, $\beta(\zeta) \leq n$. Cela lui permet pour la première fois de construire un nombre dont on sait démontrer qu'il est transcendant : *la constante de Liouville.*
- En 1909, Thue [3] améliore significativement ce résultat : pour tout ζ algébrique de degré n, $\beta(\zeta) \leq \frac{n}{2} + 1$.
- Ce résultat est encore amélioré par Siegel [4], qui obtient $\beta(\zeta) \leq \min_{1 \leq k \leq n+1}\left(\frac{n}{k+1} + k\right)$. En particulier, $\beta(\zeta) \leq 2\sqrt{n}$.
- Plusieurs autres améliorations ont lieu, jusqu'à ce que Roth démontre finalement en 1955 ce qui deviendra le théorème de Thue-Siegel-Roth : la constante 2 est optimale pour les irrationnels algébriques. Autrement dit
$$\forall \zeta \in \overline{\mathbb{Q}} \setminus \mathbb{Q}\ \beta(\zeta) = 2.$$
Plus précisément, pour tout $\zeta > 2$, l'équation présentée dans la définition 0.0.2 n'a qu'un nombre fini de solutions.
- Remarquons que Mahler avait généralisé ce théorème aux nombres p-adiques en 1933 [1] (les nombres p-adiques sont présentés au chapitre 5 de ce texte). C'est ce théorème qui se reformule en la finitude de l'équation aux S-unités sur $\mathbb{Z}$. On le reformule ici en langage moderne.

Théorème (Source du théorème 2)**.** *Soit S un ensemble fini de nombres premiers. Soit $f \in \mathbb{Z}[X]$ de degré ≥ 3 irréductible dans $\mathbb{Q}$, qui admet une racine $\sigma_P \in \mathbb{Q}_P$ pour chaque $P \in S$.*
Alors, pour tous $k \geq 1$ et $\beta > \beta_0$, où β_0 est la constante de Siegel citée plus haut,

l'équation

$$\prod_{P\in S} \min\left(1, \left|\sigma_P - \frac{p}{q}\right|_P\right) \leq k \cdot |q|^{-\beta}$$

admet seulement un nombre fini de solutions en $p, q \in \mathbb{Z}$ premiers entre eux.

• Formes binaires et équations de Thue-Mahler

Les résultats d'approximation diophantienne présentés plus haut peuvent être interprétés sous l'angle de la finitude de solutions d'équations sur des *formes binaires homogènes*.

Plus précisément, on se donne un polynôme $F = a_0X^n + a_1X^{n-1}Y + \cdots + Y^n \in \mathbb{Q}[X, Y]$, irréductible, de degré $n \geq 3$.

- Le résultat obtenu par Thue en 1909 [3] indique que pour tout $m \in \mathbb{N}^*$, l'équation

  $$F(p, q) = m$$

  a seulement un nombre fini de solutions en $p, q \in \mathbb{Z}$.
- La généralisation p-adique de Mahler en 1933 [1] permet d'étendre considérablement ce résultat. Un corollaire du résultat démontré dans cet article est que, pour tous $P_1, ..., P_t$ nombres premiers distincts, l'équation

  $$|F(p, q)| = P_1^{e_1} \cdots P_t^{e_t}$$

  a seulement un nombre fini de solutions, où les inconnues sont les $p, q \in \mathbb{Z}$ et $e_1, ..., e_t \in \mathbb{N}$. Ce type d'équation est appelé *équation de Thue-Mahler*.

• Équation aux S-unités

Ces résultats peuvent s'appliquer à l'étude des équations aux S-unités, présentées plus haut. En retour, les bornes sur le nombre de solutions d'équations aux S-unités peuvent être appliquées pour obtenir de nouveaux résultats sur des problèmes de d'approximation de type approximation diophantienne, ou des équations avec forme binaire du type équations de Thue-Mahler.

Il y a également d'autres applications plus vastes : on en présente rapidement quelques-unes un peu plus loin.

- Dès son article de 1933, Mahler [1] applique ses résultats à l'équation aux S-unités sur $\mathbb{Z}$, et démontre le théorème 2. La formulation de l'époque est que pour tous premiers distincts $p_1, ..., p_a, p_{a+1}, ..., p_b, p_{b+1}, ..., p_c$, l'équation

  $$p_1^{e_1} \cdots p_a^{e_a} + p_{a+1}^{e_{a+1}} \cdots p_b^{e_b} = p_{b+1}^{e_{b+1}} \cdots p_c^{e_c}$$

  n'admet qu'un nombre fini de solutions en les exposants $e_1, ..., e_c \in \mathbb{Z}$.

  Mahler propose déjà une borne sur le nombre de ces solutions, mais elle est très mauvaise et n'apporte que peu d'informations : c'est avant tout un résultat de finitude.

- En 1966, Lewis et Mahler collaborent [5]. En obtenant une borne bien plus explicite pour le nombre de solutions des équations de Thue-Mahler (avec une hypothèse dont on peut en fait se passer), il en déduise une borne explicite bien meilleure sur le nombre de solutions de l'équation aux S-unités dans $\mathbb{Z}$.
- Ce résultat est ensuite progressivement amélioré et généralisé, jusqu'à l'article [6] de Evertse en 1984, qui pose la terminologie d'équations aux S-unités, en se plaçant dans le cadre de $\mathcal{O}_{K,S}$, et qui traite complètement le problème, tout en apportant une borne explicite.
- On arrive à l'article qui nous intéresse : en 1996, Beukers et Schlickewei améliorent encore largement la borne, tout en obtenant un résultat qui s'applique à des sous-groupe de type fini plus généraux [2]. De façon peut-être même plus importante, cette preuve est beaucoup plus simple que les précédentes : elle s'appuie sur de nouvelles idées, en utilisant une géométrisation compatible avec la hauteur, qu'on étudiera dans ce livre. Notons l'utilisation cruciale d'un résultat sur les hauteurs de Beukers et Zagier, qui ne fut en fait publié que l'année suivante [7].
- Depuis le résultat de Beukers et Schlickewei qu'on étudie ici, le sujet reste fort actif, en particulier dans l'objectif d'obtenir des résultats plus explicites. On compte ainsi pas moins de 8 articles au sujet de « S-unit equation » publié sur arXiv entre janvier 2019 et avril 2020. Donnons comme exemple « A robust implementation for solving the S-unit equation and several applications »[8], qui implémente un solveur Sage pour l'équation aux S-unités, et en profite pour démontrer une version asymptotique du théorème de Fermat-Wiles sur des corps de nombres particuliers.

Quelques applications

Présentons quelques situations dans lesquelles le théorème de finitude pour l'équation aux S-unités peut s'appliquer.

On ne démontrera pas que ces problèmes s'y réduise bien.

Plusieurs de ces résultats sont issus de ce chapitre [9] d'un livre de 1988 dont Evertse et Györy font partie des auteurs, ou encore du livre « Lecture notes on Diophantine analysis »[10], de Umberto Zannier, publié en 2009.

- **Énoncé historique de Mahler**
  Pour tous premiers distincts $p_1, ..., p_a, p_{a+1}, ..., p_b, p_{b+1}, ..., p_c$, l'équation
  $$p_1^{e_1} \cdots p_a^{e_a} + p_{a+1}^{e_{a+1}} \cdots p_b^{e_b} = p_{b+1}^{e_{b+1}} \cdots p_c^{e_c}$$
  n'admet qu'un nombre fini de solutions en les exposants $e_1, ..., e_c \in \mathbb{Z}$.
- **Équations de Thue-Mahler**
  Soient K un corps de nombres et $f \in K[X, Y]$ un polynôme homogène de degré ≥ 3 sans facteurs multiples. Alors, pour tout ensemble fini S d'idéaux premiers de $\mathcal{O}_K$ et pour tout $c \in K^*$, l'équation
  $$f(x, y) = c$$

admet seulement un nombre fini de solutions en $x, y \in \mathcal{O}_{K,S}$.

- **Théorème de Siegel et équations hyperelliptiques**
  Soient K un corps de nombres et $f \in K[X]$ ayant au moins 3 racines simples. Soit de plus S un ensemble fini d'idéaux premiers de $\mathcal{O}_K$. L'équation

$$y^2 = f(x)$$

  n'admet qu'un nombre fini de solutions en $x, y \in \mathcal{O}_{K,S}$.

- **Collisions de suites récurrentes**

> **Définition 0.0.3.** On dit que $u \in \mathbb{C}^{\mathbb{N}}$ est une *suite récurrente linéaire de rang* $r \in \mathbb{N}^*$ s'il existe $c_1, ..., c_r \in \mathbb{C}$ tels que
>
> $$\forall n \in \mathbb{N}\ u_{n+r} = c_1 u_{n+r-1} + \cdots + c_r u_n,$$
>
> et que r est minimal pour cette propriété.
> Dans ce cas, on dispose de $f_1, ..., f_r \in \mathbb{C}[X]$ et de $\omega_1, ..., \omega_r \in \mathbb{C}^*$ distincts tels que
>
> $$\forall n \in \mathbb{N}\ u_n = f_1(n)\omega_1^n + \cdots + f_r(n)\omega_r^n.$$
>
> S'il existe i, j distincts tels que $\omega_i/\omega_j \in \mathbb{U}$, alors on dit que u *est dégénérée*. Dans le cas contraire, on dit que u *est non-dégénérée*.

  Les théorèmes de finitude pour l'équation aux S-unités permettent de démontrer le fait suivant.
  Soient $R \subset \mathbb{C}$ un sous $\mathbb{Z}$-module de $\mathbb{C}$ de type fini, et u une suite récurrente linéaire de rang ≥ 2. Si u est non dégénérée, alors l'équation

$$\zeta_{m,n} u_m = u_n$$

  n'admet qu'un nombre fini de solutions en $\zeta_{m,n} \in R \setminus \{0\}$, $m > n \geq 0$.

- Un corollaire de ce résultat est le suivant. Soit $u \in \mathbb{C}^{\mathbb{N}}$ une suite récurrente linéaire.
  Si l'ensemble $\{n \in \mathbb{N} \,|\, u_n = 0\}$ des zéros de u est infini, alors u est ultimement périodique.

- On ne s'aventurera que peu dans cette voie, mais remarquons que l'équation aux S-unités permet d'aborder des questions liées à la conjecture *abc*, comme on le voit par exemple dans cet article de 2010 [11] du hongrois Kálmán Györy, qui a beaucoup contribué à l'étude et à la communication autour des équations aux S-unités.
  La conjecture *abc* est une conjecture très célèbre de théorie des nombres, reliant leurs propriétés *additive* et *multiplicative*, et est parfois présentée comme le problème non résolu le plus important en analyse diophantienne.
  Un énoncé de cette conjecture énoncée par le français Joseph Oesterlé en 1988 et le britannique David Masser en 1985 est :

« On considère l'équation $a + b = c$, où a, b et c sont des entiers positifs sans facteur commun, et où d est le produit des facteurs premiers distincts de abc.
Pour tout $\epsilon > 0$ et pour l'ensemble des solutions, le rapport $\frac{c}{d^{1+\epsilon}}$ est borné. »

On peut percevoir qu'un lien puisse exister entre la conjecture *abc* et l'étude de l'équation aux S-unités, puisqu'elles connectent toutes deux des propriétés additives avec des propriétés multiplicatives.

Cette conjecture fait l'objet d'une intense littérature. Le japonais Shinichi Mochizuki, professeur à l'université de Kyoto, a beaucoup travaillé sur le sujet, et a publié en 2012 sur son site personnel une série d'article qui en proposent une démonstration. Cette démonstration revendiquée n'a toujours pas été validée par la communauté mathématique, bien que Mochizuki en ait obtenu la publication en avril 2020 dans le journal *Publications of the Research Institute for Mathematical Sciences*, dont il est éditeur en chef.

Mouvement du texte

• Idée de la preuve

Donnons dès maintenant l'idée globale de la démonstration de Beukers et Schlickewei, qu'on présente dans ce texte avec les notions sur lesquelles elle s'appuie.

L'objectif va être d'adopter un point de vue *géométrique* sur l'ensemble des solutions

$$X = \left\{(x, y) \in \left(\mathcal{O}_{K,S}^{\times}\right)^2 \,\middle|\, x + y = 1\right\}.$$

Plusieurs théorèmes et théories vont être mobilisées à cet effet.

- On veut plonger X dans un $\mathbb{Q}$-espace vectoriel puis un $\mathbb{R}$-espace vectoriel : on a besoin de la notion de produit tensoriel, abordée dans la partie 7.2, puis de la complétion de corps valué, abordée au chapitre 5.

  Cette géométrisation de $\mathcal{O}_{K,S}^{\times}$ est réalisée à la partie 8.1.
- On veut que cet espace soit muni d'une norme qui permet de mesurer les interactions entre les points de X – entre les solutions de l'équation. La mesure de ces interactions est fournie par la théorie de la *hauteur*, qui permet de mesurer la complexité des nombres, et qui est construite au chapitre 6 en s'appuyant sur le chapitre 5.

  On va ainsi analyser la structure de l'équation aux S-unités sous l'angle de la hauteur dans la partie 8.2, puis traduire ceci d'un point de vue géométrique.
- C'est au moment de cette analyse de la structure de l'équation par la théorie des hauteurs que Beukers et Schlickewei s'appuient de façon cruciale sur un théorème de la théorie des hauteurs issu d'un autre article [7]. On en profite pour le démontrer dans notre contexte.

  On mobilise pour cela des idées issues de l'analyse complexe, qu'on explore à la partie 7.1.

- Pour pouvoir espérer tirer des résultats de finitude de ces propriétés géométriques, on va avoir besoin que notre espace soit de dimension finie. C'est le *théorème des S-unités de Dirichlet*, démontré au chapitre 4, qui nous permet d'obtenir ceci en affirmant que $\mathcal{O}_{K,S}^\times$ est un groupe abélien *de type fini*. Ce résultat s'appuie de façon cruciale sur la structure géométrique des nombres généralisés (chapitre 2), ainsi que sur leurs propriétés arithmétiques (chapitre 3).
- À ce stade l'ensemble des solutions X a été plongé dans un espace réel, de dimension finie, muni d'une norme adaptée à la mesure de la complexité des solutions. Les interactions entre ces dernières ont de plus été traduites en inégalités numériques, puis en propriétés géométriques.

  Tout le reste n'est plus qu'arguments géométriques, et on n'a plus besoin de regarder l'équation aux S-unités ou $\mathcal{O}_{K,S}^\times$. On obtient ainsi un théorème plus général que le problème qu'on s'était posé au début.

  On met donc tout ensemble dans l'ultime partie 8.3, en s'appuyant sur des idées de recouvrement d'espaces par des boules (sous-partie 8.3.2), ainsi que sur diverse propriétés de géométrie discrète déjà mobilisées pour la géométrie des nombres (chapitre 2).

Avant de faire tout ceci, on devra bien comprendre les termes du problème, et la généralisation qu'on fait en étudiant les corps de nombres K plutôt que $\mathbb{Q}$, les anneaux d'entiers $\mathcal{O}_K$ plutôt que $\mathbb{Z}$, ce qu'on introduit au chapitre 1, puis comment généraliser l'arithmétique de $\mathbb{Z}$ à des anneaux plus sauvages, ce qui est l'objet du chapitre 3.

• Contenu du livre

L'idée de la preuve étant donnée, présentons maintenant un plan plus linéaire, permettant de parler des grandes idées présentée dans ce texte. Le lecteur qui souhaiterait y faire son marché pour découvrir des théories mathématiques, sans nécessairement aller jusqu'à l'équation aux S-unités, y est donc invité.

- Le premier chapitre introduit la démarche qui consiste à résoudre des problèmes diophantiens en prenant du recul. On généralise ainsi la notion de *nombre* et d'*entier*, en définissant les *corps de nombres* K puis leur *anneau des entiers* $\mathcal{O}_K$. On découvre ainsi progressivement les termes du problème, et on se munit d'outils qui permettent de premières manipulations et démonstrations sur ces nombres, comme la *norme*, la *trace* ou le *polynôme caractéristique*. Enfin, on conclut ce chapitre en s'interrogeant sur les différentes façons « d'incarner » ces corps de nombres, et on verra que les choix qui apparaissent à ce moment révèlent beaucoup sur le corps qu'on incarne. Ce sera l'occasion d'aborder la notion de *plongement*, et de démontrer le *théorème de l'élément primitif* (4).

  Afin de motiver ces notions, on utilisera l'exemple « fil rouge » des *équations de Pell-Fermat* qui ont été l'origine historique de leur étude.
- Le deuxième chapitre aborde un point de vue *géométrique* sur les nombres, qui se révèle être extrêmement fertile. On commence par y faire de la *géométrie discrète*, en définissant puis en caractérisant les réseaux, et on montre le remarquable *théorème de Minkowski* (6). Les outils géométriques développés ici seront appliqués dans de nombreux contextes.

On les utilise en particulier pour faire à proprement parler de la *géométrie des nombres*. On construit ainsi le *plongement canonique* de $\mathcal{O}_K$, qui permet de voir l'anneau des entiers d'un corps de nombres de degré n comme un réseau de $\mathbb{R}^n$, grâce à un théorème dû à Dedekind (5). Cela nous permet du même temps de commencer à expliciter la structure *algébrique* des entiers, puisqu'on obtient $\mathcal{O}_K \cong \mathbb{Z}^n$.

- Le troisième chapitre est un chapitre d'*arithmétique*. On y aborde des idées profondes développées par Dedekind qui, découvrant des anneaux plus sauvages que $\mathbb{Z}$, cherche à y reconstruire autant que possible l'arithmétique classique.

  Si on n'a plus toujours le théorème fondamental de l'arithmétique (7), qui exprime sur $\mathbb{Z}$ l'existence d'une décomposition unique en *éléments* premiers, on retrouve sur les *anneaux de Dedekind* une décomposition unique en *idéaux premiers* (c'est le théorème 9). Pour reconstruire l'arithmétique, il faut donc accepter de passer d'une *arithmétique des éléments* à une *arithmétique des idéaux*.

  On cherche alors, puisque c'est l'objet qui nous intéresse, à étudier l'*arithmétique de* $\mathcal{O}_K$. On définit une relation d'équivalence entre ses idéaux, et on tire partie du point de vue géométrique associant idéal et sous-réseau pour démontrer le *théorème de finitude des classes* (10). L'arithmétique classique est alors retrouvée est réinventée : on démontre que $\mathcal{O}_K$ est de Dedekind (8), et on dispose donc d'une unique factorisation en *idéaux* premiers.

  On introduit également les notions de *ramification* et d'*inertie*, qui permettent d'étudier la façon dont les idéaux premiers dans des sur-corps « vivent au-dessus » des idéaux premiers associés au corps sous-jacent et interagissent avec eux, ce qui est explicité dans le théorème 11. À cette occasion, on étudie les *localisés*, ce qui permet de commencer l'étude de $\mathcal{O}_{K,S}^\times$, l'objet sur lequel porte l'équation aux S-unités.

- Le quatrième chapitre aborde et démontre le *théorème des unités de Dirichlet* (13), puis sa généralisation : le *théorème des S-unités de Dirichlet* (12). En s'appuyant sur toute ce qui a été construit aux chapitres 1 et 2, on étudie ainsi la structure de $\mathcal{O}_K^\times$ puis $\mathcal{O}_{K,S}^\times$, ce qui révèle qu'on peut les voir comme des groupes abéliens de type fini, qui peuvent cette fois avoir une torsion.

  Ce résultat fournit une des briques de base pour construire un espace *de dimension finie* dans la preuve de Beukers et Schlickewei.

  Plus généralement, l'étude des unités est nécessaire pour se ramener aux éléments après s'être élevé dans le monde des idéaux pour y faire de l'arithmétique.

- Le cinquième chapitre aborde la théorie des *corps valués*. En s'intéressant aux différentes manières d'étudier la complexité des nombres, on est menés à s'intéresser aux différentes *valeurs absolues* dont on peut munir un corps de nombres. Comme seule la topologie induite fournit de l'information sur les nombres, on se retrouve à classifier et caractériser des *places*. C'est l'objet du *théorème d'Ostrowski*, qu'on montre sur $\mathbb{Q}$ (14) puis sur un corps de nombres général K (15).

  On voit ainsi apparaître des places *archimédiennes* porteuses d'information algébrique, et des places *ultramétriques* porteuses d'information arithmétique. Ces dernières induisent des *géométries non-archimédiennes*, quelque peu exotiques, qu'on peut prendre plaisir à explorer.

Pour tout comprendre, il est nécessaire d'étudier la *complétion* des corps valués pour ces différentes places. En plus de propriétés universelles, on s'intéresse à des complétés particuliers, ce qui est l'occasion d'une initiation au monde des nombres *p-adiques*, et même $\mathfrak{p}$-*adiques*.

- Le sixième chapitre développe la théorie de la *hauteur*, outil essentiel pour étudier la complexité des nombres et obtenir des résultats de densité et finitude sur des équations diophantiennes comme celle qui nous intéresse.

  On tire ainsi partie du chapitre précédent, pour construire la *hauteur* sur $\mathbb{Q}$, puis sur K, puis sur $\overline{\mathbb{Q}}$, en combinant astucieusement les informations fournies par les différentes *places*. « Astucieusement » signifie : en utilisant les propriétés remarquables issues de la théorie des complétions.

  On obtient une hauteur qui possède de bonnes propriétés qui permettent de la manipuler, et un puissant théorème de finitude : le théorème de Northcott, d'abord sur $\mathbb{Q}$ (16), puis sur $\overline{\mathbb{Q}}$ tout entier (17) – ce qui inclut donc tous les K.

  Ce chapitre, après le chapitre 4, fournit ainsi le deuxième outil théorique fondamental qui permet d'aborder la preuve de Beukers et Schlickewei.

- Le septième chapitre aborde d'ultimes préliminaires à la preuve, dont on ne s'est pas servi jusque-là.

  Une première partie d'analyse complexe rappelle quelques faits majeurs de cette théorie. Sur $\mathbb{C}$, le fait d'être dérivable est équivalent à être développable en série entière, et donc de classe C^∞. Cette forte rigidité, qu'on exprime en disant que les *fonctions holomorphes* sont exactement les *fonctions analytiques*, est à l'origine de phénomènes remarquables : la *formule intégrale de Cauchy*, le *principe des zéros isolés*, le *principe du prolongement analytique*, la *formule de la moyenne*, *la formule du maximum*, ... Elle présente ensuite le *théorème de Puiseux* (18) qui montre l'existence d'une décomposition, en produit de polynômes de degré 1, de n'importe quel polynôme à coefficients dans le corps des fractions des séries entières de Puiseux. Cette décomposition est « héritée », en utilisant le *lemme de Hensel* (7.1.19), de la décomposition des polynômes complexes en facteurs de degré 1.

  Une seconde partie introduit le produit tensoriel comme solution d'un certain problème universel (19). On l'étudie sur des anneaux et des modules, pour commencer à le manipuler puis à s'en servir pour construire l'*extension des scalaires*.

- Enfin, le huitième et ultime chapitre est pleinement consacré à la preuve de Beukers et Schlickewei.

  On construit ainsi dans la partie 8.1 l'espace géométrique muni d'une norme issue de la hauteur dans lequel les solutions de l'équation aux S-unités vont pouvoir s'incarner. C'est fondamentalement le fait que $\mathcal{O}_{K,S}^\times$ soit de type fini qui permet ceci, et la construction fonctionne en ne retenant que cette hypothèse.

  La partie 8.2 analyse la structure de l'équation aux S-unités sous l'angle de la hauteur pour obtenir des inégalités numériques fortes qui sont ensuite interprétées géométriquement. Pour cela, on s'appuie sur le théorème 20, dû à Beukers et Zagier [7], qui est démontré en utilisant des idées riches et diverses.

Enfin, la partie 8.3 démontre le théorème de Beukers et Schlickewei, qui étend encore un peu le résultat au-delà de l'équation aux S-unités, en mettant tous les arguments ensemble et en concluant grâce à des idées de recouvrement d'espace par des boules.

• Diagramme de dépendances

Comme nous l'avons dit plus tôt, nous espérons ainsi que les lecteurs pourront piocher les chapitres qui seront les plus intéressants à aborder pour eux.

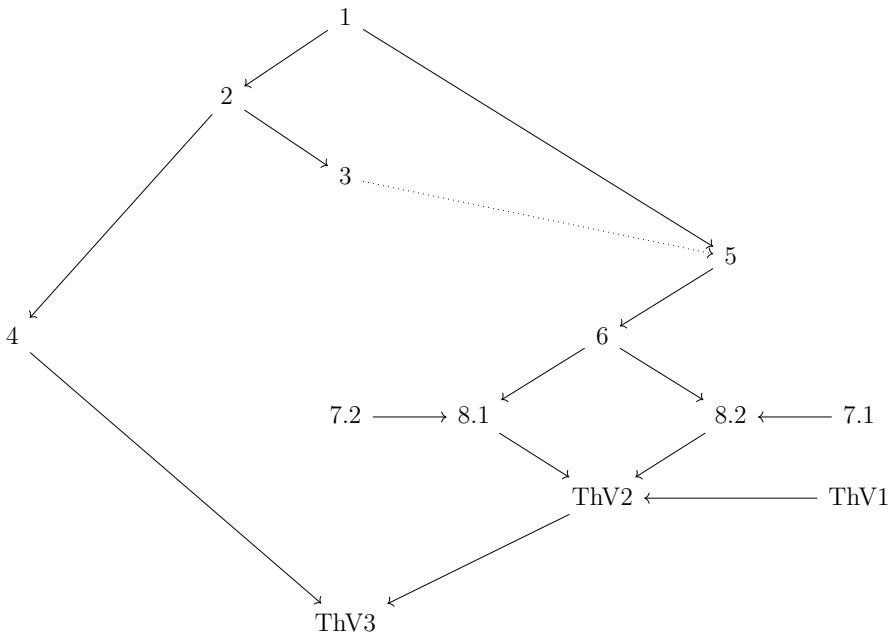
Par exemple, le lecteur qui viendrait uniquement découvrir la théorie des corps valués et les théorèmes d'Ostrowski pourra sauter directement jusqu'au chapitre 5, et récupérer ensuite – si son bagage théorique n'était pas suffisant – les quelques résultats préliminaires utilisés, qui sont cités et démontrés plus tôt dans le texte.

Au contraire, le lecteur qui souhaiterait directement étudier la démonstration de Beukers et Schlickewei, de façon plus détaillée que dans l'article original, mais sans réapprendre tous les concepts sur lesquels elle se fonde, pourra directement passer au chapitre 8.

Pour tous les lecteurs – y compris ceux souhaitant étudier tout ce livre, en en comprenant l'agencement, peut-être pour concevoir eux-mêmes leur parcours de lecture – on propose donc le diagramme de dépendance ci-dessous.

On renvoie le lecteur à l'introduction « contenu » qui est juste au-dessus, ainsi qu'au plan détaillé, pour qu'il puisse estimer son niveau de familiarité avec les théories et théorèmes abordés dans les différents chapitres.

Ce diagramme de dépendance se lit de la façon suivante : on écrit $A \longrightarrow B$ dès que B présuppose des notions ou utilise des résultats de A.



- « ThV1 » renvoie à la version géométrique du théorème dans la preuve de Beukers et Schlickewei, qui s'applique directement à un espace dans lequel on a des inégalités particulières sur les normes de points. Ces hypothèses très spécifiques étant posées, la démonstration de ce résultat n'utilise que des arguments de recouvrement de l'espace par des boules.

- « ThV2 » renvoie au résultat plus général démontré par Beukers et Schlickewei, et qui donne une borne au nombre de solutions de $x + y = 1$, où $(x, y) \in H$, où H est un sous-groupe de type fini de $(\mathbb{C}^*)^2$.
  Plus spécifiquement, il donne cette borne pour $(x, y) \in G$, où G est la $\mathbb{Q}$-clôture de H (mais on a donc en particulier $H \subset G$).
- « ThV3 » renvoie au théorème de Beukers et Schlickewei pour l'équation aux S-unités $x + y = 1$, où $\mathcal{O}_{K,S}^{\times}$.
  En utilisant le théorème de S-unités de Dirichlet démontré au chapitre 4, c'est un corollaire de « ThV2 ».

De plus, la flèche en pointillés entre 3 et 5 indique le fait que l'arithmétique des idéaux n'est utilisée que pour quelques résultats de la théorie des corps valués : les places ultramétriques d'un corps d'un nombre. En revanche, ces résultats sont cruciaux pour la théorie de la hauteur du chapitre 6.

Remerciements

Nous remercions énormément toute personne qui a rendu ce travail possible. Ce PSC nous a permis de découvrir tout un nouvel aspect du monde des mathématiques à travers les recherches bibliographiques. Ceci est donc la première étape pour sortir du monde académique où tout nous est expliqué avec une très bonne pédagogie. Ce n'est justement que le premier pas, puisque Diego Izquierdo, notre tuteur pendant ce PSC, a été là pour nous expliquer tous les résultats connus par tous les spécialistes et non détaillés dans les publications. L'aboutissement de ce projet revient en grande partie donc à l'aide inestimable de M. Izquierdo. Nous remercions également Javier Fresan, le coordinateur des PSC de Mathématiques, grâce à qui nous avons pu avoir autant de sujets variés et des tuteurs de très haut niveau. Nous remercions enfin le personnel administratif de l'école qui s'occupe d'organiser les échéances et les modalités concernant ce module pour tous les élèves de l'école.

1
INTRODUCTION AUX CORPS DE NOMBRES

L'objectif de ce rapport est, on l'a vu, d'obtenir des résultats sur une catégorie d'équations, appelées « équation des S-unités », et présenté en 3. Ce type de problèmes appartient à une famille beaucoup plus générale, celui des *équations diophantiennes*. Or, on va le voir, l'équation des S-unités est pédagogiquement intéressante dans la mesure où son étude fait appel à un grand nombre de concepts issus de cette théorie. En fait, les deux premiers chapitres de ce mémoire introduisent des notions classiques et incontournables de la théorie des équations diophantiennes. Le développement d'outils plus spécifiques et adaptés à l'équation des S-unités commence à s'opérer à partir du chapitre 3, bien que ces outils aient des applications à beaucoup d'autres problèmes diophantiens.

De façon très générale, une équation diophantienne est un problème de la forme suivante.

Définition 1.0.1 (Equation diophantienne)**.** On appelle équation diophantienne une équation d'inconnue $(x_1, ..., x_n) \in \mathbb{Z}^n$ du type

$$P(x_1, ..., x_n) = 0,$$

où P est un polynôme à n indéterminés à coefficients dans un corps K.

Il est bien connu que la résolution générale de ces équations est un problème extrêmement difficile. Citons le célèbre exemple suivant.

Exemple 1.0.1 (Dernier théorème de Fermat)**.** Soit n un entier strictement supérieur à 2. L'étude de l'équation d'inconnue $(x, y, z) \in \mathbb{Z}^3$

$$x^n + y^n = z^n$$

est appelée « Dernier théorème de Fermat », ce théorème stipulant que l'équation n'a pas de solution avec $x, y, z > 0$.

En fait ce problème est même impossible en général ! En l'an 1900, David Hilbert présente au siècle naissant une liste de 23 qui devaient marquer son histoire. Le $10^{\text{ème}}$ problème était le suivant.

Exemple 1.0.2 (Problème X de Hilbert, 1900)**.**

10. Entscheidung der Lösbarkeit einer Diophantischen Gleichung.
« Eine Diophantische Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt : man soll ein Verfahren angeben, nach

welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist. »

En français, cela donne :

X. De la possibilité de résoudre une équation diophantienne.
« On donne une équation diophantienne à un nombre quelconque d'inconnues et à coefficients entiers rationnels : on demande de trouver une méthode par laquelle, au moyen d'un nombre fini d'opérations, on pourra distinguer si l'équation est résoluble en nombres entiers rationnels. »

En 1970, le mathématicien russe Iouri Vladimirovitch Matiassevitch répond par la négative.

Exemple 1.0.3 (Théorème de Matiassevitch, 1970)**.**
Le dixième problème de Hilbert est indécidable.
Plus précisément, si on appelle ensemble diophantien tout ensemble de solutions dans $\mathbb{N}^k$ d'une équation diophantienne en k variables, alors

Les ensembles diophantiens sont exactement les ensembles récursivement énumérables.

Par conséquent, on sait par la théorie de la décidabilité qu'il ne peut exister d'algorithme *qui termine toujours en un temps fini*, qui prend en entrée une équation diophantienne quelconque en plusieurs variables et annonce en sortie si elle admet des solutions.

L'étude des équations diophantiennes est très ancienne et a mobilisé des générations de mathématiciens, et ce dès l'Antiquité, comme en témoigne la dénomination adoptée (Diophante ayant vécu vers le IIe ou IIIe siècle de notre ère). Il n'est pas du tout question ici de développer son histoire, qui mériterait un mémoire à elle seule ! Mais il est crucial de remarquer que l'approche moderne, qui commence à s'affirmer au XVIIIe siècle avec Gauss notamment, repose sur l'idée qu'*introduire de nouveaux nombres fournit un cadre plus adapté*. Considérons l'exemple éloquent suivant, qu'on reprendra souvent par la suite.

Exemple 1.0.4 (Equations de Pell-Fermat)**.** Soit d un nombre entier positif sans facteurs carrés. On cherche les solutions de l'équation d'inconnue $(a, b) \in \mathbb{Z}^2$

$$a^2 - db^2 = 1.$$

Cette équation se réécrit

$$(a + b\sqrt{d})(a - b\sqrt{d}) = 1.$$

La seconde équation invite à chercher les solutions non plus dans $\mathbb{Z}$ mais dans un nouvel ensemble stable par addition et multiplication, contenant $\mathbb{Z}$, mais aussi un nombre $\sqrt{d}$ vérifiant $\sqrt{d}^2 = d$.

Ce sont des remarques de cette nature qui ont motivé l'apparition de la notion de corps de nombres. Fondamentalement, ce concept répond à la démarche suivante.

- Je connais bien $\mathbb{Q}$, qui contient $\mathbb{Z}$ et est stable par addition, passage à l'opposé, multiplication, passage à l'inverse (c'est un corps).
- L'étude d'une équation diophantienne m'invite à regarder des nombres dont l'écriture fait intervenir des rationnels et des nombres $\zeta_1, ..., \zeta_n$ irrationnels mais « sympathiques ».
- Je me place donc dans un nouveau corps, contenant $\mathbb{Q}$ et $\zeta_1, ..., \zeta_n$, que je demande minimal. On le note $\mathbb{Q}[\zeta_1, ..., \zeta_n]$.
- Enfin, je dois redescendre de mon gros corps à l'ensemble des entiers, afin de trouver les solutions de mon équation.

Ici l'appellation de « sympathique » revient à dire que ces nombres sont certes compliqués car non rationnels, mais qu'ils apparaissent assez naturellement à partir de $\mathbb{Q}$ comme racines d'un polynôme à coefficient dans $\mathbb{Q}$. Dans ces conditions, la structure cherchée dans le troisième point est celle de *corps de nombres*, et est l'objet de ce chapitre. Détaillons maintenant les résultats obtenus.

- Dans la partie 1.1, intitulée « Qu'est-ce qu'un nombre ? », on introduit les formalismes des *extensions de corps*, ce qui permet d'aboutir à la définition d'un corps de nombres : il s'agit d'un corps qui étend $\mathbb{Q}$ et qui est un espace vectoriel de dimension finie sur $\mathbb{Q}$.
- La partie 1.2 permet de vérifier que cette définition coïncide avec la démarche présentée ci-dessus : un corps de nombres s'obtient en ajoutant des *éléments algébriques* à $\mathbb{Q}$.
- Une fois le concept de corps de nombres bien posé, on s'interroge sur la signification de la notion *d'éléments entiers* dans un tel corps, dont l'ensemble $\mathcal{O}_K$ jouerait un rôle analogue à $\mathbb{Z}$ pour $\mathbb{Q}$. Il s'agit de l'objectif de la partie 1.3. On observe alors que comme dans le cas des rationnels, on retrouve le fait que $\mathcal{O}_K$ est un anneau et que son corps des fractions de $\mathcal{O}_K$ n'est autre que K.

Une fois toutes les définitions posées, on cherche à mieux comprendre la structure de $\mathcal{O}_K$. On a vu que $\mathcal{O}_K$ était un anneau, mais est-il de type fini comme groupe additif ? Si oui, comment caractériser ses familles génératrices et son rang ? Pour répondre à ces questions, on introduit un certain nombre d'outils.

- La partie 1.4 définit ces outils, qui sont la norme, la trace ou encore le polynôme caractéristique d'un élément de K. Elle met aussi en évidence les liens qui les unissent. En particulier, on voit une manière algébrique de caractériser le fait qu'une famille d'éléments de K engendre le corps tout entier sur $\mathbb{Q}$. Cette caractérisation fait intervenir une quantité : le *discriminant de la famille*.
- Ce cadre étant posé, l'ultime partie 1.5 apporte une nouvelle pierre conceptuelle fondamentale pour l'étude de K et $\mathcal{O}_K$. L'idée principale consiste à observer qu'on peut voir K comme un sous-corps de $\mathbb{C}$ de plusieurs manières, qui correspondent aux *plongements de* K. La théorie de Galois fournit alors des résultats permettant de comprendre la façon dont ces plongements opèrent sur K. En particulier, les derniers résultats de ce chapitre annoncent l'intuition du chapitre 2 : en faisant opérer les plongements sur $\mathcal{O}_K$, on en obtient des incarnations dans $\mathbb{C}$ qui révèlent sa structure.

1.1 Qu'est-ce qu'un nombre ?

Dans toute la suite, le terme « corps » désignera un corps commutatif.

On l'a vu, la notion de base de notre problème est celle de corps de nombres. Il s'agit d'un corps obtenu à partir de $\mathbb{Q}$ en y ajoutant des éléments algébriques. Mais avant d'aborder ce point de vue, il convient de faire quelques généralités sur les extensions de corps. Le point clé va être que si L est une extension d'un corps K, alors L peut être muni d'une structure de K-espace vectoriel. Dans ce cadre, un corps de nombres est une extension finie de $\mathbb{Q}$ de dimension finie.

Cette sous-partie reprend les définitions et propriétés énoncées dans le premier chapitre du cours d'algèbre de M1 d'Olivier Debarre dispensé à l'ENS. [12].

La notion d'extension de corps admet une définition très naturelle.

Définition 1.1.1 (Extension de corps)**.** Soient K et L deux corps. On dit que L est une extension de K, noté L/K, s'il existe un morphisme de corps $j : K \to L$.

Le cas le plus simple d'extension est celui donné par le morphisme d'inclusion.

Exemple 1.1.1. $\mathbb{C}$ est une extension de $\mathbb{R}$ via le morphisme

$$j \ : \left| \begin{array}{ccc} \mathbb{R} & \to & \mathbb{C} \\ x & \mapsto & x. \end{array} \right.$$

Cet exemple donne envie de dire que si L est une extension de K, alors L est *plus gros* que K. Dans le cas du morphisme d'inclusion, on a simplement $K \subset L$. Plus généralement, cela provient du fait bien connu qu'un morphisme de corps est nécessairement injectif. Dans la suite, on identifiera donc L/K avec $K \subset L$. Ainsi le terme « d'extension » est bien justifié.

Proposition 1.1.1. *Tout morphisme de corps est injectif.*

Démonstration. Soit $j : K \to L$ un morphisme de corps. Soit $x \in \mathrm{Ker}(j)$. Supposons par l'absurde $x \neq 0$. Alors,

$$\begin{aligned} j(x)j(x^{-1}) = j(xx^{-1}) = j(1_K) = 1_L \qquad & \text{(car } j \text{ est un morphisme)} \\ \neq 0. & \end{aligned}$$

C'est absurde car $j(x) = 0$. Ainsi, $x = 0$ et j est injectif. □

Si on a une extension L/K, on peut voir L comme un espace vectoriel sur le corps K. La vérification des axiomes est immédiate. Cela amène à considérer la définition suivante.

Définition 1.1.2 (Degré d'une extension)**.** Soit L/K une extension de corps. On appelle degré d'une extension, noté $[L : K]$, le degré du K-espace vectoriel L. Si ce degré est fini, on dira que l'extension L/K est finie.

Exemple 1.1.2. En reprenant l'exemple précédent, $[\mathbb{C} : \mathbb{R}] = 2$. Mais $[\mathbb{R} : \mathbb{Q}] = \infty$. En effet, si par l'absurde on suppose qu'on a une $\mathbb{Q}$-base de $\mathbb{R}$ à n éléments $(r_1, ..., r_n)$, alors $\mathrm{Vect}_{\mathbb{Q}}(r_1, ..., r_n)$ est dénombrable, ce qui n'est pas le cas de $\mathbb{R}$.

Le calcul effectif de la dimension d'une extension peut se faire en considérant un corps intermédiaire et en exploitant le théorème de la base télescopique.

Proposition 1.1.2 (Base télescopique)**.** *Soient M/L et L/K deux extensions de corps finies. Alors M/K est finie et $[M : K] = [M : L][L : K]$.*

Démonstration. Soit $(e_1, ...e_r)$ une base du L-espace vectoriel M, et $(f_1, ..., f_s)$ une base du K-espace vectoriel L. Introduisons la famille

$$\beta = (e_1 f_1, e_1 f_2, ..., e_1 f_s, e_2 f_1, e_2 f_2, ..., e_r f_s).$$

Vérifions que β est une base du K-espace vectoriel M.

- **Liberté**
  Soient $\lambda_{1,1}, ..., \lambda_{1,s}, \lambda_{2,1}, ..., \lambda_{r,s}$ des scalaires de K tels que

  $$\sum_{j=1}^{r} \sum_{i=1}^{s} \lambda_{i,j} e_j f_i = 0.$$

  Alors,

  $$\sum_{j=1}^{r} e_j \left(\sum_{i=1}^{s} \lambda_{i,j} f_i \right) = 0.$$

  Or, les $\sum_{i=1}^{s} \lambda_{i,j} f_i$ sont des éléments de L, donc par liberté de $(e_1, ..., e_r)$,

  $$\forall j \in [\![1, r]\!] \ \sum_{i=1}^{s} \lambda_{i,j} f_i = 0.$$

  Comme $(f_1, f_2, ..., f_s)$ est une famille libre d'éléments de K, on en déduit que $\forall i \, \forall j \ \lambda_{i,j} = 0$. β est donc libre.
- **Génératrice**
  Il s'agit simplement d'une base télescopique. Pour $y \in M$, on décompose $y = \sum_{j=1}^{r} \lambda_j e_j$ dans le L-espace vectoriel M, puis on décompose chacun des λ_j dans la base $(f_1, f_2, ..., f_s)$ du K-espace vectoriel L. Cela conclut que β engendre le K-espace vectoriel M.

β est donc une base du K-espace vectoriel M, et on a directement en regardant le cardinal de β que $[M : K] = [M : L][L : K]$. □

On dispose maintenant de tous les éléments pour définir les corps de nombres. La définition est exactement celle annoncée.

Définition 1.1.3 (Corps de nombres)**.** Un corps de nombres K est une extension finie de $\mathbb{Q}$.

Exemple 1.1.3. $\mathbb{Q}$ est un corps de nombres, mais pas $\mathbb{R}$ puisque $[\mathbb{R} : \mathbb{Q}] = \infty$.

En utilisant le théorème de la base télescopique, on observe de plus le fait suivant.

Proposition 1.1.3. *Soit L/K une extension de corps de nombres. Alors l'extension est finie.*

Démonstration. Par le théorème de la base télescopique, on a

$$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}].$$

Comme $[L : \mathbb{Q}]$ est fini et $[K : \mathbb{Q}]$ non nul, $[L : K]$ est fini et donc l'extension L/K est finie. □

1.2 Algébricité et transcendance

On va voir maintenant que cette définition permet bien de se placer dans le cadre de la démarche précédente. Si je dispose d'éléments irrationnels $\zeta_1, ..., \zeta_n$ que je veux ajouter à $\mathbb{Q}$, je peux construire le plus petit corps contenant $\mathbb{Q}$ ainsi que $\zeta_1, ..., \zeta_n$, qui sera noté $\mathbb{Q}[\zeta_1, ..., \zeta_n]$. L'objectif de cette partie est de vérifier le fait suivant, rassurant d'un point de vue terminologique.

Proposition 1.2.1. *Soient $\zeta_1, ..., \zeta_n$ des éléments irrationnels et algébriques sur $\mathbb{Q}$. Alors le corps $\mathbb{Q}[\zeta_1, ..., \zeta_n]$ est un corps de nombres.*

Ici encore, on sélectionne les définitions et propriétés qui nous seront utiles pour la suite en s'appuyant sur le cours d'Olivier Debarre [12].

Mais commençons d'abord par définir les termes du problème.

Définition 1.2.1 (Élément algébrique)**.** Soit L/K une extension de corps. Soit $x \in L$. On dit que x est algébrique sur K s'il existe un polynôme $P \in K[X]$ non nul tel que $P(x) = 0$. On dit alors que P est un polynôme annulateur de x.

Définition 1.2.2 (Élément transcendant)**.** Soit L/K une extension de corps. Soit $x \in L$. On dit que x est transcendant sur K s'il n'est pas algébrique sur K.

Exemple 1.2.1. Soit L/K une extension de corps. Tout élément $x \in K$ est algébrique : $X - x$ en est un polynôme annulateur.

Exemple 1.2.2. Si on regarde $\mathbb{R}/\mathbb{Q}$, $\sqrt{2}$ est algébrique, mais π ne l'est pas (théorème d'Hermite-Lindemann, 1882).

Ce dernier exemple indique que pour une extension L/K, il n'y a aucune raison que tous les éléments de L soit algébriques. On définit donc la notion d'extension algébrique.

Définition 1.2.3 (Extension algébrique)**.** On dit qu'une extension de corps L/K est algébrique si tous les éléments de L sont algébriques sur K.

Les résultats liés aux éléments algébriques et transcendants sont nombreux et abondamment traités dans la littérature (voir par exemple le cours d'Olivier Debarre [12]). On constate le fait fondamental suivant.

Proposition 1.2.2. *Toute extension finie est algébrique.*

Démonstration. Soit L/K une extension finie de dimension $n = [L : K]$. Soit $x \in L$. La famille $(1, x, x^2, ..., x^n)$ d'éléments de L est de cardinal $n + 1$, donc liée sur K. On dispose donc de $a_0, a_1, ..., a_n \in K$ non tous nuls tels que

$$\sum_{i=0}^{n} a_i x^i = 0.$$

En posant $P = \sum_{i=0}^{n} a_i X^i \in K[X]$, on a bien $P(x) = 0$ et P non nul. Donc x est algébrique, et par suite l'extension est algébrique. □

Ce théorème permet de voir que dans le cas des corps de nombres il n'y a pas de discussion sur le caractère algébrique ou transcendant d'un élément.

Corollaire 1.2.1. *Soit K un corps de nombres. K est une extension algébrique de $\mathbb{Q}$.*

Démonstration. Par définition, $K/\mathbb{Q}$ est une extension finie, donc algébrique par la propriété précédente. □

Un élément algébrique de L/K a une infinité de polynômes annulateurs, mais l'un d'entre eux joue un rôle particulier, c'est le polynôme minimal.

Proposition 1.2.3. *Soit L/K une extension de corps. Soit $x \in L$ algébrique sur K. Il existe un unique polynôme unitaire de degré minimal à coefficients dans K qui annule x. On l'appelle polynôme minimal de x sur K, noté $\mu_{x,K}$.*

On remarquera que ce polynôme dépend du corps K, c'est pourquoi on le note $\mu_{x,K}$. Par souci de simplicité, dans le cas d'un corps de nombres qui est par défaut une extension de $\mathbb{Q}$, on adoptera la notation μ_x.

Démonstration.

- **Existence**
  L'élément x est algébrique, donc il admet un polynôme annulateur dans $K[X]$ par définition. L'idéal annulateur de x, qui est $\{P \in K[X] \,|\, P(x) = 0\}$, n'est donc pas réduit à 0. En particulier on peut choisir un polynôme annulateur de x de degré minimal, qu'on normalise ensuite pour le rendre unitaire.
- **Unicité**
  Soient P_1 et P_2 deux polynômes annulateurs de x sur K de degré minimal et unitaires. Notons d leur degré commun. On effectue la division euclidienne de P_1 par P_2. On a $Q \in K[X]$ et $R \in K_{d-1}[X]$ tels que

  $$P_1 = QP_2 + R.$$

  Par argument de degré, Q est un scalaire de K, et comme P_1 et P_2 sont unitaires, $Q = 1$. Ainsi,

  $$P_1 = P_2 + R.$$

  En évaluant cette relation en x on obtient

  $$R(x) = 0.$$

  Mais P_1 et P_2 sont des polynômes annulateurs de degré minimal d et $\deg(R) < d$. Donc $R = 0$ et $P_1 = P_2$. On a ainsi l'unicité.

□

Exemple 1.2.3. Dans $\mathbb{R}/\mathbb{Q}$, le polynôme minimal de $\sqrt{2}$ est $X^2 - 2$, mais dans $\mathbb{R}/\mathbb{Q}[\sqrt{2}]$ c'est $X - \sqrt{2}$.

L'idée à partir de maintenant va être de donner quelques propriétés sur $\mu_{x,K}$ afin de caractériser une extension $K[x]/K$ où x est algébrique sur K.

Proposition 1.2.4. *Soient L/K une extension de corps et $x \in L$.*
Alors, $\mu_{x,K}$ est irréductible dans $K[X]$.

Démonstration. Il s'agit d'une conséquence du fait que μ_x est de degré minimal. Si on a par l'absurde $P, Q \in K[X]$ non constants avec $\mu_x = P(x)Q(x)$, alors en évaluant en x on a $P(x)Q(x) = 0$.

Comme on travaille sur un corps, cela entraîne $P(x) = 0$ ou $Q(x) = 0$, ce qui fournit donc un polynôme annulateur de x de degré strictement inférieur à celui de μ_x, ce qui est absurde.

Ainsi μ_x est irréductible. □

A ce stade, on introduit les deux notations suivantes, qui n'ont aucune raison de coïncider.

Définition 1.2.4 (Sous-anneau engendré par x)**.** Soit L/K une extension de corps. Soit $x \in L$. On note $K[x] = \{P(x) \mid P \in K[X]\}$. C'est le plus petit sous-anneau de L (au sens de l'inclusion) contenant K et x.

De même, on note $K(x)$ le plus petit sous-corps de L contenant K et x. C'est donc le corps des fractions de $K[x]$.

Ces deux notions se généralisent naturellement à une familles $(x_1, ..., x_n)$.

Néanmoins, si x est algébrique la distinction n'a pas lieu d'être.

Proposition 1.2.5. *Soient L/K une extension de corps et $x \in L$. Si x est algébrique, alors $K[x]$ est un corps et $K[x] = K(x)$.*

Démonstration. On a simplement à vérifier que tout élément de $K[x]^*$ est inversible.

Soit $y = P(x) \in K[x]^*$, où $P \in K[X]$. On effectue la division euclidienne de P par $\mu_{x,K}$:

$$P = Q\mu_x + R \quad \text{où} \quad \deg R < \deg \mu_x \text{ et } R \neq 0.$$

En évaluant en x, on a $y = R(x)$. Comme $\mu_{x,K}$ est irréductible, $\mu_{x,K}$ et R sont premiers entre eux. Par le lemme de Bézout, on en déduit l'existence de $U, V \in K[X]$ tels que

$$U\mu_{x,K} + VR = 1.$$

En évaluant en x, il vient

$$V(x)R(x) = 1_K, \text{ d'où } V(x)y = 1_K.$$

Comme $V(x) \in K[x]$, on a bien montré que y était inversible, donc $K[x]$ est un corps, d'où $K[x] = K(x)$. □

Tout notre travail permet d'obtenir le résultat attendu suivant : si x est algébrique sur K, l'extension $K(x)/K$ est finie.

Proposition 1.2.6. *Soit L/K une extension de corps. Soit $x \in L$ algébrique sur K. L'extension $K(x)/K$ est de degré fini $[K(x) : K] = \deg \mu_{x,K}$.*

Démonstration. Notons $k = \deg \mu_x$. On remarque simplement que $(1, x, x^2, ..., x^{k-1})$ est une base du K-espace vectoriel $K(x)$ (qui est bien une extension de K puisque $K \subset K(x)$).

- **Liberté**

  Dire qu'on a $\lambda_0, ..., \lambda_{k-1} \in K$ avec $\sum_{i=0}^{k-1} \lambda_i x^i = 0$ revient à dire qu'on a un polynôme annulateur de x dans $K[X]$ de degré strictement inférieur à k. Comme $\mu_{x,K}$ est de degré minimal, un tel polynôme non nul n'existe pas. Cela revient à dire que $\lambda_0 = \cdots = \lambda_{k-1} = 0$ et la famille est donc libre.

- **Génératrice**

  On rappelle que par le résultat précédent $K(x) = K[x]$ puisque x est algébrique. Dès lors, soit $y = P(x) \in K[x]$ où $P \in K[X]$. On effectue la division euclidienne de P par $\mu_{x,K}$:

  $$P = Q\mu_{x,K} + R \text{ où } R \in K_{k-1}[X].$$

  En évaluant en x, on peut écrire $y = P(x) = R(x) \in \text{Vect}(1, x, .., x^{k-1})$, donc la famille est génératrice.

□

Le théorème de la base télescopique 1.1.2 permet d'obtenir par récurrence immédiate la généralisation du théorème précédent.

Proposition 1.2.7. *Soit L/K une extension de corps. Soit $x_1, ..., x_n$ des éléments de L algébriques sur K. Alors l'extension $K[x_1, ..., x_n]$ est finie, de degré inférieur à $\prod_{i=1}^{n} \deg \mu_{x_i,K}$*

On peut donc bien répondre à l'affirmative à la question du début de cette partie : étant donné $\zeta_1, ..., \zeta_n$ des éléments irrationnels algébriques sur $\mathbb{Q}$, le corps $\mathbb{Q}[\zeta_1, ..., \zeta_n]$ est un corps de nombres.

1.3 Qu'est-ce qu'un entier ?

Maintenant que les corps de nombres sont mieux compris, il est temps de chercher à s'intéresser à leurs éléments entiers. A priori, il ne semble pas vraiment y avoir de définition évidente d'une telle notion sur un corps de nombres quelconque. On peut néanmoins construire un cahier des charges par analogie du cas de $\mathbb{Z}$ par rapport à $\mathbb{Q}$. Prenons donc K un corps de nombres.

- On s'attend à ce que l'ensemble des éléments entiers sur K soit un anneau.
- On s'attend à ce que K soit le corps des fractions de cet anneau, autrement dit que K soit le plus petit corps contenant tous ses éléments entiers.
- On s'attend à ce que notre anneau d'entiers dispose, à l'instar de $\mathbb{Z}$, de propriétés arithmétiques agréables.

Dans cette partie, on vérifie les deux premiers points. Le troisième sera l'objet du chapitre 3 du rapport. On attire l'attention du lecteur sur le fait que notre cahier des charges ne constitue en rien une définition du concept d'élément entier d'un corps de nombres, mais sert à motiver la définition suivante.

On rappelle que si K est un corps de nombres, on adopte la notation abrégée $\mu_x := \mu_{x,\mathbb{Q}}$.

Définition 1.3.1 (Entier algébrique)**.** Soient K un corps de nombres et $x \in K$. On dit que x est un *entier algébrique* si$\mu_x \in \mathbb{Z}[X]$ (où μ_x est unitaire par définition).

On note $\overline{\mathbb{Z}}$ l'ensemble des entiers algébriques (de $\mathbb{C}$).

Définition 1.3.2 (Anneau $\mathcal{O}_K$ des entiers de K)**.** Soit K un corps de nombres (vu comme un sous-ensemble de $\mathbb{C}$). On note $\mathcal{O}_K$ l'ensemble des entiers algébriques appartenant à K, i.e. $\mathcal{O}_K = K \cap \overline{\mathbb{Z}}$. On l'appelle *anneau des entiers de* K.

On commence par vérifier qu'avec cette définition, on a bien $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$! Sinon, à quoi bon parler d'éléments entiers ?

Proposition 1.3.1. $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Démonstration. L'inclusion $\mathbb{Z} \subset \mathcal{O}_{\mathbb{Q}}$ est immédiate puisque pour $a \in \mathbb{Z}$, $\mu_a = X - a$ qui est bien à coefficients dans $\mathbb{Z}$.

L'inclusion réciproque requiert le lemme suivant.

Lemme 1.3.1. *Soit $\frac{p}{q} \in \mathbb{Q}$ une fraction irréductible. Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ qui annule $\frac{p}{q}$. Alors $q|a_n$ et $p|a_0$.*

En effet, on écrit

$$\begin{aligned} &\sum_{i=0}^{n} a_i \left(\frac{p}{q}\right)^i = 0, \\ \text{d'où}\quad &\sum_{i=1}^{n} a_i \left(\frac{p}{q}\right)^i = -a_0, \\ \text{d'où}\quad &p\left(\sum_{i=1}^{n} a_i p^{i-1} q^{n-i}\right) = -a_0 q^n. \end{aligned}$$

Or $(\sum_{i=1}^{n} a_i p^{i-1} q^{n-i})$ est un nombre entier. Ainsi p divise $a_0 q^n$. Mais p est premier avec q puisque $\frac{p}{q}$, donc a fortiori avec q^n. Par le lemme de Gauss, p divise a_0.

De la même manière,

$$\begin{aligned} &\sum_{i=0}^{n} a_i \left(\frac{p}{q}\right)^i = 0, \\ \text{d'où}\quad &\sum_{i=0}^{n-1} a_i \left(\frac{p}{q}\right)^i = -a_n \left(\frac{p}{q}\right)^n, \\ \text{d'où}\quad &q\left(\sum_{i=0}^{n-1} a_i p^i q^{n-1-i}\right) = -a_n p^n. \end{aligned}$$

Encore une fois, $\left(\sum_{i=0}^{n-1} a_i p^i q^{n-1-i}\right)$ est entier, donc q divise $a_n p^n$ et donc q divise a_n par le lemme de Gauss

On applique ce lemme à $r = \frac{p}{q} \in \mathcal{O}_{\mathbb{Q}}$ écrit sous forme irréductible. Le polynôme μ_r annule r, et unitaire et à coefficients dans $\mathbb{Z}$. Par le lemme, $q|1$. Donc $r = \pm p$ et $r \in \mathbb{Z}$. Donc $\mathcal{O}_{\mathbb{Q}} \subset \mathbb{Z}$.
On a donc bien $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. □

Vérifions maintenant que dans le cas général $\mathcal{O}_K$ est un anneau. Il suffit pour cela de montrer que $\overline{\mathbb{Z}}$ est un anneau.
Ce résultat peut être obtenu à l'aide de la proposition suivante.

Proposition 1.3.2.

(i) Soient $x_1, ..., x_r \in \overline{\mathbb{Z}}$. Alors $\mathbb{Z}[x_1, ..., x_r]$ est engendré (en tant que groupe additif) par un nombre fini d'éléments.

(ii) Soit $x \in \mathbb{C}$. Alors, $x \in \overline{\mathbb{Z}}$ si et seulement s'il existe $A \subset \mathbb{C}$ un sous-groupe additif finiment engendré non nul tel que $xA \subset A$.

Démonstration.

(i) Soit $x \in \overline{\mathbb{Z}}$ tel que $\forall n \in \mathbb{N}\, x^n \in \mathrm{Vect}_{\mathbb{Z}}\{x^i \,|\, 0 \leq i < \deg \mu_x\}$, où les combinaisons linéaires se font sur $\mathbb{Z}$.
On en déduit que

$$\mathbb{Z}[x_1, ..., x_r] \subset \mathrm{Vect}_{\mathbb{Z}}\left\{ \prod_j x_j^{i_j} \,\middle|\, \forall j\, 0 \leq i_j < \deg \mu_{x_j} \right\}.$$

L'inclusion réciproque est claire, ce qui conclut.

(ii) Soit $x \in \mathbb{C}$.

- Si $x \in \overline{\mathbb{Z}}$, on vérifie que $\mathbb{Z}[x]$ est finiment engendré d'après ce qui précède, et on a bien $x\mathbb{Z}[x] \subset \mathbb{Z}[x]$.
- Réciproquement, soit $A \subset \mathbb{C}$ comme dans l'énoncé, engendré par $e_1, ..., e_n$.
On dispose d'une matrice $M \in \mathcal{M}_n(\mathbb{Z})$ tel que $\forall j \in [\![1, n]\!]\, xe_j = \sum_i M_{i,j} e_i$.
On constate alors que $\mathrm{Ker}(xI_n - M)$ contient le vecteur non nul $(e_1, ..., e_n)$, d'où $\det(xI_n - M) = 0$.
Or, $\det(XI_n - M)$ est un polynôme unitaire à coefficient dans $\mathbb{Z}$: on en déduit que $x \in \overline{\mathbb{Z}}$.

□

Corollaire 1.3.1. *$\overline{\mathbb{Z}}$ est un anneau.*

Démonstration. Soient x, y deux entiers algébriques. D'après ce qui précède, $A = \mathbb{Z}[x, y]$ est finiment engendré. De plus, on a clairement $1 \in A$ d'où $A \neq \{0\}$, $(x - y)A \subset A$ et $xyA \subset A$, puisque A est ici un anneau, d'où $x - y, xy \in \overline{\mathbb{Z}}$.
On peut conclure : $\overline{\mathbb{Z}}$ est bien un anneau. □

Corollaire 1.3.2. *Soit K un corps de nombres. $\mathcal{O}_K = K \cap \overline{\mathbb{Z}}$ est un anneau comme intersection de deux anneaux.*

Le premier point de notre cahier des charges est vérifié ! Passons au second : on veut vérifier que le corps des fractions de $\mathcal{O}_K$ est K. On dispose pour ce faire de la propriété remarquable suivante.

Proposition 1.3.3. *Soit K un corps de nombres. $\mathcal{O}_K$ contient une base du $\mathbb{Q}$-espace vectoriel K.*

Démonstration. Soit $x \in K$. On écrit $\mu_x = \sum_{i=0}^{n} a_i X^i$ le polynôme annulateur minimal de x sur $\mathbb{Q}$. Tous les a_i sont dans $\mathbb{Q}$, donc en multipliant cette expression par le produit de leurs dénominateurs d, on obtient le polynôme $d\mu_x = \sum_{i=0}^{n} b_i X^i$ à coefficients dans $\mathbb{Z}$, et on a toujours $d\mu_x(x) = 0$.

En multipliant cette expression par $(b_n)^{n-1}$, on remarque que

$$d(b_n)^{n-1}\mu_x(x) = (b_n x)^n + \sum_{i=0}^{n-1} b_i (b_n)^{n-i-1} (b_n x)^i.$$

Ainsi, le polynôme $P(X) = X^n + \sum_{i=0}^{n-1} b_i (b_n)^{n-i} X^i$ est à coefficients dans $\mathbb{Z}$, unitaire, et annule $b_n x$. Enfin, reste à dire qu'il est minimal, puisque si on a un polynôme annulateur $Q \in \mathbb{Q}[X]$ de $b_n x$ de degré strictement inférieur à n, alors $Q\Big(b_n X\Big) \in \mathbb{Q}[X]$ annule x, donc est nul et Q est aussi nul.

Ainsi $b_n x \in \mathcal{O}_K$: autrement dit pour tout $x \in K$ on a $n_x \in \mathbb{Z}$ tel que $n_x x \in \mathcal{O}_K$.
Mais alors, si $(e_1, ..., e_n)$ est une base du $\mathbb{Q}$-espace vectoriel K, alors c'est aussi le cas de $(n_{e_1} e_1, ..., n_{e_n} e_n)$ qui est une famille de $\mathcal{O}_K$. Ainsi $\mathcal{O}_K$ contient une base du $\mathbb{Q}$-espace vectoriel K.

□

On en déduit immédiatement ce qu'on voulait.

Proposition 1.3.4. *Soit K un corps de nombres. Le corps des fractions de $\mathcal{O}_K$ est K.*

Démonstration. Cela provient du fait que $\mathcal{O}_K$ contient $\mathbb{Z}$ et une $\mathbb{Q}$-base de K. En particulier, tout corps L contenant $\mathcal{O}_K$ contient $\mathbb{Z}$, donc $\mathbb{Q}$, et par suite K. Mais comme $\mathcal{O}_K \subset K$, on a que K est le corps des fractions de $\mathcal{O}_K$. □

Pour clore cette partie, regardons un exemple de contexte dans lequel des anneaux d'entiers algébriques sur des corps de nombres peuvent apparaître. Cela nous aidera aussi à mieux comprendre les propriétés qu'on souhaiterait obtenir. Cet exemple est fréquemment abordé dans les documents traitants des entiers algébriques d'un corps de nombres, c'est par exemple le cas dans le document de Mathilde Gerbelli-Gauthier [13].

Exemple 1.3.1 (Équations de Pell-Fermat)**.** De façon générale, on appelle équation de Pell-Fermat l'équation suivante d'inconnues $a, b \in \mathbb{Z}$, où $m \in \mathbb{Z}$ et $n \in \mathbb{Z}$ n'est pas un carré parfait (c'est-à-dire le carré d'un nombre entier) :

$$a^2 - nb^2 = m. \tag{2}$$

Intéressons-nous au cas particulier $m = 1$. Quitte à faire coulisser des facteurs premiers de n dans b^2 et à trier les solutions ensuite, on peut supposer que n est un entier sans facteurs premiers carrés. L'équation devient donc

$$a^2 - nb^2 = 1 \quad n \text{ sans facteur carré.}$$

On cherche alors à factoriser cette expression. Comme $\sqrt{n}$ n'est pas entier, il n'est pas possible de le faire dans $\mathbb{Z}$. Néanmoins, on peut le faire en rajoutant $\sqrt{n}$ à $\mathbb{Z}$ pour former $\mathbb{Z}[\sqrt{n}]$. Ici on tolère l'écriture $\sqrt{n}$ si n est négatif (il s'agit d'un nombre avec $\sqrt{n}^2 = n$. Si on veut respecter les notations, on pourra prendre $i\sqrt{-n}$. L'équation s'écrit alors

$$(a - b\sqrt{n})(a + b\sqrt{n}) = 1.$$

On s'est donc ramené à l'étude d'un sous-ensemble d'unités (c'est-à-dire d'éléments inversibles) de $\mathbb{Z}[\sqrt{n}]$. Mais cet ensemble n'a a priori pas de *bonne structure* pour résoudre ce type de problème. En particulier, on ne sait pas à quoi ressemblent ses unités.

On remarque alors que $\mathbb{Z}[\sqrt{n}]$ peut parfois être vu comme un anneau d'entiers algébriques d'un corps de nombres. Plus précisément, on a le résultat suivant.

$$\mathcal{O}_{\mathbb{Q}(\sqrt{n})} = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{n}}{2}] & \text{si } n \equiv 1[4] \\ \mathbb{Z}[\sqrt{n}] & \text{si } n \equiv 2 \text{ ou } 3[4] \end{cases} \tag{3}$$

Avant d'aller plus loin, analysons ce résultat. Le cas $n \equiv 0[4]$ ne nous intéresse pas puisqu'alors n est divisible par $2^2 = 4$ et on peut se ramener au cas sans facteurs premiers. Si $n \equiv 2$ ou $3[4]$, on trouve de façon très commode que l'anneau qui nous intéressait $\mathbb{Z}[\sqrt{n}]$ est exactement un anneau d'entiers algébriques, $\mathcal{O}_{\mathbb{Q}(\sqrt{n})}$. Pour $n \equiv 1[4]$, l'ensemble $\mathbb{Z}[\sqrt{n}]$ est en quelque sorte *trop petit*, et on se trouve obligé d'étudier les inversibles de $\frac{1+\sqrt{n}}{2}$ (dans lequel $\mathbb{Z}[\sqrt{n}]$ est inclus).

Démontrons ce résultat : soit $a+b\sqrt{n} \in \mathbb{Q}[\sqrt{n}]$ qu'on suppose être un entier algébrique. On voit d'abord que **si b est nul**, a est un entier algébrique de $\mathbb{Q}$ (donc est entier d'après la proposition 1.3.1).

Supposons maintenant $b \neq 0$.

La clé de la preuve est de remarquer qu'un polynôme annulateur de $a+b\sqrt{n}$ est donné par $P(X) = X^2 - 2aX + (a^2 - nb^2)$. Ce polynôme est minimal puisque $a + b\sqrt{n} \notin \mathbb{Q}$. Comme on a supposé $a + b\sqrt{n}$ algébrique, on a donc le système

$$\begin{cases} 2a \in \mathbb{Z} \\ a^2 - nb^2 \in \mathbb{Z}, \end{cases} \quad \text{donc} \quad \begin{cases} 4a^2 \in \mathbb{Z} \\ 4(a^2 - nb^2) \in \mathbb{Z}, \end{cases} \quad \text{donc} \quad \begin{cases} 4nb^2 \in \mathbb{Z}. \end{cases}$$

Or, en écrivant $b = \frac{p}{q}$ sous forme irréductible, on a donc $4nb^2 \in \mathbb{Z} \Rightarrow q^2 | 4np^2$. Comme $p \wedge q = 1$ et que n n'a aucun facteur premier, on a donc $q^2|4$ ou encore $q|2$. Ainsi $2b \in \mathbb{Z}$.

On obtient finalement les conditions

$$\begin{cases} 2a \in \mathbb{Z} \\ 2b \in \mathbb{Z} \\ 4(a^2 - nb^2) \in \mathbb{Z}, \end{cases} \quad \text{ce qui se réécrit} \quad \begin{cases} 2a \in \mathbb{Z} \\ 2b \in \mathbb{Z} \\ (2a)^2 - n(2b)^2 \equiv 0[4]. \end{cases}$$

Enfin, on rappelle que pour $d \in \mathbb{Z}$, $d^2 \equiv 0$ ou $1[4]$ selon la parité de d. Dès lors, il ne reste plus qu'à distinguer selon la classe de n modulo 4.

- Si $n \equiv 1[4]$, alors $(2a)^2 \equiv (2b)^2[4]$ et les entiers $2a$ et $2b$ ont même parité. Donc $a, b \in \frac{1}{2}\mathbb{Z}$, ou encore $a + b\sqrt{n} \in \mathbb{Z}[\frac{1+\sqrt{n}}{2}]$.
- Si $n \equiv 2[4]$, alors $(2a)^2 \equiv 2(2b)^2[4]$. Mais $(2a)^2 \equiv 0$ ou $1[4]$, donc $(2b)^2 \equiv 0[4]$ et finalement $(2a)^2 \equiv 0[4]$. Donc $2a$ et $2b$ sont tous deux pairs, et $a, b \in \mathbb{Z}$. Ainsi $a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$.
- Si $n \equiv 3[4]$, on a le même phénomène : a et b sont entiers et $a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$.

On vient donc de montrer un sens de l'inclusion. Réciproquement, on vérifie aisément l'autre sens puisque tous ces éléments sont racines d'un polynôme $P(X) = X^2 - 2aX + (a^2 - nb^2)$ qui par construction est bien à coefficients entiers. Finalement, on a bien

$$\mathcal{O}_{\mathbb{Q}(\sqrt{n})} = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{n}}{2}] & \text{si } n \equiv 1[4] \\ \mathbb{Z}[\sqrt{n}] & \text{si } n \equiv 2 \text{ ou } 3[4] \end{cases}$$

Que retenir de cet exemple ? On a réécrit l'équation de Pell-Fermat comme un problème de recherche des unités d'un anneau d'entiers algébriques d'un corps de nombres. On va maintenant s'intéresser à un résultat qui donne précisément la structure de ces unités : **le théorème de Dirichlet**. On introduit pour l'instant simplement la définition suivante.

Définition 1.3.3. Soit K un corps de nombres. On note $\mathcal{O}_K^\times$ l'ensemble des unités de $\mathcal{O}_K$.

Terminons par remarquer le fait suivant.

Proposition 1.3.5. *Soit K un corps de nombres. $\mathcal{O}_K^\times$ est un groupe multiplicatif.*

Démonstration. $\mathcal{O}_K^\times$ est le groupe des unités d'un anneau. □

1.4 Manipuler les nombres

Maintenant que nous avons introduit $\mathcal{O}_K$, il s'agit de mieux comprendre sa structure. Cette partie introduit divers outils qui seront utiles à ce travail, puis expose certaines relations qui les unissent. Dans la suite K désigne, sauf mention contraire, un corps de nombres. Cette fois on s'inspire du chapitre 5 du cours de MAT552 de Gaëtan Chenevrier donné en troisième année à l'École polytechnique [14].

L'idée de départ est pour un $x \in K$ de regarder l'endomorphisme $\mathbb{Q}$-linéaire de K le plus simple : la multiplication par x.

Définition 1.4.1 (Norme et trace)**.** Soit $x \in K$. On note m_x la $\mathbb{Q}$-application linéaire

$$m_x \; : \left| \begin{array}{ccc} K & \to & K \\ y & \mapsto & xy. \end{array} \right.$$

On appelle alors norme de x, notée $N(x)$, le déterminant de cette application, et on note $\mathrm{Tr}(x)$ sa trace.

Cette définition est bien justifiée puisque K est, par définition, un $\mathbb{Q}$-espace vectoriel de dimension finie. On en déduit aussi que N et Tr sont à valeurs dans $\mathbb{Q}$.

La norme et la trace de x possèdent des propriétés tout-à-fait remarquables.

Proposition 1.4.1. *Soient $x, y \in K$. On a $N(xy) = N(x)N(y)$.*

Démonstration. Cela provient simplement du fait que $m_{xy} = m_x \circ m_y$. En effet,

$$\forall z \in K \;\; m_{xy}(z) = xyz = m_x(m_y(z)).$$

On déduit alors $N(xy) = N(x)N(y)$ par les propriétés du déterminant. □

On vérifie aussi que Tr est une application $\mathbb{Q}$-linéaire.

Proposition 1.4.2. *Pour tous $x, y \in K$, pour tout $\lambda \in \mathbb{Q}$, $\mathrm{Tr}(\lambda x + y) = \lambda \mathrm{Tr}(x) + \mathrm{Tr}(y)$.*

Démonstration. Cela découle simplement du fait que $m_{\lambda x+y} = \lambda m_x + m_y$, et de la linéarité de la trace. □

Trace et discriminant

Commençons par étudier l'application trace. Son intérêt transparaît à travers la définition et la proposition suivantes : elle préserve la liberté d'une famille.

Définition 1.4.2 (Discriminant)**.** Soit K un corps de nombres avec $n = [K : \mathbb{Q}]$. Soit $(e_1, ..., e_n)$ une famille de vecteurs de K. On note $disc(e_1, ..., e_n)$ le déterminant de la matrice $(\mathrm{Tr}(e_i e_j))_{1 \leq i,j \leq n}$.

On remarquera que la définition précédente est en fait valable pour toute extension finie L/K, sur laquelle on noterait $disc_{L/K}(e_1, ..., e_n)$.

Le discriminant permet de savoir si une famille est une $\mathbb{Q}$-base de K. En fait il fait beaucoup mieux que cela, puisqu'on verra plus tard qu'il s'agit d'une quantité invariante (en valeur absolue) pour $\mathcal{O}_K$ dans un certain sens précisé ultérieurement (voir proposition 2.2.3). Ainsi, le discriminant est en quelque sorte un déterminant « normalisé ».

Proposition 1.4.3. *Soit K un corps de nombres avec $n = [K : \mathbb{Q}]$. Soit $(e_1, ..., e_n)$ une famille de vecteurs de K.*

$$disc(e_1, ..., e_n) \neq 0 \text{ si et seulement si } (e_1, ..., e_n) \text{ est une } \mathbb{Q}\text{-base de } K.$$

Démonstration. Notons $M = (\mathrm{Tr}(e_i e_j))_{1 \leq i,j \leq n}$. On commence par remarquer le fait suivant : soit $x = \sum_{i=1}^n x_i e_i \in K$ avec les $x_i \in \mathbb{Q}$, alors,

$$M \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \mathrm{Tr}(xe_1) \\ \mathrm{Tr}(xe_2) \\ \vdots \\ \mathrm{Tr}(xe_n) \end{pmatrix}.$$

En effet, pour tout $i \in [\![1, n]\!]$, on a

$$\sum_{j=1}^n (\mathrm{Tr}(e_i e_j) x_j) = \mathrm{Tr}(e_i \sum_{j=1}^n x_j e_j) = \mathrm{Tr}(xe_i).$$

Cela donne bien la i^e coordonnée du produit $M \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$.

Dès lors, supposons que $(e_1, ..., e_n)$ est $\mathbb{Q}$-liée, c'est-à-dire qu'on a $x_1, ..., x_n \in \mathbb{Q}$ non tous nuls avec $\sum_{i=1}^n x_i e_i = 0$. Par la relation précédente appliquée à $x = 0$,

$$M \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \mathrm{Tr}(0e_1) \\ \mathrm{Tr}(0e_2) \\ \vdots \\ \mathrm{Tr}(0e_n) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Ainsi M n'est pas inversible, et $disc(e_1, ..., e_n) = \det(M) = 0$.

Réciproquement, supposons que $disc(e_1, ..., e_n) = 0$. Cela revient à dire qu'il existe

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{Q}^n \quad \text{tel que} \quad M \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Notons $x = \sum_{i=1}^n x_i e_i$, non nul, donc inversible d'inverse y. Si on suppose par l'absurde que $(e_1, ..., e_n)$ est une $\mathbb{Q}$-base de K, on a $y_1, ..., y_n \in \mathbb{Q}$ tels que $y = \sum_{i=1}^n y_i e_i$.
On remarque alors que $\mathrm{Tr}(1) = \mathrm{Tr}(I_n) = n$. On vérifie alors aisément que

$$\begin{pmatrix} y_1 & y_2 & \cdots & y_n \end{pmatrix} M \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \mathrm{Tr}(xy)$$

et $\mathrm{Tr}(xy) = n = 0$: absurde. $(e_1, ...e_n)$ n'est donc pas une $\mathbb{Q}$-base de K et l'équivalence est démontrée. □

Norme et polynôme minimal

Si la trace permet de regarder si une famille donnée est libre, la norme permet de son côté de donner une mesure de la taille d'un élément x de K. L'objectif de cette sous-partie va être de voir qu'un lien unit $N(x)$ et μ_x.

Comme on a défini $N(x)$ comme étant le déterminant de m_x, il est naturel de s'intéresser au polynôme caractéristique de cette application.

Définition 1.4.3 (Polynôme caractéristique)**.** Pour tout $x \in K$, on note χ_x le polynôme caractéristique de m_x, que l'on appelle polynôme caractéristique de x. Autrement dit,

$$\chi_x(X) = \det(X\mathrm{id} - m_x).$$

Le polynôme caractéristique d'un élément x de K est bien sûr lié à sa norme. Si on note $n = [K : \mathbb{Q}]$, en évaluant χ_x en 0, on obtient

$$\chi_x(0) = (-1)^n N(x).$$

Le théorème de Cayley-Hamilton dit que le polynôme annulateur minimal de m_x dans $\mathbb{Q}$ divise $\chi_x(X)$. En fait dans ce cas on a beaucoup mieux, puisque $\chi_x(X)$ en est une puissance. Avant de montrer cela, on observe que les notions de polynôme minimal de m_x et polynôme minimal de x coïncident.

Proposition 1.4.4. *Pour tout $x \in K$, on note p_{m_x} le polynôme annulateur minimal (donc unitaire) de m_x dans $\mathbb{Q}$.*

On a alors $\mu_x = p_{m_x}$.

Démonstration. Soit $x \in K$. La preuve repose sur le fait que, pour $P \in \mathbb{Q}[X]$, $m_{P(x)} = P(m_x)$. En effet, soit $P = \sum_{i=0}^{d} a_i X^i \in \mathbb{Q}[X]$, soit $y \in K$. On a

$$m_{P(x)}(y) = P(x)y = \sum_{i=0}^{d} a_i x^i y = \sum_{i=0}^{d} a_i m_x^i(y) = P(m_x)(y).$$

Dès lors, on a

- D'une part $\mu_x(m_x) = m_{\mu_x(x)} = m_0 = 0$. Ainsi, $p_{m_x} | \mu_x$.
- D'autre part, $m_{p_{m_x}(x)} = p_{m_x}(m_x) = 0$. En évaluant l'application $m_{p_{m_x}(x)}$ en 1, on trouve $p_{m_x}(x) = 0$. Donc $\mu_x | p_{m_x}$.

Finalement comme les deux polynômes sont unitaires, on a bien $\mu_x = p_{m_x}$. □

On écrit maintenant la proposition remarquable annoncée.

Proposition 1.4.5. *Soient K un corps de nombres et $x \in K$. On note $r = [K : \mathbb{Q}(x)]$. Alors,*

$$\chi_x = (\mu_x)^r.$$

Ce théorème est en fait valable pour toute extension finie L/K, et devient alors la proposition suivante (en adaptant les notations).

Proposition 1.4.6. *Soient L/K une extension finie et $x \in L$. On note $r = [L : K(x)]$. Alors,*

$$\chi_{x,L/K} = (\mu_{x,K})^r.$$

Dans un souci de généralité, nous démontrerons cette version puisque les deux preuves sont tout à fait identiques. L'indiçage par rapport à L/K était superflu dans le premier cas puisqu'un corps de nombres est toujours par défaut une extension finie de $\mathbb{Q}$.

Démonstration. On voit d'abord que L est bien une extension de $K(x)$ puisque $x \in L$ et $K \subset L$, donc a fortiori $K(x) \subset L$. De plus cette extension est finie puisque si on a une base du K-espace vectoriel L, cette famille engendre le $K(x)$-espace vectoriel L car $K \subset K(x)$. Donc le $K(x)$-espace vectoriel L est de dimension finie.

Notons $k = \deg(\mu_{x,K})$, et soit $(e_1, ..., e_r)$ une base du $K(x)$-espace vectoriel L. Enfin, rappelons que $(1, x, ..., x^{k-1})$ est une base du K-espace vectoriel $K(x)$ (proposition 1.2.5).

On considère alors la famille d'éléments de L

$$\beta = (e_1, xe_1, ..., x^{k-1}e_1, e_2, xe_2, ..., x^{k-1}e_r).$$

La famille β est bien une base du K-espace vectoriel L puisque c'est une base télescopique (comme dans la proposition 1.1.2).

Notons alors pour tout $j \in [\![1, r]\!]$ le sous-espace L_j de L défini par

$$L_j = \mathrm{Vect}_K(e_j, xe_j, ..., x^{k-1}e_j) = \mathrm{Vect}_{K(x)}(e_j).$$

L'application $m_x : y \mapsto xy$ stabilise L_j, et sa matrice dans la base $(e_j, xe_j, ..., x^{k-1}e_j)$ de L_j est

$$N_{x,K} = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \ddots & 0 & -a_1 \\ 0 & 1 & \ddots & 0 & -a_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & -a_{k-1} \end{pmatrix},$$

où $\mu_{x,K} = X^k + \sum_{i=0}^{k-1} a_i X^i$. Il s'agit en effet simplement de la matrice compagnon de $\mu_{x,K}$.

Dès lors, puisque $L = \bigoplus_{j=1}^{r} L_j$, la matrice de m_x dans la base β est la matrice diagonale par bloc

$$M_{x,K} = \begin{pmatrix} N_{x,K} & 0_k & \dots & 0_k & 0_k \\ 0_k & N_{x,K} & \ddots & \vdots & \vdots \\ \vdots & 0_k & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & N_{x,K} & 0_k \\ 0_k & \dots & \dots & 0_k & N_{x,K} \end{pmatrix}.$$

En utilisant alors les propriétés classiques de la matrice compagnon d'un polynôme,

$$\chi_{x,L/K} = \det(X\mathrm{id} - m_x) = \det(X\mathrm{id} - M_{x,K}) = \det(X\mathrm{id} - N_{x,K})^r = (\mu_{x,K})^r.$$

□

Ce fait étant établi, on va pouvoir obtenir toute une série de propriétés sur les normes des éléments de $\mathcal{O}_K$.

Proposition 1.4.7. *Pour tout $x \in \mathcal{O}_K$, $N(x) \in \mathbb{Z}$.*

Démonstration. Soit $x \in \mathcal{O}_K$. Par la propriété précédente et l'équation 1.4, on a

$$N(x) = (-1)^n \chi_x(0) = (-1)^n \mu_x(0)^r. \tag{4}$$

Mais $x \in \mathcal{O}_K$ et $\mu_x \in \mathbb{Z}[X]$. En particulier, $\mu_x(0) \in \mathbb{Z}$ et $N(x) \in \mathbb{Z}$. □

Exemple 1.4.1. On fera attention que la réciproque est fausse ! On peut avoir pour $x \in K$ $N(x) \in \mathbb{Z}$ mais $x \notin \mathcal{O}_K$. En effet, il suffit de considérer un élément donc le polynôme minimal a un coefficient constant entier, mais dont les autres coefficients ne sont pas entiers.

Par exemple, on voit que

$$X^2 + \frac{8}{5}X + 1 = \left(X - \frac{-4-3i}{5}\right)\left(X - \frac{-4+3i}{5}\right).$$

Si on regarde $K = \mathbb{Q}\left(\frac{-4+3i}{5}\right)$, l'élément $\frac{-4+3i}{5}$ a pour polynôme annulateur minimal $X^2 + \frac{8}{5}X + 1$, donc $N\left(\frac{-4+3i}{5}\right) = 1$, mais comme il n'est pas à coefficients entiers on n'a pas $\frac{-4+3i}{5} \in \mathcal{O}_K$.

De même, si l'on préfère les racines carrées aux nombres plus grands que 3, on peut regarder la factorisation

$$X^2 - \frac{2}{3}X + 1 = \left(X - \frac{1 - 2\sqrt{2}i}{3}\right)\left(X - \frac{1 + 2\sqrt{2}i}{3}\right)$$

qui fournit un autre exemple.

Cela permet d'obtenir la caractérisation des unités de $\mathcal{O}_K$ suivante, qui justifie encore une fois la pertinence du concept de norme. On fera attention que l'équivalence n'est valable que dans $\mathcal{O}_K$.

Proposition 1.4.8. *Soit $x \in \mathcal{O}_K$.*

$$x \in \mathcal{O}_K^\times \iff N(x) = \pm 1.$$

Démonstration. Supposons d'abord $x \in \mathcal{O}_K^\times$. Alors,

$$N(x)N(x^{-1}) = N(xx^{-1}) = N(1_k) = \det(\mathrm{id}_K) = 1.$$

Donc $N(x^{-1}) = N(x)^{-1}$. Mais $x \in \mathcal{O}_K$, donc $N(x) \in \mathbb{Z}$. Mais $x^{-1} \in \mathcal{O}_K$ par définition, et $N(x^{-1}) \in \mathbb{Z}$. Finalement on a forcément $N(x) = \pm 1$.

Réciproquement, si $N(x) = \pm 1$, l'équation 4 dit que $(-1)^n \mu_x(0)^r = \pm 1$, ou encore, en notant $\mu_x = X^k + \sum_{i=0}^{k-1} a_i X^i$, que $a_0 = \pm 1$. Mais alors,

$$x^k + \sum_{i=0}^{k-1} a_i x^i = 0,$$

$$\text{d'où} \quad x\left(x^{k-1} + \sum_{i=1}^{k-1} a_i x^{i-1}\right) = \pm 1.$$

Comme $\pm\left(x^{k-1} + \sum_{i=1}^{k-1} a_i x^{i-1}\right) \in \mathcal{O}_K$ (c'est un anneau), on en déduit que x est inversible, donc $x \in \mathcal{O}_K^\times$. □

Pour clore cette partie, on peut réécrire notre équation de Pell-Fermat avec notre nouveau vocabulaire.

Exemple 1.4.2 (Équations de Pell-Fermat)**.** On reprend l'exemple 1.3.1. On cherchait à caractériser les unités des $\mathcal{O}_{\mathbb{Q}(\sqrt{n})}$ où n était un entier sans facteur premier.

On travaille sur le corps de nombres $\mathbb{Q}(\sqrt{n})$, dont une $\mathbb{Q}$-base est bien sûr $(1, \sqrt{n})$. Soit $x = a + b\sqrt{n} \in \mathbb{Q}$. On voit immédiatement que la matrice de m_x dans la base $(1, \sqrt{n})$ est

$$M_x = \begin{pmatrix} a & nb \\ b & a \end{pmatrix}.$$

Alors $N(x) = \det(M_x) = a^2 - nb^2$. Pour $n \equiv 2$ ou $3[4]$, on avait vu que $\mathcal{O}_{\mathbb{Q}(\sqrt{n})} = \mathbb{Z}[\sqrt{n}]$. Donc dans ce cas on a exactement l'équivalence, pour $x = a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$,

$$\begin{aligned} x \in \mathbb{Z}[\sqrt{n}]^\times &\iff a^2 - nb^2 = \pm 1 \\ &\iff (a, b) \text{ est solution de l'équation de Pell-Fermat pour } m = \pm 1. \end{aligned}$$

Résoudre une équation de Pell-Fermat dans ce cas, c'est donc décrire le groupe des unités $\mathcal{O}_K^\times$.

1.5 Incarner les nombres

On introduit maintenant le dernier outil nécessaire à l'élucidation de la structure de $\mathcal{O}_K$: celui de plongement de corps de nombres. L'idée est d'abord de voir que tout corps de nombres peut-être vu comme un sous-corps de $\mathbb{C}$. En effet, les éléments d'un corps de nombres K sont algébriques sur $\mathbb{Q}$, donc sur $\mathbb{R}$ et $\mathbb{C}$ est un clôture algébrique de $\mathbb{R}$. Une question apparaît alors : étant donnée une extension de corps de nombres L/K, combien y a-t-il de façons de « plonger » L dans $\mathbb{C}$ tout préservant K (c'est-à-dire que l'image de K par le plongement est K) ?

Intuitivement, la question semble liée au degré de liberté du corps L par rapport à K. C'est en effet le cas : un résultat classique de la théorie de Galois affirme qu'il existe exactement $[L : K]$ tels plongements. On se propose dans un premier temps de le démontrer, avant de passer aux conséquences de ce résultat. En particulier, on verra que les plongements permettent d'obtenir de nouvelles écritures agréables des outils présentés à la partie précédente.

Ici encore, on suit le cours de Gaëtan Chenevrier [14].

Étude des plongements d'un corps de nombres

Définition 1.5.1 (Plongement d'un corps de nombres)**.** Soit K un corps de nombres. On appelle plongement de K un morphisme de corps $\sigma : K \to \mathbb{C}$ qui est $\mathbb{Q}$-linéaire. On note $\Sigma(K)$ l'ensemble des plongements de K.

Comme on a pris $\mathbb{Q} \subset K$, tout plongement σ préserve $\mathbb{Q}$:

$$\forall r \in \mathbb{Q}\ \sigma(r) = r.$$

On prendra dans la suite pour simplifier les notations la convention $K \subset \mathbb{C}$, de la même façon qu'on avait pris $\mathbb{Q} \subset K$. Cette convention est licite puisqu'on peut identifier une extension L/K à un sous-corps de la clôture algébrique Ω de K (qui peut elle-même être plongée dans $\mathbb{C}$). La notion de « clôture algébrique » est définie juste en-dessous.

Cette définition se généralise au cas où on fait des extensions successives de corps de nombres.

Définition 1.5.2 (Plongement d'un corps de nombres)**.** Soit L/K une extension de corps de nombres. On note $\Sigma(L/K)$ l'ensemble des plongements K-linéaires $L \to \mathbb{C}$. Autrement dit,

$$\Sigma(L/K) = \left\{ \sigma \in \Sigma(L) \,\middle|\, \sigma_{|K} = \mathrm{id}_K \right\}.$$

Avec cette définition on retrouve $\Sigma(K/\mathbb{Q}) = \Sigma(K)$.

Exemple 1.5.1. Avec ces conventions, on obtient le plongement trivial

$$\sigma \; : \left| \begin{array}{ccc} K & \to & \mathbb{C} \\ x & \mapsto & x. \end{array} \right.$$

Donnons tout de suite un exemple dans un cas particulier.

Exemple 1.5.2. Pour $K = \mathbb{Q}(\sqrt{2})$, soit $\sigma \in \Sigma(K)$. Une base de $\mathbb{Q}(\sqrt{2})$ est $(1, \sqrt{2})$. On sait déjà que $\sigma(1) = 1$ puisque σ est un morphisme. Reste à déterminer $\sigma(\sqrt{2})$.

On observe alors le fait suivant : le polynôme annulateur minimal de $\sqrt{2}$ sur $\mathbb{Q}$ est $X^2 - 2$. Mais alors,

$$0 = \sigma(0) = \sigma((\sqrt{2})^2 - 2) = \sigma(\sqrt{2})^2 - 2.$$

Donc $\sigma(\sqrt{2})$ est aussi racine de $X^2 - 2$, ce qui impose les valeurs $\pm\sqrt{2}$.

On dispose de deux plongements (on vérifie immédiatement qu'il s'agit de deux morphismes injectifs) :

$$\sigma_1 \; : \left| \begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \to & \mathbb{C} \\ a + b\sqrt{2} & \mapsto & a + b\sqrt{2}, \end{array} \right.$$

$$\sigma_2 \; : \left| \begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \to & \mathbb{C} \\ a + b\sqrt{2} & \mapsto & a - b\sqrt{2}. \end{array} \right.$$

Dans cet exemple il est clair que le nombre de plongements est donné par $\deg(\mu_{\sqrt{2}})$. On voit bien que cela fonctionne pour deux raisons :

(i) K est de la forme $\mathbb{Q}(x)$,

(ii) μ_x est scindé à racines simples sur $\mathbb{C}$, il a exactement $\deg(\mu_x)$ racines distinctes dans $\mathbb{C}$.

On ne sait pas a priori si ces deux conditions sont vérifiées pour tout corps de nombres. Les théorèmes suivants visent à généraliser ces observations, à des corps de nombres quelconques, et on va voir que les deux conditions exposées sont vérifiées dans leur cas.

Cette partie est fortement inspirée de l'article (cliquable) « extension séparable », adapté au cas particulier des corps de nombres.

Dans la suite on se replace dans le cadre plus général d'une extension de corps L/K afin de présenter quelques définitions.

Définition 1.5.3 (Clôture algébrique)**.** Une clôture algébrique d'un corps K est une extension algébrique de corps Ω/K tel que tout polynôme non constant de $\Omega[X]$ admet une racine dans Ω (c'est-à-dire que l'extension est algébriquement close).

Exemple 1.5.3. Une clôture algébrique de $\mathbb{Q}$ est l'ensemble des nombres algébrique de $\mathbb{C}$, c'est-à-dire l'ensemble des nombres complexes qui sont racines d'un polynôme à coefficients rationnels. On note cet ensemble $\overline{\mathbb{Q}}$. On remarquera qu'il ne suffit pas de prendre l'ensemble des nombres algébriques réels, puisqu'alors le polynôme X^2+1 n'admet pas de racine.

On ne s'intéressera pas ici à l'existence d'une clôture algébrique pour un corps donné (le lecteur voulant en savoir davantage pourra se reporter à [12], I.3). On se contente de rappeler les résultats suivants :

- Tout corps de nombres admet une clôture algébrique,
- Les clôtures algébriques d'un corps de nombres K sont identiques à isomorphisme près. On notera donc Ω « la » clôture algébrique de K, et on prendra $\Omega \subset \mathbb{C}$.

La définition suivante permet d'exprimer la deuxième condition que nous avions exposé : si $K = \mathbb{Q}[x]$, on va avoir besoin du fait que μ_x est scindé sur $\mathbb{C}$.

Définition 1.5.4 (Extension séparable)**.** Soient L/K une extension algébrique, Ω une clôture algébrique de K.

(i) On dit que $P \in K[X]$ est séparable si dans Ω où il est scindé il n'a que des racines simples. Il a donc autant de racines que son degré.

(ii) L'élément $x \in L$ est séparable sur K si $\mu_{x,K}$ l'est.

(iii) Le corps L est séparable sur K si tous ses éléments le sont.

(iv) Le corps K est dit parfait si toutes ses extensions algébriques sont séparables, ce qui équivaut à dire que tous les polynômes irréductibles de $K[X]$ sont séparables.

On a un critère simple de la séparabilité d'une extension par la notion de caractéristique d'un corps.

Définition 1.5.5 (Caractéristique d'un anneau)**.** Soit A un anneau. On appelle caractéristique le plus petit entier n tel que $n.1_A = 0_A$ s'il existe, et 0 sinon (A est alors dit de caractéristique nulle).

Exemple 1.5.4. Dans le cas d'un corps de nombres K, K est une extension de $\mathbb{Q}$ qui est de caractéristique nulle. Donc K est de caractéristique nulle.

Tout corps de nombres est donc parfait grâce à la propriété suivante.

Proposition 1.5.1. *Tout corps de caractéristique nulle est parfait.*

Démonstration. Soient K un corps de caractéristique nulle, Ω une clôture algébrique de K et soit L/K une extension algébrique de K. Soit $x \in L$. On sait que $\mu_{x,K}$ est irréductible dans $K[X]$ (proposition 1.2.4).

On observe alors que $\mu_{x,K}$ et $\mu'_{x,K}$ sont premiers entre eux dans $K[X]$. En effet, $\mu'_{x,K}$ est unitaire de degré $d > 0$, alors le terme de plus haut degré de $\mu'_{x,K}$ est dX^{d-1} est comme $d.1_K \neq 0_K$ car on est en caractéristique nulle, $\mu'_{x,K}$ est de degré $d-1 \geq 0$, et en particulier $\mu'_{x,K}$ n'est pas nul.

Dès lors, supposer par l'absurde que $\mu_{x,K}$ et $\mu'_{x,K}$ ne sont pas premiers entre eux dans $K[X]$ revient à dire que $\mu_{x,K}$ divise $\mu'_{x,K}$ (car $\mu_{x,K}$ est irréductible dans $K[X]$) ce qui entraîne par argument de degré que $\mu'_{x,K} = 0$, ce qui est absurde.

Ainsi $\mu_{x,K}$ et $\mu'_{x,K}$ sont premiers entre eux dans $K[X]$. Le théorème de Bézout garantit l'existence de U et $V \in K[X]$ avec

$$U\mu_{x,K} + V\mu'_{x,K} = 1.$$

Cette relation reste a fortiori vraie dans $\Omega[X]$. Mais alors si par l'absurde $\mu_{x,K}$ n'est pas séparable, c'est qu'il a une racine multiple $\omega \in \Omega$ qui est donc aussi racine de $\mu_{x,K}$. En évaluant l'équation précédente en ω, il vient $0 = 1$: absurde.

Ainsi $\mu_{x,K}$ est séparable : K est parfait. □

On définit maintenant le degré de séparabilité qui fait le lien avec les plongements.

Définition 1.5.6 (Degré de séparabilité)**.** Soit L/K une extension de corps de nombres. On appelle degré de séparabilité de L/K, noté $[L : K]_s$, le nombre de plongements K-linéaires $L \to \mathbb{C}$. Autrement dit, $[L : K]_s = |\Sigma(L/K)|$.

Comme on l'a vu dans l'exemple 1.5.2, les choses se passent bien si :

(i) L'extension est simple, c'est-à-dire de la forme $L = K(x)$,

(ii) $\mu_{x,K}$ est séparable.

On avait en effet dans l'exemple que $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}]_s = \deg(\mu_{\sqrt{2}})$. Mais on sait que $\deg(\mu_{\sqrt{2}}) = [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}]$ grâce au théorème 1.2.5. Donc dans l'exemple on a $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}]_s = [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}]$.

Le deuxième point est toujours vérifié dans un corps de nombres grâce à la proposition 1.5.1. On peut donc énoncer le théorème suivant, dont la démonstration est identique à la méthode de l'exemple 1.5.2.

Proposition 1.5.2. *Soit L/K une extension de corps de nombres de la forme $L = K(x)$. On a $[L : K]_s = [L : K]$.*

Démonstration. Soit $\sigma \in \Sigma(L/K)$.

- On sait que $\sigma_{|K} = \mathrm{id}_K$. On en déduit alors que pour tout $P \in K[X]$, on a $\sigma(P) = P(\sigma)$. En effet, soit $P = \sum_{i=0}^{d} a_i X^i \in K[X]$. Soit $y \in L$. On a

$$\sigma(P(y)) = \sigma\left(\sum_{i=0}^{d} a_i y^i\right) = \sum_{i=0}^{d} \sigma(a_i)\sigma(y^i) = \sum_{i=0}^{d} a_i \sigma(y)^i = P(\sigma)(y).$$

  Mais alors avec $P = \mu_{x,K}$, en évaluant en x, on obtient

$$\sigma(0) = \sigma(\mu_{x,K}(x)) = \mu_{x,K}(\sigma(x)) = 0.$$

  Or, l'extension est séparable (proposition 1.5.1), donc en notant $d = [K(x) : K]$ le degré de $\mu_{x,K}$, $\mu_{x,K}$ a exactement d racines distinctes dans $\mathbb{C}$, que l'on note $r_1, ..., r_d$.
  Donc $\sigma(x)$ peut prendre au maximum d valeurs distinctes. Cela permet déjà de voir que

$$[L : K]_s \leq [L : K].$$

- Pour l'égalité, soit $i \in [\![1, d]\!]$. Comme $(1, x, ..., x^d)$ forme une K base de $L = K(x)$, le morphisme de corps K-linéaire $K(x) \to \mathbb{C}$ défini par $\sigma(x) = r_i$ est bien un plongement : $\sigma \in \Sigma(K(x)/K)$.
  Comme les $r_1, ..., r_d$ sont distincts, on peut construire d tels morphismes, d'où

$$[L : K]_s = [L : K].$$

□

Pour conclure, il ne reste plus qu'à dire que toute extension finie peut se ramener à une suite finie d'extensions simples.

Proposition 1.5.3. *Soit L/K une extension de corps de nombres. On a $[L : K]_s = [L : K]$.*

Démonstration. On voit d'abord que L/K est bien une extension finie puisque L est une extension finie de $\mathbb{Q}$, et qu'une $\mathbb{Q} - base$ de L est a fortiori une K-famille génératrice de L.

Or, toute extension finie L/K peut s'écrire comme une suite d'extensions simples. Il suffit de raisonner en ajoutant successivement à K les éléments de L qui n'y sont pas jusqu'à atteindre L, ce procédé ayant une fin puisque L est de dimension finie sur K.

Dès lors on peut écrire $L = K(x_1, x_2, ..., x_k)$, et il ne reste plus qu'à raisonner par récurrence sur k.

- L'**initialisation** $k = 1$ est exactement la proposition 1.5.2.
- Pour l'**hérédité**, écrivons $L = K(x_1, ..., x_k, x_{k+1}) = (K(x_1)(x_2)...(x_k))(x_{k+1}) = K'(x_{k+1})$. Raisonnons par dénombrement. Soit $\sigma \in \Sigma(L/K)$.
  Alors a fortiori $\sigma_{|K'} \in \Sigma(K'/K)$. Mais $K' = K(x_1, ..., x_k)$, donc par HR_k $[K' : K]_s = |\Sigma(K'/K)| = [K' : K]$. On a donc $[K' : K]$ choix possibles pour $\sigma_{|K'}$.
  De plus, $L = K'(x_{k+1})$. Les valeurs que prend σ sur K' sont fixées. Il faut maintenant compter le nombre de façons qu'on a de prolonger $\sigma_{|K'}$ en un morphisme K'-linéaire. En

fait tout se passe exactement comme si $\sigma_{|K'}$ était l'identité sur K'. Il y a donc $[L : K']_s$ façons d'obtenir un tel prolongement, et ce nombre vaut $[L : K']$ par HR_1.
On a donc $[K' : K]$ façons de construire $\sigma_{|K'}$, et pour chacune d'entre elles $[L : K']$ façons de la prolonger à L. On a donc en tout $[L : K'][K' : K] = [L : K]$ K-plongements de L (où la multiplicativité du degré provient de la proposition des bases télescopiques 1.1.2). Ainsi $[L : K] = [L : K]_s$, HR_{k+1} est démontrée.

□

On a donc atteint notre premier objectif ! On conclut cette sous-partie avec une classification tout à fait naturelle des plongements.

Définition 1.5.7 (Plongements réels et complexes)**.** Soit K un corps de nombres. On dit qu'un plongement $\sigma \in \Sigma(K)$ est réel s'il ne prend que des valeurs réelles. Dans le cas contraire, il est dit complexe.

Proposition 1.5.4. *Soit K un corps de nombres. Si $\sigma \in \Sigma(K)$ est un plongement complexe, alors $\overline{\sigma} : x \mapsto \overline{\sigma(x)}$ est encore un plongement complexe de K.*

Démonstration. $\overline{\sigma} : K \to \mathbb{C}$ est encore un morphisme $\mathbb{Q}$-linéaire puisque $\mathbb{Q} \subset \mathbb{R}$ n'est pas affecté par la conjugaison. □

On peut donc grouper les prolongements complexes par paires, ce qui donne lieu à la définition suivante.

Définition 1.5.8 (Plongements réels et complexes)**.** Soit K un corps de nombres. On note $n = [K : \mathbb{Q}]$, r_1 le nombre de plongements réels de K, et r_2 le nombre de paires de plongements complexes de K. On a donc $n = r_1 + 2r_2$.

Enfin, profitons du fait qu'on parle des corps parfaits pour démontrer le théorème de l'élément primitif dans ce cadre. Il ne nous servira pas immédiatement par la suite, mais sera utile aux chapitres 6 et 7. Notons qu'il aurait pu nous être utile dans les démonstrations précédentes, mais on a préféré procéder sans.

Théorème 4 (Théorème de l'élément primitif)**.** *Soit K un corps de nombres. Il existe $x \in \overline{\mathbb{Q}}$ tel que*

$$K \cong \mathbb{Q}[x].$$

Démonstration. Soit K un corps de nombres.

- **Supposons d'abord que l'on peut écrire $K = \mathbb{Q}[\alpha, \beta]$.**
  On note $\alpha_1, ..., \alpha_s$ les conjugués de α, et $\beta_1, ..., \beta_t$ les conjugués de β. Comme $\mathbb{Q}$ est parfait, les conjugués de α (respectivement β) sont deux à deux distincts. On dispose de plus de λ dans $\mathbb{Q}$ n'appartenant pas à l'ensemble fini des éléments de la forme $\frac{\alpha_i - \alpha}{\beta_j - \beta}$ $(\beta_j \neq \beta)$.

Montrons que $\theta = \alpha + \lambda\beta$ est un élément primitif.

Soit P le polynôme minimal de α et Q celui de β sur $\mathbb{Q}$. On remarque que $\alpha = \theta - \lambda\beta$, d'où $P(\theta - \lambda\beta) = 0$. Donc, sur $\mathbb{Q}[\theta]$, le polynôme minimal de β, R, divise à la fois $S = P(\theta - \lambda X)$ et Q.

— Supposons $\deg(R) > 1$. Alors, S et Q ont au moins deux racines communes, β et β' conjugué distinct de β.

Il vient $P(\theta - \lambda\beta') = 0$ donc $\theta - \lambda\beta'$ est un conjugué α' de α.
D'où $\alpha + \lambda\beta - \lambda\beta' = \alpha'$, puis $\lambda = \frac{\alpha'-\alpha}{\beta'-\beta}$: contradiction.

— Donc $\deg(R) = 1$, puis $\beta \in \mathbb{Q}[\theta]$ et $\alpha = \theta - \lambda\beta \in \mathbb{Q}[\theta]$.

- **Supposons maintenant qu'il existe $n > 2$ tel que $K = \mathbb{Q}[\alpha_1, ..., \alpha_n]$.** On suppose le théorème de l'élément primitif vrai pour tout corps de nombre L tel qu'on peut l'écrire $L = \mathbb{Q}[\beta_1, ..., \beta_m]$ avec $m < n$.

  $K = \mathbb{Q}[\alpha_1, ..., \alpha_n] = (\mathbb{Q}[\alpha_1, \alpha_2])[\alpha_3, ..., \alpha_n]$, donc par le résultat démontré ci-dessus, on dispose de θ tel que $K = (\mathbb{Q}[\theta])[\alpha_3, ..., \alpha_n] = \mathbb{Q}[\theta, \alpha_3, ..., \alpha_n]$.

  Donc, par la supposition qu'on a faite, on dispose de γ telle que $K = \mathbb{Q}[\gamma]$.

Ainsi, par le principe de récurrence, on obtient le théorème de l'élément primitif. □

Lien avec le notions précédentes

On relie maintenant la notion de plongements à celle de polynôme caractéristique introduite plus haut (1.4.3). On a en fait un lien très fort entre ces deux concepts, puisque les plongements fournissent la factorisation de χ_x dans $\mathbb{C}[X]$. On reprend les résultats du chapitre 5 de [14].

Proposition 1.5.5. *Soit L/K une extension de corps de nombres. Soit $x \in L$. On a*

$$\chi_{x,L/K} = \prod_{\sigma \in \Sigma(L/K)} (X - \sigma(x)) \quad \textit{dans } \mathbb{C}[X].$$

Démonstration. La preuve combine tous les raisonnements vus jusqu'à présents.

On commence par raisonner sur $K(x)/K$. La preuve de la proposition 1.5.2 dit exactement que

$$\mu_{x,K} = \prod_{\sigma \in \Sigma(K(x)/K)} (X - \sigma(x))$$

Soit $\sigma \in \Sigma(K(x)/K)$ fixé. D'après la preuve de la proposition 1.5.3, il y a exactement $[L : K(x)]$ plongements $\sigma(\in \Sigma(L/K)$ qui coïncident avec σ sur $K(x)$, c'est-à-dire en fait tels que $\sigma'(x) = \sigma(x)$. De plus, toujours d'après cette même preuve, tous les $\sigma' \in \Sigma(L/K)$ se

reconstituent à partir d'un $\sigma \in \Sigma(K(x)/K)$. Dès lors,

$$\begin{aligned}\prod_{\sigma' \in \Sigma(L/K)} (X - \sigma'(x)) &= \prod_{\sigma \in \Sigma(K(x)/K)} \left(\prod_{\substack{\sigma' \in \Sigma(L/K) \\ \sigma'(x) = \sigma(x)}} (X - \sigma'(x)) \right) \\ &= \prod_{\sigma \in \Sigma(K(x)/K)} \left(\prod_{\substack{\sigma' \in \Sigma(L/K) \\ \sigma'(x) = \sigma(x)}} (X - \sigma(x)) \right) \\ &= \prod_{\sigma \in \Sigma(K(x)/K)} (X - \sigma(x))^{[L:K(x)]} \\ &= \mu_{x,K}^{[L:K(x)]} \\ &= \chi_{x,L/K}.\end{aligned}$$

où la dernière ligne provient de la proposition 1.4.6. C'est exactement ce qu'on voulait. □

On en déduit le corollaire fondamental suivant.

Corollaire 1.5.1. *Soit K un corps de nombres. Soit $x \in K$. On a*

$$N(x) = \prod_{\sigma \in \Sigma(K)} (\sigma(x)).$$

Démonstration. Rappelons le résultat de 4, avec $n = [K : \mathbb{Q}]$:

$$N(x) = (-1)^n \chi_x(0).$$

On sait que $|\Sigma(K)| = [K : \mathbb{Q}]_s = n$. Donc $(-1)^n \chi_x(0) = \prod_{\sigma \in \Sigma(K)} (\sigma(x))$. En combinant, on a bien

$$N(x) = \prod_{\sigma \in \Sigma(K)} (\sigma(x)).$$

□

On vérifie sur quelques exemples qu'on sait calculer les plongements ainsi que les normes.

Exemple 1.5.5. Retournons dans $K = \mathbb{Q}(\sqrt{2})$. On avait l'expression des plongements de K :

$$\sigma_1 : \left| \begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \to & \mathbb{C} \\ a + b\sqrt{2} & \mapsto & a + b\sqrt{2}, \end{array} \right.$$

$$\sigma_2 : \left| \begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \to & \mathbb{C} \\ a + b\sqrt{2} & \mapsto & a - b\sqrt{2}. \end{array} \right.$$

Pour un élément $x = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, on a donc $N(x) = (a + b\sqrt{2})(a - b\sqrt{2}) =$

$a^2 - 2b^2$. On retrouve bien l'expression de la norme qu'on avait vue dans l'exemple 1.4.2. Ici $r_1 = 2, r_2 = 0$.

Exemple 1.5.6. Si on veut obtenir un exemple de plongement complexe, on peut par exemple considérer $K = \mathbb{Q}(\sqrt{-n})$ où n est un entier. Le polynôme annulateur minimal de $\sqrt{-n}$ est alors $X^2 + n$. On le factorise comme $(X - i\sqrt{n})(X + i\sqrt{n})$ dans $\mathbb{C}[X]$. On a donc deux plongements complexes cette fois :

$$\sigma_1 : \left| \begin{array}{ccc} \mathbb{Q}(\sqrt{-n}) & \to & \mathbb{C} \\ a + b\sqrt{-n} & \mapsto & a + ib\sqrt{n}, \end{array} \right.$$

$$\sigma_2 : \left| \begin{array}{ccc} \mathbb{Q}(\sqrt{-n}) & \to & \mathbb{C} \\ a + b\sqrt{-n} & \mapsto & a - ib\sqrt{n}. \end{array} \right.$$

Donc $r_1 = 0, r_2 = 1$.

Exemple 1.5.7 (Polynômes cubiques à une racine réelle)**.** Pour construire un exemple où on a des plongements des deux espèces, on a besoin d'un réel dont le polynôme minimal sur $\mathbb{Q}$ a à la fois des racines réelles et complexes. C'est le cas par exemple de $\sqrt[3]{2}$ dont le polynôme minimal est $X^3 - 2 = (X - \sqrt[3]{2})(X - j\sqrt[3]{2})(X - j^2\sqrt[3]{2})$.
Ici $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})} = \mathbb{Z}[\sqrt[3]{2}] = \left\{ a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 \,\middle|\, a, b, c \in \mathbb{Z} \right\}$. On a donc trois plongements :

$$\begin{array}{rccc} \sigma_1 & : & a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 & \mapsto & a + b\sqrt[3]{2} + c\sqrt[3]{2}^2, \\ \sigma_2 & : & a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 & \mapsto & a + jb\sqrt[3]{2} + j^2c\sqrt[3]{2}^2, \\ \sigma_3 & : & a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 & \mapsto & a + j^2b\sqrt[3]{2} + jc\sqrt[3]{2}^2. \end{array}$$

Donc $r_1 = 1, r_2 = 1$.

L'utilité de l'écriture avec les plongements va transparaître avec les deux résultats qui closent cette partie, et qui seront utilisés de manière cruciale au second chapitre.

D'une part, comme on l'a annoncé plus haut, la norme d'un élément mesure bien en quelque sorte sa taille. Plus précisément, on a deux façons différentes de borner la norme.

- On peut borner chacun des $|\sigma_i(x)|$ par un $M > 0$. On va voir que dans ce cas on n'a qu'un nombre fini de x possibles. Autrement dit, $\left\{ x \in \mathcal{O}_K \,\middle|\, \forall i \in [\![1, n]\!]\, |\sigma_i(x)| \leq M \right\}$ est fini.
- On peut aussi simplement borner $|N(x)|$ par un $M > 0$. Le premier cas implique le deuxième (puisque $N(x) = \prod_{i=1}^{n}(\sigma_i(x))$, mais la réciproque est fausse, puisqu'on peut avoir des $\sigma_i(x)$ de module très petit et d'autres de module très grand, tout en conservant $N(x)$ borné. On verra dans ce cas que l'ensemble des idéaux de $\mathcal{O}_K$ de la forme $x\mathcal{O}_K$ est fini. Autrement dit, $\left\{ x\mathcal{O}_K \,\middle|\, x \in \mathcal{O}_K, |N(x)| \leq M \right\}$ est fini.

La deuxième propriété nous est inaccessible pour le moment, mais elle sera démontrée dans le chapitre 2 (voir proposition 2.2.8).

D'autre part, les plongements permettent d'obtenir une réécriture du discriminant d'une famille. Celle-ci nous sera très utile lorsqu'on étudiera le plongement canonique de notre corps de nombres.

Commençons par regarder la propriété de finitude.

Proposition 1.5.6 (Finitude si tous les plongements sont bornés)**.** *Soient K un corps de nombres et σ_1, ..., σ_n ses plongements canoniques. Soit $M > 0$.*

$$\textit{L'ensemble } \left\{ x \in \mathcal{O}_K \,\middle|\, \forall i \in [\![1, n]\!] \, |\sigma_i(x)| \leq M \right\} \textit{ est fini.}$$

Démonstration. Soit $x \in \mathcal{O}_K$ tel que $\forall i \in [\![1, n]\!] \, |\sigma_i(x)| \leq M$. D'après la proposition 1.4.6, on a

$$\chi_x = (\mu_x)^r,$$

où $r = [K : \mathbb{Q}(x)]$. Mais on sait aussi par la proposition 1.5.5 que

$$\chi_x = \prod_{\sigma \in \Sigma(K)} (X - \sigma(x)) = \prod_{i=1}^{n} (X - \sigma_i(x)).$$

Finalement,

$$(\mu_x)^r = \prod_{i=1}^{n} (X - \sigma_i(x)).$$

En particulier, les racines de μ_x sont exactement les $\sigma_i(x)$, éventuellement répétées. Alors on sait que tous les coefficients de μ_x s'expriment comme des fonctions symétriques des $\sigma_i(x)$ (relations de Viète). Comme tous les $\sigma_i(x)$ sont bornés par M, on en déduit que tous les coefficients de μ_x sont aussi bornés, et ce indépendamment de x, disons par M'.

Mais l'ensemble $\{x \in \mathcal{O}_K \,|\, \text{tous les coefficients de } \mu_x \text{ sont bornés par } M'\}$ est fini puisque pour tout $x \in \mathcal{O}_K$, μ_x est de degré au plus n à coefficients entiers, ce qui laisse un nombre fini de possibilités. On a donc un nombre fini de polynômes minimaux, et ainsi un nombre fini de x qui en sont racine.

Finalement, on obtient bien que $\{x \in \mathcal{O}_K \,|\, \forall i \in [\![1, n]\!] \, |\sigma_i(x)| \leq M\}$ est fini.

□

Enfin, on relie les plongements à la trace.

Proposition 1.5.7. *Soient K un corps de nombres et $x \in K$. On a*

$$\mathrm{Tr}(x) = \sum_{\sigma \in \Sigma(K)} \sigma(x).$$

Démonstration. Il s'agit d'une simple application de la formule de 1.5.5. On rappelle en effet que

$$\chi_x = \prod_{\sigma \in \Sigma(K)} (X - \sigma(x)).$$

Mais la trace de m_x est l'opposé du coefficient en X^{n-1} de son polynôme caractéristique, donc de χ_x. Ainsi,

$$\mathrm{Tr}(x) = \sum_{\sigma \in \Sigma(K)} \sigma(x).$$

□

On en déduit bien le corollaire annoncé.

Corollaire 1.5.2. *Soit K un corps de nombres. Soient $(e_1, ..., e_n)$ une $\mathbb{Q}$-base de K, et $\sigma_1, ..., \sigma_n$ les n plongements de K dans $\mathbb{C}$. Alors,*

$$disc(e_1, ..., e_n) = \det\left((\mathrm{Tr}(e_i e_j))_{1 \leq i,j \leq n}\right) = \det\left((\sigma_i(e_j))_{1 \leq i,j \leq n}\right)^2.$$

Démonstration. C'est une application directe du fait que $\mathrm{Tr}(x) = \sum_{\sigma \in \Sigma(K)} \sigma(x)$. En effet, soient $i, j \in [\![1, n]\!]$. On a

$$\mathrm{Tr}(e_i e_j) = \sum_{k=1}^{n} \sigma_k(e_i e_j) = \sum_{k=1}^{n} \sigma_k(e_i)\sigma_k(e_j).$$

On reconnaît l'expression du produit matriciel $(\sigma_i(e_j))^T_{1 \leq i,j \leq n} (\sigma_i(e_j))_{1 \leq i,j \leq n}$.
En passant au déterminant, le facteur carré apparaît et on a bien

$$disc(e_1, ..., e_n) = \det\left((\sigma_i(e_j))_{1 \leq i,j \leq n}\right)^2.$$

□

En combinant ce corollaire avec la propriété 1.4.3, on obtient que $(e_1, ..., e_n)$ est une base de K si et seulement si

$$\det\left((\sigma_i(e_j))_{1 \leq i,j \leq n}\right) \neq 0.$$

2
GÉOMÉTRIE DES NOMBRES

Maintenant que les outils fondamentaux de l'étude des corps des nombres et de leur anneau des entiers ont été introduits, on va pouvoir énoncer certaines propriétés sur leurs structures. Pour l'instant, nous avons vu que pour un corps de nombres K donné, $\mathcal{O}_K$ était un anneau qui contenait $\mathbb{Z}$. Mais on n'en sait à ce stade pas beaucoup plus. Dans ce chapitre, on se propose de montrer le théorème suivant, formulé et démontré par Richard Dedekind (1831-1916).

Théorème 5 (Dedekind)**.** *Soit K un corps de nombres. Le groupe additif de $\mathcal{O}_K$ admet une $\mathbb{Z}$-base à $n = [K : \mathbb{Q}]$ éléments. Autrement dit, $\mathcal{O}_K \cong \mathbb{Z}^n$ comme groupe abélien.*

L'approche adoptée ici est *géométrique*. L'idée va être de géométriser $\mathcal{O}_K$ en le plongeant dans $\mathbb{R}^n$ à travers un morphisme de groupes injectif, avant d'observer que l'image de ce morphisme est isomorphe à $\mathbb{Z}^n$. On procède donc en deux temps.

Dans la partie 2.1, on s'intéresse aux sous-groupes discrets de $\mathbb{R}^n$, appelés *sous-réseaux de* $\mathbb{R}^n$. Le point-clé est de démontrer que pour G un sous-groupe additif de $\mathbb{R}^n$, on dispose de deux définitions équivalentes de la notion de sous-réseau :

(i) G est un sous-groupe discret de $\mathbb{R}^n$.

(ii) G admet une $\mathbb{Z}$-base qui est libre sur $\mathbb{R}$. Autrement dit, le rang de G comme $\mathbb{Z}$-module est égal à la dimension de l'espace vectoriel qu'il engendre sur $\mathbb{R}$. Si cette dimension est n, G est appelé *réseau* de $\mathbb{R}^n$.

En particulier, la première définition permet une caractérisation géométrique des réseaux. On montre qu'un groupe G de $\mathbb{R}^n$ est un réseau de $\mathbb{R}^n$ si et seulement si

(i) G n'a pas de point d'accumulation dans $\mathbb{R}^n$, ce qui correspond au fait qu'il est discret,

(ii) Le volume fondamental de G est non nul, autrement G n'est pas « écrasé » et engendre tout $\mathbb{R}^n$ comme $\mathbb{R}$-espace vectoriel.

La partie 2.1 s'achève en démontrant le théorème de Minkowski, qui est utilisé dans les chapitres 3 et 4.

La partie 2.2 applique ces résultats à $\mathcal{O}_K$, et procède en deux temps.

- $\mathcal{O}_K$ est a priori un sous-groupe de $\mathbb{C}$, dans lequel il n'a aucune raison d'être discret. On s'interroge donc d'abord sur la nature du morphisme de plongement à considérer. Une étude sur un exemple indique que le *plongement canonique* σ, construit à partir des plongements de corps de nombres vus à la partie 1.5, est un bon choix. Ce plongement induit un morphisme de groupes injectif $\sigma : \mathcal{O}_K \to \mathbb{R}^n$ où $n = [K : \mathbb{Q}]$.
- On vérifie alors que $\sigma(\mathcal{O}_K)$ est bien un réseau de $\mathbb{R}^n$.
    - Son caractère discret est donné par la proposition 2.2.5 : les ensembles de la forme $\left\{x \in \mathcal{O}_K \,\middle|\, \forall i \in [\![1, n]\!]\, |\sigma_i(x)| \leq M\right\}$ sont finis.

- Le volume fondamental du réseau correspond à un facteur près au discriminant d'une famille bien choisie, et la proposition 1.5.2 indique qu'il est non nul. En particulier, on en déduit que la valeur absolue du discriminant est indépendante du choix de la $\mathbb{Z}$-base : c'est un invariant de $\mathcal{O}_K$.

Ces deux éléments permettent de conclure que $\mathcal{O}_K \cong \mathbb{Z}^n$ comme groupe abélien.

Enfin, on donne dans la partie 2.2.2 un premier résultat issu de la géométrisation de $\mathcal{O}_K$ qui annonce les grands théorèmes du chapitre 3. En effet, on s'est interrogé au premier chapitre sur les propriétés de finitude de la norme. Par exemple, les ensembles $\left\{x \in \mathcal{O}_K \,\middle|\, N(x) \leq M\right\}$ sont-ils finis ? On dispose à ce stade de deux éléments de réponse.

- Il n'est pas possible de faire « s'effondrer » tous les $\sigma_i(x)$ en même temps puisque $\sigma(\mathcal{O}_K)$ est un réseau : si c'était le cas on aurait un point d'accumulation en 0. En combinant cela avec le fait que $N(x) \in \mathbb{Z}$ si $x \in \mathcal{O}_K$ et que la norme est le produit des plongements, on a envie d'affirmer qu'à $a \in \mathbb{Z}$ donné on n'a qu'un nombre fini de $x \in \mathcal{O}_K$ tels que $N(x) = a$.
- Néanmoins, on sait que les unités de $\mathcal{O}_K$ sont de norme ± 1. Or on ne sait rien du groupe $\mathcal{O}_K^\times$: s'il est infini il n'y a aucune chance que $\left\{x \in \mathcal{O}_K \,\middle|\, N(x) \leq M\right\}$ soit fini.

La seconde remarque invite à s'abstraire des unités en considérant les idéaux principaux engendrés par les éléments de $\mathcal{O}_K$. En effet, $x\mathcal{O}_K = y\mathcal{O}_K \iff \frac{x}{y} \in \mathcal{O}_K^\times$. Dès lors, une utilisation subtile de la première remarque permet de conclure que $\left\{x\mathcal{O}_K \,\middle|\, x \in \mathcal{O}_K,\, |N(x)| \leq M\right\}$ est fini : c'est la proposition 2.2.8.

Ainsi, on voit apparaître l'intuition qui sera au cœur du troisième chapitre : les idéaux de $\mathcal{O}_K$ sont des objets simples car ils permettent d'éviter d'affronter le groupe $\mathcal{O}_K^\times$, mais suffisamment complexes pour donner des informations sur la structure de $\mathcal{O}_K$, car géométriquement ils sont des sous-réseaux du réseau induit par $\mathcal{O}_K$.

2.1 Réseaux

2.1.1 • Qu'est-ce qu'un réseau ?

Commençons par présenter quelques résultats fondamentaux de la théorie des réseaux. On reprend ici les résultats exposés dans le cours de Daniel Perrin [31].

Définition 2.1.1 (Réseaux et sous-réseaux)**.** Soient $n \in \mathbb{N}^*$, L un sous-groupe additif de $\mathbb{R}^n$ et $r \in \mathbb{N}^*$. On dit que L est un sous-réseau de $\mathbb{R}^n$ s'il existe une famille libre $(e_1, ..., e_r)$ de vecteurs de L qui est une $\mathbb{Z}$-base de L, c'est-à-dire

$$L = \left\{ \sum_{i=1}^{r} \lambda_i e_i \,\middle|\, \lambda_1, ..., \lambda_r \in \mathbb{Z} \right\}.$$

On appelle alors r le rang de L, noté $\mathrm{rg}(L)$. Si $\mathrm{rg}(L) = n$, L est appelé réseau de $\mathbb{R}^n$.

En termes de théorie des groupes, un réseau est un groupe abélien libre de type fini. Mais la réciproque est fausse, tout groupe abélien libre de type fini de $\mathbb{R}^n$ n'est pas un réseau, puisqu'on demande à avoir une $\mathbb{Z}$-base libre sur $\mathbb{R}$.

Exemple 2.1.1. Si on regarde $\mathbb{Q}[\sqrt{2}]$ dans $\mathbb{R}$, il s'agit bien d'un groupe abélien libre de type fini (il est isomorphe à $\mathbb{Z}^2$) mais ce n'est pas un réseau car $(1, \sqrt{2})$ n'est pas libre sur $\mathbb{R}$.

Avec la définition précédente, on peut se convaincre rapidement que le rang d'un réseau est bien défini. En effet, si on a une $\mathbb{Z}$-base $(e_1, ..., e_r)$ d'un sous-réseau L, alors $L \subset \text{Vect}(e_1, ..., e_r)$. Mais si on a une seconde $\mathbb{Z}$-base $(f_1, ..., f_r')$ de L, alors $\text{Vect}(f_1, ..., f_r') \subset \text{Vect}(e_1, ..., e_r)$. Les familles étant libres, $r' \leq r$ et par symétrie $r = r'$.

En particulier, le changement de base dans un réseau correspond à multiplication par une matrice de déterminant ± 1.

Proposition 2.1.1. *Soient $\beta_1 = (e_1, ..., e_n)$ et $\beta_2 = (f_1, ..., f_n)$ deux bases de $\mathbb{R}^n$. Soit L un réseau de R^n dont on suppose que β_1 est une $\mathbb{Z}$-base. Alors,*

β_2 est une $\mathbb{Z}$-base de L si et seulement si la matrice de passage P de β_1 vers β_2 est dans $GL_n(\mathbb{Z})$, c'est-à-dire à coefficients entiers et de déterminant ± 1.

Démonstration.

- Supposons que β_2 est une $\mathbb{Z}$-base de L. En particulier les f_j sont dans L, et peuvent s'écrire comme des combinaisons linéaires sur $\mathbb{Z}$ des e_i. Ainsi P est à coefficients entiers. Mais réciproquement β_1 est une $\mathbb{Z}$-base de L, donc P^{-1} est aussi à coefficients entiers. Mais alors $\det(P) \in \mathbb{Z}$, $\det(P^{-1}) = \det(P)^{-1} \in \mathbb{Z}$ donc $\det(P) = \pm 1$. Ainsi $P \in GL_n(\mathbb{Z})$.
- Réciproquement, si $P \in GL_n(\mathbb{Z})$, P est à coefficients entiers et P^{-1} aussi. Donc les e_i s'écrivent comme des $\mathbb{Z}$ combinaisons linéaires des f_j et réciproquement. En notant M le réseau engendré par les f_j, on a donc $L \subset M$ et $M \subset L$, donc $L = M$. Cela revient à dire que β_2 est une $\mathbb{Z}$-base de L.

□

Cette proposition permet de définir sans ambiguïté la notion de volume d'un réseau.

Définition 2.1.2 (Volume d'un réseau)**.** Soient L un réseau de $\mathbb{R}^n$ et $(e_1, ..., e_n)$ une $\mathbb{Z}$-base de L. On appelle volume de L, noté $vol(L)$, la valeur absolue du déterminant de $(e_1, ..., e_n)$ contre la base canonique β :

$$vol(L) = |\det_{\beta}(e_1, ..., e_n)|.$$

Puisque le changement de $\mathbb{Z}$-base se fait en multipliant le déterminant par ± 1, la notion de volume est bien définie. On peut aussi l'appréhender de la façon suivante.

Définition 2.1.3 (Domaine fondamental)**.** Soit L un réseau de $\mathbb{R}^n$. Soit $(e_1, ..., e_n)$ une $\mathbb{Z}$-base de L. On appelle domaine fondamental de L pour la base $(e_1, ..., e_n)$ le parallélotope

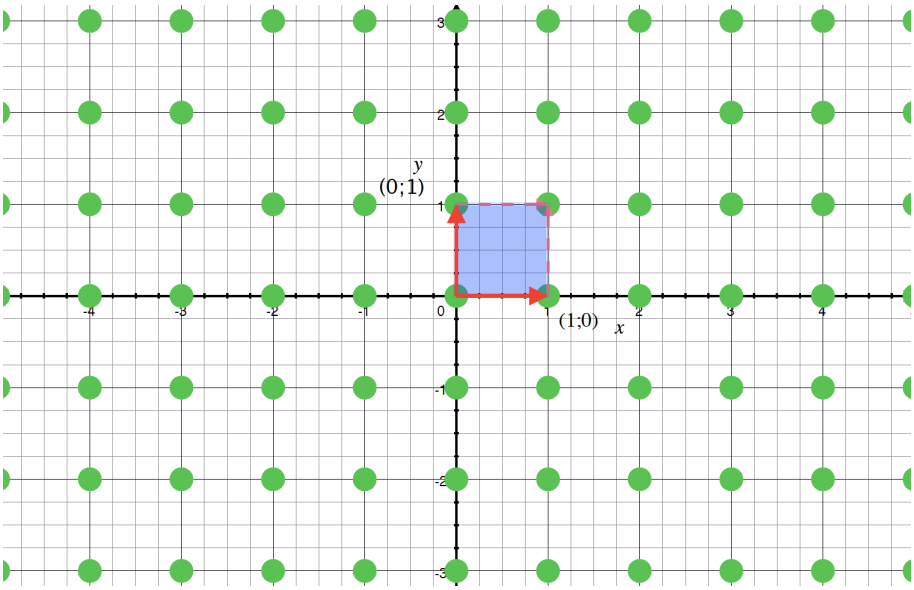
$$D = \left\{ \sum_{i=1}^{n} \lambda_i e_i \,\middle|\, 0 \leq \lambda_i < 1 \right\}.$$

On retrouve alors $vol(L) = \mu(D)$ où μ est la mesure de Lebesgue.

Exemple 2.1.2 (« Volume » d'un sous-réseau)**.** On fera attention au fait que la définition précédente n'est valide que pour un réseau de $\mathbb{R}^n$, et pas un sous-réseau de rang $r < n$. Dans ce cas, les domaines fondamentaux sont inclus dans un espace vectoriel de dimension r : leur volume par la mesure de Lebesgue est nul !

Regardons comment toutes propriétés s'expriment sur un exemple.

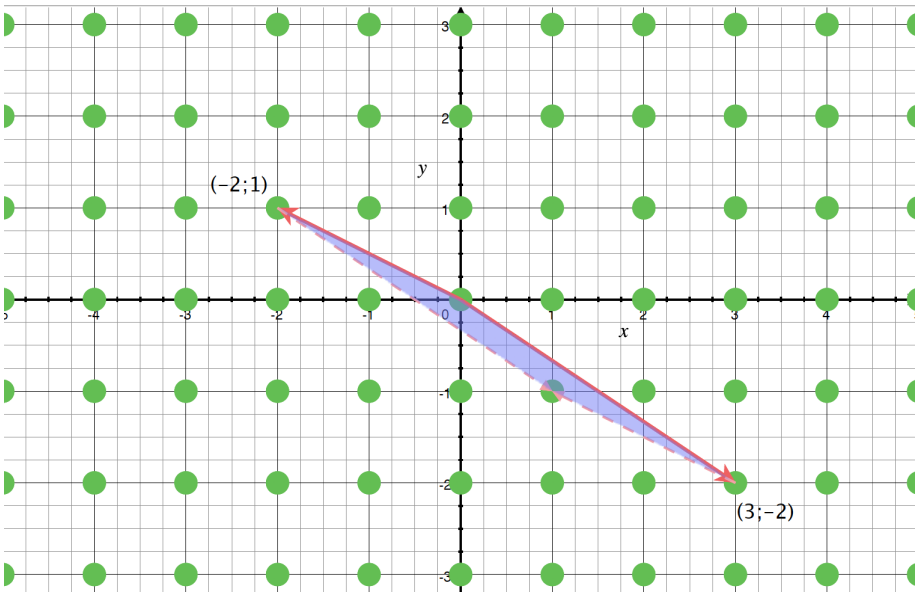
Exemple 2.1.3 (Deux bases pour un même réseau)**.** Afin de donner l'intuition de l'énoncé précédent sur le domaine fondamental, prenons le cas du réseau le plus simple : $\mathbb{Z}^2$. Une base de ce réseau est donnée par la base canonique $((1, 0), (0, 1))$, auquel cas le domaine fondamental est simplement le carré de côté 1 issu de l'origine.



Que signifie un changement de base dans ce cas ? On cherche une matrice $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ à coefficients entiers dont le déterminant dans la base canonique soit ± 1, c'est-à-dire $ad - bc = \pm 1$.

Une façon simple de construire une telle matrice est d'utiliser le théorème de Bézout, en

prenant a et b premiers entre eux. Par exemple pour $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 3 \\ -2 \end{pmatrix}$ et $\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} -2 \\ 1 \end{pmatrix}$, on obtient à nouveau le réseau $\mathbb{Z}^2$.



Le domaine fondamental obtenu est alors plus étiré, mais son aire est toujours 1.

On se propose maintenant de donner une seconde définition à la notion de réseau, qui s'avère beaucoup plus commode à manipuler. L'exemple suivant indique clairement que les points réseaux ne peuvent pas s'accumuler : cela correspond à la notion d'ensemble discret, que l'on définit de suite. Il s'agit donc d'une approche topologique. Dans la suite, $\mathbb{R}^n$ sera muni de la norme euclidienne (mais cela n'a pas beaucoup d'importance car toutes les normes sont équivalentes).

Définition 2.1.4 (Ensemble discret)**.** Un sous-ensemble A de $\mathbb{R}^n$ est dit discret si pour tout $a \in A$ il existe un ouvert Ω de $\mathbb{R}^n$ tel que $A \cap \Omega = \{a\}$.

De façon équivalente, A est dit discret si toute suite (a_n) de A qui converge vers $a \in A$ dans $\mathbb{R}^n$ est constante à partir d'un certain rang.

La notion d'ensemble discret possède une caractérisation très simple dans le cas des fermés.

Proposition 2.1.2. *Soit A une partie de $\mathbb{R}^n$. S'équivalent*

(i) A est fermé et discret.

(ii) Pour toute partie bornée B de $\mathbb{R}^n$, $A \cap B$ est fini.

Démonstration.

- $(i) \implies (ii)$.

Supposons (i). Par l'absurde, supposons qu'on a B une partie bornée de $\mathbb{R}^n$ avec $A \cap B$ infini. Mais $\overline{B}$ est compact, et $A \cap \overline{B}$ est aussi infini.
Ainsi $\overline{B}$ contient une suite (a_n) d'éléments distincts de A, qui admet une valeur d'adhérence a par le théorème de Bolzano-Weierstrass.
Mais A est fermé, donc $a \in A$. Enfin, A est discret, donc la sous-suite $(a_{\phi(n)})$ qui converge vers a est constante à partir d'un certain rang : absurde.
Ainsi, $A \cap B$ est fini.

- $(ii) \implies (i)$.
  Réciproquement, supposons (ii). Soit $a \in A$. La boule $B(a,1)$ de $\mathbb{R}^n$ est bornée, donc $A \cap B(a,1)$ est finie. Mais alors en réduisant son rayon, on obtient $\epsilon > 0$ tel que
  $$A \cap B(a,\epsilon) = \{a\}.$$
  Ainsi, A est discret.

□

Exemple 2.1.4 (Contre-exemple)**.** Le caractère fermé de A joue un rôle essentiel dans la proposition précédente, car sinon on peut fabriquer des points d'accumulation.
Par exemple, le sous-ensemble $A = \left\{ \frac{1}{n} \,\middle|\, n \in \mathbb{N}^* \right\}$ de $\mathbb{R}$ est bien discret, puisqu'on peut isoler chacun des $\frac{1}{n}$ dans un voisinage ouvert, mais pas fermé puisque $\frac{1}{n} \to 0 \notin A$. On prenant $B = [-1,1]$, on a $A \cap B = A$ infini.

Dans le cas spécifique des sous-groupes additifs, le caractère fermé est en fait superflu grâce au lemme suivant.

Proposition 2.1.3. *Soit L un sous-groupe additif de $\mathbb{R}^n$. Si L est discret, alors L est fermé.*

Démonstration. Soit (l_n) une suite de L qui converge vers l dans $\mathbb{R}^n$. On veut $l \in L$.
La suite $(l_n - l_{n+1})_{n\in\mathbb{N}}$ converge vers 0. Or L est un sous-groupe, donc $\forall n \in \mathbb{N}\,(l_n - l_{n+1}) \in L$ et $0 \in L$. On a donc une suite de L qui converge dans L.
Mais L est discret, donc la suite $(l_n - l_{n+1})$ est constante à partir d'un certain rang N égale à 0. Ainsi, $\forall n \geq N\, l_n = l_{n+1}$.
En particulier, la limite de la suite constante (l_n) est dans L, donc $l \in L$ et L est fermé. □

On a donc une nouvelle version de la proposition 2.1.2.

Proposition 2.1.4. *Soit L un sous-groupe de $\mathbb{R}^n$. S'équivalent*

(i) L est discret.

(ii) Pour toute partie bornée B de $\mathbb{R}^n$, $L \cap B$ est fini.

Cette proposition va nous permettre de démontrer le théorème fondamental suivant, qui donne une nouvelle définition de la notion de sous-réseau.

Proposition 2.1.5 (Théorème fondamental)**.** *Soit L un sous-groupe de $\mathbb{R}^n$. S'équivalent*

(i) L est discret.

(ii) L est un sous-réseau de $\mathbb{R}^n$.

Démonstration.

- $(ii) \implies (i)$.
  On commence par le sens facile. Soit $(e_1, ..., e_r)$ une $\mathbb{Z}$-base de L, c'est-à-dire $L = \mathrm{Vect}_{\mathbb{Z}}(e_1, ..., e_r)$.
  Soit $x = \sum_{i=1}^{r} x_i e_i \in L$. Posons

$$B = \left\{ y = \sum_{i=1}^{r} y_i e_i \,\middle|\, y_i \in \left]x_i - \frac{1}{3}, x_1 + \frac{1}{3}\right[\right\}.$$

  B est un ouvert de $\mathbb{R}^n$, et $L \cap B = \{x\}$.
  En effet, soit $y = \sum_{i=1}^{r} y_i e_i \in L \cap B$ (on dispose bien d'une telle écriture puisque $(e_1, ..., e_r)$ est génératrice). Soit $i \in [\![1, r]\!]$. Comme $x_i \in \mathbb{Z}$, et que

$$y_i \in \left]x_i - \frac{1}{3}, x_i + \frac{1}{3}\right[\cap \mathbb{Z},$$

  on a $y_i = x_i$. On en déduit que $y = x$.

- $(i) \implies (ii)$.
  La réciproque est plus complexe et se montre par récurrence sur n la dimension de l'espace ambiant $\mathbb{R}^n$.

  - **Initialisation**
    Soit L un sous-groupe discret de $\mathbb{R}$.

    — Si $L = \{0\}$, alors L est un sous-réseau de $\mathbb{R}$.
    Sinon, soit $r = \inf\{x \in L \,|\, x > 0\}$, bien défini car cet ensemble est non vide.

    — Supposons **par l'absurde** que $r = 0$.
    On dispose alors d'une sous-suite $(r_n) \in L_+^{\mathbb{N}}$ d'éléments strictement positifs *distincts* de L qui converge vers 0.
    Autrement dit, $L \cap [0, 1]$ est infini, ce qui est **absurde** car L est discret.
    On en déduit que $r > 0$.

    — On voit alors que $L = r\mathbb{Z}$. En effet,

    - D'une part, comme $r \in L$ qui est un groupe, $r\mathbb{Z} \subset L$.
    - D'autre part, soit **par l'absurde** $x = \lambda r \in L \setminus r\mathbb{Z}$, i.e. tel que $\lambda \notin \mathbb{Z}$.
      On a $x = \lfloor \lambda \rfloor r + (\lambda - \lfloor \lambda \rfloor) r$, et comme $r \in L$, on a encore $(\lambda - \lfloor \lambda \rfloor) r \in L$.
      Mais $(\lambda - \lfloor \lambda \rfloor) r \in]0, r[$: **absurde** d'après la minimalité de r.

    Ainsi $L = r\mathbb{Z}$: L est bien un sous-réseau de $\mathbb{R}$. L'initialisation est vérifiée.

- **Hérédité**

  Supposons que pour $n \in \mathbb{N}^*$, tous les sous-groupes discrets de $\mathbb{R}^n$ sont des sous-réseaux de $\mathbb{R}^n$.

  Soit L un sous-groupe discret de $\mathbb{R}^{n+1}$.

  — On élimine le cas évident $L = \{0\}$.

  — Par un raisonnement analogue au cas $n = 1$, on dispose de $a \in L \setminus 0$ de norme minimale.

  — Soient F un supplémentaire de $\mathrm{Vect}(a)$ et p le projecteur sur F parallèlement à $\mathrm{Vect}(a)$.

  Vérifions que $p(L)$ est un sous-réseau de F : on va s'en servir pour construire une $\mathbb{Z}$-base de L.

  - $p(L)$ est bien un sous-groupe de F puisque L est un sous-groupe.
  - Pour montrer que $p(L)$ est discret, on va utiliser la caractérisation de la proposition2.1.4.

    Observons d'abord le fait suivant :

    Si $y \in p(L)$, il existe $x \in L$ tel que $p(x) = y$ et $x = \lambda a + y$ avec $0 \leq \lambda < 1$.

    Ce résultat est simple à démontrer : si $y \in p(L)$, $y = p(x)$ où $x \in L$. Alors $x = \mu a + y$ puisque p est la projection sur F parallèlement à $\mathrm{Vect}(a)$. Mais $\mathbb{Z}a \subset L$ car L est un groupe, donc $x' = x - \lfloor \mu \rfloor a = (\mu - \lfloor \mu \rfloor)a + y = \lambda a + y \in L$, et $p(x) = y$. Comme $0 \leq \lambda < 1$, x convient.

    Dès lors, soit B une partie bornée de F, $B \subset B(0, R)$. Soit $y \in B \cap p(L)$, $y = p(x)$ où $x = \lambda a + y$ avec la convention précédente. Alors $||x|| \leq ||a|| + ||y|| \leq ||a|| + R$. Donc $|B \cap p(L)| \leq |B(0, R + ||a||) \cap L|$, qui est fini car L est discret. Donc $B \cap p(L)$ est fini. Comme $p(L)$ est un sous-groupe d'un espace de dimension n, l'hypothèse de récurrence permet de conclure que $p(L)$ est un sous-réseau.

  — Soit maintenant $(f_1, ..., f_r)$ une $\mathbb{Z}$-base de $p(L)$, avec $\forall i \, f_i = p(e_i)$ où $e_i \in L$. Montrons que $(e_1, ..., e_r, a)$ est une $\mathbb{Z}$-base de L.

  - **Liberté**

    Soit $\sum_{i=1}^{r}(x_i e_i) + \lambda a = 0$.

    En appliquant p, on obtient $\sum_{i=1}^{r}(x_i f_i) = 0$ et $x_1 = ... = x_r = 0$.

    Donc $\lambda a = 0$ et $\lambda = 0$: on a la liberté.

  - **Caractère générateur**

    Soit $x \in L$. On peut déjà écrire $x = p(x) + \lambda a$ où $y \in F$, $\lambda \in \mathbb{R}$. Donc $p(x) = \sum_{i=1}^{r} x_i f_i = \sum_{i=1}^{r}(x_i e_i) - a \sum_{i=1}^{r}(x_i \lambda_i)$ où $x_1, ..., x_r \in \mathbb{Z}$.

    Ainsi,

    $$x = \sum_{i=1}^{r}(x_i e_i) + a\left(\lambda - \sum_{i=1}^{r}(x_i \lambda_i)\right) = \sum_{i=1}^{r}(x_i e_i) - \mu a.$$

    Mais

(i) $x \in L$.

(ii) $\sum_{i=1}^{r}(x_i e_i) \in L$ car les x_i sont entiers.

(iii) $a\lfloor\mu\rfloor \in L$.

Finalement, $(\mu - \lfloor\mu\rfloor)a \in L$.

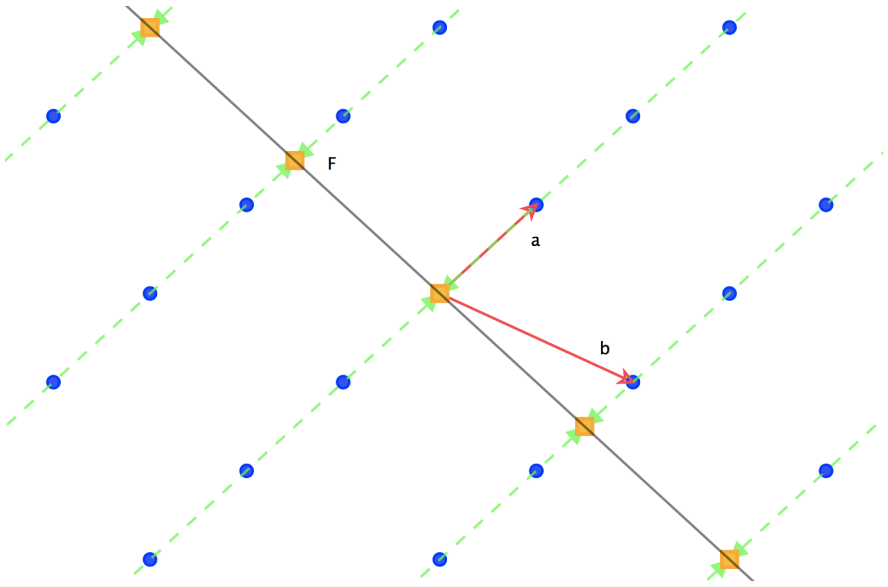
Comme on a choisi a de norme minimale, cela donne $\mu - \lfloor\mu\rfloor = 0$ et $\mu \in \mathbb{Z}$.

Ainsi $x \in \mathrm{Vect}_{\mathbb{Z}}(e_1, ..., e_r, a)$: la famille est génératrice.

On a donc bien une $\mathbb{Z}$-base de L, qui est un sous-réseau de $\mathbb{R}^{n+1}$: l'hypothèse de récurrence est vérifiée.

□

Exemple 2.1.5. On se propose ici de donner une représentation graphique de l'argument fondamental de la preuve : si on prend $a \in L/0$ de norme minimale, F un supplémentaire de $\mathrm{Vect}(a)$ dans $\mathbb{R}^n$ et p la projection sur F parallèlement à $\mathrm{Vect}(a)$, alors $p(L)$ est un sous-réseau de F. C'est exactement ce que montre le dessin suivant :



Sur ce dessin :

- On se place dans $\mathbb{R}^2$. Le réseau L correspond aux boules bleues, et les vecteurs a et b (les flèches rouges) en forment une $\mathbb{Z}$-base.
- Un supplémentaire de $\mathrm{Vect}(a)$ dans $\mathbb{R}^2$ est donné par la droite noire.
- La projection p est symbolisée par des flèches en pointillés vertes.
- Le nouveau réseau obtenu correspond aux carrés oranges.

On voit bien ici qu'on a obtenu un réseau de la droite. De plus, comme annoncé dans la preuve, $p(b)$ en est une $\mathbb{Z}$-base.

En résumé, on retiendra la propriété suivante, qui découle des propositions 2.1.4 et 2.1.5.

Proposition 2.1.6 (Caractérisation des sous-réseaux de $\mathbb{R}^n$)**.** *Soit L un sous-groupe de $\mathbb{R}^n$. S'équivalent*

(i) Pour toute partie bornée B de $\mathbb{R}^n$, $L \cap B$ est fini.

(ii) L est un sous-réseau de $\mathbb{R}^n$.

2.1.2 • Théorème de Minkowski

Maintenant qu'on a donné plusieurs définitions équivalentes des sous-réseaux, il est temps de s'attaquer à des théorèmes qui donnent une idée de la « densité » d'un réseau. Une question naturelle qu'on se pose est : étant donnés un réseau L et un sous-ensemble A de $\mathbb{R}^n$, quelles sont des conditions suffisantes pour que A contienne un élément de L ? C'est exactement à cette question que répond le théorème de Minkowski.

Dans la suite, μ désignera la mesure de Lebesgue. Si on note $\mathcal{B}(\mathbb{R}^n)$ la tribu borélienne de $\mathbb{R}^n$, alors on a les propriétés suivantes.

(i) μ est σ-additive : pour tout suite $(A_n)_n$ de $\mathcal{B}(\mathbb{R}^n)$ telle que les A_n sont deux-à-deux disjoints, $\mu\left(\bigcup_{n\geq 0} A_n\right) = \sum_{n\geq 0} \mu(A_n)$.

(ii) μ est invariante par translation : pour $A \in \mathcal{B}(\mathbb{R}^n)$ et $x \in \mathbb{R}^n$, $\mu(x + A) = \mu(A)$.

(iii) μ est homogène : pour $A \in \mathcal{B}(\mathbb{R}^n)$ et $\lambda \in \mathbb{R}$, $\mu(\lambda A) = \lambda^n \mu(A)$.

Enfin, pour L un réseau de $\mathbb{R}^n$, rappelons que $vol(L)$ est le volume d'un domaine fondamental de L : $vol(L) = \mu(D)$.

Remarquons d'emblée le fait suivant.

Proposition 2.1.7. *Soient L un réseau de $\mathbb{R}^n$ et D un domaine fondamental de L. Alors,*

$$\mathbb{R}^n = \bigcup_{a \in L} (a + D).$$

De plus, les ensembles $(a + D)$ sont disjoints.

Démonstration. Notons $(e_1, ..., e_n)$ la $\mathbb{Z}$-base de L dont est issue D. On a

$$D = \left\{ \sum_{i=1}^{n} \lambda_i e_i \,\middle|\, 0 \leq \lambda_i < 1 \right\}.$$

- L'inclusion $\bigcup_{a\in L}(a + D) \subset \mathbb{R}^n$ est automatique.
- Réciproquement, $(e_1, ..., e_n)$ est une famille libre de $\mathbb{R}^n$, donc est une base de $\mathbb{R}^n$. Soit $x \in \mathbb{R}^n$. On écrit $x = \sum_{i=0}^{n} x_i e_i$, et on peut donc écrire

$$x = \sum_{i=0}^{n} (\lfloor x_i \rfloor e_i) + \sum_{i=0}^{n} ((x_i - \lfloor x_i \rfloor) e_i).$$

Mais $\sum_{i=0}^{n}(\lfloor x_i \rfloor e_i) \in L$, et $\sum_{i=0}^{n}((x_i - \lfloor x_i \rfloor)e_i) \in D$ puisque les $(x_i - \lfloor x_i \rfloor)$ sont dans $[0, 1[$.

Ainsi $x \in \bigcup_{a\in L}(a+D)$, d'où finalement

$$\bigcup_{a\in L}(a+D) = \mathbb{R}^n.$$

- Enfin, pour $a, b \in L$, si on a $x \in (a+D)\cap(b+D)$, on peut écrire

$$\begin{aligned} x &= \left(\sum_{i=1}^{n} a_i e_i\right) + \left(\sum_{i=1}^{n} d_i e_i\right) \\ &= \left(\sum_{i=1}^{n} b_i e_i\right) + \left(\sum_{i=1}^{n} d'_i e_i\right) \end{aligned}$$

où les a_i, b_i sont dans $\mathbb{Z}$, les d_i, d'_i dans $[0,1[$. Mais par liberté de $(e_1, ..., e_n)$, puis en passant à la partie entière, on obtient que

$$\forall i \in [\![1,n]\!]\ a_i + d_i = b_i + d'_i, \text{ donc } \forall i\ \in [\![1,n]\!] a_i = b_i.$$

Donc $a = b$: les $(a+D)$ sont bien disjoints.

□

On déduit de la proposition précédente le petit lemme suivant.

Proposition 2.1.8 (Lemme de chevauchement)**.** *Soit L un réseau de $\mathbb{R}^n$. Soit A une partie de $\mathbb{R}^n$. On suppose qu'on a $\mu(A) > vol(L)$. Alors il existe $x, y \in A$ avec $x \neq y$ tels que $x - y \in L$.*

Démonstration. Soit D un domaine fondamental. On sait que $\mathbb{R}^n = \bigcup_{a\in L}(a+D)$. En intersectant avec A, cela donne $A = \bigcup_{a\in L}(a+D)\cap A$.
Mais on a vu que les $(a+D)$ étaient disjoints, donc a fortiori les $(a+D)\cap A$ aussi. Par σ-additivité,

$$\mu(A) = \sum_{a\in L} \mu((a+D)\cap A).$$

En utilisant l'invariance par translation,

$$\mu(A) = \sum_{a\in L} \mu(D\cap(-a+A)).$$

Mais $\bigcup_{a\in L}(D\cap(-a+A)) \subset D$. Si on suppose par l'absurde que les $D\cap(-a+A)$ sont disjoints, alors la σ-additivité donne

$$\mu\Big(\bigcup_{a\in L}(D\cap(-a+A))\Big) = \sum_{a\in L}\mu(D\cap(-a+A)),$$

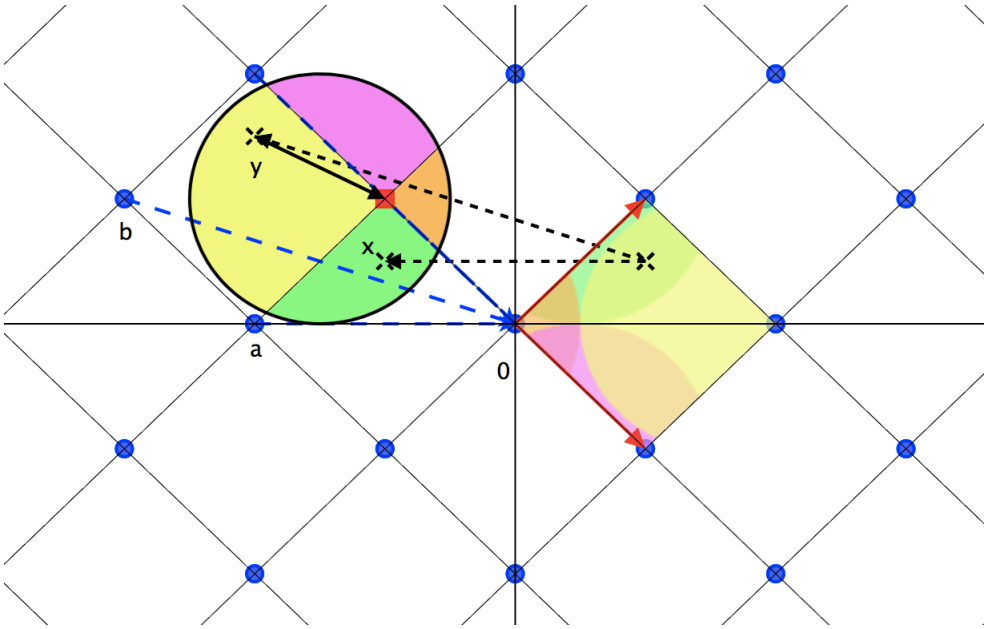
$$\text{d'où } \mu(A) = \sum_{a\in L}\mu(D\cap(-a+A)) = \mu\Big(\bigcup_{a\in L}(D\cap(-a+A))\Big) \leq \mu(D).$$

Or c'est absurde car $\mu(D) = vol(L)$ et on a supposé $\mu(A) > vol(L)$.

Ainsi, il existe a et $b \in L$, $a \neq b$ tels que $D\cap(-a+A)$ et $D\cap(-b+A)$ se rencontrent. Autrement dit, on a x et y dans A avec $-a+x = -b+y$, soit $x - y = a - b \in L$. Et $a \neq b$ donne $x \neq y$: le lemme est démontré. □

Regardons ce qu'il se passe sur des dessins.

Exemple 2.1.6. Ici on regarde le lemme de chevauchement sur un réseau de $\mathbb{R}^2$ et sur un disque A dont l'aire est strictement supérieur au volume fondamental.



La première partie de la preuve effectue un recouvrement de A par des translations du volume fondamental. Ici quatre points sont nécessaires, et on a colorié chacun des $(a+D)\cap A$ d'une couleur différente. Ensuite, on translate ces ensembles à l'origine, ce qui permet de recouvrir des parties du volume fondamental. C'est exactement ce que dit la formule $\bigcup_{a\in L}(D\cap(-a+A))\subset D$. Mais comme on le voit sur le dessin, si on suppose que nos translations $D\cap(-a+A)$ sont disjointes, alors on recouvre strictement plus que D, ce qui est absurde.

On récupère donc un point qui est dans deux translatés disjoints de $(a+D)\cap A$. Autrement dit, on a x et y dans A avec $-a+x=-b+y$, soit $x-y=a-b\in L$. On a pris un exemple de tels points sur le dessin, signalés par des croix noires. Reste alors à faire $x-y$ pour tomber sur le point de L voulu, qui est indiqué par un carré rouge.

On peut dès lors énoncer le théorème de Minkowski qui est une simple reformulation du lemme précédent dans un cas particulier.

Théorème 6 (Théorème de Minkowski)**.** *Soit L un réseau de $\mathbb{R}^n$. Soit A une partie de $\mathbb{R}^n$ convexe et symétrique par rapport à 0. On suppose que $\mu(A)>2^n vol(L)$. Alors il existe $a\in A\cap L$ avec $a\neq 0$*

Démonstration. Soit $(e_1,...,e_n)$ une $\mathbb{Z}$-base de L. Alors $(2e_1,...,2e_n)$ est une $\mathbb{Z}$-base de $2L$, qui est donc un réseau de $\mathbb{R}^n$. De plus, si D est domaine fondamental de L issu de $(e_1,...,e_n)$, alors $2D$ est celui de $2L$ issu de $(2e_1,...,2e_n)$. Par homogénéité,

$$vol(2L)=\mu(2D)=2^n vol(L).$$

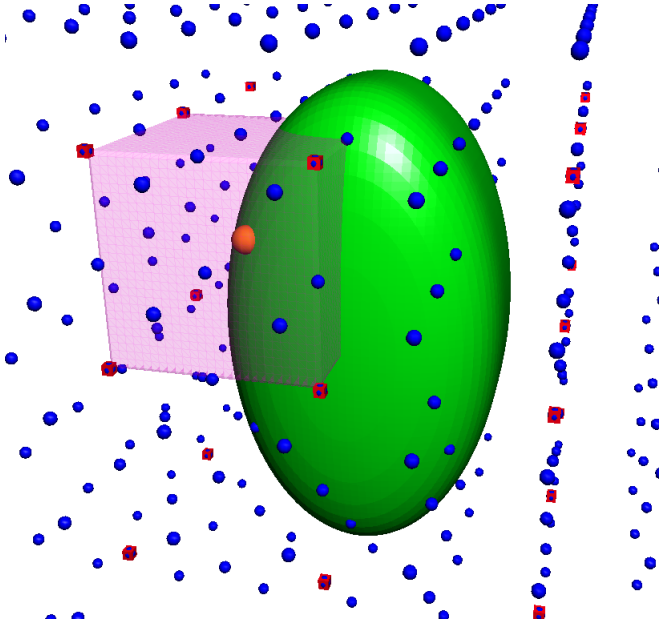
Mais $\mu(A) > 2^n vol(L) = vol(2L)$. Le lemme de chevauchement assure l'existence de $x, y \in A$ distincts avec $x - y \in 2L$. Donc $x - y = 2a$ où $a \in L$. Ainsi $\frac{x-y}{2} = a \in L$.

Or, A est symétrique par rapport à 0, donc $-y \in A$.

De plus A est convexe, donc $\frac{x-y}{2} = \frac{x+(-y)}{2} \in A$.

Finalement, $a = \frac{x-y}{2} \in A \cap L$ et $a \neq 0$, ce qui conclut. □

Exemple 2.1.7. On se propose de montrer le théorème sur un exemple, et cette fois en 3 dimension ! On se donne donc une partie convexe et symétrique A de $\mathbb{R}^3$, ainsi qu'un réseau L. Ici le cube rose correspond directement au volume du réseau $2L$, qu'on a par ailleurs indiqué avec les cubes rouges.



Le théorème de Minkowski s'applique : il existe un point non trivial de L dans A : ici le point orange convient.

2.2 $\mathcal{O}_K$ vu comme un réseau

2.2.1 • Le plongement canonique

On applique maintenant tous nos résultats sur les réseaux à $\mathcal{O}_K$. Bien sûr, $\mathcal{O}_K$ peut toujours être vu comme un sous-groupe de $\mathbb{C} \cong \mathbb{R}^2$. Mais il n'a aucune raison d'y être discret, comme on va le voir dans l'exemple suivant. Il est donc naturel de se demander dans quel $\mathbb{R}^k$ il est sage de plonger $\mathcal{O}_K$ si on veut espérer en faire un réseau, et quel est le morphisme qu'on peut choisir pour le faire. L'exemple suivant permet de voir ce qu'il se passe dans un cas particulier.

Exemple 2.2.1 (Quel espace ambiant considérer ?)**.** Regardons le cas $K = \mathbb{Q}(\sqrt{2})$. On avait vu à l'exemple 1.3.1 que dans ce cas, $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. Une idée naturelle serait de dire que comme $K \subset \mathbb{R}$, on veut considérer $\mathcal{O}_K$ comme un réseau de $\mathbb{R}$.

Néanmoins, $\mathbb{Z}[\sqrt{2}]$ n'est pas discret. On peut par exemple remarquer que $|\sqrt{2}-1| < \frac{1}{2}$, ce qui implique que $(\sqrt{2}-1)^n \to 0$. Mais $\mathbb{Z}[\sqrt{2}]$ est un anneau, donc $\forall n\, (\sqrt{2}-1)^n \in \mathbb{Z}[\sqrt{2}]$ et on a un point d'accumulation en 0.

Ainsi, $\mathbb{R}$ est un espace ambiant trop petit pour regarder $\mathbb{Z}[\sqrt{2}]$ comme un réseau. L'idée est alors de regarder les plongements de $\mathbb{Z}[\sqrt{2}]$. On avait vu qu'il s'agissait des deux plongements réels :

$$\begin{array}{rcl|ccc} \sigma_1 & : & & \mathbb{Q}(\sqrt{2}) & \to & \mathbb{R} \\ & & & a+b\sqrt{2} & \mapsto & a+b\sqrt{2}, \end{array}$$

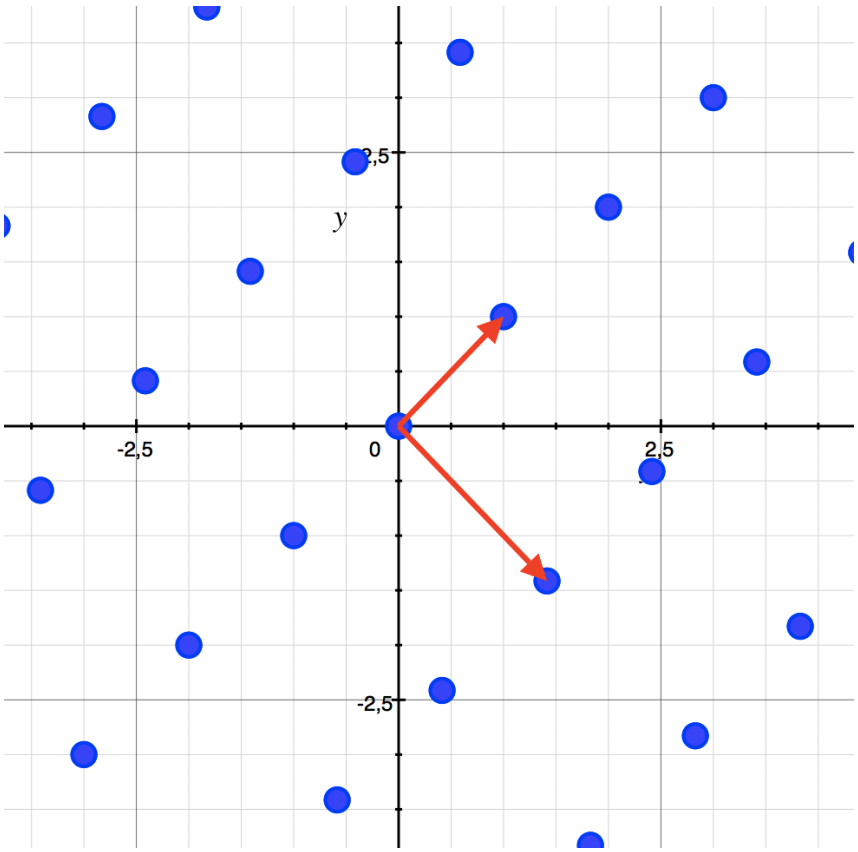
$$\begin{array}{rcl|ccc} \sigma_2 & : & & \mathbb{Q}(\sqrt{2}) & \to & \mathbb{R} \\ & & & a+b\sqrt{2} & \mapsto & a-b\sqrt{2}. \end{array}$$

On définit alors le *plongement canonique* $\sigma = (\sigma_1, \sigma_2)$:

$$\begin{array}{rcl|ccc} \sigma & : & & \mathbb{Q}(\sqrt{2}) & \to & \mathbb{R}^2 \\ & & & a+b\sqrt{2} & \mapsto & (a+b\sqrt{2}, a-b\sqrt{2}). \end{array}$$

Ainsi, $\sigma(\mathcal{O}_K) = \left\{(a+b\sqrt{2}, a-b\sqrt{2}) \,\middle|\, a,b \in \mathbb{Z}\right\} = \mathrm{Vect}_{\mathbb{Z}}\Big((1,1),(\sqrt{2},-\sqrt{2})\Big)$. Or la famille $\Big((1,1),(\sqrt{2},-\sqrt{2})\Big)$ est libre sur $\mathbb{R}$: on vient de montrer qu'il s'agissait d'une $\mathbb{Z}$-base de $\sigma(\mathcal{O}_K)$.

Visuellement on obtient le réseau suivant.



Ainsi $\sigma(\mathcal{O}_K)$ est un réseau de $\mathbb{R}^2$. Enfin, reste à constater que comme tous les σ_i sont injectifs, et que σ est un morphisme de groupes, σ induit un isomorphisme de groupes $\mathcal{O}_K \to \sigma(\mathcal{O}_K)$.

On vient donc d'identifier $\mathcal{O}_K$ à un réseau de $\mathbb{R}^2$ par un isomorphisme ! Nous allons maintenant généraliser cette démarche.

Définition 2.2.1 (Plongement canonique)**.** Soit K un corps de nombres de dimension n. Soient $\sigma_1, ..., \sigma_n$ ses n plongements, que l'on a numéroté de telle sorte que $\sigma_1, ..., \sigma_{r_1}$ sont ses r_1 plongements réels, et que $\forall i \in [\![1, r_2]\!]\, \sigma_{r_1+i} = \overline{\sigma_{r_1+r_2+i}}$. Autrement dit on a mis tous les plongements conjugués à la fin. On définit alors le plongement canonique σ de K par

$$\sigma \; : \left| \begin{array}{ccc} K & \to & \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ x & \mapsto & (\sigma_1(x), ..., \sigma_{r_1+r_2}(x)). \end{array} \right.$$

On remarquera que le plongement canonique est défini à l'ordre des plongements près, mais cela ne joue aucun rôle pour les résultats de structure suivants. On parlera donc bien *du* plongement canonique de K.

Proposition 2.2.1. *Soient K un corps de nombres et σ son plongement canonique. σ est un morphisme de groupes $\mathbb{Q}$-linéaire injectif.*

Démonstration. Cela découle directement de la $\mathbb{Q}$-linéarité des σ_i, qui fait partie de leur définition.

Pour l'injectivité, on sait que chaque σ_i est un morphisme de corps, donc est injectif. □

On vient donc d'identifier un morphisme injectif potentiel $\mathcal{O}_K \to \mathbb{R}^n$. Reste à vérifier que $\sigma(\mathcal{O}_K)$ est un réseau de $\mathbb{R}_n$. Comme annoncé dans l'introduction, on vérifie facilement à l'aide des résultats du premier chapitre qu'on affaire à un groupe discret, et que le volume fondamental est strictement positif.

Proposition 2.2.2. *Soient K un corps de nombres de dimension n et σ son plongement canonique. $\sigma(\mathcal{O}_K)$ est un réseau de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^{r_1+2r_2} = \mathbb{R}^n$.*

Démonstration. On sait que $\mathcal{O}_K$ est un anneau, et que σ est un morphisme de groupes. Donc $\sigma(\mathcal{O}_K)$ est un sous-groupe de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

Démontrons d'abord qu'il s'agit d'un sous-réseau de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, c'est-à-dire que c'est un sous-ensemble discret par la proposition 2.1.6.

Soit donc B une partie bornée de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, par exemple $B \subset [-R, R]^{r_1} \times B_{\mathbb{C}}(0, R)^{r_2}$. Soit $x \in \mathcal{O}_K$ tel que $\sigma(x) \in B$. On a donc, en identifiant valeur absolue et module,

$$\forall i \in [\![1, r_1 + r_2]\!] \; |\sigma_i(x)| \leq R.$$

Mais les r_2 derniers plongements complexe sont les conjugués des r_2 premiers d'après la définition du plongement canonique : ils ont donc même module. On peut donc affirmer que

$$\forall i \in [\![1, n]\!] \; |\sigma_i(x)| \leq R.$$

La proposition 2.2.5 permet de conclure que l'ensemble de $x \in \mathcal{O}_K$ vérifiant cela est fini. Donc $\sigma(\mathcal{O}_K) \cap B$ est fini, et $\sigma(\mathcal{O}_K)$ est un sous-réseau de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

Pour montrer qu'il s'agit d'un réseau, on utilise la proposition 1.3.3, qui disait que $\mathcal{O}_K$ contenait une base du $\mathbb{Q}$-espace vectoriel K, qu'on note $(e_1, ..., e_n)$. On sait alors par le corollaire 1.5.2 que $\det\left((\sigma_i(e_j))_{1 \leq i,j \leq n}\right) \neq 0$.

Notre but est de montrer que $(\sigma(e_j))_{1 \leq j \leq n}$ est libre sur $\mathbb{R}$. Or, pour $x \in K$, la décomposition de $\sigma(x)$ dans la $\mathbb{R}$-base canonique de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ est

$$\sigma(x) = (\sigma_1(x), ..., \sigma_{r_1}(x), Re(\sigma_{r_1+1}(x)), Im(\sigma_{r_1+1}(x)), ..., Re(\sigma_{r_1+r_2}(x)), Im(\sigma_{r_1+r_2}(x)).$$

Mais pour σ un plongement complexe, on observe directement que

$$\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \begin{pmatrix} Re(\sigma(e_1)) & Re(\sigma(e_2)) & ... & Re(\sigma(e_n)) \\ Im(\sigma(e_1)) & Im(\sigma(e_2)) & ... & Im(\sigma(e_n)) \end{pmatrix} = \begin{pmatrix} \sigma(e_1) & \sigma(e_2) & ... & \sigma(e_n) \\ \overline{\sigma}(e_1)) & \overline{\sigma}(e_2)) & ... & \overline{\sigma}(e_n)) \end{pmatrix}.$$

On remarque alors deux choses.

- D'une part $\left|\det\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}\right| = 2$.
- D'autre part, pour σ_{r_1+i} un plongement complexe, $\overline{\sigma}_{r_1+i} = \sigma_{r_1+r_2+i}$.

Autrement dit, le déterminant de la famille $(\sigma(e_j))_{1\leq j\leq n}$ sur $\mathbb{R}$ s'obtient à partir de celui de la matrice $\left((\sigma_i(e_j))_{1\leq i,j\leq n}\right)$ en combinant des lignes. Au total, on trouve

$$\left|\det_{\mathbb{R}}(\sigma(e_j))_{1\leq j\leq n}\right| = 2^{-r_2}\left|\det\left((\sigma_i(e_j))_{1\leq i,j\leq n}\right)\right| = 2^{-r_2}\left|disc(e_1,...,e_n)\right|^{\frac{1}{2}}.$$

Ici ce n'est pas véritablement la valeur qui nous intéresse, mais plutôt le fait que le déterminant soit non nul. La famille $(\sigma(e_j))_{1\leq j\leq n}$ est libre sur $\mathbb{R}$.

Le sous-groupe $\sigma(\mathcal{O}_K)$ est donc un sous-réseau du $\mathbb{R}$-espace vectoriel de dimension n $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$. De plus, il contient une famille $\mathbb{R}$-libre de cardinal n : il est donc exactement de rang n.

Ainsi $\sigma(\mathcal{O}_K)$ est un bien réseau de $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$. □

En fait on a manipulé de façon cachée le volume fondamental de notre réseau dans la preuve : il s'agissait à un facteur près du discriminant de la base. Ainsi on peut montrer la proposition suivante.

Proposition 2.2.3. *Soit $(e_1,...,e_n)$ une $\mathbb{Z}$-base de $\mathcal{O}_K$ contenue dans $\mathcal{O}_K$. La valeur de $|disc(e_1,...,e_n)|$ est indépendante du choix de la base.*

Démonstration. On sait maintenant que $\mathcal{O}_K$ admet des $\mathbb{Z}$-bases de cardinal n.

On observe simplement que dans la preuve précédente, on ne dit rien sur la famille $(e_1,...,e_n)$ à part que c'est une $\mathbb{Q}$-base contenue dans $\mathcal{O}_K$. Comme ici notre $(e_1,...,e_n)$ une $\mathbb{Z}$-base de $\mathcal{O}_K$, par définition elle est libre sur $\mathbb{Q}$, et est donc une $\mathbb{Q}$-base de K.

Ensuite, reste à remarquer que la famille $(\sigma(e_1),...,\sigma(e_n))$ est automatiquement une $\mathbb{Z}$-base de $\sigma(\mathcal{O}_K)$. Mais alors on peut écrire

$$vol(\sigma(\mathcal{O}_K)) = |\det_{\mathbb{R}}(\sigma(e_j))_{1\leq j\leq n}| = 2^{-r_2}|disc(e_1,...,e_n)|^{\frac{1}{2}}.$$

Ainsi $|disc(e_1,...,e_n)|$ est indépendant du choix de la base. □

On introduit naturellement la définition suivante.

Définition 2.2.2 (Discriminant de $\mathcal{O}_K$)**.** On note $disc(\mathcal{O}_K)$ la valeur commune des $|disc(e_1,...,e_n)|$ où $(e_1,...,e_n)$ est une $\mathbb{Z}$-base de $\mathcal{O}_K$.

Alternativement, on peut définir

$$disc(\mathcal{O}_K) = |disc(e_1,...,e_n)| = (2^{r_2}vol(\sigma(\mathcal{O}_K)))^2.$$

On notera qu'on aurait pu montrer que toutes les $\mathbb{Z}$-bases de $\mathcal{O}_K$ ont même discriminant de la même façon qu'on avait montré que le volume d'un réseau était indépendant de la base choisie. Mais pour cela il fallait avoir montré que $\mathcal{O}_K$ admettait des $\mathbb{Z}$-bases, ce qui est le cas maintenant !

En conclusion, on vient bien de démontrer le théorème attendu.

Théorème (5). *Soit K un corps de nombres. Le groupe additif de $\mathcal{O}_K$ admet une $\mathbb{Z}$-base à $n = [K : \mathbb{Q}]$ éléments. Autrement dit, $\mathcal{O}_K \cong \mathbb{Z}^n$ comme groupe abélien.*

On peut en donner une reformulation avec le langage des modules.

Proposition 2.2.4. *Soit K un corps des nombres de dimension n.*
Alors, $\mathcal{O}_K$ est un $\mathbb{Z}$-module libre de rang n.

2.2.2 • Finitude sur $\mathcal{O}_K$

Pour clore ce chapitre, on se propose de démontrer un premier résultat de finitude pour la norme. Rappelons qu'on a démontré à la proposition 2.2.5 le résultat suivant.

Proposition 2.2.5 (Finitude si tous les plongements sont bornés). *Soient K un corps de nombres et σ_1, ..., σ_n ses plongements canoniques. Soit $M > 0$.*

$$\text{L'ensemble } \left\{ x \in \mathcal{O}_K \,\middle|\, \forall i \in [\![1, n]\!]\, |\sigma_i(x)| \leq M \right\} \text{ est fini.}$$

On cherche maintenant à savoir si on peut écrire un résultat équivalent pour la norme. Naïvement, on pourrait vouloir s'interroger sur la finitude de $\left\{ x \in \mathcal{O}_K \,\middle|\, N(x) \leq M \right\}$. Mais comme on l'a noté en introduction, cela demanderait de connaître le groupe des inversibles $\mathcal{O}_K^\times$, dont les éléments sont de norme ± 1.

Pour se débarrasser du problème des inversibles, on décide de regarder non plus les éléments de $\mathcal{O}_K$ mais ses idéaux principaux. Pour le lecteur n'ayant pas encore rencontré la théorie des idéaux, nous en proposons une introduction rapide au chapitre suivant. D'ici là, il suffit de voir $x\mathcal{O}_K$ comme étant l'ensemble $\left\{ xy \,\middle|\, y \in \mathcal{O}_K \right\}$.

Proposition 2.2.6. *Soient x et $y \in \mathcal{O}_K$. On a l'équivalence*

$$x\mathcal{O}_K = y\mathcal{O}_K \iff \frac{x}{y} \in \mathcal{O}_K^\times.$$

Démonstration.

- Si $x\mathcal{O}_K = y\mathcal{O}_K$, alors pour tout $\alpha \in \mathcal{O}_K$ il existe $\beta \in \mathcal{O}_K$ tel que $x\alpha = y\beta$. En particulier, pour $\alpha = 1$, on obtient $x = y\beta$, on encore $\frac{x}{y} = \beta$. Donc $\frac{x}{y} \in \mathcal{O}_K$. On obtient de même $\frac{y}{x} \in \mathcal{O}_K$, et finalement $\frac{x}{y} \in \mathcal{O}_K^\times$. On peut donc écrire $x = yu$ où $u \in \mathcal{O}_K^\times$.
- Réciproquement, si $x = yu$ où $u \in \mathcal{O}_K^\times$, alors pour tout $\alpha \in \mathcal{O}_K$, $\alpha u \in \mathcal{O}_K$ et $x\alpha = yu\alpha \in y\mathcal{O}_K$. Mais comme on a aussi $y = xu^{-1}$, on obtient encore $y\mathcal{O}_K \subset x\mathcal{O}_K$ et finalement $x\mathcal{O}_K = y\mathcal{O}_K$.

□

Une fois le problème des inversibles éliminé, le résultat escompté devient donc :

$$\text{L'ensemble } \left\{ x\mathcal{O}_K \,\middle|\, x \in \mathcal{O}_K,\ |N(x)| \leq M \right\} \text{ est fini.}$$

On se propose ici de donner deux approches de ce résultat. La première est algébrique et est accessible avec les résultats que nous avons obtenu jusqu'à maintenant, mais elle ne donne que peu d'intuition sur ce qu'il se passe réellement. La seconde est géométrique, et elle ne sera qu'esquissée ici. Elle permettra de mieux comprendre cette proposition et annoncera le chapitre 3, dans lequel on développera tous les outils nécessaires à sa démonstration rigoureuse. Commençons donc par l'approche algébrique. La démarche est la suivante.

- Pour tout $x \in \mathcal{O}_K$, $N(x) \in \mathbb{Z}$. Donc on cherche juste à montrer que l'ensemble des $x\mathcal{O}_K$ tel que $N(x) = a$ pour un certain $a \in \mathbb{Z}$ est fini.
- À $a \in \mathbb{Z}$ fixé, le groupe quotient $\mathcal{O}_K/a\mathcal{O}_K$ est isomorphe à $(\mathbb{Z}/a\mathbb{Z})^n$, donc est fini.
- On montre alors que pour x et y dans $\mathcal{O}_K$ avec $N(x) = N(y) = a$ et qui sont dans la même classe de $\mathcal{O}_K/a\mathcal{O}_K$, on a $x\mathcal{O}_K = y\mathcal{O}_K$. Cela conclut.

La preuve repose sur le lemme suivant.

Proposition 2.2.7. *Soit $x \in \mathcal{O}_K$ non nul. Alors $\frac{N(x)}{x} \in \mathcal{O}_K$. En particulier, $N(x) \in x\mathcal{O}_K$.*

Démonstration. Notons $\mu_x = \sum_{i=0}^{d} a_i X^i$. On rappelle que $d = [\mathbb{Q}(x) : \mathbb{Q}]$ Par changement de variable, on obtient l'expression

$$\mu_x = \sum_{i=0}^{d} a_{d-i} X^{d-i}.$$

En évaluant en x, on obtient

$$\mu_x(x) = \sum_{i=0}^{d} a_{d-i} x^{d-i} = x^d \sum_{i=0}^{d} a_{d-i} x^{-i} = 0.$$

Enfin, comme $x \neq 0$, on peut simplifier en

$$\sum_{i=0}^{d} a_{d-i} x^{-i} = 0.$$

Cela donne donc un polynôme annulateur $\sum_{i=0}^{d} a_{d-i} X^i$ pour $\frac{1}{x}$. Mais alors, puisque $x \neq 0$, $a_0 \neq 0$, on peut écrire

$$\frac{N(x)^d}{a_0} \sum_{i=0}^{d} \frac{a_{d-i}}{N(x)^i} \left(\frac{N(x)}{x}\right)^i = \sum_{i=0}^{d} \frac{a_{d-i} N(x)^{d-i}}{a_0} \left(\frac{N(x)}{x}\right)^i = 0.$$

On a donc obtenu le polynôme annulateur $P = \sum_{i=0}^{d} \frac{a_{d-i} N(x)^{d-i}}{a_0} X^i$ pour $\frac{N(x)}{x}$. Reste à vérifier qu'il est unitaire, à coefficients entiers et minimal.

- P est unitaire, puisque pour $i = d$ on obtient $\frac{a_{d-i} N(x)^{d-i}}{a_0} = 1$.

- Les coefficients de P sont à coefficients entiers, puisque l'on sait par la proposition 1.4.6 que $\chi_x = (\mu_x)^r$ avec $r = [K : \mathbb{Q}(x)]$. En particulier, $a_0^r = (-1)^r N(x)$ et donc $a_0 | N(x)$. Tous les $\frac{a_{d-i} N(x)^{d-i}}{a_0}$ sont donc bien entiers.
- Enfin, reste à voir que ce polynôme est minimal.
  Il est de degré $d = [\mathbb{Q}(x) : \mathbb{Q}] = [\mathbb{Q}(\frac{1}{x}) : \mathbb{Q}] = [\mathbb{Q}\left(\frac{N(x)}{x}\right) : \mathbb{Q}]$, puisque $N(x) \in \mathbb{Z} \subset \mathbb{Q}$.

Ainsi P est bien le polynôme annulateur minimal de $\frac{N(x)}{x}$ et $P = \mu_{\frac{N(x)}{x}}$, ce qui permet de conclure que $\frac{N(x)}{x} \in \mathcal{O}_K$. □

Reste à conclure en utilisant le lemme.

Proposition 2.2.8 (Finitude à norme bornée)**.** *Soit K un corps de nombres. Soit $M > 0$.*

$$\left\{ x\mathcal{O}_K \,\middle|\, x \in \mathcal{O}_K,\ |N(x)| \leq M \right\} \text{ est fini.}$$

Démonstration. On sait déjà que si $x \in \mathcal{O}_K$, alors $N(x) \in \mathbb{Z}$ par la proposition 1.4.7. Ainsi, on a juste à montrer que, pour tout $a \in \mathbb{Z}$,

$$\left\{ x\mathcal{O}_K \,\middle|\, x \in \mathcal{O}_K,\ N(x) = a \right\} \text{ est fini.}$$

Éliminons d'abord le cas $a = 0$, puisque l'unique $x \in \mathcal{O}_K$ qui vérifie $N(x) = 0$ est $x = 0$. On prend $a \neq 0$.

Montrons donc qu'il n'y a bien qu'un nombre fini d'idéaux de la forme $x\mathcal{O}_K$ avec $N(x) = a$.

On sait que $\mathcal{O}_K \cong \mathbb{Z}^n$, donc $\mathcal{O}_K/(a\mathcal{O}_K) \cong \mathbb{Z}^n/(a\mathbb{Z}^n) \cong (\mathbb{Z}/a\mathbb{Z})^n$ qui est donc fini. Remarquons que $a\mathcal{O}_K$ est bien un idéal de $\mathcal{O}_K$ puisque $a \in \mathbb{Z} = \mathcal{O}_{\mathbb{Q}} \subset \mathcal{O}_K$.

Soient x et $y \in \mathcal{O}_K$ tels que $N(x) = N(y) = a$ et tels qu'ils ont même classe dans $\mathcal{O}_K/(a\mathcal{O}_K)$. On va montrer que $x\mathcal{O}_K = y\mathcal{O}_K$, ce qui revient à montrer que $\frac{x}{y} \in \mathcal{O}_K^\times$.

Puisque x et y sont de même classe dans $\mathcal{O}_K/(a\mathcal{O}_K)$, il existe $\alpha \in \mathcal{O}_K$ tel que $x = y + a\alpha$.

En divisant par y, on obtient

$$\frac{x}{y} = 1 + \frac{a}{y}\alpha.$$

Puisque $\alpha \in \mathcal{O}_K$, on a donc $1 + \frac{N(y)}{y}\alpha \in \mathcal{O}_K$ et in fine $\frac{x}{y} \in \mathcal{O}_K$.

Mais de même, on divise l'équation $x = y + a\alpha$ par x pour obtenir

$$\frac{y}{x} = 1 - \frac{a}{x}\alpha = 1 - \frac{N(x)}{x}\alpha.$$

Comme on a encore $\frac{N(x)}{x} \in \mathcal{O}_K$, on voit que $\frac{y}{x} \in \mathcal{O}_K$.

Finalement, $\frac{x}{y} \in \mathcal{O}_K^\times$, et on peut conclure que $x\mathcal{O}_K = y\mathcal{O}_K$. On vient donc de montrer que, pour $x, y \in \mathcal{O}_K$ avec $N(x) = N(y) = a$,

$$\overline{x} = \overline{y} \text{ dans } \mathcal{O}_K/(a\mathcal{O}_K) \implies x\mathcal{O}_K = y\mathcal{O}_K.$$

Enfin, on rappelle que $\mathcal{O}_K/(a\mathcal{O}_K)$ est fini, de cardinal $|a|^n$.

Cela permet d'affirmer que l'ensemble $\left\{ x\mathcal{O}_K \,\middle|\, x \in \mathcal{O}_K,\ N(x) = a \right\}$ est fini de cardinal au plus $|a|^n$: c'est ce qu'on voulait. □

Passons maintenant à l'approche géométrique. L'idée repose sur le fait que les idéaux de $\mathcal{O}_K$ peuvent être identifiés aux réseaux inclus dans le réseau $\sigma(\mathcal{O}_K)$ de $\mathbb{R}^n$. Trouver les idéaux principaux $x\mathcal{O}_K$ avec $N(x) = a$ peut se faire grâce à l'approche suivante.

- On a vu que tous les idéaux principaux $x\mathcal{O}_K$ avec $N(x) = a$ ont un élément non trivial en commun : c'est a.
- Géométriquement, un idéal de $\mathcal{O}_K$ réalise un réseau inclus dans le réseau $\sigma(\mathcal{O}_K)$ de $\mathbb{R}^n$. Ce point sera démontré rigoureusement dans le troisième chapitre (voir proposition 3.2.3). Cette intuition est assez naturelle : un exemple graphique en est donné en 3.2.2.
- Le problème revient alors à chercher tous les réseaux de $\sigma(\mathcal{O}_K)$ qui contiennent un certain point : en l'occurrence $(a, ..., a)$ puisque $a \in \mathbb{Z}$.

Le problème est qu'il y a a priori un nombre infini de tels sous-réseaux. En fait, on dispose d'une contrainte supplémentaire : le volume fondamental du sous-réseau correspond à l'idéal $\mathcal{O}_K$ est à facteur près $|N(x)|$ (c'est la proposition 3.2.8). Dès lors, on cherche les réseaux de $\sigma(\mathcal{O}_K)$ de volume fondamental fixé et contenant un point donné : il y en a un nombre fini. Le résultat en découle.

Bref, cette proposition nous invite à poursuivre au sein du paradigme géométrique, qui fournit un point de vue très éclairant sur la structure de $\mathcal{O}_K$. On généralise cette approche dans le chapitre 3.

3
ARITHMÉTIQUE DES IDÉAUX

Maintenant que la structure de $\mathcal{O}_K$ est mieux connue, on se propose de dégager quelques propriétés arithmétiques fondamentales de cet anneau. Notre prototype sera $\mathbb{Z}$: ce dernier dispose en effet de caractéristiques tout à fait remarquables, qu'on souhaiterait idéalement retrouver sur $\mathcal{O}_K$. La plus importante d'entre elles est sans doute le *théorème fondamental de l'arithmétique*.

Théorème 7 (Théorème fondamental de l'arithmétique)**.** *Tout nombre entier strictement positif admet une unique factorisation comme produit de nombres premiers à l'ordre des facteurs près.*

L'intérêt de ce théorème est qu'il permet de pratiquer une *arithmétique modulaire* : on pourra pratiquer des réductions modulo p, considérer des valuations p-adiques... Ces outils permettent de *distinguer les nombres d'un point de vue arithmétique*. Or c'est précisément cette approche qui nous intéresse.

Néanmoins, la construction d'une arithmétique sur $\mathcal{O}_K$ présente deux difficultés, qui proviennent du fait qu'on s'est éloigné de la configuration initiale de $\mathbb{Z}$.

- Sur $\mathbb{Z}$, les factorisations sont valables à un signe ± 1 près. Cela ne constitue pas un problème insurmontable, puisque 1 et -1 sont bien connus. Sur $\mathcal{O}_K$, le groupe des unités peut être plus vaste. On a vu par exemple que dans le cas des corps quadratiques $\mathbb{Q}[\sqrt{d}]$, il correspondait à la résolution de l'équation de Pell-Fermat, ce qui est un problème difficile. Dès lors, la factorisation en élément premier devient ineffective puisqu'elle s'opère à un facteur unitaire près.
- Sur $\mathcal{O}_K$, il y a en quelque sorte un défaut de nombres premiers. Il est possible d'écrire des décompositions différentes d'un même élément en facteurs irréductibles.

Un exemple fort célèbre de ce problème est donné par $\mathbb{Q}[i\sqrt{5}]$, dont on a vu à l'exemple 1.3.1 que l'anneau des entiers était $\mathbb{Z}[i\sqrt{5}]$ (puisque $-5 \equiv 3[4]$). On a alors les deux factorisations de 6 suivantes.

$$6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

Bien sûr, dans $\mathbb{Z}$ obtenir deux factorisations d'un même nombre est fréquent. Mais en factorisant davantage, on arrive toujours à une unique décomposition. Or ici ces quatre nombres sont irréductibles : leurs seuls diviseurs sont eux-mêmes et 1 (à un facteur unitaire près) – on justifiera cela rigoureusement plus loin. Dès lors, il semble qu'il « manque » des nombres premiers, qui seraient en fait dans ce cas des diviseurs de 2, 3 et $1 \pm i\sqrt{5}$.

Pour résoudre cette difficulté, Ernst Kummer (1810-1983) propose d'ajouter ces nombres premiers manquants à $\mathcal{O}_K$, qu'il appelle « *nombres idéaux* ». Imaginons par exemple que l'on possède des nombres a, b, c et d irréductibles tels que $2 = ab$, $3 = cd$, $1 + i\sqrt{5} = ac$, $1 - i\sqrt{5} = bd$. Alors la factorisation de 6 présentée plus haut est en fait unique, et on tombe sur

$6 = abcd$. De tels nombres permettraient de continuer les factorisations et d'arriver à l'unicité des décompositions.

Cette approche pose cependant le problème de la construction et de l'existence de tels facteurs idéaux. C'est pour contourner cette difficulté que Richard Dedekind (1831-1916) introduit la notion d'*idéal*. Fondamentalement, l'idée est de considérer non plus les nombres idéaux, mais *les ensembles de nombres de $\mathcal{O}_K$ qu'ils divisent*. Regardons ce qu'il se passe sur $\mathbb{Z}$. Prenons un $n \in \mathbb{Z}$ et notons $n\mathbb{Z}$ l'ensemble des nombres entiers divisés par n.

- $n\mathbb{Z}$ est stable par addition : c'est un sous-groupe additif de $\mathbb{Z}$.
- Pour tous $a \in n\mathbb{Z}$ et $b \in \mathbb{Z}$, ab est divisible par n, donc $ab \in n\mathbb{Z}$.

Si les nombres idéaux « existent », alors l'ensemble de leurs multiples respectifs vérifient ces propriétés. L'intuition géniale de Dedekind et que dans $\mathcal{O}_K$ on a une réciproque : derrière tout ensemble de ce type se cache un diviseur idéal. Il appelle ces ensembles les *idéaux*.

Définition 3.0.1 (Idéal)**.** Soit $(A, +, \times)$ un anneau commutatif. Soit I une partie de A. On dit que I est un idéal de A si

- I est un sous-groupe additif de A,
- Pour tout $a \in A$, pour tout $x \in I$, $ax \in I$. Autrement dit I est stable par multiplication par tout élément de A.

Dans $\mathbb{Z}$, ce résultat est vrai sans avoir recours aux nombres idéaux : les idéaux de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$. Mais dans $\mathcal{O}_K$ ce n'est plus le cas. Néanmoins, les idéaux suffisent effectivement à obtenir des décompositions uniques en facteurs premiers sur $\mathcal{O}_K$, et ils ont le bon goût d'exister et d'être bien définis (contrairement aux nombres idéaux). Un anneau dans lequel on peut décomposer les idéaux en produits d'idéaux premiers sera appelé *anneau de Dedekind*. On se propose de montrer à travers les deux premières sections de ce chapitre le théorème suivant.

Théorème 8. *Soit K un corps de nombres. L'anneau $\mathcal{O}_K$ est de Dedekind.*

Enfin, on remarque que les idéaux permettent d'oublier les unités de $\mathcal{O}_K$, comme on l'a remarqué au chapitre précédent pour les idéaux principaux. Finalement, ils constituent bien la brique de base avec laquelle on veut construire notre arithmétique de $\mathcal{O}_K$.

Ainsi, on se propose dans ce chapitre d'étudier l'arithmétique des idéaux dans $\mathcal{O}_K$, en commençant par prouver qu'elle y est bien définie, puis en observant les propriétés qu'elle vérifie. Plus précisément, notre cheminement sera le suivant.

- La partie 3.1 présente les deux approches évoquées dans l'introduction. On s'intéresse d'abord la factorisation en éléments irréductibles (ce qui correspond à la notion *d'anneau factoriel*), puis à celle en idéaux premiers, en fournissant pour chacune les propriétés algébriques que l'anneau doit vérifier. Cette première partie peut sembler optionnelle : après tout on vient de voir que les anneaux d'entiers sur un corps de nombres n'étaient pas nécessairement factoriels. Il nous cependant semblé utile de l'inclure : elle permet d'introduire des notions et concepts qu'on utilise par la suite, et met en évidence le « défaut de factorialité » de $\mathcal{O}_K$, qui est en un certain sens un « défaut de principalité ».

- La partie 3.2 montre que $\mathcal{O}_K$ est effectivement de Dedekind. La preuve exploite les outils présentés aux chapitres 1 et 2, et particulièrement la géométrisation de $\mathcal{O}_K$ réalisée par le plongement canonique. On observe notamment le fait que les idéaux sont des réseaux inclus dans $\sigma(\mathcal{O}_K)$, ce qui permet de définir le concept de *norme d'un idéal*, qui généralise la norme sur K. Ensuite, on introduit le notion de *groupe des classes d'idéaux*. Ce groupe est trivial si l'anneau considéré est principal : il mesure donc en quelque sorte le « défaut de principalité » de $\mathcal{O}_K$. On montre alors que dans le cas des corps de nombres, ce groupe est fini (c'est le théorème 10), ce qui entraîne que $\mathcal{O}_K$ est de Dedekind.

Les deux dernières sous-parties s'intéressent aux propriétés de cette arithmétique. Elles développent toute la machinerie qui nous permettra de définir de façon agréable le concept de *hauteur* aux chapitres 5 et 6.

- La sous-partie 3.2.4 pose sur $\mathcal{O}_K$ des concepts analogues à ceux utilisés sur $\mathbb{Z}$. On définit ainsi des valeurs $\mathfrak{p}$-adiques pour des idéaux premiers, dont on vérifie le comportement. De plus, on étend ces notions à K tout entier, en exploitant le fait qu'il est le corps des fractions de $\mathcal{O}_K$. Enfin, on note que la norme des idéaux se comporte très agréablement à l'égard des décompositions. Ces propriétés sur la norme, en apparence anecdotique, vont être au cœur de la section suivante, car elles induisent des propriétés de rigidités remarquables lorsqu'on cherche à calculer les factorisations effectives des idéaux.
- La sous-partie 3.2.5 s'intéresse au comportement de la factorisation dans les extensions. Plus précisément, si on dispose d'une extension de corps de nombres L/K, un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ peut être plongé dans $\mathcal{O}_L$ en considérant l'idéal $\mathfrak{p}\mathcal{O}_L$, qui admet alors une décomposition en idéaux premiers de $\mathcal{O}_L$. Les idéaux premiers qui interviennent dans cette factorisation, ainsi que leurs puissances dans l'écriture, sont décrits par le théorème 11, qui est démontré à l'aide de la norme des idéaux et de la notion *d'anneau localisé*. Ce résultat est remarquable, car il permettra d'obtenir une *mesure absolue* indépendante de l'extension considérée, ce qui n'était le cas d'aucun des concepts présentés jusqu'à alors. Enfin, cette section sera l'occasion d'introduire une première définition de $\mathcal{O}_{K,S}$.

3.1 Arithmétique dans un anneau commutatif intègre

Commençons donc par regarder de quelles façons on peut obtenir un résultat analogue au théorème fondamental de l'arithmétique dans le cas d'un anneau commutatif intègre (qui recouvre l'étude de $\mathcal{O}_K$). Comme on l'a vu en introduction, il existe deux types d'anneaux qui satisfont une propriété de factorisation satisfaisante :

- Les éléments des *anneaux factoriels* admettent une unique décomposition en facteurs irréductibles.
- Les idéaux des *anneaux de Dedekind* admettent une unique décomposition en produit d'idéaux premiers.

On va donc étudier successivement ces deux notions. On pourrait croire que le cadre des anneaux factoriels est superflu : en effet, l'introduction a donné l'exemple d'un anneau d'entiers

d'un corps de nombres qui n'est pas factoriel ($\mathbb{Z}[i\sqrt{5}]$). Néanmoins, il permet de présenter la situation idéale dans laquelle on aimerait se situer. En particulier, on verra que les notions d'anneaux factoriel et de Dedekind coïncident dans celle d'anneau principal, ce qui donne une intuition puissante sur la démarche qu'on adoptera par la suite sur $\mathcal{O}_K$: ce dernier sera de Dedekind s'il n'est pas « trop loin » d'être principal. C'est ce défaut de principalité que mesure de le groupe des classes, dont on verra qu'il est fini.

Dans les deux sections, notre mode opératoire sera le même :

- On introduit d'abord quelques définitions, qui permettent d'identifier les « éléments premiers » qu'on souhaite voir apparaître dans notre décomposition.
- On s'intéresse ensuite aux conditions de l'unicité de la factorisation, puis de l'existence.
- Enfin, on relie les conditions obtenus à différents anneaux connus, notamment les idéaux principaux.

On termine cette partie en confrontant les notions d'anneaux factoriel et de Dedekind, et en regardant quels anneaux appartiennent aux deux catégories ou non.

3.1.1 • Décomposition en éléments irréductibles

Commençons donc par étudier la factorisation en éléments irréductibles. Ici on s'appuie sur le cours d'Olivier Debarre [12] (chapitre 3), mais on ne fait que présenter les notions de base qui nous seront utiles par la suite. Le lecteur intéressé pourra se référer à cet ouvrage s'il souhaite approfondir.

Étant donné qu'on utilisera nos résultats sur des $\mathcal{O}_K$, on ne s'intéressera qu'à des anneaux A vérifiant des propriétés analogues, c'est-à-dire :

- A commutatif.
- A unitaire.
- A intègre : $\forall a, b \in A\ (ab = 0 \implies a = 0 \text{ ou } b = 0)$.

Si on oublie de le rappeler, notre anneau A vérifiera toujours ces trois propriétés.

On l'aura compris, notre but est de formuler un théorème analogue au théorème fondamental de l'arithmétique sur $\mathbb{Z}$ pour de tels anneaux :

Théorème (7)**.** *Tout nombre entier strictement positif admet une unique factorisation comme produit de nombres premiers à l'ordre des facteurs près.*

Dans le cas de la décomposition en éléments irréductibles, les arguments qui entrent en jeu sont les suivants :

- L'existence la décomposition s'obtient en assouplissant la définition d'anneau principal : on ne demande plus aux idéaux d'être monogènes, mais d'être engendrés par un nombre fini d'éléments. D'une certaine manière, cela garantit qu'on ne peut pas factoriser « à l'infini » et qu'on tombera forcément sur une écriture en éléments irréductibles.
- L'unicité demande que l'écriture fasse intervenir des éléments premiers. C'est pourquoi elle est équivalente au fait que les notions d'élément premier et élément irréductible coïncident.

Commençons donc par voir à quoi correspond la notion « d'élément premier dans le cadre d'un anneau commutatif intègre quelconque ».

Les éléments irréductibles

Le lecteur attentif aura remarqué qu'au cours de l'introduction on a parfois utilisé le terme « d'élément premier » et parfois « d'élément irréductible ». C'est que ces deux notions ne coïncident pas sur un anneau quelconque. On verra par contre que c'est le cas sur un anneau factoriel.

Définition 3.1.1 (Élément irréductible)**.** Soit A un anneau intègre commutatif. On dit que $a \in A$ non nul est irréductible s'il n'est ni inversible, ni produit de deux éléments non inversibles, c'est à dire que

$$a = bc \implies b \in A^\times \text{ ou } c \in A^\times.$$

Définition 3.1.2 (Élément premier)**.** Soit A un anneau intègre commutatif. On dit que $p \in A$ non nul et non inversible est premier si pour tout produit ab multiple de p, p divise a ou p divise b. Autrement dit,

$$p|ab \implies p|a \text{ ou } p|b.$$

Exemple 3.1.1. Dans $\mathbb{Z}[i\sqrt{5}]$, 2 est irréductible, mais pas premier puisqu'il divise le produit $(1+i\sqrt{5})(1-i\sqrt{5})$ sans diviser aucun des deux termes.

On a néanmoins un lien entre les deux notions :

Proposition 3.1.1. *Dans un anneau commutatif intègre, tout élément premier est irréductible.*

Démonstration. Soit $p \in A$ premier. Soient $a, b \in A$ tels que

$$p = ab.$$

Alors, $a|p$ et $b|p$. Mais p est premier, et $p|ab$. D'après la définition, $p|a$ ou $p|b$. On suppose que $p|a$ sans perte de généralité.

Comme $a|p$ et $p|a$, on peut écrire $p = a\eta_1 = p\eta_1\eta_2$, où $\eta_1, \eta_2 \in A$.

Ainsi,

$$p(1 - \eta_1\eta_2) = 0.$$

Par intégrité de l'anneau,

$$\eta_1\eta_2 = 1,$$

donc $\eta_1 \in A^\times$. Or, on peut écrire

$$p = a\eta_1 = ab,$$

d'où, encore par intégrité,

$$b = \eta_1 \in A^\times.$$

p est donc irréductible. □

Au vu de l'introduction et de l'exemple de $\mathbb{Z}[i\sqrt{5}]$, il semble plus sage de demander un produit en *éléments irréductibles*. En effet, la définition correspond exactement à l'idée qu'on ne peut pas factoriser plus les écriture, ce qui n'est a priori pas le cas pour élément premier. On définit donc la notion d'anneau factoriel de cette façon.

Définition 3.1.3 (Anneau factoriel)**.** Soit A un anneau commutatif intègre. On dit que A est factoriel si tous ses éléments non nuls et non inversibles admettent une décomposition unique en facteurs irréductibles au sens suivant.

(i) Tout élément $a \in A$ non nul et non inversible s'écrit $a = p_1 \cdots p_r$ où les p_i sont des éléments irréductibles de A.

(ii) Cette décomposition est unique à l'ordre des facteurs près : si $a = p_1 \cdots p_r = q_1 \cdots q_s$ avec les p_i et les q_j irréductibles, alors $r = s$ et on a une permutation σ telle que pour tout i on a $p_{\sigma(i)} = \mu_i q_i$ avec $\mu_i \in A^\times$.

Exemple 3.1.2. L'anneau $\mathbb{Z}$ est factoriel.

Avant d'aller plus loin, on remarque qu'on peut réécrire la factorisation d'une façon plus agréable à l'aide du concept d'éléments irréductibles associés.

Une façon commode d'écrire la condition d'unicité est d'introduire le concept d'éléments irréductibles associés.

Définition 3.1.4 (Éléments associés)**.** Soient a et b deux éléments de A, un anneau commutatif intègre. On dit que a et b sont associés s'ils vérifient l'une des trois conditions suivantes, qui sont équivalentes.

(i) $(a) = (b)$.

(ii) $a|b$ et $b|a$.

(iii) Il existe $u \in A^\times$ tel que $a = ub$.

La condition d'unicité de la décomposition peut se réécrire en disant que les facteurs irréductibles sont associés (à permutation près).

En utilisant l'axiome du choix, on voit qu'on peut trouver une famille maximale $(p_i)_{i\in I}$ d'éléments irréductibles de A au sens suivant.

- Pour tout $p \in A$ irréductible, il existe un $i \in I$ tel que p et p_i sont associés.
- Pour tous indices $i \neq j$ de I, p_i et p_j ne sont pas associés.

Exemple 3.1.3. Dans $\mathbb{Z}$, les éléments irréductibles sont les $\pm p$ où p est un nombre premier. On en déduit qu'un exemple de telle famille est tout simplement $\mathcal{P}$ l'ensemble des nombres premiers positifs.

Une fois qu'on s'est donné cette famille $(p_i)_{i\in I}$, on obtient la reformulation suivante du théorème fondamental de l'arithmétique dans un anneau factoriel, qui rappelle fortement la décomposition dans $\mathbb{Z}$.

Proposition 3.1.2. *Soit A un anneau factoriel. Tout élément $a \in A$ non nul s'écrit de façon unique*

$$a = u \prod_{i\in I} p_i^{v_{p_i}(a)},$$

où $u \in A^\times$ et les $v_{p_i}(a)$ sont dans $\mathbb{N}$.

On appelle la fonction $v_{p_i} : A \to \mathbb{N}$ la valuation p_i-adique.

On remarquera qu'ici on autorise a à être un inversible, puisqu'alors $u = a$ et toutes les valuations p-adiques sont nulles.

Démonstration. L'existence et l'unicité découlent de la définition d'anneau factoriel et de la famille $(p_i)_{i\in I}$. On écrit la décomposition

$$a = q_1 \cdots q_r,$$

et on rassemble les q_i dans les p_i qui leur sont associés, d'où l'apparition du $u \in A^\times$. □

En plus du cas de $\mathbb{Z}[i\sqrt{5}]$, on peut regarder des exemples bien plus pathologiques d'anneaux non factoriels, comme $\overline{\mathbb{Q}}$: en effet cet anneau ne contient aucun élément irréductible !

Exemple 3.1.4. Soit $a \in \overline{\mathbb{Q}}$ non inversible. Soit $P \in \mathbb{Q}[X]$ tel que $P(a) = 0$. Soit b l'une des racines de l'équation $x^2 = a$. Alors b est racine du polynôme $P(X^2) \in \mathbb{Q}[X]$, donc $b \in \overline{\mathbb{Q}}$. Mais b est non inversible (sinon a serait inversible), et comme $b^2 = a$, on en déduit que a n'est pas irréductible.

Ainsi, $\overline{\mathbb{Q}}$ n'a pas d'éléments irréductibles.

Une condition d'existence

Maintenant que la définition d'anneau factoriel est bien posée, nous allons donner une condition d'existence de la factorisation en éléments irréductibles. Celle-ci repose sur la notion d'anneau nœthérien (celle-ci étant nommée en l'honneur d'Emmy Noether, 1882-1935).

Définition 3.1.5 (Anneau nœthérien)**.** Soit A un anneau commutatif. On dit que A est nœthérien si tous ses idéaux sont de type fini, c'est-à-dire s'ils admettent tous une famille génératrice finie comme A-module. On notera alors $I = (a_1, ..., a_n)$.

On fera attention que la définition d'anneau nœthérien ne demande pas l'intégrité. Néanmoins, nous serons pour notre part toujours dans ce cas.

On voit alors que la notion d'anneau nœthérien est un assouplissement de celle d'anneau principal, puisqu'on autorise à avoir plus d'un générateur. Rappelons peut-être d'abord formellement les définitions liées aux anneaux principaux, qu'on a déjà rencontrés plus haut.

Définition 3.1.6 (Idéal principal)**.** Soit I un idéal d'un anneau commutatif intègre A. On dit que I est principal s'il existe $a \in A$ tel que $I = aA$. On note dans ce cas $I = (a)$.

Définition 3.1.7 (Anneau principal)**.** Un anneau commutatif intègre A est dit principal si tous ses idéaux sont principaux.

Exemple 3.1.5. C'est un fait bien connu que $\mathbb{Z}$ est principal, car tous ses idéaux sont de la forme (n) où $n \in \mathbb{Z}$.

Comme on vient de le dire, la notion d'anneau nœthérien assouplit celle d'anneau principal. Il s'agit d'une intuition importante à avoir, et qui expliquera pourquoi on retrouvera les anneaux principaux plus tard. On a en tout cas automatiquement la propriété suivante :

Proposition 3.1.3. *Tout anneau principal est nœthérien.*

En tout généralité, on a plutôt envie de définir la notion de module nœthérien. Dans ce cas, la notion d'anneau nœthérien est juste un cas particulier en voyant l'anneau A comme un module sur lui-même. On introduit quand même cette définition, qui est tout à fait naturelle une fois qu'on a compris la première.

Définition 3.1.8 (Module nœthérien)**.** Soient A un anneau commutatif et M un module sur A. On dit que M est nœthérien si tous ses sous-modules sont de type fini.

On dispose aussi des définitions équivalentes suivantes, qui sont dans les faits très pratiques.

Proposition 3.1.4. *Soit M un A-module (toujours avec A commutatif). S'équivalent*

(i) M est nœthérien.

(ii) Toute suite de sous-modules de M croissante pour l'inclusion est stationnaire à partir d'un certain rang.

(iii) Toute famille non vide de sous-modules de M admet un élément maximal pour l'inclusion.

On rappelle ici qu'élément maximal signifie qu'il n'existe aucun élément plus grand. En conséquence, x est dit élément maximal d'une famille ordonnée $(\mathcal{F}, \leq)$ si

$$\forall y \in \mathcal{F} \;\; x \leq y \implies x = y.$$

Démonstration.

- $(i) \implies (ii)$
  Soit $N_0 \subset N_1 \subset ...$ une suite croissante de sous-modules de M. On pose $N = \bigcup_{i \geq 0} N_i$. N est alors un sous-module de M.
  Puisque (i) est vérifiée, on sait que N est engendré par $x_1, ..., x_k$. Donc on a un indice r tel que tous les $x_1, ..., x_k$ sont dans N_r. Mais alors pour tout $i \geq r$,

  $$(x_1, ..., x_k) \subset N_r \subset N_i \subset N = (x_1, ..., x_k).$$

  Donc la suite est stationnaire à partir du rang r.
- $(ii) \implies (iii)$
  Soit $\mathcal{F}$ une famille de sous-modules de M, dont on suppose par l'absurde qu'elle ne possède pas d'élément maximal.
  Alors pour tout $N \in \mathcal{F}$, il existe $N' \in \mathcal{F}$ avec $N \subsetneq N'$ (sinon N serait maximal).
  On construit donc par récurrence (car $\mathcal{F}$ est non vide) une suite de sous-modules de M strictement croissante, ce qui est absurde puisqu'on a supposé (ii).
- $(iii) \implies (i)$
  Soit N un sous-module de M. Soit $\mathcal{F}$ la famille des sous-modules de N de type fini. $\mathcal{F}$ est non vide car elle contient (0).
  Par (iii), on a donc un élément maximal N' de $\mathcal{F}$. On sait déjà que $N' \subset N$.
  Soit $n \in N$. $N' + An$ est alors un sous-module de N de type fini puisque N' est de type fini.
  De plus, $N' \subset N' + An$, et par maximalité $N' = N' + An$.
  Il vient donc $n \in N'$, et ainsi $N \subset N'$.
  In fine, on trouve $N = N'$, et en particulier N est de type fini.

□

On peut reformuler la proposition précédente dans le langage des idéaux pour un anneau nœthérien.

Proposition 3.1.5. *Soit A un anneau. S'équivalent*

(i) A est nœthérien.

(ii) Toute suite d'idéaux de A croissante pour l'inclusion est stationnaire à partir d'un certain rang.

(iii) Toute famille non vide d'idéaux de A admet un élément maximal pour l'inclusion.

Ce sont ces propriétés qui permettent d'obtenir l'existence d'une décomposition en éléments irréductibles sur un anneau nœthérien. La preuve repose sur l'idée que si on suppose par l'absurde l'existence d'éléments non nuls, non inversibles et non décomposables en produits fini d'éléments irréductibles, l'élément maximal de cette famille sera décomposable, ce qui est absurde.

Proposition 3.1.6 (Existence d'une décomposition en éléments irréductibles dans un anneau nœthérien)**.** *Soit A est un anneau nœthérien intègre.*

Alors, tout élément de A non nul et non inversible se décompose en un produit fini d'éléments irréductibles.

Cette décomposition n'est pas nécessairement unique.

Démonstration. Posons

$$\mathscr{I} = \left\{ (a) \,\middle|\, a \in A \text{ avec } a \text{ non nul, non inversible et non produit fini d'irréductibles} \right\}.$$

On veut montrer $\mathscr{I} = \emptyset$. Supposons par l'absurde que ce n'est pas le cas. D'après le (iii) de la proposition 3.1.5, on sait que $\mathscr{I}$ admet un élément maximal (a), avec a non nul, non inversible et non décomposable en un produit fini d'éléments irréductibles. En particulier, a n'est pas irréductible, donc on peut écrire $a = bc$ avec b et c non inversibles. Autrement dit,

$$(a) \subset (b) \quad \text{et} \quad (a) \subset (c).$$

De plus, les inclusions sont strictes : si on suppose par l'absurde $(a) = (b)$, alors $a = db$ pour un $d \in A$, et on a

$$a = bc = adc,$$

mais par intégrité, $dc = 1$ est c est inversible : absurde.

En particulier, comme (a) est un élément maximal de $\mathscr{I}$ et que b et c sont non nuls et non inversibles, on ne peut pas avoir $(b) \in \mathscr{I}$ ou $(c) \in \mathscr{I}$. Donc b et c admettent une décomposition en un produit fini d'éléments irréductibles, donc $a = bc$ aussi : absurde car $a \in \mathscr{I}$.

Finalement, on a bien $\mathscr{I} = \emptyset$, et tous les éléments de A admettent une décomposition en facteurs irréductibles. □

La condition d'unicité

Maintenant qu'on a donné une condition d'existence, on s'intéresse à ce qu'il se passe pour l'unicité. Dans ce cas, on donne une condition nécessaire et suffisante à l'unicité de la décomposition en facteurs irréductibles. L'idée de constater que sur $\mathbb{Z}$, les notions d'éléments premiers et irréductibles coïncident, et que ce fait joue de façon essentielle dans la preuve de l'unicité de la factorisation donnée par le théorème fondamental de l'arithmétique. En fait, il s'agit de la condition cherchée : sous réserve d'existence, on a unicité de la décomposition en facteurs irréductibles si et seulement si les irréductibles sont premiers.

Pour le montrer, il sera commode de raisonner avec le langage des idéaux. En effet, on va voir que les notions *d'idéal maximal* et *d'idéal premier* jouent un rôle analogue aux éléments irréductibles et premier respectivement.

Définition 3.1.9. Soit A un anneau commutatif. On dit qu'un idéal I de A (distinct de A) est maximal si le seul idéal qui le contient strictement est A tout entier.
C'est équivalent au fait de demander que A/I est un corps.

Démonstration. .

- $\Longrightarrow$
  Supposons I maximal. Soit $\overline{a} \in A/I$ non nul. On veut vérifier que $\overline{a}$ est inversible. Comme $\overline{a}$ est non nul, cela signifie que a n'est pas dans I. Alors $I + aA$ est un idéal de A qui contient strictement I, donc c'est A.
  Ainsi, on a $i \in I$ et $b \in A$ tels que
  $$i + ab = 1.$$
  Autrement dit, $\overline{ab} = \overline{a}\overline{b} = \overline{1}$ et $\overline{a}$ est inversible. Donc A/I est un corps.
- $\Longleftarrow$
  Supposons que A/I est un corps. Soit J un idéal de A qui contient strictement I. Alors on a $a \in J$ tel que $a \notin I$. Donc $\overline{a}$ est non nul, et admet un inverse $\overline{b}$. Autrement dit, il existe $i \in I$ tel que
  $$i + ab = 1.$$
  Comme $a \in J$ et $i \in J$, on a donc $1 \in J$ et $J = A$. Ainsi, I est maximal.

□

On remarque que l'on dispose du résultat suivant, qui découle en fait de l'axiome du choix.

Proposition 3.1.7. *Soit A un anneau. Tout idéal propre est contenu dans un idéal maximal.*

De même, on définit les idéaux premiers.

Définition 3.1.10. Soit A un anneau commutatif. Soit I un idéal de A distinct de A (on dit que I est un idéal propre). On dit que I est un idéal premier si
$$\forall a, b \in A \;\; ab \in I \Rightarrow a \in I \text{ ou } b \in I.$$
Il est équivalent de demander que A/I soit intègre.

Démonstration. La preuve est évidente une fois qu'on voit que $\overline{a} = \overline{0}$ dans A/I si et seulement si $a \in I$. □

On a donc immédiatement le corollaire suivant.

Proposition 3.1.8. *Tout idéal maximal est premier.*

Démonstration. Cela provient simplement du fait qu'un corps est intègre, donc si A/I est un corps, il est aussi intègre. □

Comme on pouvait s'y attendre, on a un lien entre la notion d'élément premier (définition 3.1.2) et celle d'idéal premier.

Proposition 3.1.9. *Soient A un anneau commutatif intègre et $p \in A$ non nul. On a alors l'équivalence*

$$(p) \text{ est un idéal premier de } A \Leftrightarrow p \text{ est un élément premier de } A.$$

Démonstration. La preuve est évidente une fois qu'on a compris que $a \in (p) \iff p|a$. On notera que le fait de demander que (p) est un idéal propre (donc distinct de A) entraîne que p n'est pas inversible. □

On a aussi un lien entre la notion d'idéal premier et d'élément irréductible.

Proposition 3.1.10. *Soient A un anneau intègre et $p \in A$ non nul. Si (p) est premier, alors p est irréductible.*

Démonstration. Déjà, (p) est premier, donc n'est pas A tout entier et p n'est pas inversible.

Ensuite, écrivons $p = ab$. Comme (p) est premier, cela donne $a \in (p)$ ou $b \in (p)$, disons le premier cas. Donc $a = pc$, et $p = pcd$. Par intégrité, il vient $cd = 1$, et donc d est inversible.

Ainsi, p est bien irréductible. □

La réciproque de cette proposition correspond en fait à l'unicité de la décomposition en facteurs irréductibles, comme le montre le théorème fondamental suivant.

Proposition 3.1.11. *Soit A un anneau intègre tel que tous ses éléments non nuls et non inversibles se décomposent en un produit fini d'éléments irréductibles.*

Cette décomposition est unique au sens de la définition 3.1.3 (et donc l'anneau est factoriel) si et seulement si pour tout élément irréductible $p \in A$ l'idéal (p) est premier.

Démonstration.

- **Le sens direct** est une sorte de lemme de Gauss : soit p un élément irréductible. Soient $a, b \in A$ tels que $ab \in (p)$. Il existe alors $c \in A$ tel que

$$ab = cp.$$

On écrit alors les décompositions en facteurs irréductibles de a et b, ce qui fournit par produit l'unique décomposition en facteurs irréductibles de ab. On fait de même avec c. Comme $ab = cp$, par unicité de la décomposition p doit apparaître dans la décomposition de ab, qui est la juxtaposition de celles de a et b. Ainsi p apparaît dans la décomposition de a ou b, ce qui revient à dire $a \in (p)$ ou $b \in (p)$. Donc (p) est premier.

- **Le sens indirect** peut se faire par récurrence sur le nombre des facteurs. On veut montrer que pour toute écriture de la forme

$$p_1 \cdots p_m = u q_1 \cdots q_n,$$

avec u une unité, les $p_1, ..., p_m, q_1, ..., q_n$ irréductibles et $m \leq n$, on a $m = n$ et les p_i et les q_i sont associés à permutation près. On raisonne donc par récurrence sur m.

  - Si $m = 0$, on a écrit $1 = u q_1 \cdots q_n$. Donc $n = 0$ car sinon q_1 serait inversible, ce qui est impossible car il est irréductible.
  - On suppose le résultat établi au rang $m-1$ pour $m \in \mathbb{N}^*$. Prenons une écriture $p_1 \cdots p_m = u q_1 \cdots q_n$. En passant dans $A/(p_1)$, on obtient

$$\overline{q_1 \cdots q_n} = \overline{0}.$$

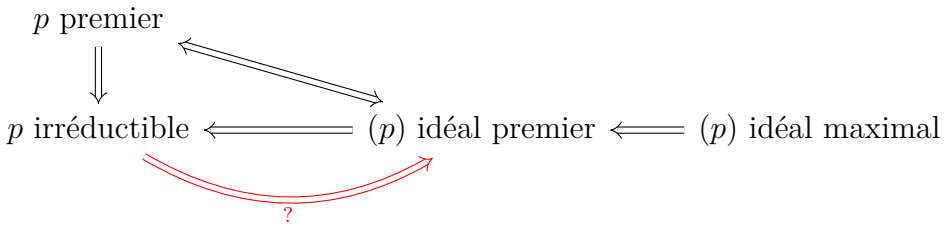
Mais (p_1) est un idéal premier par hypothèse, et il s'ensuit que $A/(p_1)$ est intègre. Donc p_1 divise l'un des q_i, disons q_1, qui lui est donc associé puisque q_1 est irréductible. On peut ainsi écrire $p_1 = v q_1$ avec v un inversible, et comme A est intègre, on a la simplification

$$p_2 \cdots p_m = uv q_2 \cdots q_n.$$

Par HR_{m-1}, les p_i et les q_i sont associés à l'ordre près, ce qui conclut quant à l'unicité.

□

En résumé, on a montré l'ensemble des implications suivantes :



La flèche rouge est équivalente à l'unicité de la décomposition en facteurs irréductibles (sous réserve d'existence).

Le cas des anneaux principaux

On montre maintenant qu'il existe une catégorie d'anneaux bien connus qui sont factoriels : ce sont les anneaux principaux. On a déjà vu à la proposition 3.1.3 que ces anneaux étaient nœthériens, ce qui donnait l'existence. Pour l'unicité, on va utiliser la notion *d'éléments premiers entre eux* ainsi que le *théorème de Bachet-Bézout*, qui permettent d'affirmer que les irréductibles sont premiers.

Définition 3.1.11 (Éléments premiers entre eux)**.** Soit A un anneau commutatif intègre. On dit que a et b sont premiers entre eux s'ils vérifient l'une des deux conditions suivantes, qui sont équivalentes.

(i) $c|a$ et $c|b \implies c \in A^\times$.

(ii) Le seul idéal principal contenant a et b est A.

Proposition 3.1.12 (Théorème de Bachet-Bézout)**.** *Soit A un anneau principal. Soient $x, y \in A$ premiers entre eux. Alors il existe a et $b \in A$ tels que*

$$ax + by = 1.$$

Autrement dit,

$$(a) + (b) = A.$$

Démonstration. Posons $I = (a) + (b)$. L'anneau A est principal, donc $I = (c)$. Mais (c) contient a et b, qui sont premiers entre eux. Donc $I = A$. On a donc bien

$$A = (a) + (b).$$

□

Or, dans un anneau principal, on peut réécrire un cas particulier du théorème de Bachet-Bézout (3.1.12) avec les idéaux.

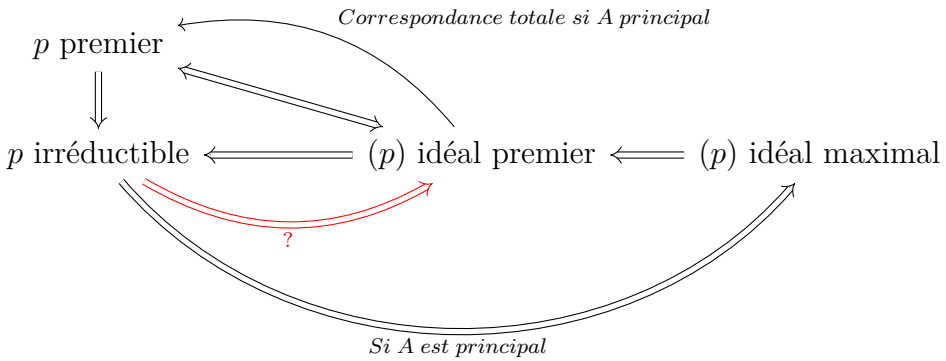
Proposition 3.1.13. *Soient A un anneau principal et $p \in A$ irréductible. Alors (p) est maximal, donc premier. En particulier, p est premier.*

Démonstration. Soit I un idéal de A contenant strictement (p). Alors on a $a \in I$ tel que $a \notin (p)$. Alors a et p sont premiers entre eux puisque p est irréductible, et par le lemme de Bézout,

$$(p) + (a) = A.$$

Mais $(p) + (a) \subset I$, et donc $I = A$. Ainsi (p) est maximal, donc premier par la propriété 3.1.8. □

Cela donne donc le diagramme d'implications suivant, où la flèche rouge correspond à l'équivalence demandée par l'unicité de la décomposition en facteurs irréductibles, d'après le théorème 3.1.11.



La flèche "correspondance totale" signifie que dans un anneau principal, les idéaux premiers sont exactement les (p) où p est un élément premier de A.

En lisant sur le diagramme, on obtient automatiquement la proposition suivante.

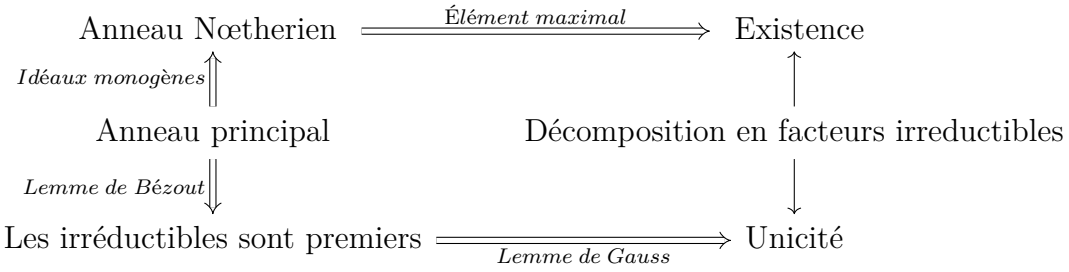
Proposition 3.1.14. *Soit A un anneau principal. Alors A est nœthérien et factoriel. De plus les idéaux maximaux de A non nuls sont exactement les idéaux premiers, et ils sont tous engendrés par un élément irréductible.*

Démonstration. On a déjà que A était nœthérien en 3.1.3. En particulier, on a l'existence d'une décomposition en facteurs irréductibles par 3.1.6.

Ensuite, A est intègre, et vérifie le critère de 3.1.11 d'après la proposition précédente (tous les idéaux (p) avec p irréductible sont premiers). Ainsi la décomposition est unique. Donc A est factoriel.

Enfin, soit (p) un idéal non nul premier de A. Par 3.1.10, p est irréductible. Mais toujours d'après le résultat précédent, (p) est maximal. Donc les notions d'idéal maximal et d'idéal premier coïncident (sauf pour $\{0\}$ qui est premier mais pas maximal), et ils sont tous engendrés par les éléments irréductibles. □

Le diagramme suivant résume les principaux arguments qu'on a utilisés jusqu'à maintenant :



On le comprend, dans le cas d'un anneau principal tout se passe merveilleusement bien en ce qui concerne la décomposition en facteurs irréductibles. En fait, comme on va le voir, même dans le cas de la décomposition en idéaux premiers il vaut mieux n'être « pas trop loin » du cas principal.

3.1.2 • Décomposition en idéaux premiers

Comme on l'a vu en introduction, certains anneaux ne vérifient pas l'équivalence « p premier $\iff$ p irréductible ». Dans ce cas, il convient de passer à la décomposition des idéaux, qui permettent selon l'expression de Ernst Kummer « d'ajouter des nombres idéaux ». On peut se convaincre que c'est le cas de certains $\mathcal{O}_K$, en reprenant par exemple l'étude de $\mathbb{Z}[i\sqrt{5}]$ évoquée en introduction.

Exemple 3.1.6. On a affirmé que dans $\mathbb{Z}[i\sqrt{5}]$, on avait les deux décompositions de 6 en éléments irréductibles :

$$6 = 2 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

Il faut donc vérifier que ces éléments sont bien irréductibles dans $\mathbb{Z}[i\sqrt{5}]$. Un moyen de le voir facilement est de regarder leur norme. On obtient immédiatement $N(2) = 4$, $N(3) = 9$, $N(1 + i\sqrt{5}) = N(1 - i\sqrt{5}) = 6$.

Mais alors, si on écrit par exemple $2 = xy$ où $x, y \in \mathbb{Z}[i\sqrt{5}]$, le passage à la norme donne $4 = N(x)N(y)$. En particulier, ces deux normes sont entières, et si l'une des deux vaut ± 1 on affaire à une racine de l'unité.

Ainsi, on cherche à savoir s'il existe des éléments de norme 2 ou 3 dans $\mathbb{Z}[i\sqrt{5}]$. Mais il suffit de dire que la norme de $a + bi\sqrt{5}$ est $a^2 + 5b^2$ pour se rendre compte que c'est impossible car a et b sont entiers.

Ainsi, $2, 3, 1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductibles, ce qui montre bien que $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

Ici, on procède d'une manière un peu différente de celle adoptée dans la section précédente. En effet, l'étude générale des anneaux de Dedekind est complexe. On pourra par exemple se référer au cours de Lionel Duclos donné à l'université de Poitiers sur le sujet [15], et qui donne un très grand nombre de résultats sur les anneaux de Dedekind. Nous avons pour notre part décidé de choisir une caractérisation de ces anneaux, qui correspond bien avec l'étude de $\mathcal{O}_K$. En l'occurrence, nous dirons qu'un anneau commutatif intègre A est de Dedekind si tous ses idéaux non nuls sont inversibles dans un certain sens. Cette condition est ici présentée comme simplement suffisante pour obtenir la décomposition en idéaux premiers. On pourrait raffiner le propos et montrer qu'elle est nécessaire, mais ce n'est pas le sujet ici.

Remarquons déjà que, comme pour la section précédente, il semble qu'il y ait confusion entre « idéal irréductible » et « idéal premier ». Mais déjà, quel serait un bon équivalent de la notion d'élément irréductible pour les anneaux ? Au vu de ce qu'on vient de voir, il s'agit naturellement du concept « d'idéal maximal »

- Un élément irréductible a n'a pour diviseurs que les ua et les u, pour $u \in A^\times$.
- Un idéal maximal n'est contenu que dans deux idéaux : lui-même et A tout entier.

On remarquera que comme on l'a noté, le passage aux idéaux fait disparaître les subtilités quant au groupe des inversibles. De plus on verra que si on a une décomposition, les notions d'idéal maximal et d'idéal premier coïncide (comme dans le cas factoriel) : on peut donc bien parler de *décomposition en idéaux premiers*.

Le propos de cette section s'organise de la manière suivante :

- Après avoir introduit les produits d'idéaux, on généralise le concept d'idéal en définissant les idéaux fractionnaires. Ces idéaux permettent de faire apparaître une structure de groupes d'idéaux, auquel il manque les inversibles. La notion d'anneau de Dedekind correspond au cas où on a bel et bien affaire à un groupe. Dans ce cas, on dispose de propriétés remarquables sur l'arithmétique des idéaux.
- On vérifie ensuite que notre définition d'anneau de Dedekind entraîne l'existence et l'unicité de la factorisation en idéaux maximaux (qui sont encore premiers dans ce cas).
- Enfin, on confronte les concepts d'anneaux factoriel et de Dedekind.

Produits d'idéaux, idéaux fractionnaires, anneau de Dedekind

On peut donc commencer par chercher une décomposition de tout idéal en produit d'idéaux premiers. Mais d'abord, qu'est-ce qu'un produit d'idéaux ?

Définition 3.1.12. Soit A un anneau commutatif. Soient I et J deux idéaux de A.

On définit le produit IJ comme l'idéal engendré sur A par les générateurs xy où $x \in I$, $y \in J$.

Autrement dit, IJ est l'ensemble des combinaisons A-linéaire finies des xy.

Par définition, IJ est un idéal de A.

En particulier, on a une notion naturelle de divisibilité.

Définition 3.1.13. Soient I et J deux idéaux de A. On dit que I divise J, noté $I|J$, s'il existe un idéal J' de A tel que $J = IJ'$.

On observe immédiatement le fait suivant.

Proposition 3.1.15. *Si $I|J$, alors $J \subset I$.*

Démonstration. Si $I|J$, alors $J = IJ'$. Mais I est un idéal, donc $IJ' \subset I$. Ainsi $J \subset I$. □

A priori, la condition donnée dans la proposition 3.1.15 n'est pas une équivalence.

Néanmoins, on aimerait beaucoup avoir des résultats plus forts analogues à la divisibilité sur $\mathbb{Z}$ par exemple. En fait, deux résultats souhaitables seraient les suivants, pour I, J et J' des idéaux de A un anneau commutatif intègre :

$$(\mathcal{P}_1) \quad IJ = IJ' \Leftrightarrow J = J'$$

$$(\mathcal{P}_2) \quad I|J \Leftrightarrow J \subset I$$

Quelle serait une bonne façon d'obtenir ces propriétés ? On voit qu'il s'agit peu ou prou à chaque fois d'« inverser » les idéaux. Essayons donc de donner une bonne définition de l'inverse d'un idéal. En fait il vaut mieux pour cela passer d'abord dans le corps des fractions de A, qui est bien défini car A est intègre.

Définition 3.1.14 (Corps de fractions)**.** Soit A un anneau commutatif intègre. On appelle corps de fractions de K le plus petit corps contenant A.

Cette construction nous permettra en passant dans K de diviser par les éléments non nuls de A. Le résultat ne sera alors pas forcément dans A. En particulier, on introduit la notion d'idéal fractionnaire qui correspond à ce type d'opérations.

Définition 3.1.15 (Idéal fractionnaire)**.** Soient A un anneau commutatif intègre et K son corps de fractions. Soit I un idéal de A. Pour tout $x \in K$ non nul, on définit xI par

$$xI = \left\{ xy \,\middle|\, y \in I \right\} \subset K.$$

On appelle idéal fractionnaire tout $x^{-1}I$ où $x \in A$ est non nul et x^{-1} l'inverse de x est dans K.

On fera bien attention qu'un idéal fractionnaire n'est en général pas un idéal de K ! En effet, K est un corps et ne contient que les idéaux $\{0\}$ et K. Pour bien différencier, on peut appeler les idéaux de A « idéaux entiers », qu'on notera I, et les fractionnaires seront notés $\mathcal{I}$. Regardons quelques exemples.

Exemple 3.1.7. Tous les idéaux entiers d'un anneau A sont fractionnaires.

Exemple 3.1.8. On se place dans l'anneau $\mathbb{Z}$, dont le corps des fractions est $\mathbb{Q}$. Les idéaux de $\mathbb{Z}$, sont les (n), on en déduit donc que les idéaux fractionaires de $\mathbb{Z}$ sont les $\frac{(n)}{m}$ où $m \in \mathbb{Z}^*$. Autrement dit il s'agit des ensembles

$$\left\{ a\frac{n}{m} \,\middle|\, a \in \mathbb{Z} \right\},$$

où $\frac{n}{m} \in \mathbb{Q}$.

On fera bien attention que dans l'écriture de 3.1.15 il n'y a aucune raison qu'il y ait unicité des membres. Par exemple pour $\mathbb{Z}$, on a $\frac{(8)}{4} = \frac{(4)}{2}$ mais $(8) \neq (4)$ et $2 \neq 4$.

Comme pour les idéaux entiers, on peut multiplier les idéaux fractionnaires. On a en fait presque une structure de groupe :

(i) La multiplication d'idéaux fractionnaires donne un idéal fractionnaire.

(ii) L'idéal A est un élément neutre.

(iii) Mais on n'a pas nécessairement existence d'un inverse...

On distingue donc les idéaux inversibles.

Définition 3.1.16. Un idéal fractionnaire $\mathcal{I}$ est dit inversible s'il existe un idéal fractionnaire $\mathcal{J}$ avec $\mathcal{I}\mathcal{J} = A$.

Cette définition permet de concevoir l'inversibilité des idéaux entiers, qui prend la forme suivante. On fera attention qu'on n'a pas du tout unicité de l'inverse avec cette définition.

Proposition 3.1.16. *Soit I un idéal entier de A. I est inversible (comme idéal fractionnaire) si et seulement s'il existe un idéal entier J de A tel que IJ est principal.*

Démonstration. Cela se déduit immédiatement du fait qu'un idéal fractionnaire s'écrit $x^{-1}J$ avec $x \in A$ et J un idéal de A. □

Remarquons de suite qu'on retrouve une intuition vue dans la section précédente : si tous les idéaux de A sont inversibles, alors A n'est pas très loin d'être principal, au sens où pour tout idéal I de A on a un idéal J tel que IJ est principal.

Cette intuition est vérifiée, et l'intérêt des idéaux inversibles est condensé dans la proposition suivante : les propriétés $\mathcal{P}_1$ et $\mathcal{P}_2$ introduites plus tôt sont valables !

Proposition 3.1.17. *Soient I, J, J' des idéaux de A intègre avec I inversible.*

- *($\mathcal{P}_1$) Si $IJ = IJ'$, alors $J = J'$*
- *($\mathcal{P}_2$) $J \subset I$ si et seulement si I divise J. Dans ce cas, il existe un unique idéal J' tel que $J = IJ'$.*

Démonstration.

- Pour la première assertion, I est inversible, donc il existe un idéal I' non nul de A tel que
$$II' = (\alpha).$$
avec $\alpha \in A$, qui est donc non nul.
Mais on sait que $IJ = IJ'$, et en multipliant par I', il vient
$$\alpha J = \alpha J'.$$
En divisant par α, on obtient bien $J = J'$.
- Pour la seconde affirmation, on a déjà vu que $I|J \implies J \subset I$.
Réciproquement, supposons $J \subset I$. On écrit à nouveau $II' = (\alpha)$. On exploitant le fait que la multiplication est commutative, on tombe sur
$$J = I(\alpha^{-1}I'J).$$
On vérifie alors que $\alpha^{-1}I'J$ est bien un idéal de A. Comme $J \subset I$ par hypothèse, on a $I'J \subset II' = (\alpha)$. Mais alors $(\alpha)^{-1}I'J \subset (1) = A$. Donc $J' = \alpha^{-1}I'J$ est bien un idéal de A.
On vient donc de montrer que $J = IJ'$, et donc que $I|J$.

- Pour l'unicité, si on a deux idéaux J' et J'' tels que $J = IJ' = IJ''$, la première assertion permet de simplifier par I et d'obtenir $J' = J''$, d'où l'unicité.

□

D'après ce qu'on vient de dire, si on suppose tous les idéaux non nuls inversibles on devrait pouvoir faire de l'arithmétique comme on le souhaite. Cela nous pousse donc à donner un nom aux anneaux qui vérifient cette propriété, qui est celui d'anneau de Dedekind (1831-1916). Il s'agit d'ailleurs de la définition historique donnée par Dedekind, puisqu'il existe beaucoup de façons équivalentes de définir ce type d'anneau.

Définition 3.1.17. On dit qu'un anneau commutatif intègre est de Dedekind si tout idéal non nul y est inversible au sens de la définition 3.1.16.

Sur les anneaux de Dedekind, on retrouve un résultat qu'on avait vu sur les anneaux principaux à la section précédente (en 3.1.14) : tous les idéaux premiers non nuls sont maximaux !

Proposition 3.1.18. *Soit A un anneau de Dedekind. Tous les idéaux premiers non nuls sont maximaux.*

Démonstration. Soit I un idéal premier non nul. On sait qu'il existe J un idéal maximal de A tel que

$$I \subset J.$$

Supposons par l'absurde que $I \neq J$. A est de Dedekind, donc ces idéaux sont inversibles car non nuls. En vertu de la $\mathcal{P}_2$ de la proposition 3.1.17,

$$J \mid I,$$

donc il existe I' un idéal de A tel que

$$I = I'J.$$

On sait déjà que $I \subset I'$. Réciproquement, on a supposé que $I \neq J$, donc on a $x \in J$ tel que $x \notin I$. Mais pour tout $y \in I'$ on sait que

$$xy \in I.$$

Comme I est premier et que $x \notin I$, $y \in I$. Finalement, on a $I = I'$, et on peut écrire

$$I = IA = IJ.$$

Comme I est inversible, la $\mathcal{P}_1$ de la propriété 3.1.17 permet de conclure que $J = A$, ce qui est absurde car J est un idéal propre. Ainsi, $I = J$ et I est maximal. □

Unicité de la décomposition dans un anneau de Dedekind

Au départ, on cherchait une décomposition des idéaux en produit d'idéaux maximaux. Dans un anneau de Dedekind, il est totalement équivalent de chercher une décomposition en idéaux premiers. Afin de conserver la terminologie de $\mathbb{Z}$, on parlera donc maintenant de décomposition en idéaux premiers. De plus, pour souligner le parallèle entre les deux cadres, nous noterons maintenant $\mathfrak{p}$ les idéaux premiers, $\mathfrak{m}$ les maximaux. Plus généralement, un idéal quelconque pourra être noté $\mathfrak{a}$. On retrouve donc des écritures familières, comme par exemple dans l'énoncé suivant, qui montre bien la pertinence des anneaux de Dedekind.

Proposition 3.1.19. *Soit A un anneau de Dedekind. Soit $\mathfrak{a}$ un idéal de A qui soit un produit d'idéaux premiers :*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

Alors, à l'ordre des facteurs près, cette décomposition est unique.

Démonstration. Soit $\mathfrak{a}$ un idéal qui s'écrit comme produit d'idéaux premiers :

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Ainsi, $\mathfrak{p}_1 | \mathfrak{q}_1 \cdots \mathfrak{q}_s$. D'après $\mathcal{P}_2$, $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subset \mathfrak{p}_1$.

On utilise alors le fait que $\mathfrak{p}_1$ est un idéal premier, ce qui implique qu'il existe un i tel que $\mathfrak{q}_i \subset \mathfrak{p}_1$. En effet, si par l'absurde ce n'est pas le cas, alors on peut se donner des $q_i \in \mathfrak{q}_i$ et $q_i \notin \mathfrak{p}_1$. Mais alors,

$$q_1 \cdots q_s \in \mathfrak{p}_1.$$

Comme $\mathfrak{p}_1$ est premier, on a (par récurrence élémentaire sur s) un indice i tel que $q_i \in \mathfrak{p}_1$: absurde.

Soit donc i tel que $\mathfrak{q}_i \subset \mathfrak{p}_1$, disons $\mathfrak{q}_1 \subset \mathfrak{p}_1$. D'après la proposition 3.1.18, on sait que les idéaux premiers sont maximaux. Donc $\mathfrak{q}_1 = \mathfrak{p}_1$. On obtient donc

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{p}_1 \cdots \mathfrak{q}_s.$$

Mais $\mathfrak{p}_1$ est inversible, on peut donc simplifier en

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

Par récurrence élémentaire, on obtient $r = s$, et les deux côtés de l'équation sont identiques. □

Ainsi, dans les anneaux de Dedekind la décomposition des idéaux en produits d'idéaux premiers est unique !

Existence de la décomposition dans un anneau de Dedekind

Qu'en est-il de l'existence d'une telle décomposition ? Dans le cas de la décomposition des éléments, on avait vu qu'il fallait demander le caractère nœthérien de l'anneau. On voit en fait que cela fonctionne ici sur la décomposition pour les idéaux, et les deux preuves sont assez semblables.

Proposition 3.1.20. *Soit A un anneau nœthérien et de Dedekind. Alors tout idéal de A s'écrit comme un produit d'idéaux premiers, qui est donc unique.*

Démonstration. Soit $\mathscr{I}$ l'ensemble des idéaux non nuls de A qui ne se factorise pas en produits d'idéaux premiers. On veut $\mathscr{I} = \emptyset$. Comme A est nœthérien, on a un élément maximal $\mathfrak{a}$ de $\mathscr{I}$, nécessairement non nul. On sait que $\mathfrak{a}$ est inclus dans un idéal maximal $\mathfrak{m}$. Par la $\mathcal{P}_2$ de la proposition 3.1.17, on sait que $\mathfrak{m}|\mathfrak{a}$. On peut donc écrire

$$\mathfrak{a} = \mathfrak{m}\mathfrak{b}.$$

En particulier, $\mathfrak{b} \subset \mathfrak{a}$. Si l'inclusion est stricte, alors $\mathfrak{b}$ n'est pas dans $\mathscr{I}$ puisque $\mathfrak{a}$ en est un élément maximal. Mais alors $\mathfrak{b}$ admet une décomposition en idéaux premiers. Reste à dire que $\mathfrak{m}$ est maximal, donc premier, et l'écriture

$$\mathfrak{a} = \mathfrak{m}\mathfrak{b}$$

fournit une écriture de $\mathfrak{a}$ comme produit d'idéaux premiers, ce qui est absurde car $\mathfrak{a} \in \mathscr{I}$. C'est la contradiction souhaitée.

Reste à écarter le cas $\mathfrak{a} = \mathfrak{b}$, c'est-à-dire

$$\mathfrak{a} = \mathfrak{m}\mathfrak{a}.$$

Mais alors, par $\mathcal{P}_1$ de la proposition 3.1.17, on peut simplifier par $\mathfrak{a}$. On obtient donc

$$\mathfrak{m} = A.$$

Or, c'est absurde car $\mathfrak{m}$ est maximal, donc distinct de A. □

Or demander qu'un anneau de Dedekind soit nœthérien est sans objet : tous les anneaux de Dedekind sont nœthériens. On montre d'abord le lemme suivant :

Proposition 3.1.21. *Soit A un anneau commutatif intègre. Soient $\mathcal{I}$ et $\mathcal{J}$ deux idéaux fractionnaires tels que $\mathcal{I}\mathcal{J} = A$. Alors $\mathcal{I}$ et $\mathcal{J}$ sont des A-modules de type fini.*

Démonstration. $\mathcal{I}$ et $\mathcal{J}$ sont bien des A-modules puisqu'ils s'écrivent $x^{-1}I$ où I est un idéal de A.

Pour le caractère fini : on sait que $1 \in \mathcal{I}\mathcal{J}$. Donc on peut écrire

$$1 = i_1 j_1 + \cdots + i_n j_n$$

avec $i_1, ..., i_n \in \mathcal{I}$ et $j_1, ..., j_n \in \mathcal{J}$.

On voit alors que $\mathcal{I} = \langle i_1, ..., i_n \rangle$ et $\mathcal{J} = \langle j_1, ..., j_n \rangle$ comme A-modules. On sait déjà que

$$\langle i_1, .., i_n \rangle \subset \mathcal{I} \quad \text{et} \quad \langle j_1, .., j_n \rangle \subset \mathcal{J}.$$

Mais on a aussi, en rappelant que le produit d'idéaux correspond à l'ensemble des combinaisons A-linéaires finies engendrées par les produits d'éléments,

$$\mathcal{J} = \mathcal{J} \cdot 1 \subset \mathcal{J} \cdot \langle i_1, ..., i_n \rangle \cdot \langle j_1, ..., j_n \rangle \subset \mathcal{J} \cdot \mathcal{I} \cdot \langle j_1, ..., j_n \rangle = A \cdot \langle j_1, ..., j_n \rangle = \langle j_1, ..., j_n \rangle.$$

De même,

$$\mathcal{I} = \langle i_1, ..., i_n \rangle.$$

□

On en déduit immédiatement :

Proposition 3.1.22. *Tout anneau A qui est de Dedekind est aussi nœthérien.*

Démonstration. Par définition, tous les idéaux non nuls de A sont inversibles, ce qui revient à dire qu'ils sont inversibles comme idéaux fractionnaires. En particulier, ils entrent dans le cadre de la définition suivante, et sont donc des A-modules de type fini. Ainsi A est nœthérien. □

On peut donc conclure par le théorème suivant. Il s'agit en fait d'une équivalence, mais on se contentera de cette simplication qui s'intègre parfaitement au cas de l'étude de $\mathcal{O}_K$.

Théorème 9. *Soit A un anneau intègre de Dedekind. Alors tout idéal de $\mathfrak{a}$ de A s'écrit de façon unique, à l'ordre des facteurs près, comme un produit d'idéaux premiers de A :*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n.$$

Le cas des anneaux principaux

Pour clore cette partie, regardons quelques exemples d'anneaux de Dedekind. De façon assez peu surprenante, les anneaux les plus « sympathiques », c'est-à-dire les principaux, sont de Dedekind.

Proposition 3.1.23. *Soit A un anneau commutatif intègre. Si A est principal, alors il est de Dedekind.*

Démonstration. Tout idéal non nul $\mathfrak{a}$ de A s'écrit $\mathfrak{a} = (a)$ et a donc pour inverse (a^{-1}), au sens des idéaux fractionnaires. □

On a une réciproque au sens suivant.

Proposition 3.1.24. *Soit A un anneau de Dedekind. Alors A est factoriel si et seulement s'il est principal.*

Démonstration. On a déjà vu un sens : si A est principal, il est factoriel. La réciproque est plus intéressante. Soit donc A un anneau de Dedekind factoriel. Soit $\mathfrak{a}$ un idéal non nul de A, et on veut montrer que $\mathfrak{a}$ est principal.

Soit $\alpha \in \mathfrak{a}$. On écrit donc $\alpha = p_1 \cdots p_n$ sa décomposition en facteurs irréductibles, car A est factoriel. Or en vertu de 3.1.11, on sait que les idéaux (p_i) sont premiers car les p_i sont irréductible. On obtient donc la factorisation

$$(\alpha) = (p_1) \cdots (p_n).$$

Or, $(\alpha) \subset \mathfrak{a}$, donc $\mathfrak{a} | (\alpha)$. Or, A est de Dedekind, donc $\mathfrak{a}$ admet une unique décomposition en idéaux premiers, qui est donc de la forme

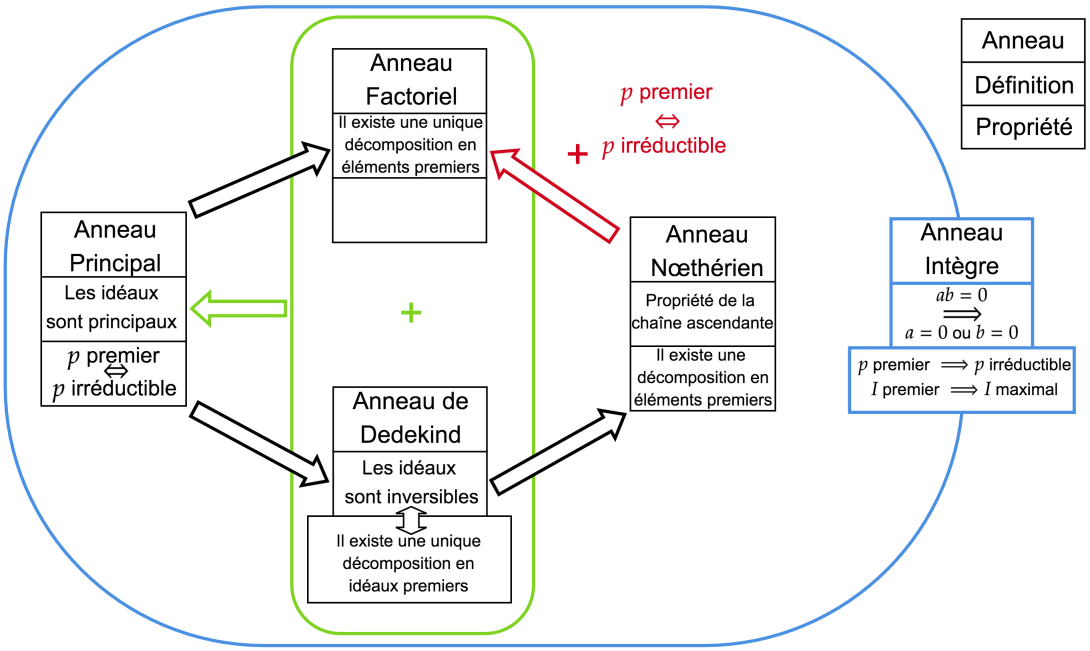
$$\mathfrak{a} = \prod_{i \in I} (p_i) = \left(\prod_{i \in I} p_i \right),$$

où I est une partie de $[\![1, n]\!]$. Ainsi $\mathfrak{a}$ est principal, et donc A aussi. □

On retiendra que les anneaux principaux sont les seuls dans lesquels on peut pratiquer des décompositions en éléments et en idéaux premiers. En particulier, cela donne l'intuition (qui sera vérifiée à la section importe) que le caractère de Dedekind d'un anneau dépend de son *manque de principalité*. Le groupe des classes en donne en quelque sorte une mesure.

Enfin, on se propose de résumer le jeu des implications sur un schéma.

- Les anneaux sont représentés par trois boîtes, contenant successivement leur nom, leur définition et une propriété fondamentale.
- Tous nos anneaux sont commutatifs et intègres, c'est pour quoi on a ajouté un cercle bleu afin de montrer que tous rentraient dans cette catégorie.
- Le cercle vert concerne l'implication verte : les deux éléments sont nécessaires.
- La flèche rouge nécessite la condition en rouge pour être valable.



3.2 Arithmétique dans $\mathcal{O}_K$

On va maintenant s'intéresser à l'arithmétique sur $\mathcal{O}_K$, en utilisant tous les résultats généraux établis à la partie précédente. L'approche adoptée ici est géométrique, et fondée sur l'utilisation du théorème de Minkowski. Elle est grandement inspirée du cours de Gaëtan Chenevier [14]. On établira successivement les résultats suivants :

- On poursuit l'approche géométrique des idéaux développée au chapitre 2, et consiste à identifier les idéaux de $\mathcal{O}_K$ à des réseaux inclus dans $\sigma(\mathcal{O}_K)$. En particulier, on définit le concept de *norme d'un idéal*, lié au volume fondamental induit par l'idéal.
- On voit alors que $\mathcal{O}_K$ est nœthérien dans la proposition 3.2.4, en généralisant l'approche géométrique de la proposition 2.2.2.

À ce stade, il faudra savoir si $\mathcal{O}_K$ est factoriel ou de Dedekind. Comme la notion d'idéal inversible se traduit très bien en termes de classe d'idéal, on s'intéressera donc à cet ensemble.

- On introduira l'ensemble des classes des idéaux à la définition 3.2.5, qui comme on l'a déjà évoqué mesure le défaut de principalité de $\mathcal{O}_K$.
- On démontrera que l'ensemble des classes est fini au théorème 10. Cela nous permettra de dire que $\mathcal{O}_K$ n'est pas très loin d'être principal.
- On en déduira que tout idéal non nul de $\mathcal{O}_K$ est inversible, ce qui montrera donc *in fine* que $\mathcal{O}_K$ est de Dedekind. C'est l'enjeu de la partie 3.2.3.

3.2.1 • Géométrie des idéaux

Ici on reprend l'approche géométrique développée dans le chapitre 2. Le théorème 2.2.4 a permis de voir que $\mathcal{O}_K \cong \mathbb{Z}^n$, où $n = [K : \mathbb{Q}]$. Ce résultat va grandement nous aider à étudier les idéaux de $\mathcal{O}_K$. On procède en deux temps :

- On observe d'abord que la preuve du théorème 2.2.4 repose fondamentalement sur le fait que $\mathcal{O}_K$ est un *ordre* de K, ce qui est aussi le cas des idéaux de $\mathcal{O}_K$. Ainsi les idéaux vont pouvoir être identifiés à des réseaux inclus dans $\sigma(\mathcal{O}_K)$.
- En particulier, il va être possible de parler du volume fondamental d'un idéal : cela va nous permettre de généraliser la notion de *norme*, qui étendra celle qu'on a déjà pour les éléments de K. On observe cela sur un exemple.

La norme des idéaux nous servira à la question suivante pour montrer le théorème de la finitude des classes. On utilisera alors le théorème de Minkowski 6.

Soit donc K un corps de nombres de dimension n. On sait que K est le corps des fractions de $\mathcal{O}_K$ (proposition 1.3.4).

La clé de cette section est d'observer qu'il existe d'autres sous-anneaux de $\mathcal{O}_K$ dont le corps des fractions est le corps de nombres K. On les appelle ordres de K.

Définition 3.2.1 (Ordre d'un corps de nombres)**.** On appelle ordre d'un corps de nombres K un sous-anneau $A \subset \mathcal{O}_K$ qui contient une $\mathbb{Q}$-base de K.

Exemple 3.2.1. En vertu de la proposition 1.3.3, $\mathcal{O}_K$ est un ordre de K.

En reprenant la preuve de 2.2.2, on observe alors qu'il est facile de la généraliser à un ordre de K quelconque. En effet, on avait vu que que $\sigma(\mathcal{O}_K)$ était un réseau de $\mathbb{R}^n$. La preuve se décomposait en deux parties :

- On montrait d'abord que $\sigma(\mathcal{O}_K)$ était un sous-groupe additif discret de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$. Cela reposait uniquement sur le fait qu'on regardait des éléments de $\mathcal{O}_K$. On obtenait donc que $\sigma(\mathcal{O}_K)$ était un sous-réseau de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.
- On utilisait ensuite le fait que $\mathcal{O}_K$ contenait une $\mathbb{Q}$-base de K pour conclure qu'il s'agissait d'un réseau.

On se rappelle de plus qu'on avait montré que

$$vol(\sigma(\mathcal{O}_K)) = 2^{-r_2} disc(\mathcal{O}_K)^{\frac{1}{2}}.$$

On comprend alors qu'on va pouvoir généraliser ce raisonnement à n'importe quel ordre de K. C'est exactement ce que dit la proposition suivante.

Proposition 3.2.1. *Soit A un ordre de K. Alors A est un $\mathbb{Z}$-module libre de type fini de rang n.*

Démonstration. La preuve est exactement identique à celle que 2.2.2. On utilise le fait que $A \subset \mathcal{O}_K$ pour le caractère discret de $\sigma(A)$, et le fait qu'il contient une $\mathbb{Q}$-base de $\mathcal{O}_K$ pour le fait que c'est un réseau.

Ainsi, $\sigma(A)$ est un réseau de $\mathbb{R}^n$, et A est un $\mathbb{Z}$-module libre de rang n. □

Cela permet aussi de généraliser la notion de discriminant pour un ordre.

Définition 3.2.2. Soit A un ordre de K. On note $disc(A)$ la valeur commune des $|disc(e_1, ..., e_n)|$ où $(e_1, ..., e_n)$ est une $\mathbb{Z}$-base de A.

Alternativement, et de façon équivalente, on peut définir

$$disc(A) = |disc(e_1, ..., e_n)| = \left(2^{r_2} vol(\sigma(A))\right)^2.$$

Élargissons encore le champ d'application de notre raisonnement ! En fait dans tout ce qui a précédé on a utilisé trois choses, pour A un ordre de K :

- $A \subset \mathcal{O}_K$.
- A est un sous-groupe additif.
- A contient une $\mathbb{Q}$-base de K.

On peut donc généraliser le théorème 3.2.1.

Proposition 3.2.2. *Soit G un sous-groupe additif de $\mathcal{O}_K$ qui contient une $\mathbb{Q}$-base de K. Alors G est un $\mathbb{Z}$-module libre de rang n.*

$$G \cong \mathbb{Z}^n.$$

On pourra donc encore généraliser la définition de discriminant à de tels G.
Cette généralisation est utile pour la propriété suivante.

Proposition 3.2.3. *Soient A un ordre de K et $I \subset A$ un idéal non nul. Alors I admet une $\mathbb{Z}$-base à n-éléments, autrement dit c'est un $\mathbb{Z}$-module libre de rang n.*

Démonstration. L'idéal I est un sous-groupe additif de $\mathcal{O}_K$, reste à voir qu'il contient une $\mathbb{Q}$-base de K.

Le sous-groupe A est un ordre : il contient une $\mathbb{Q}$-base de K $(e_1, ..., e_n)$. Mais pour $x \in I$ non nul, $(xe_1, ..., xe_n)$ est une famille de I qui est encore une $\mathbb{Q}$-base de K.

En vertu de la proposition précédente,

$$I \cong \mathbb{Z}^n.$$

□

On retrouve alors une propriété fondamentale annoncée à la section précédente, et qui donne donc l'existence d'une décomposition de tout élément de $\mathcal{O}_K$ en facteurs irréductibles.

Proposition 3.2.4. *Soit K un corps de nombres. $\mathcal{O}_K$ est un anneau nœthérien.*

Démonstration. Si les idéaux de $\mathcal{O}_K$ sont des $\mathbb{Z}$-modules libres de type fini, ils sont *a fortiori* des $\mathcal{O}_K$-modules libres de type fini puisque $\mathbb{Z} \subset \mathcal{O}_K$. Donc $\mathcal{O}_K$ est nœthérien. □

Avant toute chose, on voit que le résultat 3.2.3 a un corollaire utile pour le calcul effectif des idéaux de $\mathcal{O}_K$.

Proposition 3.2.5. *Soit I un idéal de $\mathcal{O}_K$ tel qu'il existe une famille $(e_1, ..., e_n)$ de $\mathcal{O}_K$ libre sur $\mathbb{Q}$ avec*

$$\forall i \in [\![1, n]\!] \; e_i \in I.$$

Alors l'idéal engendré par cette famille, noté $(e_1, ..., e_n)$, est I tout entier :

$$(e_1, ..., e_n) = I.$$

Démonstration. La condition dit que l'idéal $(e_1, ..., e_n)$ est inclus dans I. Mais $(e_1, ..., e_n)$ est libre sur $\mathbb{Q}$, donc est une $\mathbb{Z}$-base de I en vertu de la proposition 3.2.3. Ainsi,

$$I = \mathrm{Vect}_{\mathbb{Z}}(e_1, ..., e_n) \subset (e_1, ..., e_n) \subset I,$$

donc

$$I = (e_1, ..., e_n).$$

□

On en déduit donc la proposition suivante.

Proposition 3.2.6. *Tout idéal de $\mathcal{O}_K$ est engendré par au plus n générateurs formant une famille libre sur $\mathbb{Q}$.*

Retournons à notre approche géométrique. D'après tout ce qu'on vient de voir, pour I un idéal de $\mathcal{O}_K$, $\sigma(I)$ est un réseau de $\mathbb{R}^n$ inclus dans $\sigma(\mathcal{O}_K)$. Voyons voir ce qui se passe sur un exemple simple mais très instructif.

Exemple 3.2.2. Retournons dans notre exemple du corps de nombres $K = \mathbb{Q}(\sqrt{2})$. On avait vu à l'exemple 2.2.1 qu'on pouvait voir $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ comme le réseau de $\mathbb{R}^2$ engendré par $\left((1,1),(\sqrt{2},-\sqrt{2})\right)$. Regardons le cas de l'idéal principal $I = 2\mathcal{O}_K$ de $\mathcal{O}_K$. Ici on a donc $I = 2\mathbb{Z}[\sqrt{2}]$, qui est clairement un $\mathbb{Z}$-module libre de rang 2.

En explicitant,

$$I = \left\{ 2a + 2b\sqrt{2} \,\middle|\, a, b \in \mathbb{Z} \right\}.$$

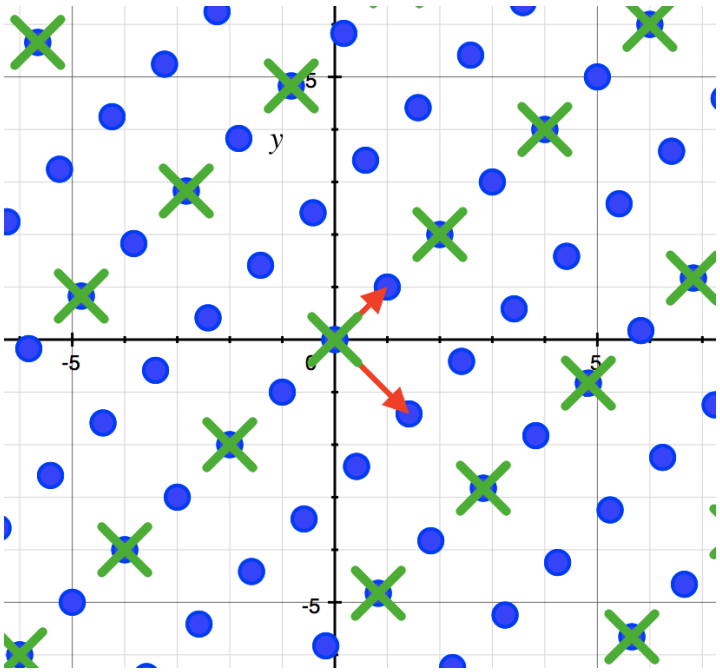
Rappelons qu'on avait l'expression du plongement canonique dans ce cas.

$$\sigma \;:\; \begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \to & \mathbb{R}^2 \\ a + b\sqrt{2} & \mapsto & (a + b\sqrt{2}, a - b\sqrt{2}). \end{array}$$

Ainsi on a

$$\sigma(I) = \left\{ \left(2a + 2b\sqrt{2}, 2a - 2b\sqrt{2}\right) \,\middle|\, a, b \in \mathbb{Z} \right\} = 2\sigma(\mathcal{O}_K).$$

On retrouve bien le fait que $\sigma(I)$ est un réseau de $\mathbb{R}^2$ inclus dans le réseau $\sigma(\mathcal{O}_K)$. On le visualise sur la figure suivante avec des croix vertes, en surimposition du réseau initial $\sigma(\mathcal{O}_K)$:



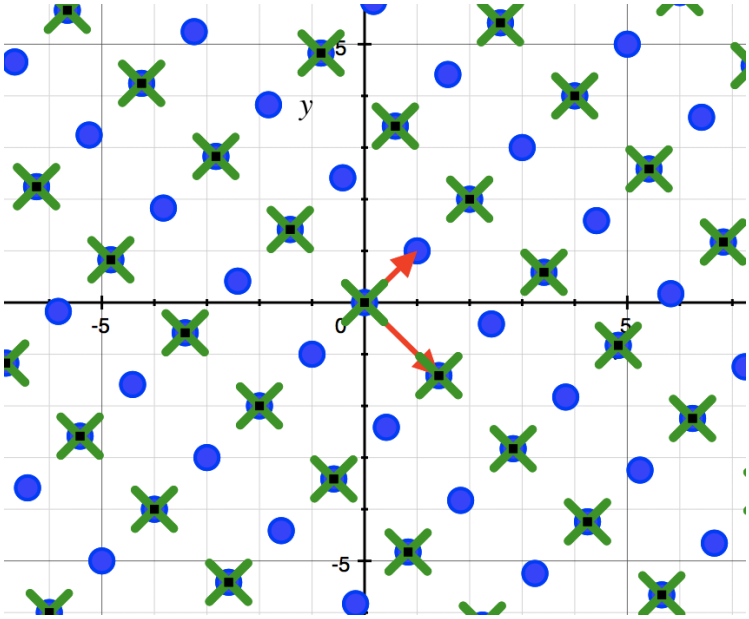
Regardons maintenant un autre idéal principal de $\mathcal{O}_K$, $I' = \sqrt{2}\mathcal{O}_K = \sqrt{2}\,\mathbb{Z}[\sqrt{2}]$.
Là encore on peut expliciter

$$I' = \left\{ 2a + \sqrt{2}b \,\middle|\, a, b \in \mathbb{Z} \right\}.$$

En particulier on remarque que $I \subset I'$.
Cette fois on a l'expression du $\sigma(I')$:

$$\sigma(I') = \left\{ \left(2a + \sqrt{2}b, 2a - \sqrt{2}b\right) \,\middle|\, a, b \in \mathbb{Z} \right\}.$$

On visualise à nouveau ce que cela donne en surimposition de $\sigma(\mathcal{O}_K)$, ici encore avec des croix vertes :



Le réseau $\sigma(I')$ fournit donc un maillage plus fin que $\sigma(I)$ dans $\sigma(\mathcal{O}_K)$. Si on voulait donner une mesure quantitative du gain de précision, on pourrait comparer les volumes fondamentaux des deux réseaux. En calculant les déterminants des $\mathbb{Z}$-bases on obtient :

- $\Big((2,2),(2\sqrt{2},-2\sqrt{2})\Big)$, $\mathbb{Z}$-base de $\sigma(I) \implies vol(\sigma(I)) = 8\sqrt{2}$.
- $\Big((2,2),(\sqrt{2},-\sqrt{2})\Big)$, $\mathbb{Z}$-base de $\sigma(I') \implies vol(\sigma(I')) = 4\sqrt{2}$.

Ainsi,

$$\frac{vol(\sigma(I))}{vol(\sigma(I'))} = 2.$$

Comme interpréter cette valeur ? On voit qu'elle correspond au nombres de copies distinctes de $\sigma(I)$ qu'on peut placer dans $\sigma(I')$: la première est $\sigma(I)$ lui-même, la seconde peut s'obtenir en décalant l'origine au point $(\sqrt{2},-\sqrt{2})$. Fondamentalement, on retrouve le fait que

$$|I'/I| = 2.$$

En effet, tout élément de $I' = \{2a + \sqrt{2}b \,|\, a,b \in \mathbb{Z}\}$ peut s'écrire sous la forme

$$2a + b\sqrt{2} = 2a + 2c\sqrt{2} + \epsilon\sqrt{2},$$

où $\epsilon \in \{0,1\}$ selon la parité de b. On a donc bien $|I'/I| = 2$ comme prévu.

L'exemple précédent indique que les idéaux induisent des réseaux inclus dans le réseau $\sigma(\mathcal{O}_K)$ et que les quotients des volumes donnent des indications sur les cardinaux des groupes de classes. On généralise cette observation dans la proposition suivante.

Proposition 3.2.7. *Soient A et B deux sous-groupes additifs de $\mathcal{O}_K$ tels que $A \subset B$ et que A contient une $\mathbb{Q}$-base de K.*

Alors, A est d'indice fini dans B et cet indice vaut

$$|B/A| = \frac{|disc(A)|^{\frac{1}{2}}}{|disc(B)|^{\frac{1}{2}}} = \frac{vol(\sigma(A))}{vol(\sigma(B))}.$$

Démonstration. $A \subset B$ et $\sigma(A)$ et $\sigma(B)$ sont des réseaux de $\mathbb{R}^n$. On en déduit que pour D_A un domaine fondamental de $\sigma(A)$:

$$\sigma(B) = \bigcup_{e \in \sigma(B) \cap D_A} (\sigma(A) + e).$$

Comme σ est un isomorphisme, que $|B/A|$ est fini (car $\sigma(B)$ est discret et D_A borné), on a alors l'expression

$$|B/A| = |\sigma(B) \cap D_A|.$$

Enfin, notons D_B un domaine fondamental de B, et montrons que la partie D définie par

$$D = \bigcup_{e \in \sigma(B) \cap D_A} (D_B + e).$$

est un volume fondamental de $\sigma(A)$. Cela se voit simplement par

$$\begin{aligned} \bigcup_{\lambda \in \sigma(A)} (\lambda + D) &= \bigcup_{e \in \sigma(B) \cap D_A} \bigcup_{\lambda \in \sigma(A)} (\lambda + D_B + e) \\ &= \bigcup_{\lambda \in \sigma(B)} (\lambda + D_B) \\ &= \mathbb{R}^n. \end{aligned}$$

Ainsi, comme l'union est disjointe, par additivité de la mesure de Lebesgue μ :

$$vol(\sigma(A)) = \mu\left(\bigcup_{e \in \sigma(B) \cap D_A} (D_B + e) \right) = |B/A| vol(\sigma(B)).$$

Ainsi, on exploitant l'expression du discriminant obtenue précédemment,

$$|B/A| = \frac{vol(\sigma(A))}{vol(\sigma(B))} = \frac{|disc(A)|^{\frac{1}{2}}}{|disc(B)|^{\frac{1}{2}}}.$$

□

Ce résultat s'applique en particulier pour $B = \mathcal{O}_K$ et I un idéal de $\mathcal{O}_K$ en vertu de la proposition précédente, donc $|\mathcal{O}_K/I|$ est fini. On peut donc définir la notion de norme d'un idéal.

Définition 3.2.3. Soit I un idéal de $\mathcal{O}_K$. On appelle norme de I, notée $\mathcal{N}(I)$, la valeur $|\mathcal{O}_K/I|$. Il s'agit donc de la $\frac{vol(\sigma(I))}{vol(\sigma(\mathcal{O}_K)}$

Le terme « norme » n'a pas été choisi au hasard, et on retombe en fait sur la définition de la norme d'un élément de $\mathcal{O}_K$ dans le cas d'un idéal principal.

Proposition 3.2.8. *Soit $x \in \mathcal{O}_K$ non nul.*

$$|N(x)| = \mathcal{N}(x\mathcal{O}_K).$$

Démonstration. On rappelle que si $(e_1, ..., e_n)$ est une $\mathbb{Z}$-base de $\mathcal{O}_K$, alors on a défini le discriminant de $\mathcal{O}_K$ par :

$$disc(\mathcal{O}_K) = disc(e_1, ..., e_n) = \det\left((\mathrm{Tr}(e_i e_j))_{1\leq i,j\leq n}\right) = \det\left((\sigma_i(e_j))_{1\leq i,j\leq n}\right)^2,$$

où l'on exploite le corollaire 1.5.2. Mais $(xe_1, ..., xe_n)$ est une $\mathbb{Z}$-base de l'idéal $x\mathcal{O}_K$, et donc

$$\begin{aligned} disc(x\mathcal{O}_K) = disc(xe_1, ..., xe_n) &= \det\left((\sigma_i(xe_j))_{1\leq i,j\leq n}\right)^2 \\ &= \prod_{i=1}^{n} |\sigma_i(x)|^2 \det\left((\sigma_i(e_j))_{1\leq i,j\leq n}\right)^2 \\ &= |N(x)|^2 disc(\mathcal{O}_K), \end{aligned}$$

où on utilise l'expression de la norme donnée par 1.5.1. Mais alors par la proposition précédente,

$$|\mathcal{O}_K/x\mathcal{O}_K| = \frac{|disc(x\mathcal{O}_K)|^{\frac{1}{2}}}{|disc(\mathcal{O}_K)|^{\frac{1}{2}}} = |N(x)|.$$

On a donc bien

$$|N(x)| = \mathcal{N}(x\mathcal{O}_K).$$

□

La norme d'un idéal ne passe a priori pas au produit, sauf dans un cas particulier : celui des idéaux premiers entre eux.

Définition 3.2.4. Soit A un anneau commutatif. Deux idéaux I et J de A sont dits premiers entre eux si $I + J = A$.

Il est bien connu que dans ce cas on dispose du théorème des restes chinois généralisé. Il nous permet d'obtenir le résultat suivant.

Proposition 3.2.9. *Soient $\mathfrak{p}$ et $\mathfrak{q}$ deux idéaux premiers entre eux de $\mathcal{O}_K$. On a alors*

$$\mathcal{N}(\mathfrak{pq}) = \mathcal{N}(\mathfrak{p})\mathcal{N}(\mathfrak{q}).$$

Démonstration. Comme $\mathfrak{p}$ et $\mathfrak{q}$ sont premiers entre eux, on sait qu'on a un isomorphisme

$$\mathcal{O}_K/(\mathfrak{p}\cap\mathfrak{q}) = \mathcal{O}_K/(\mathfrak{pq}) \cong (\mathcal{O}_K/\mathfrak{p}) \times (\mathcal{O}_K/\mathfrak{q}).$$

En passant au cardinal,

$$|\mathcal{O}_K/(\mathfrak{pq})| = |\mathcal{O}_K/\mathfrak{p}||\mathcal{O}_K/\mathfrak{q}|.$$

C'est exactement la définition de la norme. Ainsi,

$$\mathcal{N}(\mathfrak{pq}) = \mathcal{N}(\mathfrak{p})\mathcal{N}(\mathfrak{q}).$$

□

Cette propriété se généralise par récurrence à un produit de k idéaux premiers entre eux. On remarquera en particulier que c'est vrai si $\mathfrak{p}$ et $\mathfrak{q}$ sont deux idéaux maximaux distincts.

A ce stade, on n'a pas en général pour deux idéaux I et J de $\mathcal{O}_K$, $\mathcal{N}(IJ) = \mathcal{N}(I)\mathcal{N}(J)$, mais on verra bientôt que c'est vrai.

3.2.2 • Finitude des classes

Maintenant que la géométrisation des idéaux est achevée, on va s'intéresser au caractère de Dedekind ou non de $\mathcal{O}_K$. Pour ce faire, on introduit l'ensemble des classes de l'anneau. En effet, on a vu qu'il nous fallait montrer que $\mathcal{O}_K$ n'était pas très loin d'être principal, ce qui correspond ici au fait que ses idéaux non nuls sont inversibles. Il est alors utile de quotienter l'ensemble des idéaux par la relation d'équivalence suivante, qui fournit une caractérisation simple du fait d'être de Dedekind pour un anneau (cf proposition 3.2.12) :

Définition 3.2.5 (Relation d'équivalence)**.** Deux idéaux I et J de A sont dits équivalents, ce qui est noté $I \sim J$, s'il existe $a, b \in A$ non nuls tels que $aI = bJ$. Cela revient à dire qu'il existe $x \in K^*$ tel que $xI = J$.

$\sim$ définit une relation d'équivalence sur les idéaux non nuls de A, et on note $Cl(A)$ l'ensemble de ses classes.

Le fait qu'il s'agisse d'une relation d'équivalence est évident, et on voit qu'avec nos notations $\frac{a}{b} \in K^*$, ce qui justifie la deuxième définition.

On observe que cette relation d'équivalence fournit une caractérisation simple des idéaux principaux.

Proposition 3.2.10. *Un idéal non nul I de A est principal si et seulement si $I \sim A$.*

On en déduit immédiatement que A est principal si et seulement si $|Cl(A)| = 1$.

Démonstration. Le sens indirect est évident puisque pour $I = (a) = aA$, on a bien sûr $aA \sim A$.

Réciproquement, si $I \sim A$, alors $I = zA$ où $z \in K^*$. Mais alors, comme $1 \in A$ on a $z \in I \subset A$. Donc $I = zA$ est principal. □

En quelque sorte, la taille de l'ensemble des classes mesure le défaut de primalité de l'anneau. Cet ensemble n'est pas très loin d'être un groupe, car le produit passe bien sur l'ensemble des classes et permet de le munir d'une loi de composition interne.

Proposition 3.2.11. *La multiplication des idéaux induit une loi de composition interne sur $Cl(A)$. Cette loi est commutative est associative, et son élément neutre est la classe de A, c'est-à-dire la classe des idéaux principaux.*

Démonstration. Soient I, I', J, J' des idéaux de A avec $I \sim I'$ et $J \sim J'$. On vérifie que $IJ \sim I'J'$.

Par définition, il existe x et $y \in K^\times$ tels que $I = xI'$ et $J = yJ'$. Mais alors $IJ = (xy)I'J'$. Mais $xy \in K^\times$, donc $IJ \sim I'J'$.

Ensuite, le caractère commutatif et associatif de cette loi provient des propriétés de la multiplication sur K.

Enfin, soit (x) un idéal principal non nul de A. Comme $(x)I{=}xI$, on a immédiatement $(x)I \sim I$, et classe des idéaux principaux est bien un élément neutre pour la loi de multiplication. □

On a l'inversibilité si et seulement si l'anneau est de Dedekind :

Proposition 3.2.12. *Soit A un anneau commutatif intègre. Alors A est de Dedekind si et seulement si $Cl(A)$ est un groupe, ce qui revient à dire que tous ses éléments sont inversibles.*

Démonstration. Si A est de Dedekind, alors tous les idéaux non nuls sont inversibles, c'est-à-dire que pour tout idéal I de A on a un idéal J de A tel que IJ est principal. Ainsi $\overline{IJ} = \overline{A}$ dans $Cl(A)$, $\overline{I}$ est inversible.

Réciproquement, si I est un idéal non nul, alors $\overline{I}$ est un élément de $Cl(A)$, qui est un groupe. Donc il existe $\overline{J} \in Cl(A)$ tel que $\overline{IJ} = \overline{1}$, c'est-à-dire que IJ est principal. Donc I est inversible. □

Notre but va donc être d'étudier $Cl(A)$ dans le cas $A = \mathcal{O}_K$. On raisonne en fait en deux étapes :

- On voit d'abord que dans le cas de $\mathcal{O}_K$, l'ensemble des classes est fini : c'est l'enjeu du théorème 10 dont le reste de cette sous-section est une démonstration.
- La sous-section suivante en déduit que l'ensemble des classes est un groupe, et donc que $\mathcal{O}_K$ est de Dedekind.

Venons-en à la structure de la preuve du théorème de la finitude du nombre des classes. Elle procède en trois temps :

- La proposition 3.2.13 exploite le caractère géométrique des idéaux ainsi que le théorème de Minkowski pour montrer que dans tout idéal I, on a un élément de petite norme x, au sens où $N(x) \leq \mathcal{N}(I)$ avec C une constante ne dépendant que de $\mathcal{O}_K$.
- Cet élément permet de fabriquer un nouvel idéal, équivalent à I, et contenant un petit nombre entier. En effet, $x\mathcal{O}_K$ définit un réseau inclus dans I, et le rapport $N = \frac{vol(\sigma(x\mathcal{O}_K)}{vol(I)}$ est borné par C et entier. On vérifie alors que $\frac{N}{x}I$ est un idéal de $\mathcal{O}_K$ contenant N.

- Reste à voir qu'il y a un nombre fini d'idéaux de $\mathcal{O}_K$ contenant un nombre entier donné, ce qui achève la démonstration.

Reste donc à démontrer tous ces résultats.

Proposition 3.2.13. *Il existe $C > 0$ tel que pour tout idéal I de $\mathcal{O}_K$ non nul il existe $x \in I$ non nul tel que*

$$|N(x)| \leq C\mathcal{N}(I).$$

Dans les faits, la valeur $C = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{disc(\mathcal{O}_K)} = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} 2^{r_2} vol(\sigma(\mathcal{O}_K))$ convient.

Démonstration. Il s'agit d'appliquer le théorème de Minkoswki (6) au réseau $\sigma(I)$ de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

Pour tout $t > 0$, on définit le sous-ensemble C_t de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ par

$$C_t = \left\{(x_1, ..., x_{r_1+r_2}) \in \mathbb{R}_1^r \times \mathbb{C}_2^r \,\middle|\, \sum_{i=1}^{r_1} |x_i| + 2\sum_{i=r_1+1}^{r_1+r_2} |x_i| \leq t\right\}.$$

On voit facilement que C_t est symétrique convexe, et $\mu(C_t) = Mt^n$ où M est une constante dépendant de n et de r_1 et r_2.

On observe alors le fait suivant : par convexité, pour $(x_1, ..., x_{r_1+r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, on a

$$|N(x)|^{1/n} = \left(\prod_{i=1}^{r_1} |x_i| \prod_{i=r_1+1}^{r_1+r_2} |x_i|^2\right) \leq \frac{1}{n}\left(\sum_{i=1}^{r_1} |x_i| + 2\sum_{i=r_1+1}^{r_1+r_2} |x_i|\right).$$

où l'on a exploité le fait qu'on avait ordonné les plongements complexes dans le plongement canonique pour avoir tous les conjugués.

Autrement dit, pour $x \in I$, on a

$$\sigma(x) \in C_t \Longrightarrow |N(x)| \leq n^{-n}t^n.$$

Reste à choisir t tel que $\mu(C_t) = Mt^n = 2^n vol(\sigma(I))$.

Par le théorème de Minkowski, on dispose de $x \in I$ non nul tel que $\sigma(x) \in C_t$. Ainsi,

$$|N(x)| \leq n^{-n}t^n \leq M' vol(\sigma(I)),$$

où M' est encore une constante.

Enfin,

$$vol(\sigma(I)) = \frac{disc(\sigma(I))^{\frac{1}{2}}}{2^{r_2}} = |\mathcal{O}_K/I| \frac{disc(\sigma(\mathcal{O}_K))^{\frac{1}{2}}}{2^{r_2}} = \mathcal{N}(I) vol(\mathcal{O}_K)$$

en exploitant la proposition 3.2.7.

Finalement, comme $vol(\mathcal{O}_K)$ est constant, on peut bien écrire qu'on a trouvé $x \in I$ non nul avec

$$|N(x)| \leq C\mathcal{N}(I),$$

où C est indépendante de I. □

Dans la proposition précédente on a caché le calcul de C qui n'est pas très instructif, mais c'est ainsi qu'on peut retrouver la valeur indiquée dans la proposition. Regardons ce que cela donne pour un exemple.

Exemple 3.2.3. On repart dans $K = \mathbb{Q}(\sqrt{2})$ et on prend l'idéal principal $I = \sqrt{2}\mathcal{O}_K$. La force de la proposition précédente est de donner un C indépendant de l'idéal choisi. Ici, comme on sait qu'en vertu de la proposition 3.2.8 on a $|N(\sqrt{2})| = \mathcal{N}(I) = 2$, on a juste besoin de $C \geq 1$.

Ici $n = 2, r_1 = 2, r_2 = 0$. Donc $\sigma = (\sigma_1, \sigma_2)$. En particulier pour $x \in \mathcal{O}_K$ on a $|N(x)| = |\sigma_1(x)||\sigma_2(x)|$.

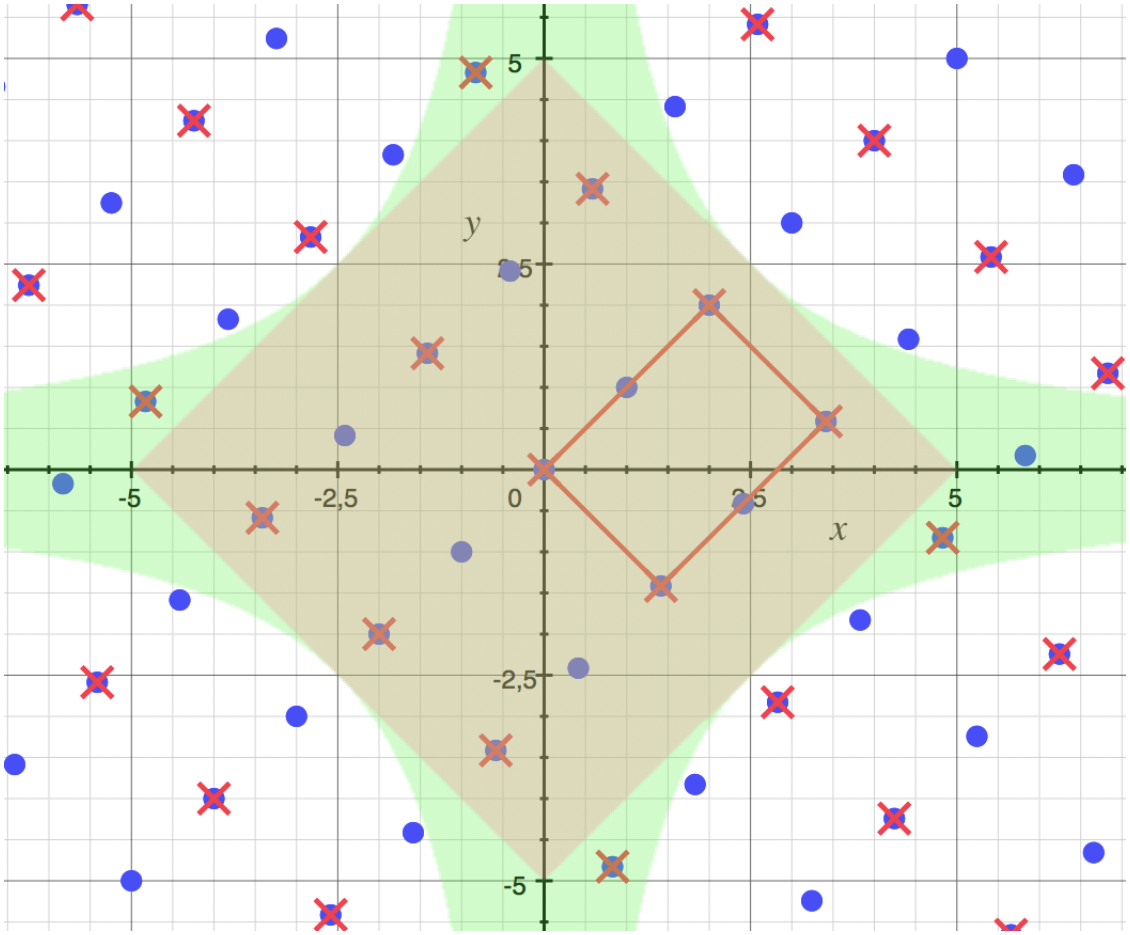
De plus, C_t est un carré d'aire t^2 : avec les notations de la preuve $M = 1$.

Enfin, on avait vu que $vol(\sigma(I)) = 4\sqrt{2}$. On cherche donc t tel que

$$t^2 \geq 2^2 4\sqrt{2} \simeq 23.$$

On constate que $t = 5$ convient. La figure suivante présente la situation. On a :

- Le réseau $\sigma(\mathcal{O}_K)$ représenté par les points bleus.
- Le réseau $\sigma(I)$ représenté par les croix rouges.
- Le rectangle rouge est un domaine fondamental de $\sigma(I)$.
- L'aire rouge est C_t pour $t = 5$.
- L'aire verte correspond aux points (x, y) avec $|x||y| \leq n^{-n}t^n = 6.25$, qui sert donc à mesurer la norme des éléments de $\mathcal{O}_K$.

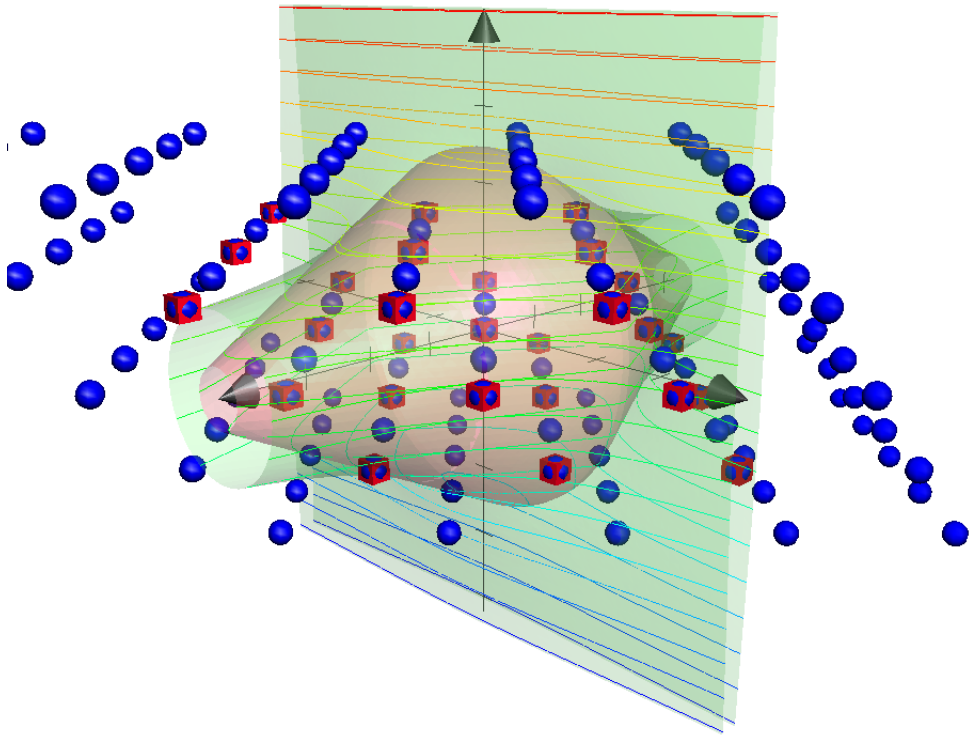


Le théorème de Minkowski assure qu'il existe un $x \in I$ non nul tel que $\sigma(x) \in C_t$. Ici on voit que c'est bien le cas. L'aire rouge étant incluse dans l'aire verte, on peut affirmer qu'un tel x vérifie

$$|N(x)| \leq 6.25.$$

Ici on a un peu triché en choisissant par commodité un t entier, ce qui nous amène à trouver une borne pour la norme trop haute (6.25, alors qu'on aurait pu avoir $2 = \sqrt{2}\mathcal{N}(I)$). Néanmoins les choses sont plus visibles sur la figure avec ce choix.

Exemple 3.2.4 (Et en trois dimensions ?)**.** Le lecteur avide de sensations fortes pourra regarder l'exemple de $K = \mathbb{Q}(\sqrt[3]{2})$ qui fournit un exemple en trois dimensions. On a repris le même code couleur, avec l'idéal $\sqrt[3]{2}\mathcal{O}_K$ représenté avec des carrés rouges.



Cette propriété est très utile car elle nous permet d'aller chercher dans tout idéal un élément de *petite norme*. On va pouvoir en déduire le théorème de la finitude des classes $Cl(\mathcal{O}_K)$. Juste avant d'en arriver là, déduisons-en le corollaire suivant.

Proposition 3.2.14. *Il existe $C > 0$ tel que pour tout idéal I de $\mathcal{O}_K$ il existe $x \in I$ tel que $|I/x\mathcal{O}_K| \leq C$.*

Démonstration. On prend le même C qu'à la proposition précédente. Soit I un idéal de $\mathcal{O}_K$. On dispose d'un $x \in I$ non nul tel que

$$|N(x)| \leq C\mathcal{N}(I).$$

Comme $x\mathcal{O}_K \subset I$, on peut écrire

$$\begin{aligned} & |\mathcal{O}_K/x\mathcal{O}_K| = |\mathcal{O}_K/I||I/x\mathcal{O}_K|, \\ \text{d'où} \quad & |N(x)| = \mathcal{N}(I)|I/x\mathcal{O}_K|, \\ \text{d'où} \quad & |I/x\mathcal{O}_K| \leq C. \end{aligned}$$

□

On en déduit le théorème fondamental suivant, qui fait le lien avec la relation d'équivalence sur les idéaux d'un ordre de K qu'on avait posée plus tôt. Ici on se contente de l'énoncer pour un ordre particulier : $\mathcal{O}_K$, mais elle est valable pour tout ordre.

Théorème 10 (Finitude des classes)**.** *$Cl(\mathcal{O}_K)$ est fini.*

Démonstration. Soit I un idéal non nul de $\mathcal{O}_K$. Par la proposition précédente, on dispose d'un $x \in I$ non nul tel que

$$|I/x\mathcal{O}_K| \leq C,$$

où C est indépendant de I. Notons N le cardinal de $I/x\mathcal{O}_K$. Le théorème de Lagrange dit que N annule $I/x\mathcal{O}_K$. Autrement dit,

$$NI \subset x\mathcal{O}_K,$$
$$\text{donc} \quad \frac{N}{x} I \subset \mathcal{O}_K.$$

De plus $N = \frac{N}{x}x \in \frac{N}{x}I$. On a donc aussi $N\mathcal{O}_K \subset \frac{N}{x}I$. Finalement,

$$N\mathcal{O}_K \subset \frac{N}{x} I \subset \mathcal{O}_K.$$

Regardons alors l'idéal de $\mathcal{O}_K$ suivant : $J = \frac{N}{x}I$. On a $I \sim J$ puisque $xJ = NI$ et $N \in \mathbb{Z} \subset \mathcal{O}_K$.

De plus $N\mathcal{O}_K \subset J$, donc $N \in J$. Mais il n'y a qu'un nombre fini d'idéaux J de $\mathcal{O}_K$ tels que $N \in J$. En effet,

$$\mathcal{O}_K/N\mathcal{O}_K \cong (\mathbb{Z}/N\mathbb{Z})^n,$$

et $(\mathbb{Z}/N\mathbb{Z})^n$ est fini. Or, on a par la propriété universelle du quotient une correspondance entre les idéaux de $\mathcal{O}_K$ contenant $N\mathcal{O}_K$ (donc contenant N) et les idéaux de $\mathcal{O}_K/N\mathcal{O}_K$. Or ces idéaux sont en nombre fini. Ainsi, l'ensemble des classes $Cl(\mathcal{O}_K)$ est fini. □

À ce stade, on peut s'arrêter un moment et s'intéresser au groupe des classes de quelques anneaux d'entiers algébriques. L'exemple le plus simple possible est le suivant.

Exemple 3.2.5 (Le cas de $\mathbb{Z}$)**.** Si on se place dans $K = \mathbb{Q}$ et donc $\mathcal{O}_K = \mathbb{Z}$, c'est un fait bien connu que les tous les idéaux de $\mathbb{Z}$ sont principaux, donc de la forme $I = (n)$. Or on a vu que les idéaux principaux appartenaient tous à la même classe, celle de $\mathbb{Z}$. Ainsi,

$$|Cl(\mathcal{O}_K)| = 1.$$

Ici notre anneau est donc principal : tous ses idéaux sont principaux (et $\mathbb{Z}$ est intègre). On peut légitimement se demander si c'est le cas pour tous nos anneaux d'entiers algébriques, mais on aurait raison de croire que les choses ne sont pas aussi simples ! Essayons donc de nous convaincre que ce n'est pas le cas sur quelques exemples.

En observant la preuve du théorème 10 qui précède, on voit qu'on vient en fait de démontrer le fait suivant, qui est en pratique très commode pour déterminer l'ensemble des classes des idéaux de $\mathcal{O}_K$.

Proposition 3.2.15. *Dans toute classe d'idéaux de $\mathcal{O}_K$ il existe un idéal qui contient un nombre entier inférieur à* $\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{disc(\mathcal{O}_K)} = \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}2^{r_2}vol(\sigma(\mathcal{O}_K))$.

Une méthode générale va donc être de calculer cette valeur puis de chercher tous les idéaux contenant des nombres plus petits que cette borne. Il ne restera plus ensuite qu'à voir si à combien de classes distinctes appartiennent ces idéaux pour conclure. On va regarder ce que cela donne pour de petits exemples. Prenons par exemple le cas des $K = \mathbb{Q}(\sqrt{d})$. On avait alors vu que

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{si } d \equiv 1[4] \\ \mathbb{Z}[\sqrt{d}] & \text{si } d \equiv 2 \text{ ou } 3[4]. \end{cases}$$

$\mathcal{O}_K$ est donc ici toujours de la forme $\mathbb{Z}[\omega]$, et admet pour $\mathbb{Z}$-base $(1, \omega)$. Dans notre cas, où $d > 0$, on a deux plongements réels et aucun complexe : $r_1 = 2, r_2 = 0, n = 2$. Ainsi, il ne nous reste plus qu'à calculer $disc(\mathcal{O}_K)$. On rappelle les différentes formules dont l'on dispose pour cette quantité : si $(e_1, ..., e_n)$ est une $\mathbb{Z}$-base de $\mathcal{O}_K$, alors on a défini le discriminant de $\mathcal{O}_K$ par

$$disc(\mathcal{O}_K) = disc(e_1, ..., e_n) = \det\left((\mathrm{Tr}(e_i e_j))_{1\leq i,j\leq n}\right) = \det\left((\sigma_i(e_j))_{1\leq i,j\leq n}\right)^2.$$

La dernière expression est très simple ici, puisqu'on connaît exactement l'expression de nos plongements (qui sont l'identité et l'unique conjugaison). De façon très générale, on a donc

$$disc(\mathcal{O}_K) = \begin{vmatrix} 1 & \omega \\ 1 & \sigma(\omega) \end{vmatrix}^2.$$

On peut donc en déduire des formules explicites :

$$disc(\mathcal{O}_K) = \begin{cases} \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = d & \text{si } d \equiv 1[4], \\ \\ \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4d & \text{si } d \equiv 2 \text{ ou } 3[4]. \end{cases}$$

Enfin, on regarde notre formule de la propriété 3.2.15, et on observe que $\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n} = \frac{1}{2}$. On peut donc reformuler notre proposition dans le cas très particuliers des $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

Proposition 3.2.16. *Soit d un entier naturel qui n'est pas un carré. Dans toute classe d'idéaux de $\mathcal{O}_K$ il existe un idéal qui contient un nombre entier inférieur à*

$$\begin{cases} \frac{\sqrt{d}}{2} & \textit{si } d \equiv 1[4], \\ \sqrt{d} & \textit{si } d \equiv 2 \textit{ ou } 3[4]. \end{cases}$$

On observe alors immédiatement le corollaire-exemple suivant.

Exemple 3.2.6. Les anneaux des entiers de $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ et $\mathbb{Q}(\sqrt{5})$ sont principaux. En effet, on observe par la propriété 3.2.16 que toute classe d'idéaux de ces anneaux contient un idéal contenant un entier plus petit que $\sqrt{2}$, $\sqrt{3}$ et $\frac{\sqrt{5}}{2}$ respectivement, qui sont tous trois strictement plus petits que 2. Ainsi, toute classe contient un idéal contient 1, c'est-à-dire $\mathcal{O}_K$ tout entier. L'unique classe est donc celle des idéaux principaux : $|Cl(\mathcal{O}_K)| = 1$.

Cette méthode va être mise en défaut à partir de $d = 6$. En effet, la borne donnée par la propriété 3.2.16 est $\sqrt{6} \approx 2,45$. Ainsi, notre résultat affirme que toute classe d'idéaux contient un idéal qui contient 1 ou 2. Bien sûr, on n'est pas assurés qu'un idéal qui contient 2 soit toujours principal. On observe que c'est néanmoins le cas pour $d = 6$ et $d = 7$, mais plus pour $d = 8$, qui nous fournit donc notre premier exemple d'anneaux d'entiers algébriques non principal. Dans la suite, on va traiter simplement ces trois petits exemples. Il existe des méthodes très efficaces pour déterminer l'ensemble des idéaux contenant un nombre premier donné (ici 2). Le lecteur intéressé pourra se reporter à la proposition 6.10 du cours de théorie algébrique des nombres de Gaëtan Chenevier [14], dont on s'inspire pour la méthode utilisée ci-dessous.

Exemple 3.2.7 (Le cas de $\mathbb{Q}(\sqrt{6})$**.** Ici $6 \equiv 2[4]$, donc $\mathcal{O}_{\mathbb{Q}(\sqrt{6})} = \mathbb{Z}[\sqrt{6}]$. Soit I un idéal de $\mathbb{Z}[\sqrt{6}]$. On souhaite montrer que I est principal. A priori, on a déjà l'inclusion $(2) \subset I$. On élimine le cas $(2) = I$, qui est un cas où I est principal. On a alors un élément

$$z = a + b\sqrt{6} \in I \text{ avec } a \text{ et } b \text{ non tous les deux pairs.}$$

Mais $(2) \subset I$, donc en particulier $2c$ et $2(c + c\sqrt{6}) \in I$ pour $c \in \mathbb{Z}$, et ainsi $2c\sqrt{(6)} \in I$. On peut donc soustraire à z les quantités $2\lfloor \frac{a}{2} \rfloor$ et $2\lfloor \frac{b}{2} \rfloor \sqrt{6}$, pour se ramener au restes de a et b par la division euclidienne par 2. Finalement, cela donne trois cas, non mutuellement exclusifs :

(i) Ou bien $1 \in I$, et donc I est principal.

(ii) Ou bien $\sqrt{6} \in I$.

(iii) Ou bien $1 + \sqrt{6} \in I$.

Les deux derniers cas disent que $(2, \sqrt{6}) \subset I$ et $(2, 1 + \sqrt{6}) \subset I$. Mais ces deux familles sont libres sur $\mathbb{Q}$, et on sait en vertu du théorème 3.2.6 qu'on a respectivement $(2, \sqrt{6}) = I$ et $(2, 1+\sqrt{6}) = I$. On s'est donc ramenés à montrer que les idéaux $(2, \sqrt{6})$ et $(2, 1+\sqrt{6})$ sont principaux dans $\mathbb{Z}[\sqrt{6}]$. Ici, du bidouillage fonctionne. Par exemple on voit pour $(1, \sqrt{6})$ que

$$(2 - \sqrt{6})(-2 - \sqrt{6}) = 2,$$
$$(2 - \sqrt{6})(-3 - \sqrt{6}) = \sqrt{6},$$

donc $(1, \sqrt{6}) = (2 - \sqrt{6})$ et l'idéal est principal. L'autre cas est encore plus simple : il suffit de voir que

$$1 = 6 - 1 - 4 = (1 + \sqrt{6})(-1 + \sqrt{6}) - 2 \cdot 2 \in I,$$

donc $1 \in (1, 1 + \sqrt{6})$ et $I = \mathbb{Z}[\sqrt{6}]$.

Ainsi tous ces idéaux sont principaux : on a une seule classe et $|Cl(\mathcal{O}_{\mathbb{Q}[\sqrt{6}]})| = 1$

Exemple 3.2.8 (Le cas de $\mathbb{Q}(\sqrt{7})$**.** On peut raisonner exactement de la même manière que pour $d = 6$. Ici, on a encore $\mathcal{O}_{\mathbb{Q}(\sqrt{7})} = \mathbb{Z}[\sqrt{7}]$. La borne de la proposition 3.2.16 est $\sqrt{7} \approx 2,65$. Donc on veut voir que si un idéal I contient 2, il est principal. Par les mêmes arguments,

(i) Ou bien $1 \in I$, et donc I est principal.

(ii) Ou bien $\sqrt{7} \in I$.

(iii) Ou bien $1 + \sqrt{7} \in I$.

On s'est donc ramenés à montrer que $(2, \sqrt{7})$ et $(2, 1 + \sqrt{7})$ étaient principaux dans $\mathbb{Z}[\sqrt{7}]$.

Pour $(2, \sqrt{7})$, on voit que

$$1 = 7 - 6 = \sqrt{7}\sqrt{7} - 2 \cdot 3 \in I,$$

donc I est principal.

Ensuite, $(2, 1 + \sqrt{7})$, d'où

$$(3 + \sqrt{7})(3 - \sqrt{7}) = 2,$$
$$(3 + \sqrt{7})(-2 + \sqrt{7}) = 1 + \sqrt{7},$$

donc $I = (3 + \sqrt{7})$, I est principal.

Finalement on n'a encore qu'une seule classe, $|Cl(\mathcal{O}_{\mathbb{Q}[\sqrt{7}]})| = 1$.

Comme on l'a annoncé, cela ne fonctionne plus pour $d = 8$: il y a des idéaux non principaux dans $\mathbb{Z}[\sqrt{8}]$. Calculons maintenant le cardinal du groupe des classes dans ce cas.

Exemple 3.2.9 (Le cas de $\mathbb{Q}(\sqrt{8})$)**.** Le début du raisonnement est bien sûr valable. On a $\mathcal{O}_{\mathbb{Q}(\sqrt{8})} = \mathbb{Z}[\sqrt{8}]$. La borne donnée par le théorème 3.2.16 est $\sqrt{8} \approx 2,82$. Donc toute classe d'idéaux contient un idéal contenant 1 ou 2. Soit I un idéal avec $2 \in I$. Comme avant :

(i) Ou bien $1 \in I$, et donc I est principal.

(ii) Ou bien $\sqrt{8} \in I$ et $I = (2, \sqrt{8})$.

(iii) Ou bien $1 + \sqrt{8} \in I$ et $I = (2, 1 + \sqrt{8})$.

Dans le cas $I = (2, 1+\sqrt{8})$, on a bien affaire à un anneau principal car,

$$1 = 8 - 1 - 6 = (1+\sqrt{8})(\sqrt{8}-1) - 3 \cdot 2 \in I,$$

donc $I = \mathbb{Z}[\sqrt{8}]$.

Mais cela ne marche pas pour $I = (2, \sqrt{8})$. Supposons par l'absurde que I est principal, $I = (z)$ où $z \in \mathbb{Z}[\sqrt{8}]$. Alors on a x et $y \in \mathbb{Z}[\sqrt{8}]$ tels que

$$2 = xz,$$
$$\sqrt{8} = yz.$$

En passant à la norme sur la première égalité, il vient

$$N(2) = 2 = N(xz) = N(x)N(z),$$

mais $N(x)$ et $N(z)$ sont des entiers (proposition 1.4.7), donc $N(z) \in \{-2, -1, 1, 2\}$.

Si $N(z) \in \{-1, 1\}$, alors z est inversible (proposition 1.4.8), ce qui revient à dire que $I = (z) = \mathbb{Z}[\sqrt{2}]$. Alors en particulier $1 \in I$. Mais c'est absurde, car les éléments de $I = (2, \sqrt{8})$ s'écrivent

$$2(a + b\sqrt{8}) + \sqrt{8}(c + d\sqrt{8}) = (2a + 8d) + \sqrt{8}(2b + c)$$

avec a, b, c, d entiers. En particulier on ne peut pas avoir $2a + 8d = 1$, ce qui est bien absurde.

Ainsi, on a $N(x) \in \{-1, 1\}$, et c'est donc lui qui est inversible dans $\mathbb{Z}[\sqrt{2}]$. On obtient

$$z = 2x^{-1},$$

puis en réinjectant dans la seconde équation

$$\sqrt{8} = 2yx^{-1},$$

mais cela est encore absurde, puisque si on écrit $yx^{-1} = a + b\sqrt{8}$, il vient

$$\sqrt{8} = 2(a + b\sqrt{8}).$$

Or, ne peut pas avoir b entier et $2b = 1$: c'est la contradiction cherchée.

Ainsi $(2, \sqrt{8})$ n'est pas principal, et sa classe est donc distincte de la classe de $\mathbb{Z}[\sqrt{8}]$. Comme notre recherche était exhaustive, on trouve

$$|Cl(\mathcal{O}_{\mathbb{Q}[\sqrt{8}]})| = 2.$$

Ainsi, tous les anneaux d'entiers algébriques $\mathcal{O}_K$ ne sont pas principaux. Signalons que dans le cas général, énumérer tous les corps de nombres ayant un nombre de classes égal à un entier N est un problème très difficile. Dans le cas des corps quadratiques réels (de la forme $K = \mathbb{Q}[\omega]$ où ω est un réel), il existe une conjecture de Gauss, qui n'est pas encore démontrée, selon

laquelle il existe une infinité de tels corps dont le nombre de classes est 1.

Au-delà de ces considérations techniques, on peut retenir le fait suivant : avec les outils dont nous disposons pour l'instant, l'étude exhaustive des idéaux de $\mathcal{O}_K$ est difficile. Si $\mathcal{O}_K$ avait été principal (donc si $|Cl(\mathcal{O}_K)| = 1$), tous les idéaux auraient été de la forme $I = (a)$ avec $a \in \mathcal{O}_K$.

3.2.3 • $\mathcal{O}_K$ est de Dedekind

Au vu de tout le travail effectué jusqu'à maintenant, il ne nous reste plus à vérifier que l'ensemble des classes est bien un groupe pour conclure que $\mathcal{O}_K$ est de Dedekind. Pour rappel, cela revient à se demander si pour tout idéal I de $\mathcal{O}_K$ il existe un idéal non nul J de $\mathcal{O}_K$ tel que IJ est principal. Le résultat n'est plus très loin. La finitude des classes et le principe des tiroirs nous disent que pour tout idéal I de $\mathcal{O}_K$ on $i < j$ tels que $I^i \sim I^j$. Autrement dit :

$$(yI^{j-i})I^i = (x)I^i$$

Il ne resterait donc qu'à simplifier par I^i pour conclure. C'est précisément ce que permet de faire le lemme de Nakayama (proposition 3.2.17). C'est la démarche utilisée dans l'excellent cours [14].

Pour la culture, on donne un nom à l'ensemble des éléments inversibles de $Cl(\mathcal{O}_K)$. Cet ensemble a surtout de l'intérêt sur des anneaux qui ne sont pas de Dedekind, et donc dans lesquels tous les idéaux non nuls ne sont pas inversibles.

Définition 3.2.6. On appelle groupe de Picard de $\mathcal{O}_K$, noté $Pic(\mathcal{O}_K)$, l'ensemble des éléments de $Cl(\mathcal{O}_K)$ qui sont inversibles.

Cet ensemble muni de la loi de multiplication des idéaux donne bien un groupe abélien.

Exemple 3.2.10. La classe des idéaux principaux de $\mathcal{O}_K$ est inversible.

On veut donc obtenir $Pic(\mathcal{O}_K) = Cl(\mathcal{O}_K)$. Cela découle de l'argument suivant, propre à $\mathcal{O}_K$ et faux sur un anneau commutatif quelconque.

Proposition 3.2.17 (Lemme de Nakayama)**.** *Soient J et J' deux idéaux non nuls de $\mathcal{O}_K$ tels que $JJ' = (\alpha)J'$ avec $\alpha \in \mathcal{O}_K$. Alors $J = (\alpha)$.*

Démonstration. On montre d'abord la propriété pour $\alpha = 1$, soit $JJ' = J'$. On veut donc $J = \mathcal{O}_K$.

D'après la propriété 3.2.3, on peut prendre $(f_1, ..., f_n)$ une $\mathbb{Z}$-base de J'.

Soit $j \in [\![1, n]\!]$. Comme $J' = JJ'$, on peut écrire $f_j = xy$ où $x \in J$, $y \in J'$. On décompose alors y dans notre $\mathbb{Z}$-base de J', ce qui donne

$$f_j = \sum_{i=1}^{n} x\lambda_{i,j} f_i = \sum_{i=1}^{n} m_{i,j} f_i.$$

Or, J est un idéal de $\mathcal{O}_K$ et $\mathbb{Z} \subset \mathcal{O}_K$, donc les $m_{i,j} = x\lambda_{i,j}$ sont dans J. Finalement, en notant $M = (m_{i,j})$ qui est une matrice à coefficients dans J, on obtient le système

$$(I_n - M) \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

puis comme les f_j sont non nuls,

$$\det(I_n - M) = 0.$$

En notant Q le polynôme caractéristique de M, on a donc $Q(1) = 0$. Mais tous les coefficients de M sont dans J, donc en développant on obtient que tous les coefficients de Q sauf le dominant (qui est 1) sont dans J. Mais en évaluant en 1, on obtient

$$0 = Q(1) \in 1 + J.$$

Autrement dit, $1 \in J$. Comme J est un idéal, $J = \mathcal{O}_K$, c'est exactement ce qu'on voulait. Pour le cas général, on a donc maintenant $JJ' = (\alpha)J'$ où $\alpha \in \mathcal{O}_K$ qui est donc non nul. Soit $y \in J$. Comme $\frac{1}{\alpha}JJ' = J'$, on a

$$\frac{y}{\alpha}J' \subset J'.$$

Or, J' est un idéal de $\mathcal{O}_K$, et il a une $\mathbb{Z}$-base par la proposition 3.2.3. Mais par la proposition 1.3.2, on a $\frac{y}{\alpha} \in \overline{\mathbb{Z}} \cap K = \mathcal{O}_K$.

Autrement dit, $J'' = \frac{1}{\alpha}J$ est un idéal de $\mathcal{O}_K$. Mais alors, il suffit d'écrire $J''J' = J'$ pour retomber dans le cas $\alpha = 1$.

Ainsi, $J'' = \mathcal{O}_K$, et donc $J = (\alpha)$. □

Le lemme de Nakayama permet de démontrer que $Cl(\mathcal{O}_K)$ est un groupe.

Proposition 3.2.18. *Tout idéal non nul de $\mathcal{O}_K$ est inversible. Autrement dit,*

$$Cl(\mathcal{O}_K) = Pic(\mathcal{O}_K).$$

Démonstration. Soit I un idéal non nul de $\mathcal{O}_K$. Par le théorème 10, on sait que $Cl(\mathcal{O}_K)$ est fini. Par le principe des tiroirs, cela implique qu'on peut trouver $0 \leq i < j$ tels que

$$I^i \sim I^j.$$

Ainsi, on a x et $y \in \mathcal{O}_K$ non nuls tels que $xI^i = yI^j$. Cela se réécrit

$$(yI^{j-i})I^i = (x)I^i.$$

Par le lemme de Nakayama, on a donc

$$yI^{j-i} = (x),$$

donc $I^{j-i} \sim (x)$ et I^{j-i} est principal. Mais alors on a, en notant $[I]$ la classe de I,

$$[I][I^{j-i-1}] = [\mathcal{O}_K],$$

donc I est inversible, et donc $Cl(\mathcal{O}_K) = Pic(\mathcal{O}_K)$. □

On en déduit le corollaire assez joli suivant, où la notation h_K provient de Dedekind.

Proposition 3.2.19. *Pour tout idéal non nul I de $\mathcal{O}_K$, l'idéal I^{h_K} est principal, où on a noté $h_K = |Cl(\mathcal{O}_K)|$.*

En vertu de la proposition 3.2.12, on obtient donc le théorème suivant qui conclut la première partie de cette section.

Théorème (8)**.** *Soit K un corps de nombres. L'anneau $\mathcal{O}_K$ est de Dedekind.*

3.2.4 • L'arithmétique classique retrouvée

Maintenant qu'on a posé une arithmétique sur $\mathcal{O}_K$, il est temps de voir les propriétés qu'elle nous permet d'obtenir. Pour ce faire, on dispose de deux ingrédients principaux :

- Bien sûr on utilisera en permanence le fait que $\mathcal{O}_K$ est de Dedekind, ce qui nous permettra de décomposer nos idéaux en produits d'idéaux premiers.
- Mais la vision géométrique de $\mathcal{O}_K$ apporte une notion supplémentaire : celle de la *norme* des idéaux. Cet outil se combine très bien avec le fait que $\mathcal{O}_K$ est de Dedekind, puisqu'on va voir qu'il passe aux produits d'idéaux : $\mathcal{N}(\mathfrak{ab}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b})$. Cette propriété induit une forme de rigidité lorsqu'on regarde le comportement des idéaux dans les extensions de corps de nombres, et sera au cœur de la sous-section suivante.

En ce qui concerne cette sous-section, elle se découpe en trois temps successifs, qui vérifient que tous nos outils ont des comportements agréables face à l'arithmétique des idéaux.

- On montre d'abord que la norme passe au produit des idéaux de $\mathcal{O}_K$ comme annoncé. Comme on sait déjà que cette propriété est vraie pour les idéaux premiers entre eux (proposition 3.2.9), il suffit d'exploiter la décomposition en idéaux premiers.
- On élargit notre cadre afin de nous donner une arithmétique sur K. En effet, il suffit d'observer que les idéaux fractionnaires admettent aussi des décompositions en idéaux premiers, mais en autorisant les puissances négatives. Dès lors, on pourra étudier la factorisation des idéaux fractionnaires principaux $x\mathcal{O}_K$ pour $x \in K$.
- On conclut cette partie en s'intéressant aux *valuations $\mathfrak{p}$-adiques* induites par nos décompositions. Sur $\mathbb{Z}$, il est clair qu'à n'importe quel choix de valuations on peut associer un élément qui le réalise. Mais sur $\mathcal{O}_K$ ce n'est pas le cas. On dispose néanmoins d'une certaine liberté à cet égard. En particulier, on étudie les possibilités de simplification des fractions. Pour $r \in \mathbb{Q}$ avec $v_p(r) \leq 0$, on peut toujours rassembler les facteurs p au numérateur pour écrire $r = \frac{a}{b}$ avec $v_p(b) = 0$. Un tel résultat est loin d'être évident sur K.

Ici on s'inspire à nouveau du mémoire [16], mais en s'éloignant quelque peu : en effet, cet ouvrage ne parle pas de la décomposition en facteurs premiers des idéaux fractionnaires, que nous introduisons donc ici.

Le cas des idéaux de $\mathcal{O}_K$

Dans la suite, par analogie avec $\mathbb{Z}$, n adoptera l'écriture suivante, pour $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$:

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})},$$

où $\mathfrak{p}$ parcourt l'ensemble des idéaux premiers de $\mathcal{O}_K$, et ce produit est fini au sens où il n'y a qu'un nombre fini de $v_{\mathfrak{p}}(\mathfrak{a})$ différents de 0. Plus précisément, on peut définir les $v_{\mathfrak{p}}(\mathfrak{a})$ par

$$v_{\mathfrak{p}}(\mathfrak{a}) = \max\left\{t \in \mathbb{N} \,\middle|\, \mathfrak{p}^t \mid \mathfrak{a}\right\} = \max\left\{t \in \mathbb{N} \,\middle|\, \mathfrak{a} \subset \mathfrak{p}^t\right\}, \tag{5}$$

où l'on sait de plus que cette décomposition est unique.

On peut par ailleurs étendre cette définition aux éléments de $\mathcal{O}_K$ via les idéaux principaux.

Définition 3.2.7. Soit $x \in \mathcal{O}_K$. Pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$, on note $v_{\mathfrak{p}}(x)$ la valuation $\mathfrak{p}$-adique de l'idéal (x).

Cette décomposition va nous permettre d'obtenir des résultats sur la norme des idéaux. En effet, on rappelle qu'on avait vu dans la proposition 3.2.9 que si on prenait $\mathfrak{p}$ et $\mathfrak{q}$ deux idéaux de $\mathcal{O}_K$ premiers entre eux, on avait alors

$$\mathcal{N}(\mathfrak{pq}) = \mathcal{N}(\mathfrak{p})\mathcal{N}(\mathfrak{q}).$$

En particulier, cela fonctionnait si on avait deux idéaux maximaux distincts, donc premiers entre eux. On en déduit le fait suivant.

Proposition 3.2.20. *Soient $\mathfrak{p}$ et $\mathfrak{q}$ deux idéaux premiers non nuls distincts de $\mathcal{O}_K$. Alors,*

$$\mathcal{N}(\mathfrak{pq}) = \mathcal{N}(\mathfrak{p})\mathcal{N}(\mathfrak{q}).$$

Démonstration. On utilise simplement la proposition 3.1.18 qui dit que les idéaux premiers non nuls d'un anneau de Dedekind sont maximaux. □

On a donc très envie de passer à la norme dans l'équation 5 afin d'écrire la norme d'un idéal comme le produit des normes de ses facteurs premiers. On doit simplement vérifier qu'on peut bien utiliser la multiplicativité. C'est l'objet des propositions suivantes.

Proposition 3.2.21. *Soient $\mathfrak{p}$, $\mathfrak{q}$ et $\mathfrak{r}$ trois idéaux non nuls de $\mathcal{O}_K$ tels que $\mathfrak{p}$ est premier avec $\mathfrak{q}$ et $\mathfrak{r}$. Alors, $\mathfrak{p}$ est premier avec $\mathfrak{qr}$.*

Démonstration. Montrons que

$$\mathfrak{p} + \mathfrak{qr} = \mathcal{O}_K.$$

Cela revient à trouver un triplet $(p, q, r) \in \mathfrak{p} \times \mathfrak{q} \times \mathfrak{r}$ tel que

$$p + qr = 1.$$

Or, $\mathfrak{p}$ est premier avec $\mathfrak{q}$ et $\mathfrak{r}$, donc on dispose de deux couples $(p_1, q) \in \mathfrak{p} \times \mathfrak{q}$ et $(p_2, r) \in \mathfrak{p} \times \mathfrak{r}$ tels que

$$\begin{aligned} p_1 + q &= 1, \\ p_2 + r &= 1. \end{aligned}$$

On écrit donc

$$\begin{aligned} qr + p_1 r + p_2 &= r(p_1 + q) + p_2 \\ &= r + p_2 \\ &= 1. \end{aligned}$$

Or, $p_1 r + p_2 \in \mathfrak{p}$, ce qui permet de conclure que $\mathfrak{p}$ est premier avec $\mathfrak{qr}$. □

On a donc le corollaire immédiat suivant, qui s'établit par récurrence.

Proposition 3.2.22. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux non nuls de $\mathcal{O}_K$. Alors $\mathfrak{a}$ et $\mathfrak{b}$ sont premiers entre eux si et seulement s'ils n'ont aucun facteur premier en commun.*

Démonstration. Le sens direct se voit par contraposée : si on a $\mathfrak{p}$ un idéal premier de $\mathfrak{a}$ et $\mathfrak{b}$ apparaissant dans leurs décompositions, alors $\mathfrak{p}$ divise $\mathfrak{a}$ et $\mathfrak{b}$, donc $\mathfrak{a} + \mathfrak{b} \subset \mathfrak{p} \neq \mathcal{O}_K$.

Le sens indirect est une utilisation immédiate de la proposition précédente et du fait que deux idéaux premiers (donc maximaux dans un anneau de Dedekind) distincts sont premiers entre eux. □

Cette proposition permet de s'occuper des facteurs distincts dans la décomposition. Mais qu'en est-il des idéaux premiers qui apparaissent avec des valuations plus grandes que 2 ? La proposition suivante traite ce cas.

Proposition 3.2.23. *Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Alors on a, pour tout entier k,*

$$\mathcal{N}(\mathfrak{p}^k) = \mathcal{N}(\mathfrak{p})^k.$$

Démonstration. Ici on exploite l'écriture $\mathcal{N}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$. Cela permet de dire dans notre cas que

$$\mathcal{N}(\mathfrak{p}^k) = |\mathcal{O}_K/\mathfrak{p}^k| = |\mathcal{O}_K/\mathfrak{p}||\mathfrak{p}/\mathfrak{p}^2| \cdots |\mathfrak{p}^{k-1}/\mathfrak{p}^k|.$$

On a juste à montrer que, pour tout k,

$$|\mathcal{O}_K/\mathfrak{p}| = |\mathfrak{p}^k/\mathfrak{p}^{k+1}|.$$

Soit donc k un entier. On voit qu'il existe un $\pi \in \mathfrak{p}^k$ tel que $\pi \notin \mathfrak{p}^{k+1}$ et π non nul. Si ce n'était pas le cas, on aurait $\mathfrak{p}^k = \mathfrak{p}^{k+1}$ et en simplifiant, $\mathfrak{p} = \mathcal{O}_K$: absurde. On pose

$$\Phi \ : \left| \begin{array}{ccc} \mathcal{O}_K & \to & \mathfrak{p}^k/\mathfrak{p}^{k+1} \\ x & \mapsto & \overline{\pi x}, \end{array} \right.$$

où $\overline{a}$ désigne la classe de $a \in \mathfrak{p}^k$ dans $\mathfrak{p}^k/\mathfrak{p}^{k+1}$.

- Cette application est bien définie puisque pour tout $x \in \mathcal{O}_K$ on a $\pi x \in \mathfrak{p}^k$. De plus c'est un morphisme de groupes.
- On observe alors que Φ est surjective. En effet, soit $y \in \mathfrak{p}^k$. On veut voir qu'il existe un $x \in \mathcal{O}_K$ tel que $x\pi - y \in \mathfrak{p}^{k+1}$. Cela revient à écrire

$$(\pi) + \mathfrak{p}^{k+1} = \mathfrak{p}^k.$$

Écrivons la décomposition en facteurs premiers de (π) :

$$(\pi) = \mathfrak{p}^k \prod_{\mathfrak{q}} \mathfrak{q}^{v_{\mathfrak{q}}(\pi)},$$

puisque par définition $v_{\mathfrak{p}}(\pi) = k$. Notons $\mathfrak{a} = \prod_{\mathfrak{q}} \mathfrak{q}^{v_{\mathfrak{q}}(a)}$. D'après la proposition 3.2.22, $\mathfrak{p}$ et $\mathfrak{q}$ sont premiers entre eux. Ainsi,

$$\mathfrak{q} + \mathfrak{p} = \mathcal{O}_K.$$

On peut donc écrire,

$$(\pi) + \mathfrak{p}^{k+1} = \mathfrak{p}^k(\mathfrak{q} + \mathfrak{p}) = \mathfrak{p}^k.$$

C'est exactement ce qu'on voulait, donc Φ est surjective.

- De plus, le noyau de Φ est exactement $\mathfrak{p}$. Il est déjà clair que $\mathfrak{p} \subset Ker()$. Réciproquement, soit $x \in \mathcal{O}_K$ avec $\Phi(x) = 0$, soit $\pi x \in \mathfrak{p}^{k+1}$. Alors, en particulier,

$$(\pi x) = (\pi)(x) \subset \mathfrak{p}^{k+1} \Leftrightarrow \mathfrak{p}^{k+1} | (\pi)(x).$$

Par unicité de la décomposition en facteurs premiers, cela entraîne $\mathfrak{p}|(x)$, ou encore $x \in \mathfrak{p}$, ce qui conclut.

On peut donc écrire une factorisation bijective

$$\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^k/\mathfrak{p}^{k+1},$$

ce qui conclut. □

On déduit donc de toutes les propositions précédentes l'écriture suivante.

Proposition 3.2.24. *Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$. On écrit sa décomposition*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}.$$

Alors,

$$\mathcal{N}(\mathfrak{a}) = \prod_{\mathfrak{p}} \mathcal{N}(\mathfrak{p})^{v_{\mathfrak{p}}(\mathfrak{a})}.$$

Ceci permet de déboucher comme prévu sur la multiplicativité de la norme.

Proposition 3.2.25. *Soit $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux non nuls de $\mathcal{O}_K$. Alors,*

$$\mathcal{N}(\mathfrak{ab}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b}).$$

Démonstration. On écrit la décomposition de $\mathfrak{ab}$, qui est la juxtaposition des décompositions de $\mathfrak{a}$ et $\mathfrak{b}$ par unicité, et on conclut par la multiplicativité de la norme. □

La propriété 3.2.24 donne aussi une expression alternative de la norme d'un élément de $\mathcal{O}_K$.

Proposition 3.2.26. *Soit $x \in \mathcal{O}_K$. Alors,*

$$|N(x)| = \prod_{\mathfrak{p}} \mathcal{N}(\mathfrak{p})^{v_{\mathfrak{p}}(x)}.$$

Démonstration. Il suffit d'écrire

$$|N(x)| = \mathcal{N}(x\mathcal{O}_K) = \mathcal{N}\Big(\prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)}\Big) = \prod_{\mathfrak{p}} \mathcal{N}(\mathfrak{p})^{v_{\mathfrak{p}}(x)}.$$

□

En particulier, on voit que sur $\mathbb{Q}$ la propriété 3.2.24 a une expression très naturelle.

Exemple 3.2.11. Sur $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, les idéaux sont exactement les (n), et la décomposition en idéaux premiers correspond exactement à la décomposition en facteurs premiers (à un signe $\pm$ près). Ainsi,

$$\forall p \in \mathcal{P}\ v_p(n) = v_{(p)}(n).$$

De plus, pour tout nombre premier p, on a

$$\mathcal{N}((p)) = |\mathbb{Z}/p\mathbb{Z}| = p,$$

donc la formule de la norme redonne bien

$$|n| = \prod_{p \in \mathcal{P}} p^{v_p(n)} = \mathcal{N}((n)).$$

On retrouve alors le fait que sur $\mathbb{Q}$, $N(x) = x$.

Extension de l'arithmétique à K

Sur $\mathbb{Q}$, il est possible d'étendre l'arithmétique issue de $\mathbb{Z}$ en écrivant les nombres rationnels comme $r = \frac{a}{b}$ avec $a \wedge b = 1$. On peut alors parler de la valuation p-adique de r, qui est bien définie comme $v_p(r) = v_p(a) - v_p(b)$.

On souhaite étendre une telle construction à K. On sait déjà que tout élément de K peut s'écrire $x = \frac{a}{b}$ avec $a, b \in \mathcal{O}_K$ (proposition 1.3.4). Etant donné qu'on dispose d'une écriture

unique de (a) et (b) en produits d'idéaux premiers, on va pouvoir réussir à choisir (a) et (b) premiers entre eux. A partir de là, il suffit de vérifier que tous nos outils opèrent dans le monde fractionnaire, ce qui est bien le cas.

Pour commencer, on s'assure que les idéaux fractionnaires admettent bien une unique décomposition en idéaux premiers, avec des puissances négatives. Avec la définition de 3.1.15, c'est automatique.

Proposition 3.2.27. *Soit $\mathcal{I}$ un idéal fractionnaire de $\mathcal{O}_K$. Alors $\mathcal{I}$ admet une unique décomposition en facteurs premiers, de la forme*

$$\mathcal{I} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathcal{I})},$$

où les $v_{\mathfrak{p}}(\mathcal{I})$ sont des entiers relatifs tous nuls sauf un nombre fini. Plus précisément, si $\mathcal{I} = x^{-1}I$, alors on a pour tout $\mathfrak{p}$ la relation $v_{\mathfrak{p}}(\mathcal{I}) = v_{\mathfrak{p}}(I) - v_{\mathfrak{p}}(x)$.

Démonstration. On utilise l'existence et l'unicité de la décomposition des idéaux de $\mathcal{O}_K$. Prenons une écriture

$$\mathcal{I} = x^{-1}I.$$

En tant qu'idéal fractionnaire, on peut écrire l'inverse de (x) sous la forme

$$(x)^{-1} = (x^{-1}).$$

En écrivant

$$(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)},$$

on en déduit l'expression de l'inverse

$$(x)^{-1} = \prod_{\mathfrak{p}} \mathfrak{p}^{-v_{\mathfrak{p}}(x)},$$

d'où

$$\mathcal{I} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)-v_{\mathfrak{p}}(x)}.$$

L'unicité découle de l'unicité de la décomposition sur les idéaux entiers. □

On peut de même étendre la norme aux idéaux fractionnaires.

Définition 3.2.8. Soit $\mathcal{I}$ un idéal fractionnaire de $\mathcal{O}_K$, qu'on écrit $\mathcal{I} = x^{-1}I$ avec $x \in \mathcal{O}_K$ non nul et I un idéal de $\mathcal{O}_K$. On définit la norme de $\mathcal{I}$ par

$$\mathcal{N}(\mathcal{I}) = \frac{\mathcal{N}(I)}{|N(x)|},$$

où $N(x)$ est la norme de l'élément x.

On vérifie que cette définition est bien licite, donc indépendante de l'écriture. Soient $x, y \in \mathcal{O}_K$ et I, J deux idéaux de $\mathcal{O}_K$ tels que

$$x^{-1}I = y^{-1}J,$$

ce qui est équivalent à

$$yI = xJ.$$

En passant à la norme, il vient

$$\mathcal{N}(yI) = \mathcal{N}((y)I) = \mathcal{N}((y))\mathcal{N}(I) = |N(y)|\mathcal{N}(I).$$

Ainsi,

$$\frac{\mathcal{N}(I)}{|N(y)|} = \frac{\mathcal{N}(J)}{|N(x)|},$$

et $\mathcal{N}(\mathcal{I})$ est bien défini.

Cela permet en particulier d'écrire les propositions rassurantes suivantes.

Proposition 3.2.28. *Soient $\mathcal{I}$ et $\mathcal{J}$ deux idéaux fractionnaires non nuls de $\mathcal{O}_K$.*

- *On a $\mathcal{N}(\mathcal{I}\mathcal{J}) = \mathcal{N}(\mathcal{I})\mathcal{N}(\mathcal{J})$.*
- *Si $\mathcal{I}$ n'est pas nul (donc inversible), $\mathcal{N}(\mathcal{I}^{-1}) = \mathcal{N}(\mathcal{I})^{-1}$.*

Démonstration. Cela découle directement de la définition et du fait que $\mathcal{N}(\mathcal{O}_K) = 1$. □

Enfin, on n'a plus qu'à utiliser ces résultats pour obtenir une arithmétique sur K. Comme dans le cas entier, on veut considérer les idéaux fractionnaires principaux $x\mathcal{O}_K$ pour $x \in \mathcal{O}_K$. Mais avec la définition de 3.1.15 ces ensembles ne sont pas automatiquement des idéaux principaux. En fait il aurait peut-être été plus naturel d'appeler idéal fractionnaire les ensembles de la forme

$$\mathcal{I} = xI$$

où x est un élément de K quelconque, et I un idéal de $\mathcal{O}_K$. On voit alors que ces deux définitions sont équivalentes en reprenant la preuve du théorème 1.3.3. Rappelons ce fait.

Proposition 3.2.29. *Soit $x \in K$. Alors il existe $n \in \mathbb{Z}$ tel que $nx \in \mathcal{O}_K$*

Cela permet de vérifier que les $x\mathcal{O}_K$ sont bien des idéaux fractionnaires.

Proposition 3.2.30. *Soit $x \in K$ non nul. On note (x) l'ensemble*

$$(x) = x\mathcal{O}_K = \left\{ ax \,\middle|\, a \in \mathcal{O}_K \right\}.$$

Alors (x) est un idéal fractionnaire au sens de la définition 3.1.15, c'est-à-dire qu'il

existe $y \in \mathcal{O}_K$ non nul, et I un idéal de $\mathcal{O}_K$ tels que

$$(x) = y^{-1} I.$$

Démonstration. On sait qu'il existe $n \in \mathbb{Z}$ tel que $nx \in \mathcal{O}_K$. Mais alors il suffit d'écrire que

$$\begin{aligned}(x) &= \left\{ ax \,\middle|\, a \in \mathcal{O}_K \right\} \\ &= \left\{ \frac{anx}{n} \,\middle|\, a \in \mathcal{O}_K \right\} \\ &= \frac{1}{n}(nx).\end{aligned}$$

Comme (nx) est un idéal de $\mathcal{O}_K$, et que $n \in \mathcal{O}_K$, on en déduit que (x) est un idéal fractionnaire. □

On peut donc bien étendre la valuation $\mathfrak{p}$-adique à K. Donnons nous une petite notation supplémentaire pour alléger :

Définition 3.2.9. Soit $x \in K$ non nul. On note(x) l'idéal fractionnaire

$$(x) = x\mathcal{O}_K.$$

Il ne reste plus qu'à poser la définition suivante :

Définition 3.2.10 (Valuation $\mathfrak{p}$-adique)**.** Soit $x \in K$ non nul. L'idéal fractionnaire (x) admet une unique décomposition de la forme

$$(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)}.$$

Les nombres $v_{\mathfrak{p}}(x)$ sont des entiers relatifs appelés valuations $\mathfrak{p}$-adiques de x, et sont tous nuls sauf un nombre fini d'entre eux.

Par convention, on prendra pour tout $\mathfrak{p}$, $v_{\mathfrak{p}}(0) = \infty$.

De plus, au vu de la preuve de 3.2.30, on a la proposition suivante.

Proposition 3.2.31. *Soit $x \in K$, qui s'écrit $x = \frac{a}{b}$ avec a et $b \in \mathcal{O}_K$. Alors, pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ on a*

$$v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(a) - v_{\mathfrak{p}}(b).$$

On vérifie alors que tous nos outils coïncident, et que notre norme des idéaux étend bien la norme sur K.

Proposition 3.2.32. *Soit $x \in K$. Alors on a l'expression*

$$|N(x)| = \prod_{\mathfrak{p}} \mathcal{N}(\mathfrak{p})^{v_{\mathfrak{p}}(x)}.$$

Démonstration. Écrivons $x = \frac{a}{b}$. Par multiplicativité de la norme, on obtient

$$|N(x)| = \frac{|N(a)|}{|N(b)|}.$$

Mais d'après ce qu'on a dit avant,

$$\begin{aligned}\prod_{\mathfrak{p}} \mathcal{N}(\mathfrak{p})^{v_{\mathfrak{p}}(x)} &= \prod_{\mathfrak{p}} \mathcal{N}(\mathfrak{p})^{v_{\mathfrak{p}}(a)-v_{\mathfrak{p}}(b)} \\ &= \frac{\prod_{\mathfrak{p}} \mathcal{N}(\mathfrak{p})^{v_{\mathfrak{p}}(a)}}{\prod_{\mathfrak{p}} \mathcal{N}(\mathfrak{p})^{v_{\mathfrak{p}}(b)}} \\ &= \frac{|N(a)|}{|N(b)|}.\end{aligned}$$

□

Ainsi tous nos outils ont été généralisés sur K !

Une première étude des valuations $\mathfrak{p}$-adiques

On se propose maintenant de voir comment les valuations $\mathfrak{p}$-adiques se comportent sur K. D'abord il convient de vérifier que le terme « valuation » est bien adapté.

Définition 3.2.11 (Valuation)**.** Soit K un corps de nombre. On appelle *valuation* sur K toute application $v : K \to \mathbb{R} \cup \{\infty\}$ telle que

(i) $\forall x \in K\, v(x) = \infty \iff x = 0$.

(ii) $\forall x, y \in K\, v(xy) = v(x) + v(y)$.

(iii) $\forall x, y \in K\, v(x + y) \geq \min(v(x), v(y))$.

Proposition 3.2.33. *Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. L'application $v_{\mathfrak{p}}$ définie en 3.2.10 est bien une valuation.*

Démonstration.

- Pour le (i), on a défini $v_{\mathfrak{p}}(0) = \infty$. Réciproquement, tout $x \in K$ non nul admet une décomposition comme dans la définition 3.2.10, donc $v_p(x)$ est un entier relatif.
- Pour le (ii), cela découle directement du fait que

$$(xy) = (x)(y) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(a)} \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(b)} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(a)+v_{\mathfrak{p}}(b)}$$

et de l'unicité de la décomposition.

- Enfin, pour le (iii), on fait apparaître les facteurs communs à (x) et (y) :

$$\begin{aligned}(x+y) &\subset (x)+(y)\\ &= \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)} + \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(y)}\\ &= \prod_{\mathfrak{p}} \mathfrak{p}^{\min(v_{\mathfrak{p}}(x),v_{\mathfrak{p}}(y))} \left(\prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)-\min(v_{\mathfrak{p}}(x),v_{\mathfrak{p}}(y))} + \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(y)-\min(v_{\mathfrak{p}}(x),v_{\mathfrak{p}}(y))} \right).\end{aligned}$$

  Or, $\prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)-\min(v_{\mathfrak{p}}(x),v_{\mathfrak{p}}(y))}$ et $\prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(y)-\min(v_{\mathfrak{p}}(x),v_{\mathfrak{p}}(y))}$ sont deux idéaux entiers de $\mathcal{O}_K$ sans facteurs premiers communs : ils sont donc premier entre eux et leur somme est $\mathcal{O}_K$. On peut donc écrire

$$(x+y) \subset \prod_{\mathfrak{p}} \mathfrak{p}^{\min(v_{\mathfrak{p}}(x),v_{\mathfrak{p}}(y))}.$$

  Cela garantit que pour tout $\mathfrak{p}$ on a

$$v_{\mathfrak{p}}(x+y) \geq \min(v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y)).$$

□

Comme sur $\mathbb{Q}$, les valuations $\mathfrak{p}$-adiques permettent aussi de caractériser de façon naturelle les inversibles de $\mathcal{O}_K$.

Proposition 3.2.34. *Soit $x \in K$. On a l'équivalence*

$$x \in \mathcal{O}_K^\times \Leftrightarrow \forall \mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)\, v_{\mathfrak{p}}(x) = 0.$$

Démonstration. Il suffit d'écrire, pour $x \in K$

$$x \in \mathcal{O}_K^\times \iff x\mathcal{O}_K = \mathcal{O}_K \iff \forall \mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)\, v_{\mathfrak{p}}(x) = 0$$

par unicité de la décomposition. □

On fera attention que cela redonne le fait que pour tout $x \in \mathcal{O}_K^\times$ on a $N(x) = \pm 1$, mais pas la réciproque.

Exemple 3.2.12. Avec toutes ces définitions, on voit par exemple que dans le cas $K = \mathbb{Q}$ et donc $\mathcal{O}_K = \mathbb{Z}$, on a simplement défini la valuation p-adique des rationnels. En effet, $\mathbb{Z}$ est un anneau principal, donc factoriel et de Dedekind, et la décomposition en idéaux premiers coïncide avec celle en éléments premiers (aux unités près). Ainsi, pour tous nombre premier $p \in \mathcal{P}$ et $r \in \mathbb{Q}$,

$$v_{(p)}(r) = v_p(r).$$

On retombe bien sur la définition habituelle. Par ailleurs, on observe qu'on a toujours

$$|r| = \prod_{p \in \mathcal{P}} p^{v_p(r)}.$$

Sur $\mathbb{Z}$, les valuations p-adiques d'un nombre n le décrivent complètement à un facteur ± 1 près. De plus, pour tout choix d'une famille d'entiers relatifs tous nuls sauf un nombre fini $(s_p)_{s \in \mathcal{P}}$, il existe un entier n tel que

$$\forall p \in \mathcal{P}\, v_p(n) = s_p.$$

Dans le cas général, on a encore la caractérisation à un élément inversible de $\mathcal{O}_K$ près.

Proposition 3.2.35. *Soient x et $y \in K$ non nuls. Alors, $\forall \mathfrak{p}$, $v_\mathfrak{p}(x) = v_\mathfrak{p}(y)$ si et seulement si $\frac{x}{y} \in \mathcal{O}_K^\times$.*

Démonstration. Cette condition se produit si et seulement si $x\mathcal{O}_K = y\mathcal{O}_K$, donc si et seulement si $\frac{x}{y} \in \mathcal{O}_K^\times$. □

De plus, la surjectivité de $x \mapsto (v_\mathfrak{p}(x))$ dans l'ensemble des familles de $\mathbb{Z}$ indicées sur $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ nulles sauf en un nombre fini de termes correspond à la principalité de $\mathcal{O}_K$.

Proposition 3.2.36. *L'anneau $\mathcal{O}_K$ est principal si et seulement si pour toute famille $(s_\mathfrak{p})$ de $\mathbb{Z}$ indicée sur $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ nulle sauf en un nombre fini de termes il existe $x \in K$ tel que*

$$\forall \mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)\, v_\mathfrak{p}(x) = s_\mathfrak{p}.$$

Démonstration. Si $\mathcal{O}_K$ est principal, on a des $x_\mathfrak{p}$ de $\mathcal{O}_K$ tels que $\mathfrak{p} = (x_\mathfrak{p})$. Pour une famille $s_\mathfrak{p}$ donnée, nulle sauf en un nombre fini de termes, il suffit de prendre

$$x = \prod_{\mathfrak{p}} {x_\mathfrak{p}}^{s_\mathfrak{p}} \in K.$$

Réciproquement, si l'application est surjective, on a en particulier pour tous $\mathfrak{p}$ un $x_\mathfrak{p}$ tel que

$$\forall \mathfrak{q} \neq \mathfrak{p},\ v_\mathfrak{q}(x_\mathfrak{p}) = 0 \ \text{ et } v_\mathfrak{p}(x_\mathfrak{p}) = 1.$$

Ainsi, $\mathfrak{p} = (x_\mathfrak{p})$. Donc les idéaux premiers sont principaux, et tous les idéaux de $\mathcal{O}_K$ sont donc principaux puisqu'il s'écrivent comme produit fini d'idéaux premiers. Donc $\mathcal{O}_K$ est principal. □

Dans le cas général, on ne pourra donc pas prendre un élément $x \in K$ avec n'importe quelles valuations. Néanmoins, on peut toujours toujours trouver un élément de $\mathcal{O}_K$ dont la valuation s'annule sur un ensemble fini de $\mathfrak{p}$, et qui est strictement positive sur un autre ensemble fini de $\mathfrak{p}$.

Proposition 3.2.37. *Soient $\mathcal{S}$ et $\mathcal{S}'$ deux ensembles finis et disjoints d'idéaux premiers non nuls de $\mathcal{O}_K$. Alors il existe $x \in \mathcal{O}_K$ tel que*

$$\forall\, \mathfrak{p} \in \mathcal{S}\ v_{\mathfrak{p}}(x) = 0,$$
$$\forall\, \mathfrak{p} \in \mathcal{S}'\ v_{\mathfrak{p}}(x) > 0.$$

Démonstration. La condition se réécrit

$$\forall\, \mathfrak{p} \in \mathcal{S}\ x \notin \mathfrak{p},$$
$$\forall\, \mathfrak{p} \in \mathcal{S}'\ x \in \mathfrak{p}.$$

Il suffit d'utiliser le lemme chinois, car les idéaux premiers distincts sont deux à deux premiers entre eux. Cela garantit qu'on a un isomorphisme

$$\mathcal{O}_K \Big/ \left(\prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p} \prod_{\mathfrak{p}\in\mathcal{S}'} \mathfrak{p} \right) \cong \prod_{\mathfrak{p}\in\mathcal{S}} (\mathcal{O}_K/\mathfrak{p}) \times \prod_{\mathfrak{p}\in\mathcal{S}'} (\mathcal{O}_K/\mathfrak{p}).$$

En particulier, aucun des $\mathcal{O}_K/\mathfrak{p}$ n'est trivial puisqu'il s'agit d'idéaux propres. Dès lors, on peut donc choisir $x \in \mathcal{O}_K$ tel que

$$\forall\, \mathfrak{p} \in \mathcal{S}\ \overline{x} = \overline{1} \ \text{ dans } \mathcal{O}_K/\mathfrak{p}$$
$$\forall\, \mathfrak{p} \in \mathcal{S}'\ \overline{x} = \overline{0} \ \text{ dans } \mathcal{O}_K/\mathfrak{p}.$$

Cela garantit que x vérifie les conditions souhaitées. □

Simplification des fractions

On s'intéresse maintenant aux possibilités de simplifications des fractions. Pour $r \in \mathbb{Q}$ avec $v_p(r) \leq 0$, on peut toujours rassembler les facteurs p au numérateur pour écrire $r = \frac{a}{b}$ avec $v_p(b) = 0$. Un tel résultat est loin d'être évident sur K. En effet, on a vu qu'on ne pouvait a priori pas choisir des éléments de valuations quelconques.

Ainsi, il n'est pas évident que pour $x \in K$ avec $v_{\mathfrak{p}}(x) \leq 0$ pour un certain $\mathfrak{p}$, on ait a et b dans $\mathcal{O}_K$ avec $v_{\mathfrak{p}}(b) = 0$, $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(x)$ et $x = \frac{a}{b}$. Il s'avère cependant que c'est le cas, comme on le montre à travers les deux résultats suivants.

Le premier résultat confronte classe d'idéaux et décomposition en idéaux premiers :

Proposition 3.2.38. *Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$. Alors dans toute classe de $Cl(\mathcal{O}_K)$, il existe un idéal $\mathfrak{b}$ de $\mathcal{O}_K$ tels que $\mathfrak{a}$ et $\mathfrak{b}$ sont premiers entre eux.*

Démonstration. Soit $[\mathfrak{c}]$ une classe. On cherche donc un idéal $\mathfrak{b}$ de $\mathcal{O}_K$ tel que $\mathfrak{b} = x\mathfrak{c}$ avec $x \in K$ et tel que $\mathfrak{a}$ et $\mathfrak{b}$ sont premiers entre eux. Notons $\mathcal{S}_{\mathfrak{a}}$ l'ensemble (fini) des idéaux premiers apparaissant dans la décomposition de $\mathfrak{a}$. On sépare alors $\mathfrak{c}$ en deux parties :

$$\mathfrak{c} = \prod_{\mathfrak{p}\in\mathcal{S}_{\mathfrak{a}}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{c})} \prod_{\mathfrak{p}\notin\mathcal{S}_{\mathfrak{a}}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{c})} = \left(\prod_{\mathfrak{p}\in\mathcal{S}_{\mathfrak{a}}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{c})} \right) \mathfrak{r}.$$

Ainsi, $\mathfrak{a}$ et $\mathfrak{r}$ est sont premiers entre eux. On prend ensuite $x \in \prod_{\mathfrak{p}\in\mathcal{S}_\mathfrak{a}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{c})}$. On peut donc écrire une décomposition de (x) :

$$(x) = \prod_{\mathfrak{p}\in\mathcal{S}_\mathfrak{a}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{c})} \prod_{\mathfrak{p}\in\mathcal{T}_\mathfrak{a}} \mathfrak{p}^{v_\mathfrak{p}(x)}$$

où $\mathcal{T}_\mathfrak{a}$ est en ensemble fini, distinct de $\mathcal{S}_\mathfrak{a}$, d'idéaux premiers non nuls. À ce stade, on peut écrire

$$\frac{\mathfrak{c}}{x} = \frac{\mathfrak{r}}{\prod_{\mathfrak{p}\in\mathcal{T}_\mathfrak{a}} \mathfrak{p}^{v_\mathfrak{p}(x)}}.$$

Pour faire disparaître le numérateur, on utilise la proposition précédente : on dispose de $y \in \mathcal{O}_K$ tel que

$$\forall\, \mathfrak{p} \in \mathcal{S}_\mathfrak{a}\ v_\mathfrak{p}(y) = 0$$
$$\forall\, \mathfrak{p} \in \mathcal{T}_\mathfrak{a}\ v_\mathfrak{p}(y) > 0.$$

Quitte à prendre un y^k, on peut supposer

$$\forall\, \mathfrak{p} \in \mathcal{S}_\mathfrak{a}\ v_\mathfrak{p}(y) = 0,$$
$$\forall\, \mathfrak{p} \in \mathcal{T}_\mathfrak{a}\ v_\mathfrak{p}(y) \geq v_\mathfrak{p}(x).$$

Ainsi,

$$\frac{y}{x}\mathfrak{c} = \mathfrak{q}\mathfrak{r}$$

où $\mathfrak{q}$ est un idéal de $\mathcal{O}_K$ sans aucun facteur premier commun avec $\mathfrak{a}$. En notant $\mathfrak{b} = \frac{y}{x}\mathfrak{c}$, $\mathfrak{b}$ est bien un idéal entier de $\mathcal{O}_K$, et on a $\mathfrak{b} \sim \mathfrak{c}$. De plus, $\mathfrak{a}$ et $\mathfrak{b}$ sont premiers entre eux. □

On utilise cette propriété pour récupérer le résultat souhaité.

Proposition 3.2.39. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. Soit $x \in K$ non nul tel que $v_\mathfrak{p}(x) \geq 0$. Alors il existe a et $b \in \mathcal{O}_K$ tels que $x = \frac{a}{b}$ et $v_\mathfrak{p}(b) = 0$.*

Démonstration. On écrit l'idéal fractionnaire $x\mathcal{O}_K$ en rassemblant de part et d'autre les exposants positifs et négatifs, de sorte que

$$x\mathcal{O}_K = \mathfrak{a}\mathfrak{b}^{-1},$$

où $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux (entiers) de $\mathcal{O}_K$ sans facteurs premiers communs. Comme $v_\mathfrak{p}(x) \geq 0$, $\mathfrak{b}$ est premier avec $\mathfrak{p}$. De plus,

$$x\mathfrak{b} = \mathfrak{a}.$$

Ainsi, $\mathfrak{a}$ et $\mathfrak{b}$ sont dans la même classe de $Cl(\mathcal{O}_K)$. Par le résultat précédent, on se donne $\mathfrak{c}$ un idéal entier premier avec $\mathfrak{p}$ et dans la classe $[\mathfrak{a}]^{-1} = [\mathfrak{b}]^{-1}$. Donc on peut écrire, pour a et b dans $\mathcal{O}_K$

$$\mathfrak{a}\mathfrak{c} = (a),$$
$$\mathfrak{b}\mathfrak{c} = (b).$$

Mais alors, $\mathfrak{b}$ et $\mathfrak{c}$ sont premiers avec $\mathfrak{p}$, donc $v_\mathfrak{p}(b) = 0$. Dès lors, reste à écrire

$$\begin{aligned}(x) &= \mathfrak{a}\mathfrak{b}^{-1} \\ &= \mathfrak{a}\mathfrak{c}(\mathfrak{b}\mathfrak{c})^{-1} \\ &= (a)(b)^{-1} \\ &= \left(\frac{a}{b}\right),\end{aligned}$$

donc $x = \frac{ua}{b}$ avec $u \in \mathcal{O}_K^\times$, et on a bien $v_\mathfrak{p}(b) = 0$. □

3.2.5 • Ramification et inertie

Une fois n'est pas coutume, commençons cette sous-section par une introduction. Pour clore ce chapitre, nous allons confronter la factorisation en idéaux premiers avec celle d'extension de corps. Plus précisément, soit L/K une extension de corps de nombres. Soit $\mathfrak{p}$ un idéal de $\mathcal{O}_K$. Alors l'ensemble $\mathfrak{p}\mathcal{O}_L = \left\{ pa \in \mathcal{O}_L \,\middle|\, p \in \mathfrak{p}, a \in \mathcal{O}_L \right\}$ est un idéal de $\mathcal{O}_L$, qui admet une factorisation en idéaux premiers de $\mathcal{O}_L$ puisque ce dernier est un anneau de Dedekind. On peut donc introduire la définition suivante.

Définition 3.2.12. Soit L/K une extension de corps de nombres. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. On dit qu'un idéal premier $\mathfrak{P}$ de $\mathcal{O}_L$ vit « au-dessus » de $\mathfrak{p}$ si $\mathfrak{P}$ apparaît dans la décomposition de $\mathfrak{p}\mathcal{O}_L$ dans $\mathcal{O}_L$. De même, on dira que $\mathfrak{p}$ vit « au-dessous » de $\mathfrak{P}$. On le note abusivement $\mathfrak{P}|\mathfrak{p}$ et on adopte alors la notation suivante :

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})},$$

où $e(\mathfrak{P}/\mathfrak{p}) \in \mathbb{N}^*$. Les $e(\mathfrak{P}/\mathfrak{p})$ sont appelés indices de ramification de $\mathfrak{P}/\mathfrak{p}$.

Cette définition ne mange pas de pain : on a juste réécrit nos théorèmes en donnant un nom aux facteurs qui apparaissaient. La question va être maintenant de mieux comprendre les termes qui apparaissent dans cette décomposition.

On se propose de procéder en trois temps, qui permettront d'appréhender totalement la situation.

- On commence par mieux comprendre que ce la situation d'être « en-dessous » et « au-dessus » signifient. Pour ce faire, on regarde d'abord l'exemple classique de l'extension $K/\mathbb{Q}$, avant de généraliser les résultats à L/K. On montrera alors que, avec les notations précédentes tout, $\mathfrak{P}$ est au-dessus d'un $\mathfrak{p}$, et que $\mathfrak{p}$ est en-dessous d'au moins un $\mathfrak{P}$.
- On s'attaquera ensuite à la caractérisation des indices de ramification dans le cas $K/\mathbb{Q}$. On verra apparaître une relation remarquable, qui mettra aussi en jeu des *indices d'inertie* ainsi que $[L : K]$. On utilisera de façon cruciale les normes d'idéaux.

- On voudra alors traiter le cas d'une extension L/K. Le travail sera plus difficile, par les idéaux premiers de K ne sont plus nécessairement principaux. Pour contourner cette difficulté, on introduira la notion d'*anneaux localisés* qui auront l'avantage d'être principaux. Cela nous permettra d'atteindre le théorème 11 qui généralisera le cas précédent. Enfin, on en profite aussi pour introduire $\mathcal{O}_{K,S}$ à travers la notion d'anneau localisé.

Toute la section suivante s'inspire beaucoup de l'excellent mémoire de Gilles Auriol [16]. On adopte parfois un point de vue différent (puisque notre objectif n'est pas le même que le sien), et on enrichit d'exemples. On a choisi en particulier de distinguer le cas $K/\mathbb{Q}$ du cas L/K, le premier permettant de bien mieux comprendre le second. Néanmoins, notre travail est fortement tributaire du sien, qui nous a beaucoup aidé à comprendre l'arithmétique dans $\mathcal{O}_K$.

Au-dessus et en-dessous

Commençons donc par regarder le cas d'une extension $K/\mathbb{Q}$ avec K un corps de nombres. Cette situation est très agréable, car les idéaux premiers de $\mathbb{Z}$ sont bien connus : ce sont les $p\mathbb{Z}$ où $p \in \mathcal{P}$. Le théorème suivant permet déjà de voir qu'on a toujours un nombre premier dans les idéaux premiers de $\mathcal{O}_K$.

Proposition 3.2.40. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. Alors $\mathfrak{p}$ contient un unique nombre premier de $\mathbb{N}^*$.*

Démonstration. On voit déjà que tout idéal non nul de $\mathcal{O}_K$ contient un nombre entier. En effet, soit $x \in \mathfrak{p}$ non nul. On sait que x a un polynôme annulateur à coefficient dans $\mathbb{Z}$. Autrement dit,

$$a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0 = 0$$

où les a_i sont dans $\mathbb{Z}$. De plus, on peut prendre $a_0 \neq 0$, car sinon on factorise par x et on utilise l'intégrité de $\mathcal{O}_K$. Ainsi, on a

$$a_0 = x(-a_1 - \cdots - a_d x^{d-1}),$$

mais $x \in \mathfrak{p}$, et $-a_1 - \cdots - a_d x^d \in \mathcal{O}_K$ donc $a_0 \in \mathfrak{p} \cap \mathbb{Z}$, ce qui conclut.

Dès lors, on revient au cas spécifique où $\mathfrak{p}$ est un idéal premier. Notons p le plus petit entier positif contenu dans $\mathfrak{p}$. Comme notre idéal est premier, il est distinct de $\mathcal{O}_K$ donc $p > 1$. On suppose alors que p n'est pas premier dans $\mathbb{Z}$, et on écrit $p = ab$ avec $a > 1, b > 1$. Mais alors, a et b sont dans $\mathcal{O}_K$, et $ab \in \mathfrak{p}$ dit que par primalité $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$, ce qui est absurde. Ainsi a est premier.

Pour l'unicité, on invoque le théorème de Bézout. Si on a un autre entier premier $p' \in \mathfrak{p}$, alors on peut écrire $up + vp' = 1$ pour $u, v \in \mathbb{Z}$, ce qui implique $1 \in \mathfrak{p}$ et donc $\mathfrak{p} = \mathcal{O}_K$: absurde. □

La proposition suivante conclut donc le cas de $K/\mathbb{Q}$.

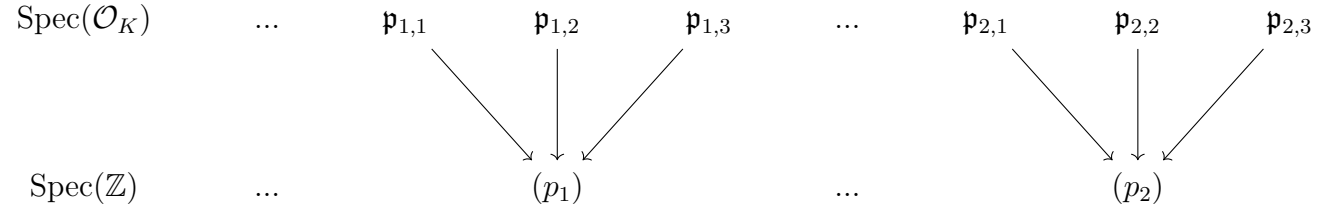
Proposition 3.2.41. *Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Alors $\mathfrak{p}$ est au-dessus d'un unique idéal premier (p) de $\mathbb{Z}$. Réciproquement, pour tout nombre premier $p \in \mathcal{P}$ il existe un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ tel que $\mathfrak{p}$ est-dessus de (p).*

Démonstration. Il suffit d'utiliser la proposition précédente et d'écrire

$$\begin{aligned} p \in \mathfrak{p} &\Leftrightarrow (p) \subset \mathfrak{p} \\ &\Leftrightarrow \mathfrak{p} | (p) \\ &\Leftrightarrow \mathfrak{p} \text{ apparaît dans la décomposition de } (p) \\ &\Leftrightarrow \mathfrak{p} \text{ est au-dessus de } (p). \end{aligned}$$

Pour la question de l'existence du $\mathfrak{p}$ au-dessus de (p), il suffit de voir que $p\mathcal{O}_K$ est un idéal de $\mathcal{O}_K$, et que donc il existe un $\mathfrak{m}$ maximal tel que $(p) \subset \mathfrak{m}$. □

On voit donc apparaître une sorte de correspondance qu'on illustre ici avec un schéma :



Le cas $K/\mathbb{Q}$ est facile car nos idéaux sont principaux, donc il suffit que le générateur p soit dans $\mathfrak{p}$ pour que $\mathfrak{p}$ vive au-dessus de (p). La situation se corse un peu dans le cas d'une extension L/K. On peut déjà caractériser un peu mieux ce que « être en-dessous » et « être au-dessus » signifient.

Proposition 3.2.42. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. Soit $\mathfrak{P}$ un idéal premier non nul de $\mathcal{O}_L$. Les conditions suivantes sont équivalentes.*

1. *$\mathfrak{P}$ divise $\mathfrak{p}\mathcal{O}_L$*
2. *$\mathfrak{p} \subset \mathfrak{P}$*
3. *$\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$*

Démonstration. La première équivalence est claire puisqu'on est sur des anneaux de Dedekind :

$$\mathfrak{P} | \mathfrak{p}\mathcal{O}_L \Leftrightarrow \mathfrak{p}\mathcal{O}_L \subset \mathfrak{p} \Leftrightarrow \mathfrak{p} \subset \mathfrak{P}.$$

Pour la troisième proposition, on a déjà un sens :

$$\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p} \Rightarrow \mathfrak{p} \subset \mathfrak{P}.$$

Réciproquement, supposons $\mathfrak{p} \subset \mathfrak{P}$. Alors l'idéal de $\mathcal{O}_K$, $\mathfrak{P} \cap \mathcal{O}_K$ contient $\mathfrak{p}$. Or $\mathfrak{p}$ est maximal, ainsi on a deux possibilités :

- Soit $\mathfrak{P} \cap \mathcal{O}_K = \mathcal{O}_K$. Mais alors $1 \in \mathfrak{P}$, ce qui est absurde car l'idéal est propre.

- Soit $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$: c'est ce qu'on voulait.

□

Cela donne donc une définition alternative mais naturelle de la situation.

Définition 3.2.13. Soit $\mathfrak{p}$ et $\mathfrak{P}$ qui vérifient les hypothèses de 3.2.42. Alors on dit que $\mathfrak{p}$ est au-dessous de $\mathfrak{P}$, et que $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$.

On peut donc démontrer notre théorème, qui généralise l'observation faite sur $L/\mathbb{Q}$.

Proposition 3.2.43. *Tout idéal premier $\mathfrak{P}$ de $\mathcal{O}_L$ est au-dessus d'un unique idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$.*

Tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ est au-dessous d'au moins un idéal premier $\mathfrak{P}$ de $\mathcal{O}_L$.

Démonstration. Le premier sens est facile : si $\mathfrak{P}$ est un idéal premier non nul de $\mathcal{O}_L$, alors $\mathfrak{P} \cap \mathcal{O}_K$ est un idéal premier non nul de $\mathcal{O}_K$ (car il contient un entier non nul en vertu de 3.2.40), qui convient.

Réciproquement, soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. Alors on sait que

$$N_L(\mathfrak{p}\mathcal{O}_L) = N_K(\mathfrak{p})^n > 1,$$

puisque $\mathfrak{p} \neq \mathcal{O}_K$. Donc $\mathfrak{p}\mathcal{O}_L$ est un idéal de $\mathcal{O}_L$ distinct de $\mathcal{O}_L$. En particulier, il est contenu dans un idéal maximal (donc premier) $\mathfrak{P}$ de $\mathcal{O}_L$. Dès lors, $\mathfrak{p} \subset \mathfrak{P}$ et $\mathfrak{P}$ vit au-dessus de $\mathfrak{p}$. □

Cela permet d'obtenir une écriture plus précise de la définition 3.2.12.

Proposition 3.2.44. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. Alors les idéaux premiers au-dessus de $\mathfrak{p}$ sont exactement ceux qui interviennent dans la décomposition de $\mathfrak{p}\mathcal{O}_L$. On peut donc écrire*

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{p} \subset \mathfrak{P}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})},$$

où $e(\mathfrak{P}/\mathfrak{p}) \in \mathbb{N}^*$

Démonstration. Cela découle immédiatement du fait que $\mathfrak{P}$ est au dessus de $\mathfrak{p}$ si et seulement si $\mathfrak{P} | \mathfrak{p}\mathcal{O}_L$ □

Cette relation permet par ailleurs de répondre à un problème naturel, celui de l'*extension des valuations*. Considérons L/K une extension de corps de nombres et $\mathfrak{p}$ un idéal premier de K. Posons-nous la question suivante :

Quels sont les idéaux premiers $\mathfrak{P}$ de $\mathcal{O}_L$ tels que $v_{\mathfrak{P}}$ étend $v_{\mathfrak{p}}$?

A priori, la notion *d'extension* de notre valuation voudrait dire que $(v_{\mathfrak{P}})_{|K} = v_{\mathfrak{p}}$. Mais en fait on autorise $(v_{\mathfrak{P}})_{|K} = av_{\mathfrak{p}}$ pour $a \in \mathbb{N}^*$, puisqu'on le verra, *les valuations égales à transformation linéaire près définissent la même topologie*. Cela sera plus clair à la lecture du chapitre 5. Soit $x \in K$, on écrit sa décomposition dans $\mathcal{O}_K$:

$$x\mathcal{O}_K = \prod_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)} \mathfrak{p}^{v_{\mathfrak{p}}(x)}$$

Mais alors la décomposition de l'idéal $x\mathcal{O}_L$ est automatique :

$$x\mathcal{O}_L = (x\mathcal{O}_K)\mathcal{O}_L = \Big(\prod_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)} \mathfrak{p}^{v_{\mathfrak{p}}(x)}\Big)\mathcal{O}_L = \prod_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)} (\mathfrak{p}\mathcal{O}_L)^{v_{\mathfrak{p}}(x)}.$$

On utilise alors les notations précédentes, ce qui donne :

$$x\mathcal{O}_L = \prod_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)} \prod_{\mathfrak{p} \subset \mathfrak{P}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})v_{\mathfrak{p}}(x)}$$

Les produits sont finis, on peut donc inverser et récupérer :

$$x\mathcal{O}_L = \prod_{\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_L)} \prod_{\mathfrak{p} \subset \mathfrak{P}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})v_{\mathfrak{p}}(x)}.$$

Mais on sait que pour chaque $\mathfrak{P}$, il y a un unique idéal $\mathfrak{p}$ en-dessous de $\mathfrak{P}$. En particulier, pour tout idéal premier non nul $\mathfrak{P}$ de $\mathcal{O}_L$ on a

$$\forall x \in K,\ v_{\mathfrak{P}}(x) = e(\mathfrak{P}/\mathfrak{p})v_{\mathfrak{p}}(x).$$

où $\mathfrak{p}$ est l'unique idéal premier de $\mathcal{O}_K$ vivant en-dessous de $\mathfrak{P}$

On peut donc conclure :

Proposition 3.2.45. *Soit L/K une extension de corps de nombres. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Les valuations $\mathfrak{P}$-adiques de L qui étendent $v_{\mathfrak{p}}$ sont exactement celles issues des $\mathfrak{P}$ vivant au-dessus de $\mathfrak{p}$.*

Au chapitre 5, on verra que les valuations $\mathfrak{p}$-adiques correspondent à des normes *ultramétriques*. En particulier, la proposition précédente permettra de caractériser les extensions possibles d'une topologie ultramétrique sur K à un sur-corps L.

Ramifications et inerties dans le cas $K/\mathbb{Q}$

Essayons maintenant de comprendre ce qu'il se passe dans le cas d'une extension $K/\mathbb{Q}$. On l'a vu, l'avantage du cas de $\mathbb{Q}$ est que $\mathbb{Z}$ est principal. En particulier, on peut manipuler avec beaucoup d'aisance les normes des idéaux, puisqu'ils correspondent aux normes des éléments.

Jusqu'à maintenant, on avait parlé des normes N et $\mathcal{N}$ sans faire de référence au corps de nombres K, car il n'y en avait qu'un seul. Dans la suite, comme on travaillera avec des extensions de corps de nombres L/K, on indicera nos normes par K et L.

Rappelons d'abord le fait très général suivant :

Proposition 3.2.46. *Soit L/K une extension de corps de nombres, de degré $r = [L : K]$. Alors on a pour tout $x \in K$:*

$$|N_L(x)| = |N_K(x)|^r$$

Démonstration. Soit $x \in K$. Par la proposition 1.4.6, on sait qu'on a les deux équations :

$$\chi_{x,L/\mathbb{Q}} = (\mu_{x,\mathbb{Q}})^{[L:\mathbb{Q}]}$$
$$\chi_{x,K/\mathbb{Q}} = (\mu_{x,\mathbb{Q}})^{[K:\mathbb{Q}]}$$

Or on sait aussi que :

$$|N_L(x)| = |\chi_{x,L/\mathbb{Q}}(0)|$$
$$|N_K(x)| = |\chi_{x,K/\mathbb{Q}}(0)|$$

Enfin, le théorème de la base télescopique donne $[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = r[K : \mathbb{Q}]$. On peut donc conclure que :

$$|N_L(x)| = |N_K(x)|^r.$$

□

Cette propriété passe donc aux idéaux principaux en vertu de la proposition 3.2.8, et on peut écrire :

Proposition 3.2.47. *Soit L/K une extension de corps de nombres, de degré $r = [L : K]$. Alors on a pour tout $x \in K$:*

$$\mathcal{N}_L(x\mathcal{O}_L) = \mathcal{N}_K(x\mathcal{O}_K)^r.$$

où $x\mathcal{O}_K$ et $x\mathcal{O}_L$ désignent les idéaux fractionnaires principaux engendrés par x dans K et L respectivement.

Dès lors, on va pouvoir obtenir une formule liant nos indices de ramification pour un $p \in \mathcal{P}$ donné. Fixons p premier, et soit $\mathfrak{p}$ un idéal de $\mathcal{O}_K$ vivant au-dessus de p. On connaît les faits suivants :

- $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ est un corps fini, puisque $\mathfrak{p}$ est maximal.
- p est l'unique premier dans $\mathfrak{p}$, donc $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension finie.

Cette dimension est appelée degré d'inertie de $\mathfrak{p}$.

Définition 3.2.14. Soit K un corps de nombres. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$, et (p) en-dessous de $\mathfrak{p}$. On appelle degré d'inertie de $\mathfrak{p}/(p)$, noté $f(\mathfrak{p}/p)$ le degré de l'extension $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)/(\mathbb{Z}/p\mathbb{Z})$.

Avec cette notation, on va pouvoir calculer la norme des $\mathfrak{p}$.

Proposition 3.2.48. *Soit K un corps de nombres. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$, et (p) en-dessous de $\mathfrak{p}$. On a la relation*

$$\mathcal{N}_K(\mathfrak{p}) = p^{f(\mathfrak{p}/p)}$$

Démonstration. Cela découle immédiatement de la définition. □

Nous sommes donc armés pour montrer le théorème qui nous intéresse. Comme on est simplement sur $K/\mathbb{Q}$, il ne s'agit pour l'instant que d'une proposition.

Proposition 3.2.49. *Soit K un corps de nombres de degré n. Soit $p \in \mathcal{P}$. On écrit sa décomposition dans $\mathcal{O}_K$:*

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

avec pour tout i, $e_i = e(\mathfrak{p}_i/p)$. On pose de plus, pour tout i, $f_i = f(\mathfrak{p}_i/p)$. On a alors l'égalité

$$\sum_{i=1}^{r} e_i f_i = n.$$

Démonstration. Il suffit de passer à la norme dans l'égalité $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$. On obtient

$$\begin{aligned}\mathcal{N}_K(p\mathcal{O}_K) &= \mathcal{N}_K(\mathfrak{p}_1)^{e_1} \cdots \mathcal{N}_L(\mathfrak{p}_r)^{e_r} \\ &= p^{e_1 f_1} \cdots p^{e_r f_r} \\ &= p^{\sum_{i=1}^{r} e_i f_i},\end{aligned}$$

où on a exploité 3.2.48 pour la dernière égalité. Mais par 3.2.47, on sait qu'on a aussi puisqu'on travaille avec des idéaux principaux :

$$\mathcal{N}_K(p\mathcal{O}_K) = \mathcal{N}_{\mathbb{Q}}(p)^n = p^n.$$

Reste à dire que $p > 1$, ce qui assure que

$$\sum_{i=1}^{r} e_i f_i = n.$$

□

Ramifications et inerties dans le cas L/K

On va maintenant essayer d'obtenir une relation analogue à celle de la proposition 3.2.49, mais pour une extension de corps de nombres quelconque L/K. Ici le problème est que la proposition 3.2.47 n'est a priori plus valable puisque les idéaux premiers de $\mathcal{O}_K$ ne sont plus principaux. Pour contourner cette difficulté, on va devoir se placer dans de nouveaux anneaux où c'est le cas : c'est la notion *d'anneau localisé*. Précisons notre propos :

Définition 3.2.15 (Partie multiplicative, localisé)**.** Soit A un anneau commutatif intègre. On note K son corps des fractions.

On appelle partie multiplicative de A une partie $S \subset A$ telle que

(i) S est stable pour la multiplication : $(s, s') \in S^2 \implies ss' \in S$.

(ii) S contient 1.

(iii) S ne contient pas 0.

On appelle de plus localisé en S de A, noté $S^{-1}A$, l'ensemble

$$S^{-1}A = \left\{ \frac{a}{s} \in K \,\middle|\, a \in A,\, s \in S \right\}.$$

On observe immédiatement que le localisé de A en S est un anneau commutatif intègre.

Fondamentalement, l'idée d'un localisé est *d'autoriser l'inversion par des éléments de la partie multiplicative considérée.*

Exemple 3.2.13. Le cas plus simple est $S = A \setminus \{0\}$, ce qui revient à rendre inversible tous les éléments de l'anneau. Dans ce cas, $S^{-1}A = K$.

Exemple 3.2.14. Si on prend $\mathfrak{p}$ un idéal premier de A, alors $A \setminus \mathfrak{p}$ est une partie multiplicative. En effet,

- Par contraposée de la définition d'idéal premier, si a et b ne sont pas dans $\mathfrak{p}$, alors ab n'est pas dans $\mathfrak{p}$,
- 1 n'est pas dans $\mathfrak{p}$,
- 0 est dans $\mathfrak{p}$.

Par exemple, dans $A = \mathbb{Z}$, on peut prendre $\mathfrak{p} = 2\mathbb{Z}$. Dans ce cas l'expression du localisé de $\mathbb{Z}$ en $\mathbb{Z} \setminus 2\mathbb{Z}$ est

$$\mathbb{Z}\left[\frac{1}{3}, \frac{1}{5}, \frac{1}{7} \ldots\right] = \left\{ \frac{n}{m} \,\middle|\, n \in \mathbb{Z},\, m \in \mathbb{Z}^* \text{ impair} \right\}.$$

En particulier, dans cet anneau tout nombre entier qui n'est pas multiple de 2 admet un inverse.

Une catégorie d'anneaux localisés va particulièrement nous intéresser : celle de ceux obtenus à partir de $\mathcal{O}_K$ et d'un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$.

Définition 3.2.16. On reprenant l'exemple précédent, si K est un corps de nombres et $\mathfrak{p}$

un idéal premier non nul de $\mathcal{O}_K$, on note $\mathcal{O}_{K,\mathfrak{p}}$ le localisé de $\mathcal{O}_K$ en $\mathcal{O}_K \setminus \mathfrak{p}$. Autrement dit,

$$\mathcal{O}_{K,\mathfrak{p}} = \left\{ \frac{a}{b} \in K \,\middle|\, a \in \mathcal{O}_K,\, b \in \mathcal{O}_K \setminus \mathfrak{p} \right\}.$$

Bien que cela ne nous intéresse pas directement ici, on ne résiste pas à la tentation d'en profiter pour introduire $\mathcal{O}_{K,S}$, qui est au centre de notre étude !

Définition 3.2.17. Soit K un corps de nombres. Soit S un ensemble fini d'idéaux premiers non nuls de $\mathcal{O}_K$. On note $\mathcal{S}$ l'ensemble des éléments x de $\mathcal{O}_K$ dont la décomposition de (x) ne fait intervenir que des idéaux de S.

On note alors $\mathcal{O}_{K,S}$ le localisé de $\mathcal{O}_K$ en la partie multiplicative $\mathcal{S}$.

On vérifie que $\mathcal{S}$ est bien une partie multiplicative.

- Si x et $y \in \mathcal{S}$, alors la décomposition de (xy) est le produit des décompositions de (x) et (y), donc $xy \in \mathcal{S}$.
- La décomposition de $(1) = \mathcal{O}_K$ ne fait intervenir aucun idéal premier, donc $1 \in \mathcal{S}$.
- La décomposition de (0) fait (par convention) intervenir tous les idéaux premiers, donc $0 \notin \mathcal{S}$.

Exemple 3.2.15. Plaçons nous dans $\mathbb{Z}$, et prenons $S = \{2\mathbb{Z}, 3\mathbb{Z}\}$. Alors, on a

$$\mathcal{S} = \left\{ \pm 2^n 3^m \,\middle|\, n \in \mathbb{N},\, m \in \mathbb{N} \right\},$$

d'où

$$\mathcal{O}_{\mathbb{Q},S} = \left\{ \frac{a}{2^n 3^m} \,\middle|\, a \in \mathbb{Z},\, n \in \mathbb{N},\, m \in \mathbb{N} \right\}.$$

Dans ce cas, on autorise l'inversibilité des éléments multiples de 2 et 3, donc

$$\mathcal{O}_{\mathbb{Q},S}^{\times} = \left\{ \pm 2^n 3^m \,\middle|\, n \in \mathbb{Z},\, m \in \mathbb{Z} \right\}.$$

On va maintenant montrer l'intérêt des $\mathcal{O}_{K,\mathfrak{p}}$ pour nous. On l'a vu, la difficulté qu'on rencontre maintenant est que $\mathfrak{p}$ n'est pas un idéal principal de $\mathcal{O}_K$. Mais on va montrer que $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ l'est dans $\mathcal{O}_{K,\mathfrak{p}}$, ce qui nous permettra de conclure.

Commençons par voir une propriété fondamentale des localisés est que les idéaux du localisé forment une sous-partie des idéaux de l'anneau de départ, au sens suivant.

Proposition 3.2.50. *Soit A un anneau commutatif intègre. Soit S une partie multiplicative de A.*

Alors pour tout idéal $\mathfrak{P}$ de $S^{-1}A$, on a

$$(\mathfrak{P} \cap A)S^{-1}A = \mathfrak{P},$$

et l'application

$$\phi : \mathfrak{P} \mapsto \mathfrak{P} \cap A$$

est une injection de l'ensemble des idéaux de $S^{-1}A$ dans l'ensemble des idéaux de A.

Démonstration. Soit $\mathfrak{P}$ un idéal de $S^{-1}A$. Comme $A \subset S^{-1}A$, on obtient

$$\mathfrak{P} \cap A \subset \mathfrak{P},$$

donc

$$(\mathfrak{P} \cap A)S^{-1}A \subset \mathfrak{P}.$$

Réciproquement, soit $x \in \mathfrak{P}$, qu'on écrit $x = \frac{a}{s}$ où $a \in A$ et $s \in S$. Alors $sx \in \mathfrak{P}$ puisque $s \in S \subset A \subset A'$ et $\mathfrak{P}$ est un idéal de $S^{-1}A$.

Ainsi $a = sx \in \mathfrak{P} \cap A$. Comme $\frac{1}{s} \in S^{-1}A$, on peut donc conclure

$$x = \frac{a}{s} \in (\mathfrak{P} \cap A)S^{-1}A,$$

et ainsi

$$(\mathfrak{P} \cap A)S^{-1}A = \mathfrak{P}.$$

En notant

$$\theta : \mathfrak{P} \mapsto \mathfrak{P}S^{-1}A,$$

on constate finalement que $\theta \circ \phi = id$, donc ϕ est injective. □

Cette proposition permet aussi d'obtenir une propriété sur des localisations « emboîtées ».

Proposition 3.2.51. *Soit A un anneau intègre. Soient S une partie multiplicative et $\mathfrak{a}$ un idéal de A tels que $S \cap \mathfrak{a} = \emptyset$. Alors,*

$$(S^{-1}A)/(\mathfrak{a}S^{-1}A) \cong A/\mathfrak{a}.$$

Démonstration. On dispose déjà du morphisme d'anneaux composés

$$A \hookrightarrow S^{-1}A \twoheadrightarrow (S^{-1}A)/\mathfrak{a}S^{-1}A.$$

Ce morphisme a pour noyau $(\mathfrak{a}S^{-1}A) \cap A = \mathfrak{a}$ d'après la proposition précédente. Cela permet donc de récupérer l'injection

$$\phi : A/\mathfrak{a} \hookrightarrow S^{-1}A/\mathfrak{a}S^{-1}A.$$

Reste à voir la surjectivité de ϕ. Soit $x = \frac{a}{s} \in S^{-1}A$. On a $s \in S$, donc $s \notin \mathfrak{a}$ puisque $S \cap \mathfrak{a} = \emptyset$.

Or $\mathfrak{a}$ est maximal, donc $\overline{s}$ est inversible dans $A/\mathfrak{a}$ (qui est un corps). On a donc $b \in A$ tel que

$$\overline{bs} = \overline{1} \text{ dans } A/\mathfrak{a},$$

d'où on déduit immédiatement que

$$\frac{a}{s} - ab = \frac{a}{s}(1 - bs) \in \mathfrak{a}S^{-1}A.$$

Ainsi,

$$\phi(\overline{ab}) = \overline{(\frac{a}{s})} = \overline{x} \text{ dans } (S^{-1}A/\mathfrak{a}S^{-1}A),$$

donc ϕ est une bijection, ce qui conclut. □

Exemple 3.2.16. Cette proposition semble quelque peu indigeste. Regardons ce qu'il se passe sur un exemple. Prenons $A = \mathbb{Z}$, $S = \mathbb{Z} \setminus 2\mathbb{Z}$, donc $A' = \mathbb{Z}_{(2)}$. Dans $\mathbb{Z}$, les idéaux premiers sont maximaux, donc on peut prendre $\mathfrak{a} = 3\mathbb{Z}$. Ainsi,

$$A/\mathfrak{a} = \mathbb{Z}/3\mathbb{Z}.$$

De l'autre côté, on peut exprimer $\mathfrak{a}A'$:

$$\mathfrak{a}A' = \left\{ \frac{m}{n} \,\middle|\, m \text{ multiple de } 3 \text{ , } n \text{ impair} \right\}.$$

Il est donc assez clair que les classes d'un élément de $\mathbb{Z}_{(2)}$ modulo $3\mathbb{Z}_{(2)}$ ne dépendent que de la classe du numérateur modulo 3, d'où l'isomorphisme

$$\mathbb{Z}_{(2)}/3\mathbb{Z}_{(2)} \cong \mathbb{Z}/3\mathbb{Z}.$$

Au vu de la proposition 3.2.50, il est assez naturel de se demander s'il est possible de caractériser simplement les idéaux d'un anneau localisé. C'est le cas lorsqu'on regarde la situation particulière d'un $\mathcal{O}_{K,\mathfrak{p}}$.

Exemple 3.2.17. Si on reprend notre exemple de $\mathcal{O}_{\mathbb{Q},2\mathbb{Z}}$. On voit que les idéaux de cet anneau sont les

$$\mathfrak{a} = 2^n \mathcal{O}_{\mathbb{Q},2\mathbb{Z}},$$

où n est un nombre entier.

En effet, si on prend $\mathfrak{a}$ un idéal de $\mathcal{O}_{\mathbb{Q},2\mathbb{Z}}$, on sait que

$$\mathfrak{a} = (\mathfrak{a} \cap \mathbb{Z})\mathcal{O}_{\mathbb{Q},2\mathbb{Z}},$$

mais on peut écrire la factorisation de $\mathfrak{a} \cap \mathbb{Z}$ dans $\mathbb{Z}$:

$$\mathfrak{a} \cap \mathbb{Z} = (2\mathbb{Z})^n \mathfrak{b},$$

où $2\mathbb{Z}$ et $\mathfrak{b}$ sont premiers entre eux. Donc $\mathfrak{b}$ contient des nombres impairs, qui sont inversibles dans $\mathcal{O}_{\mathbb{Q},2\mathbb{Z}}$. Ainsi,

$$\mathfrak{b}\mathcal{O}_{\mathbb{Q},2\mathbb{Z}} = \mathcal{O}_{\mathbb{Q},2\mathbb{Z}}.$$

Reste à écrire que

$$\mathfrak{a} = (\mathfrak{a} \cap \mathbb{Z})\mathcal{O}_{\mathbb{Q},2\mathbb{Z}} = (2\mathbb{Z})^n \mathfrak{b}\mathcal{O}_{\mathbb{Q},2\mathbb{Z}} = (2\mathbb{Z})^n \mathcal{O}_{\mathbb{Q},2\mathbb{Z}}.$$

On observe donc que les idéaux de notre $\mathcal{O}_{K,\mathfrak{p}}$ sont ici de la forme

$$\mathfrak{P} = \mathfrak{p}^n \mathcal{O}_{K,\mathfrak{p}}.$$

C'est en fait un fait très général. On le généralise à la proposition suivante, dont la démonstration est quasiment mot pour mot celle qu'on vient de faire.

Proposition 3.2.52. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. Alors tout idéal de $\mathcal{O}_{K,\mathfrak{p}}$ est de la forme $\mathfrak{p}^n \mathcal{O}_{K,\mathfrak{p}}$ pour $n \in \mathbb{N}$.*

Démonstration. Soit $\mathfrak{a}$ un idéal de $\mathcal{O}_{\mathbb{Q},\mathfrak{p}}$, on sait que

$$\mathfrak{a} = (\mathfrak{a} \cap \mathcal{O}_K)\mathcal{O}_{K,\mathfrak{p}},$$

mais on peut écrire la factorisation de $\mathfrak{a} \cap \mathcal{O}_K$ dans $\mathcal{O}_K$:

$$\mathfrak{a} \cap \mathbb{Z} = \mathfrak{p}^n \mathfrak{b},$$

où $\mathfrak{p}$ et $\mathfrak{b}$ sont premiers entre eux. Donc $\mathfrak{b}$ contient des éléments de $\mathcal{O}_K \setminus \mathfrak{p}$, qui sont inversibles dans $\mathcal{O}_{K,\mathfrak{p}}$. Ainsi,

$$\mathfrak{b}\mathcal{O}_{K,\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}$$

Reste à écrire que

$$\mathfrak{a} = (\mathfrak{a} \cap \mathcal{O}_K)\mathcal{O}_{K,\mathfrak{p}} = \mathfrak{p}^n \mathfrak{b}\mathcal{O}_{K,\mathfrak{p}} = \mathfrak{p}^n \mathcal{O}_{K,\mathfrak{p}},$$

ce qui conclut. □

On en déduit le fait fondamental suivant, qui justifie qu'on regarde les anneaux localisés ici.

Proposition 3.2.53. *Soient K un corps de nombres et $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. Alors l'anneau commutatif intègre $\mathcal{O}_{K,\mathfrak{p}}$ est principal. En particulier, il est de Dedekind. De plus, son unique idéal maximal $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ s'écrit $\pi\mathcal{O}_{K,\mathfrak{p}}$ où $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$.*

Démonstration. Au vu de la proposition 3.2.52, on a juste à prouver que $\mathfrak{q} = \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ est principal. On sait que $\mathfrak{p} \neq \mathfrak{p}^2$, donc on peut prendre un $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. En particulier, on a $\pi \in \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$, mais aussi $\pi \notin (\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}})^2$. En effet, si par l'absurde $\pi \in (\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}})^2$, on peut écrire :

$$\pi = pq\frac{a}{b}$$

avec $p, q \in \mathfrak{p}$, $a \in \mathcal{O}_K$ et $b \in \mathcal{O}_K/\mathfrak{p}$. Mais alors en évaluant la valuation $\mathfrak{p}$-adique de cette expression il vient :

$$1 = v_{\mathfrak{p}}(p) + v_{\mathfrak{p}}(q) + v_{\mathfrak{p}}(a) \geq 2$$

C'est absurde. Ainsi on a un tel π. Mais $\pi\mathcal{O}_{K,\mathfrak{p}}$ est un idéal de $\mathcal{O}_{K,\mathfrak{p}}$, donc on a n entier tel que

$$\pi\mathcal{O}_{K,\mathfrak{p}} = \mathfrak{p}^n\mathcal{O}_{K,\mathfrak{p}}.$$

Enfin, $n \geq 2$ est exclu puisque sinon on aurait $\pi \in \mathfrak{p}^2$. Ainsi,

$$\pi\mathcal{O}_{K,\mathfrak{p}} = \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}},$$

et $\mathcal{O}_{K,\mathfrak{p}}$ est bien principal. □

Reste maintenant à exploiter notre nouvel anneau (localisé) pour conclure. On regarde à présent le localisé de $\mathcal{O}_L$ par rapport à un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$.

A partir maintenant, on par souci de clarté $\mathfrak{p}\mathcal{O}_K$ l'ensemble des $x \in \mathcal{O}_L$ tels que $x \in \mathfrak{p}$, qui est donc une sous-partie de $\mathcal{O}_L$, mais pas un idéal de $\mathcal{O}_L$. On voit alors que $\mathcal{O}_K/(\mathfrak{p}\mathcal{O}_K)$ est une partie multiplicative de $\mathcal{O}_L$:

- Si a et $b \in \mathcal{O}_K/\mathfrak{p}$, alors $ab \in \mathcal{O}_K$ mais $ab \notin \mathfrak{p}$ car l'idéal est premier dans $\mathcal{O}_K$
- $1 \in \mathcal{O}_K/\mathfrak{p}$
- $0 \notin \mathcal{O}_K/\mathfrak{p}$

Cela permet de regarder la définition suivante.

Définition 3.2.18. Soit L/K une extension de corps de nombres de degré n. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. On note $\mathcal{O}_{L,\mathfrak{p}}$ l'anneau :

$$\mathcal{O}_{L,\mathfrak{p}} = \left\{ \frac{a}{b} \in L \,\middle|\, a \in \mathcal{O}_L,\, b \in \mathcal{O}_K \setminus \mathfrak{p} \right\}$$

$\mathcal{O}_{L,\mathfrak{p}}$ est donc le localisé de $\mathcal{O}_L$ en $\mathcal{O}_K \setminus \mathfrak{p}$.

Le point clé de cette définition est de constater les deux propriétés suivantes, qui vont bien permettre de conclure.

Proposition 3.2.54.

(i) $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}$

(ii) $\mathcal{O}_{L,\mathfrak{p}}$ *est un* $\mathcal{O}_{K,\mathfrak{p}}$*-module libre de rang* n*.*

Démonstration. Le (i) découle de la proposition 3.2.51. En effet, rappelons que $\mathcal{O}_{L,\mathfrak{p}}$ est le localisé de $\mathcal{O}_L$ par rapport à $\mathcal{O}_K \setminus \mathfrak{p}$. Or ici , $\mathfrak{p}\mathcal{O}_L$ est un idéal de $\mathcal{O}_L$ qui n'intersecte pas $\mathcal{O}_K \setminus \mathfrak{p}$ puisque $(\mathfrak{p}\mathcal{O}_L) \cap \mathcal{O}_K = \mathfrak{p}$. Par la proposition 3.2.51, on peut conclure que :

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}$$

Pour le (ii), on généralise les résultats obtenus jusqu'à maintenant en ce qui concerne le rang de $\mathcal{O}_K$ comme $\mathbb{Z}$-module libre. On a vu en 2.2.4 que ce rang était $[K : \mathbb{Q}]$. On pourrait tout-à-fait refaire les preuves en se plaçant dans une extensions de corps de nombres L/K et non plus $K/\mathbb{Q}$. On obtient alors le résultat suivant :

$$\mathcal{O}_L \text{ est un } \mathcal{O}_K\text{-module libre de rang } n = [L : K]$$

Dès lors, soit $(e_1, ..., e_n)$ une $\mathcal{O}_K$-base de $\mathcal{O}_L$. D'après la définition de $\mathcal{O}_{L,\mathfrak{p}}$, on voit immédiatement que cette famille génère $\mathcal{O}_{L,\mathfrak{p}}$ sur $\mathcal{O}_{K,\mathfrak{p}}$. En ce qui concerne la liberté, on se donne une combinaison $\mathcal{O}_{K,\mathfrak{p}}$ linéaire nulle

$$\sum_{i=1}^{n} \frac{a_i}{b_i} e_i = 0.$$

avec les a_i dans $\mathcal{O}_K$ et les b_i dans $\mathcal{O}_K \setminus \mathfrak{p}$. On multiplie par $\prod_{i=1}^n b_i$.

$$\sum_{i=1}^{n} \Big(a_i \prod_{j \neq i} b_j\Big) e_i = 0.$$

Par liberté sur $\mathcal{O}_K$, il vient :

$$\forall i \in \{1, ..., n\},\ a_i \prod_{j \neq i} b_j = 0.$$

Reste à diviser à nouveau par $\prod_{i=1}^n b_i$ (qui est non nul) pour conclure que les $\frac{a_i}{b_i}$ étaient nuls : cela donne la liberté qu'on souhaitait. Ainsi $\mathcal{O}_{L,\mathfrak{p}}$ est un $\mathcal{O}_{K,\mathfrak{p}}$-module libre de rang n. □

On en déduit le lemme suivant qui montre tout l'intérêt du passage aux localisés : on est parvenu à contourner la difficulté posée par le fait que $\mathfrak{p}$ n'était pas principal !

Proposition 3.2.55. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. Alors on a l'égalité*

$$|\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L| = |\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K|^n.$$

Démonstration. On sait déjà que tous ces ensembles sont finis : leurs cardinaux sont les normes des idéaux concernés. On dispose de plus des deux isomorphismes suivants, issus respectivement du (i) de la proposition précédente et de la proposition 3.2.51.

$$\mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}} \cong \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$$
$$\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} \cong \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K.$$

On veut donc montrer que :

$$(\mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}) \cong (\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}})^n$$

Le (ii) de la proposition précédente dit que $\mathcal{O}_{L,\mathfrak{p}}$ est un $\mathcal{O}_{K,\mathfrak{p}}$ module libre de rang $n = [L : K]$. Soit $(e_1, ..., e_n)$ une $\mathcal{O}_{K,\mathfrak{p}}$-base de $\mathcal{O}_{L,\mathfrak{p}}$. On dispose donc de l'isomorphisme de $\mathcal{O}_{K,\mathfrak{p}}$-modules

$$\Phi \ : \left| \begin{array}{ccc} \mathcal{O}_{L,\mathfrak{p}} & \to & (\mathcal{O}_{K,\mathfrak{p}})^n \\ \sum_{i=1}^n \frac{a_i}{b_i} e_i & \mapsto & (\frac{a_1}{b_1}, ..., \frac{a_n}{b_n}). \end{array} \right.$$

avec les a_i dans $\mathcal{O}_K$ et les b_i dans $\mathcal{O}_K \setminus \mathfrak{p}$. On considère alors le morphisme de $\mathcal{O}_{K,\mathfrak{p}}$-modules surjectif :

$$\tilde{\Phi} \ : \left| \begin{array}{ccc} \mathcal{O}_{L,\mathfrak{p}} & \to & (\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}})^n \\ \sum_{i=1}^n \frac{a_i}{b_i} e_i & \mapsto & (\overline{\frac{a_1}{b_1}}, ..., \overline{\frac{a_n}{b_n}}). \end{array} \right.$$

Reste à montrer que $\ker(\tilde{\Phi}) = \mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}$.

On a déjà un sens facile. Soit $x \in \mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}$, on peut écrire $x = \pi y$ où $\pi \in \mathfrak{p}$ et $y \in \mathcal{O}_{L,\mathfrak{p}}$. Mais si on écrit $y = \sum_{i=1}^n \frac{a_i}{b_i} e_i$, il vient :

$$x = \sum_{i=1}^n \frac{\pi a_i}{b_i} e_i$$

Mais les πa_i sont dans $\mathcal{O}_K$, donc $\Phi(x) = (\overline{\frac{\pi a_1}{b_1}}, ..., \overline{\frac{\pi a_n}{b_n}})$ et $\tilde{\Phi}(x) = 0$. Ainsi $\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}} \subset \ker(\tilde{\Phi})$.

Pour l'autre sens, on sait par la proposition 3.2.53 que $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ est un idéal principal de $\mathcal{O}_{K,\mathfrak{p}}$, et même qu'il s'écrit $\pi\mathcal{O}_{K,\mathfrak{p}}$ avec $\pi \in \mathfrak{p}$. Dès lors, soit $x \in \ker(\tilde{\Phi})$. Cela revient à dire que $x = \sum_{i=1}^n \frac{a_i}{b_i} e_i$ où tous les $\frac{a_i}{b_i}$ sont dans $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$. Mais alors, on peut dire que pour tout i

$$\frac{a_i}{b_i} = \pi \frac{a_i'}{b_i'}$$

où les $\frac{a_i'}{b_i'}$ sont dans $\mathcal{O}_{K,\mathfrak{p}}$. Dès lors, il vient

$$x = \pi \sum_{i=1}^n \frac{a_i'}{b_i'} e_i \in \mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}.$$

Ainsi on a bien $\ker(\tilde{\Phi}) = \mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}$. On peut donc conclure qu'on a l'isomorphisme de $\mathcal{O}_{K,\mathfrak{p}}$-modules :

$$(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) \cong (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^n$$

Cela conclut que

$$|\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L| = |\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K|^n.$$

□

C'est exactement ce qu'il nous fallait ! On réécrit cela avec les normes.

Proposition 3.2.56. *Soit L/K une extension de corps de nombres de degré n. Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$. Alors on a l'égalité*

$$\mathcal{N}_L(\mathfrak{a}\mathcal{O}_L) = \mathcal{N}_K(\mathfrak{a})^n.$$

Démonstration. On vient de le montrer pour les idéaux premiers de $\mathcal{O}_K$. La formule générale vient en décomposant les idéaux de $\mathcal{O}_K$ en facteurs premiers et en utilisant la multiplicativité de la norme. □

Comme dans le cas de $\mathbb{Q}$, on fait maintenant intervenir les degrés d'inertie. Si $\mathfrak{P}$ est au dessus de $\mathfrak{p}$, alors ces idéaux sont maximaux dans $\mathcal{O}_L$ et $\mathcal{O}_K$ respectivement. En particulier, $\mathcal{O}_L/\mathfrak{P}$ et $\mathcal{O}_K/\mathfrak{p}$ sont des corps. De plus, on a le morphisme composé

$$\mathcal{O}_K \hookrightarrow \mathcal{O}_L \to \mathcal{O}_L/\mathfrak{P}.$$

Son noyau est exactement $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$ en vertu de 3.2.42. Donc on a une injection

$$\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P}.$$

Donc $\mathcal{O}_L/\mathfrak{P}$ est une extension de corps de $\mathcal{O}_K/\mathfrak{p}$, qui est finie car les corps sont finis (leur cardinaux sont les normes des idéaux). On peut donc définir et rappeler les notions suivantes.

Définition 3.2.19. Soit $\mathfrak{P}$ un idéal de $\mathcal{O}_L$ qui vit au-dessus de $\mathfrak{p}$ un idéal de $\mathcal{O}_K$. Alors,

- On appelle indice de ramification de $\mathfrak{P}/\mathfrak{p}$ l'entier $e(\mathfrak{P}/\mathfrak{p}) = v_{\mathfrak{P}}(\mathfrak{p}\mathcal{O}_L)$,
- On appelle degré d'inertie de $\mathfrak{P}/\mathfrak{p}$, noté $f(\mathfrak{P}/\mathfrak{p})$ le degré de l'extension $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$.

On obtient exactement la proposition 3.2.48 qu'on avait jusqu'à maintenant uniquement dans le cas $K/\mathbb{Q}$.

Proposition 3.2.57. *Sous ces conditions, on a l'égalité*

$$\mathcal{N}_L(\mathfrak{P}) = \mathcal{N}_K(\mathfrak{p})^{f(\mathfrak{P}/\mathfrak{p})}.$$

Démonstration. Par définition, $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$ est une extension de degré $f(\mathfrak{P}/\mathfrak{p})$. Mais ces deux corps sont de cardinal fini, donc

$$|\mathcal{O}_L/\mathfrak{P}| = |\mathcal{O}_K/\mathfrak{p}|^{f(\mathfrak{P}/\mathfrak{p})}.$$

C'est exactement ce qu'on voulait. □

On obtient alors le théorème fondamental suivant, qui généralise 3.2.49.

Théorème 11. *Soit L/K une extension de corps de nombres de degré n. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. On écrit sa décomposition dans $\mathcal{O}_L$:*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

et on pose de plus, pour tout i, $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. On a alors l'égalité

$$\sum_{i=1}^{r} e_i f_i = n.$$

Démonstration. Il suffit de passer à la norme dans l'égalité $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. On obtient

$$\begin{aligned} \mathcal{N}_L(\mathfrak{p}\mathcal{O}_L) &= \mathcal{N}_L(\mathfrak{P}_1)^{e_1} \cdots \mathcal{N}_L(\mathfrak{P}_r)^{e_r} \\ &= \mathcal{N}_K(\mathfrak{p})^{e_1 f_1} \cdots \mathcal{N}_K(\mathfrak{p})^{e_r f_r} \\ &= \mathcal{N}_K(\mathfrak{p})^{\sum_{i=1}^{r} e_i f_i}, \end{aligned}$$

où on a exploité 3.2.57 pour la dernière égalité. Mais par 3.2.56, on sait qu'on a aussi

$$\mathcal{N}_L(\mathfrak{p}\mathcal{O}_L) = \mathcal{N}_K(\mathfrak{p})^n.$$

Reste à dire que $\mathcal{N}_K(\mathfrak{p}) > 1$, ce qui assure que

$$\sum_{i=1}^{r} e_i f_i = n.$$

□

Tout cela appelle un peu de terminologie.

Définition 3.2.20. En reprenant les notations du théorème 11,

1. Si l'un des e_i n'est pas 1, on dit que $\mathfrak{p}$ est ramifié sur L, et totalement ramifié si $r = 1$ et $e_1 = n$, c'est-à-dire si $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^n$,
2. Si $r = 1$ et $e_1 = 1$, (ie $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}$), on dit que $\mathfrak{p}$ est inerte sur L,
3. Si pour tout i on a $e_i = f_i = 1$, on dit que $\mathfrak{p}$ est décomposé sur L : $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_n$.

Exemple 3.2.18. On peut reprendre notre exemple de $K = \mathbb{Q}(\sqrt{d})$ pour d un entier sans facteurs carrés. L'extension $K/\mathbb{Q}$ est de degré 2, et les idéaux premiers de $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$ sont donnés par les nombres premiers. Soit $p \in \mathcal{P}$. Comme $\sum_{i=1}^{r} e_i f_i = 2$, on n'a que trois cas possibles :

1. $r = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1$. Donc $p\mathbb{Z}$ est décomposé dans K,
2. $r = 1$, $e_1 = 1$, $f_1 = 2$. Donc $p\mathbb{Z}$ est inerte dans K,
3. $r = 1$, $e_1 = 2$, $f_1 = 1$. Donc $p\mathbb{Z}$ se ramifie dans K.

A quoi cela a-t-il servi ? On verra au chapitre 6 que le théorème 11 va permettre de choisir un bon système de représentant afin que toutes les valeurs absolues disponibles sur K se compensent exactement. Ce choix est permis par les deux résultats fondamentaux que nous avons montrés :

- La *taille* d'un élément est mesuré par sa norme N. Pour L/K une extension de degré n et $x \in K$, on a vu en 3.2.46 qu'on avait $|N_L(x)| = |N_K(x)|^n$: regarder x en dimension n fois supérieure induit un facteur n.
- La *complexité arithmétique* d'un élément apparaît à travers les idéaux premiers. Or on a vu en 3.2.57 que pour $\mathfrak{P}_\mathfrak{i}$ au-dessus de $\mathfrak{p}$ on avait $\mathcal{N}_L(\mathfrak{P}_\mathfrak{i}) = \mathcal{N}_K(\mathfrak{p})^{f_i}$, et que de plus $\sum_{i=1}^{r} e_i f_i = n$.

Durant ce chapitre, ces deux points de vue sont apparus successivement et ont paru s'articuler naturellement. Or le chapitre 5 montrera qu'il s'agit d'un résultat tout-à-fait exceptionnel. Lorsqu'on regarde K en cherchant les différentes valeurs absolues qu'il est possible d'y définir, on découvre effectivement qu'elles se séparent en deux classes qui correspondent aux deux

cas exposés juste avant, et qui s'expriment en un certain sens à travers la norme de éléments d'une part et les idéaux premiers intervenant dans leur décomposition d'autre part. Ainsi, les résultats de cette sous-partie permettront d'unir ces points de vue afin de bien définir la notion de *hauteur*, qui reflète la complexité d'un élément de K.

4
LE THÉORÈME DES UNITÉS DE DIRICHLET

Maintenant que nous avons clos le chapitre lié à l'arithmétique sur $\mathcal{O}_K$, on retourne à la question du groupe des unités $\mathcal{O}_K^\times$. On a souvent dit jusqu'à présent que ce groupe était compliqué et finalement assez mystérieux. L'une des motivations du passage à l'étude des idéaux était d'ailleurs qu'elle permettait d'oublier totalement les unités. On se propose maintenant d'affronter $\mathcal{O}_K^\times$ et d'élucider sa structure : c'est l'enjeu du *théorème des unités de Dirichlet* (1805-1859).

Avant de nous lancer, justifions la pertinence de l'étude de ce groupe pour notre propos. Puisque nous avons construit notre arithmétique à l'aide des idéaux, on peut légitimement s'interroger sur l'intérêt de ce chapitre. Pourtant, outre le fait que le *théorème des unités* est un résultat remarquable en soi qui mérite à ce titre d'être mentionné et démontré, il va jouer un rôle crucial dans la démonstration du théorème final. En effet, il permet d'élucider la structure de $\mathcal{O}_{K,S}^\times$, qui est l'ensemble dans lequel vivent les inconnues de l'équation aux S-unités.

On déjà rencontré $\mathcal{O}_{K,S}$ à deux reprises : en introduction bien sûr, mais aussi à la fin du chapitre précédent où on l'avait défini à l'aide de la notion d'anneau localisé. Rappelons la définition que nous avions vu alors.

Définition 4.0.1. Soit K un corps de nombres. Soit S un ensemble fini d'idéaux premiers non nuls de $\mathcal{O}_K$. On note $\mathcal{S}$ l'ensemble des éléments x de $\mathcal{O}_K$ dont la décomposition de l'idéal fractionnaire (x) ne fait intervenir que des idéaux de S.

On note alors $\mathcal{O}_{K,S}$ le localisé de $\mathcal{O}_K$ en la partie multiplicative $\mathcal{S}$.

$\mathcal{O}_{K,S}$ peut donc aussi se définir à partir des valuations $\mathfrak{p}$-adiques : ses éléments sont ceux qui sont entiers en dehors de S. On a donc la définition équivalente suivante.

Définition 4.0.2. Soit K un corps de nombres. Soit S un ensemble fini d'idéaux premiers non nuls de $\mathcal{O}_K$. On note $\mathcal{O}_{K,S}$ l'ensemble

$$\mathcal{O}_{K,S} = \left\{ x \in K \,\middle|\, \forall \mathfrak{p} \notin S, v_\mathfrak{p}(x) \geq 0 \right\}.$$

$\mathcal{O}_{K,S}^\times$ apparaît alors comme le groupe des unités de cet anneau. Résumons les deux approches.

- En regardant $\mathcal{O}_{K,S}$, comme localisé, on a autorisé la division par les éléments s ne s'écrivant qu'avec des idéaux de S. Donc si on veut les unités de cet anneau, on va aussi devoir imposer que les numérateurs de nos fractions ne s'écrivent qu'avec des idéaux de S.
- En regardant $\mathcal{O}_{K,S}$ avec la définition utilisant la valuation $\mathfrak{p}$-adique, on voit directement que si $x \in \mathcal{O}_{K,S}^\times$, alors pour tous les $\mathfrak{p}$ hors de S on a $v_\mathfrak{p}(x) = 0$ puisque de façon générale $v_\mathfrak{p}(x^{-1}) = -v_\mathfrak{p}(x)$.

Ces deux définitions donnent la même intuition : $\mathcal{O}_{K,S}^\times$ est l'ensemble des éléments de K dont la décomposition en idéaux premiers ne fait intervenir que des idéaux de S. À abus de langage près, *il s'agit de la restriction de K aux éléments qui ne s'expriment qu'avec S.*

Définition 4.0.3 (S-unités)**.** Soit S un ensemble d'idéaux premiers de $\mathcal{O}_K$. On dit que $x \in K$ est une S-unité si la décomposition de l'idéal fractionnaire (x) ne fait intervenir que des idéaux de S (avec puissances positives ou négatives). Autrement dit, il s'agit de l'ensemble

$$\left\{ x \in K \,\middle|\, \forall \mathfrak{p} \notin S \, v_\mathfrak{p}(x) = 0 \right\}.$$

L'ensemble des S-unités est donc exactement égal au groupe $\mathcal{O}_{K,S}^\times$.

Motivation : déterminer la dimension d'un espace vectoriel

Il s'agit donc maintenant d'élucider la structure de $\mathcal{O}_{K,S}^\times$. Plus précisément, la preuve du théorème final repose sur l'extension de $\mathcal{O}_{K,S}^\times$ en un $\mathbb{Q}$-espace vectoriel de dimension finie. A partir de là, on pourra pratiquer de la géométrie à l'aide d'une norme reflétant la complexité des éléments. Ce processus est largement détaillé dans la partie 8. Notons dès maintenant que, puisque $\mathcal{O}_{K,S}^\times$ est multiplicatif, le $+$ de notre espace vectoriel correspondra à la multiplication dans notre groupe.

Regardons d'abord une façon de construire un $\mathbb{Q}$ espace vectoriel à partir d'un sous-groupe multiplicatif H de $\mathbb{C}^*$ quelconque. Deux obstructions apparaissent.

- D'abord, on peut munir H d'une multiplication externe par des éléments de $\mathbb{Z}$ (définie par $n \cdot x = x^n$), mais *a priori* pas par $\mathbb{Q}$. Cela reviendrait en effet à prendre des racine n-ième des éléments de H, qui n'ont aucune raison d'être dans ce groupe. Elles ne sont d'ailleurs définies dans $\mathbb{C}$ qu'à multiplication par une racine de l'unité près.
- Cette première obstruction peut se résoudre en considérant un groupe G plus gros avec ces racines : c'est le processus de $\mathbb{Q}$-*clôture*. De façon plus précise,

  $$G = \left\{ x \in \mathbb{C}^* \,\middle|\, \exists n \in \mathbb{N}^* x^n \in H \right\}.$$

  Encore faut-il régler le sort des racines de l'unité qui gênent pour bien définir de façon unique l'opération $\frac{1}{n} \cdot x = x^{\frac{1}{n}}$.

Cette dernière observation invite à quotienter le groupe G par sa torsion.

Définition 4.0.4 (Torsion d'un groupe)**.** Soit $(G, *)$ un groupe abélien, et e son élément neutre. On dit que $x \in G$ est de torsion s'il est d'ordre fini, c'est-à-dire s'il existe $n \in \mathbb{N}^*$ tel que $n \cdot x = e$. On appelle *torsion de G* l'ensemble de ses éléments de torsion. Il s'agit d'un sous-groupe de G, noté habituellement $T(G)$.

Ici, la torsion de G correspond exactement aux racines de l'unité. En particulier $G/T(G)$ peut-être bien être muni d'une structure de $\mathbb{Q}$-espace vectoriel, comme on le montre en détails

en 8.1.1. On verra aussi que ce processus coïncide en fait avec l'opération $H \otimes_{\mathbb{Z}} \mathbb{Q}$, qui sera là encore décrite en détails dans le chapitre 7.

Maintenant qu'on a sommairement explicité ce processus de construction, il faut vérifier que quand on l'applique à $\mathcal{O}_{K,S}^{\times}$ on récupère bien un $\mathbb{Q}$-espace vectoriel de dimension finie, ce qui n'a aucune raison d'être le cas pour un groupe quelconque. Cette question appelle la définition suivante.

Définition 4.0.5 (Rang sans torsion)**.** Soit $(G, *)$ un groupe abélien. On appelle *rang sans torsion* de G le cardinal maximal (potentiellement infini) des familles de G libres sur $\mathbb{Z}$.

On fera bien attention que le rang sans torsion d'un groupe abélien de type fini n'est pas nécessairement son rang au sens habituel du terme, c'est-à-dire le cardinal de la plus petite famille qui le génère. En fait ces deux définitions coïncident si et seulement si le groupe est sans torsion. On a d'ailleurs la définition alternative de rang sans torsion.

Définition 4.0.6 (Rang sans torsion)**.** Soit $(G, *)$ un groupe abélien. On appelle *rang sans torsion* de G le rang du groupe abélien $G/T(G)$. Il s'agit du plus grand sous-groupe abélien libre de G.

On l'aura compris, le rang sans torsion de $\mathcal{O}_{K,S}^{\times}$ sera exactement la dimension du $\mathbb{Q}$-espace vectoriel $\mathcal{O}_{K,S}^{\times} \otimes_{\mathbb{Z}} \mathbb{Q}$ que nous construirons au chapitre 8. Ce fait naturel sera vérifié à la proposition 8.1.1. Il s'agit donc maintenant de s'assurer que le rang sans torsion de $\mathcal{O}_{K,S}^{\times}$ est fini, et si possible de le déterminer.

Théorème des S-unités : le rang sans torsion de $\mathcal{O}_{K,S}^{\times}$ est fini

Maintenant que le décor est planté, présentons le théorème que nous nous proposons de montrer dans chapitre. Ce dernier permet de déterminer automatiquement le rang sans torsion de $\mathcal{O}_{K,S}^{\times}$.

Théorème 12 (Théorème des S-unités)**.** *Soit K un corps de nombres. Soit S un ensemble d'idéaux premiers de $\mathcal{O}_K$. On a l'isomorphisme de groupes*

$$\mathcal{O}_{K,S}^{\times} \cong \mu(K) \times \mathbb{Z}^{r+s},$$

où

- *$\mu(K)$ est le groupe cyclique fini des racines de l'unité de $\mathcal{O}_K^{\times}$,*
- *$r = r_1 + r_2 - 1$, où on note r_1 le nombre de plongements réels $K \hookrightarrow \mathbb{C}$ et $2r_2$ le nombre de plongements complexes,*
- *s est le cardinal de S.*

En particulier, le rang sans torsion de $\mathcal{O}_{K,S}^{\times}$ est $r + s$.

Ce théorème répond exactement à nos attentes. Mais l'énoncer ainsi cache d'une certaine façon la nature de la preuve. La bonne manière d'envisager ce résultat est la suivante :

$$\mathcal{O}_{K,S}^{\times} \cong \mathcal{O}_K^{\times} \times \mathbb{Z}^s$$

Cette relation est tout-à-fait naturelle. En effet, on a dit que les éléments de $\mathcal{O}_{K,S}^{\times}$ étaient exactement les $x \in K$ dont la décomposition en idéaux premiers ne faisait intervenir que des idéaux de S. Mais alors ces éléments sont définis par les puissances apparaissant dans leurs décomposition (partie $\mathbb{Z}^s$ de la formule), et à produit par une unité de $\mathcal{O}_K$ près puisque ces dernières engendrent l'idéal principal $\mathcal{O}_K$ tout entier. Finalement, on retrouve bien « avec les mains » la relation $\mathcal{O}_{K,S}^{\times} \cong \mathcal{O}_K^{\times} \times \mathbb{Z}^s$. On démontrera tout à fait rigoureusement cela à la partie 4.2.

Ainsi, on s'est ramené à l'élucidation de la structure de $\mathcal{O}_K^{\times}$. Celle-ci est donnée par le *théorème des unités de Dirichlet*, que l'on se propose de démontrer dans cette partie.

Théorème 13 (Théorème des unités de Dirichlet)**.** *Soit K un corps de nombres. On note n son degré, r_1 le nombre de ses plongements réels, $2r_2$ celui de ses plongements complexes et $r = r_1 + r_2 - 1$.*

Le groupe $\mathcal{O}_K^{\times}$ des unités de $\mathcal{O}_K$ est isomorphe à $\mu(K) \times \mathbb{Z}^r$, où $\mu(K)$ est le groupe cyclique des racines de l'unité de $\mathcal{O}_K$.

Autrement dit, il existe ζ une racine de l'unité, η_1, ..., η_r des éléments de $\mathcal{O}_K^{\times}$ tels que tout $x \in \mathcal{O}_K^{\times}$ s'écrive de manière unique sous la forme

$$x = \zeta^k \eta_1^{n_1} \eta_2^{n_2} ... \eta_r^{n_r},$$

où $0 \leq k \leq d-1$ avec d le cardinal de $\mu(K)$, et $n_1, ..., n_r \in \mathbb{Z}$.

4.1 Structure de $\mathcal{O}_K^{\times}$: le théorème des unités

Passons maintenant à la preuve proprement dite du théorème des unités de Dirichlet. On reprend ici l'idée de la démonstration de Mathilde Gerbelli-Gauthier présentée dans son article dédié [13], ainsi que par Michel Cretin dans son cours de théorie algébrique des nombres [17]. Le mode opératoire est le suivant, et repose sur une géométrisation de $\mathcal{O}_K^{\times}$, dont on cherche à obtenir une représentation comme un sous-réseau d'un certain $\mathbb{R}^d$.

- Pour construire notre réseau, il nous faut d'abord un plongement. $\mathcal{O}_K^{\times}$ est un groupe multiplicatif. En particulier le plongement canonique σ que nous avons utilisé au chapitre 2 pour $\mathcal{O}_K$ est inopérant. On définit donc le *plongement logarithmique* L, qui est simplement le plongement canonique passé au log, et on vérifie qu'il définit bien un morphisme de groupes sur $\mathcal{O}_K^{\times}$ (proposition 4.1.1).

- On identifie ensuite le noyau de L en 4.1.2. On montre qu'il s'agit exactement du groupe des racines de l'unité $\mu(K)$, et l'utilisation repose crucialement sur les résultats de finitude de la partie 1.5. En particulier, on voit que $\mu(K)$ est un sous groupe-fini de $K^\times$, donc est un corps.
- On s'intéresse ensuite à l'image de L. Comme prévu, on obtient facilement à la proposition 4.1.4 qu'il s'agit d'un sous-réseau de $\mathbb{R}^{r_1+r_2}$.
- La difficulté est alors d'identifier le rang de ce sous-réseau, qui s'avère être $r = r_1 + r_2 - 1$. Il s'agit du cœur de la preuve, et du travail de la proposition 4.1.5.
  - On voit d'abord que ce rang est bien inférieur à r en incluant notre sous-réseau dans un hyperplan $\mathcal{H}$ de $\mathbb{R}^{r_1+r_2}$.
  - Pour montrer l'égalité, on montre que toute forme linéaire f de $\mathbb{R}^{r_1+r_2}$ non nulle sur $\mathcal{H}$ est aussi non nulle sur $L(\mathcal{O}_K^\times)$.
  - Pour ce faire, on construit une suite x_n de $\mathcal{O}_K$ telle que $N(x_n)$ est bornée et $f(L(x_n)) \longrightarrow \infty$. La construction de cette suite repose sur le théorème de Minkowski.
  - Il ne reste alors plus qu'à invoquer le théorème 2.2.8, qui dit qu'on a de termes de notre suite vérifiant $x_n\mathcal{O}_K = x_m\mathcal{O}_K$, soit $\frac{x_n}{x_m} \in \mathcal{O}_K^\times$. Par construction on obtient $f(L(\frac{x_n}{x_m})) = f(L(x_n)) - f(L(x_m)) \neq 0$ et la preuve est achevée.
- Le premier théorème de l'isomorphisme donne $\mathbb{Z}^r \cong \mathcal{O}_K^\times/\mu(K)$. Un bout d'algèbre permet de conclure que $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^r$.

Maintenant que la structure de la preuve est claire, passons la démonstration en elle-même.

Définition 4.1.1 (Plongement logarithmique)**.** On définit le plongement logarithmique de $\mathcal{O}_K^\times$ dans $\mathbb{R}^{r_1+r_2}$ par

$$L \; : \left| \begin{array}{ccc} \mathcal{O}_K^\times & \longrightarrow & \mathbb{R}^{r_1+r_2} \\ x & \mapsto & \Big(\ln(|\sigma_1(x)|), ..., \ln(|\sigma_{r_1+r_2}(x)|)\Big), \end{array} \right.$$

où les $\sigma_1, ..., \sigma_n$ sont les n plongements complexes de K, avec $\sigma_1, ..., \sigma_{r_1}$ les r_1 plongements réels, et r_2 plongements complexes $\sigma_{r_1+1}, ..., \sigma_{r_1+r_2}$ r_2 tels que $\sigma_{r_1+i} = \overline{\sigma}_{r_1+r_2+i}$.

Proposition 4.1.1. *L est un morphisme entre les groupes $(\mathcal{O}_K^\times, \times)$ et $(\mathbb{R}^{r_1+r_2}, +)$.*

Démonstration. C'est immédiat, puisque les σ_i sont des morphismes de corps. On a donc, pour $x, y \in \mathcal{O}_K^\times$,

$$\begin{aligned} L(xy) &= (\ln(|\sigma_1(xy)|), ..., \ln(|\sigma_{r_1+r_2}(xy)|)) \\ &= (\ln(|\sigma_1(x)||\sigma_1(y)|), ..., \ln(|\sigma_{r_1+r_2}(x)||\sigma_{r_1+r_2}(y)|)) \\ &= (\ln(|\sigma_1(x)|), ..., \ln(|\sigma_{r_1+r_2}(x)|)) + (\ln(|\sigma_1(y)|), ..., \ln(|\sigma_{r_1+r_2}(y)|)) \\ &= L(x) + L(y). \end{aligned}$$

□

On comprend que L va jouer pour $\mathcal{O}_K^\times$ un rôle analogue à celui de σ pour $\mathcal{O}_K$. Le passage au logarithme permet en effet de préserver la structure multiplicative de $\mathcal{O}_K^\times$. On va maintenant étudier la façon dont L transforme $\mathcal{O}_K^\times$. Notre but va être en effet d'établir les deux résultats suivants :

- $\mathrm{Ker}(L) = \mu(K)$.
- $\mathrm{Im}(L)$ est un sous-réseau de $\mathbb{R}^{r_1+r_2}$ de rang $r = r_1 + r_2 - 1$, donc $\mathrm{Im}(L) \cong \mathbb{Z}^r$.

On sait alors, d'après le premier théorème d'isomorphisme, que

$$\mathrm{Im}(L) \cong \mathcal{O}_K^\times / \mathrm{Ker}(L),$$

dont on verra qu'on peut déduire dans notre cas

$$\mathcal{O}_K^\times \cong \mathrm{Ker}(L) \times \mathrm{Im}(L),$$

ce qui donnera bien

$$\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^r.$$

Commençons par regarder le cas du noyau.

Proposition 4.1.2. *Le noyau de L est exactement le sous-groupe des racines de l'unité de $\mathcal{O}_K^\times$. Autrement dit,*

$$\mathrm{Ker}(L) = \mu(K).$$

Démonstration. On raisonne par double inclusion.

- Soit $x \in \mu(K)$. On a donc $m \in \mathbb{N}$ tel que $x^m = 1$. Mais alors, pour tout i, on a
$$|\sigma_i(x^m)| = |\sigma_i(x)|^m = 1,$$
donc $|\sigma_i(x)| = 1$, et $L(x) = (0, ..., 0)$.
Ainsi $x \in \mathrm{Ker}(L)$.
- Réciproquement,soit $x \in \mathrm{Ker}(L)$. On a donc pour tout $i \in [\![1, r_1 + r_2]\!]$ $|\sigma_i(x)| = 1$. Mais on sait qu'on a pris les r_2 premiers plongements complexes de façon à avoir tous les conjugués. On peut donc affirmer que
$$\forall i \in [\![1, n]\!] \, |\sigma_i(x)| = 1.$$
Par la proposition 2.2.5, on peut affirmer que l'ensemble des $x \in \mathcal{O}_K^\times$ vérifiant cela est fini. Ainsi, $\mathrm{Ker}(L)$ est fini.
Reste à vérifier qu'il s'agit bien du sous-groupe des racines de l'unité. Soit $x \in \mathrm{Ker}(L)$. Alors pour tout $m \in \mathbb{N}$, on a bien sûr $L(x^m) = mL(x) = 0$. Donc $x^m \in \mathrm{Ker}(L)$. Mais alors $\{x^m \,|\, m \in \mathbb{N}\} \subset \mathrm{Ker}(L)$ est fini. On a donc $m_1 > m_2$ tels que
$$x^{m_1} = x^{m_2},$$
d'où, puisque x est inversible,
$$x^{m_1 - m_2} = 1.$$
Ainsi, x est une racine de l'unité : $\mathrm{Ker}(L) \subset \mu(K)$.

On peut conclure :

$$\mathrm{Ker}(L) = \mu(K).$$

□

D'après ce qu'on vient de voir, $\mu(K)$ est donc un sous-groupe multiplicatif fini du corps K. Un théorème bien connu permet de voir qu'il est cyclique, c'est-à-dire monogène et fini.

Proposition 4.1.3. *Soit K un corps (commutatif). Tout sous-groupe fini de $K^\times$ est cyclique.*

Démonstration. Soient K un corps, G un sous-groupe de $K^\times$ et $x \in G$. On note N le cardinal de G et q l'ordre de x.

On a $< x > \cong \mathbb{Z}/q\mathbb{Z}$. Le polynôme $X^q - 1$ admet donc q racines dans K, exactement les éléments de $< x >$, et le polynôme est scindé à racines simples. Il suit que tous les éléments d'ordre q exactement sont dans $< x >$ et donc au nombre de $\varphi(q)$. Ainsi, en notant N_d le nombre d'éléments de G d'ordre d exactement, $N_d = 0$ ou $N_d = \varphi(d)$. De plus, par le théorème de Lagrange et un argument de cardinal, on a

$$\sum_{d|N} N_d = N.$$

Or, en admettant le résultat classique qui affirme que

$$\sum_{d|N} \varphi(d) = N,$$

on en déduit que pour tout d diviseur de N, $N_d = \varphi(d)$. En particulier, $N_N = \varphi(N) \geq 1$, c'est à dire que G admet un élément d'ordre N : G est cyclique. □

Passons maintenant à l'étude de $\mathrm{Im}(L)$. On a d'abord le résultat facile suivant.

Proposition 4.1.4. $\mathrm{Im}(L)$ *est un sous-réseau de* $\mathbb{R}^{r_1+r_2}$.

Démonstration. On sait déjà que $\mathrm{Im}(L)$ est un sous-groupe de $\mathbb{R}^{r_1+r_2}$. Il ne reste plus qu'à utiliser la caractérisation donnée par la proposition 2.1.6.

Soit donc B une partie bornée de $\mathbb{R}^{r_1+r_2}$, disons $B \subset [-R, R]^{r_1+r_2}$. On a donc que

$$\forall i \in [\![1, r_1 + r_2]\!] \, |\sigma_i(x)| \leq e^R.$$

Mais on a les r_2 plongements restants via leurs conjugués. On peut donc affirmer que

$$\forall i \in [\![1, n]\!] \, |\sigma_i(x)| \leq e^R.$$

Reste à invoquer la proposition 2.2.5 pour conclure que $\mathrm{Im}(L) \cap B$ est fini. Ainsi $\mathrm{Im}(L)$ est un sous-réseau de $\mathbb{R}^{r_1+r_2}$. □

Cette proposition permet de conclure que $\mathrm{Im}(L) \cong \mathbb{Z}^k$ où $1 \leq k \leq r_1 + r_2$. Toute la difficulté va maintenant être de prouver que $k = r_1 + r_2 - 1$. C'est l'objet de la proposition suivante.

Proposition 4.1.5.

$$\mathrm{Im}(L) \cong \mathbb{Z}^{r_1+r_2-1}.$$

Démonstration. Notons $\mathrm{Im}(L) \cong \mathbb{Z}^k$.

- Il est déjà assez facile de voir que $k \leq r$ où on rappelle que $r = r_1 + r_2 - 1$.
  En effet, regardons l'hyperplan de $\mathbb{R}^{r_1+r_2}$ défini par

$$\mathcal{H} = \left\{ x = (x_1, ..., x_{r_1+r_2}) \,\middle|\, \sum_{i=1}^{r_1} x_i + \sum_{i=r_1+1}^{r_1+r_2} 2x_i = 0 \right\}.$$

  On voit que $\mathrm{Im}(L) \subset \mathcal{H}$. En effet, soit $x \in \mathcal{O}_K^\times$. On sait alors que $|N(x)| = 1$, ou autrement dit que $\prod_{i=1}^n |\sigma_i(x)| = 1$. En passant au logarithme et en se souvenant que $\sigma_{r_1+i} = \overline{\sigma}_{r_1+r_2+i}$, on obtient

$$\sum_{i=1}^{n} \ln(|\sigma_i(x)|) = \sum_{i=1}^{r_1} \ln(|\sigma_i(x)|) + 2 \sum_{i=r_1+1}^{r_1+r_2} \ln(|\sigma_i(x)|) = 0.$$

  Cela revient exactement à dire que $L(x) \in \mathcal{H}$. Ainsi on a bien $\mathrm{Im}(L) \subset \mathcal{H}$. Mais comme $\mathcal{H}$ est de dimension r, on vient de montrer que $k \leq r$.

- Reste à voir l'égalité. Si par l'absurde $k < r$, alors il existe un sous-espace vectoriel F de $\mathcal{H}$ de dimension k tel que $\mathrm{Im}(L) \subset F$. De façon équivalente, cela revient à dire qu'il existe une forme linéaire $f : \mathbb{R}^{r_1+r_2} \to \mathbb{R}$ non nulle sur $\mathcal{H}$ mais qui annule F.
  Soit donc f une forme linéaire sur $\mathbb{R}^{r_1+r_2}$ non nulle sur $\mathcal{H}$. Par dualité on dispose de $c = (c_1, ..., c_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2}$ tel que

$$\forall x = (x_1, ..., x_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} \; f(x) = \sum_{i=1}^{r_1+r_2} c_i x_i.$$

  Comme on veut éliminer la forme linéaire nulle sur $\mathcal{H}$, on prend $c \neq (1, ..., 1, 2, ..., 2)$. L'idée va être de fabriquer un $\zeta \in \mathcal{O}_K^\times$ tel que $f(L(\zeta)) \neq 0$, et ce grâce au théorème de Minkowski.

  - Avant de nous lancer dans la construction de notre ζ, expliquons l'idée de la preuve. On a vu au théorème 2.2.8 que pour un M donné, l'ensemble

$$\left\{ x\mathcal{O}_K \,\middle|\, x \in \mathcal{O}_K, \, |N(x)| \leq M \right\}$$

    était fini. On avait aussi vu que $x\mathcal{O}_K = y\mathcal{O}_K$ voulait dire que $x = \zeta y$ où $\zeta \in \mathcal{O}_K^\times$.
    Imaginons qu'on ait trouvé un M et une suite (x_n) de $\mathcal{O}_K$ telle que
    (i) $\forall n \in \mathbb{N} \, |N(x_n)| \leq M$,
    (ii) La suite $f(L(x_n))$ prend une infinité de valeur. On pourra par exemple la prendre telle que $f(L(x_n)) \longrightarrow \infty$.
    Alors, par le principe des tiroirs (de Dirichlet !), il existe n_1 et $n_2 \in \mathbb{N}$ tels que

(i) $x_{n_1}\mathcal{O}_K = x_{n_2}\mathcal{O}_K$,
(ii) $f(L(x_{n_1})) \neq f(L(x_{n_2}))$.

Mais alors on peut écrire $x_{n_1} = \zeta x_{n_2}$ avec $\zeta \in \mathcal{O}_K^\times$. En appliquant $f \circ L$, on obtient

$$f(L(\zeta)) = f(L(x_{n_1})) - f(L(x_{n_2})) \neq 0.$$

Ainsi l'unité cherchée est trouvée. Reste donc à construire une telle suite, ce qui exploite le théorème de Minkowski.

- On a vu au théorème 2.2.2 que $\sigma(\mathcal{O}_K)$ était un réseau de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Soit $\alpha \in \mathbb{N}$ tel que $\alpha > \frac{2^n vol(\sigma(\mathcal{O}_K))}{2^{r_1}\pi^{r_2}}$.
Pour tout $\lambda = (\lambda_1, ..., \lambda_{r_1+r_2}) \in \mathbb{R}_+^{r_1+r_2}$, on note B_λ le sous-ensemble de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ défini par

$$B_\lambda = \left\{ x = (x_1, ..., x_{r_1}, z_1, ..., z_{r_2}) \,\middle|\, |x_i| \leq \lambda_i,\ |z_j| \leq \lambda_j \right\}.$$

Les B_λ sont symétriques, convexes, et leur volume est

$$\begin{aligned}\mu(B_\lambda) &= \prod_{i=1}^{r_1} 2\lambda_i \prod_{i=r_1}^{r_1+r_2} \pi {\lambda_i}^2 \\ &= 2^{r_1}\pi^{r_2} \prod_{i=1}^{r_1} \lambda_i \prod_{i=r_1}^{r_1+r_2} {\lambda_i}^2.\end{aligned}$$

On va maintenant fixer λ. Plus précisément, on le prend tel que

$$\prod_{i=1}^{r_1} \lambda_i \prod_{i=r_1}^{r_1+r_2} {\lambda_i}^2 = \alpha.$$

Cela permet de dire que $\mu(B_\lambda) = 2^{r_1}\pi^{r_2}\alpha > 2^n vol(\sigma(\mathcal{O}_K))$. On peut donc appliquer le théorème de Minkowski (théorème 6).

$$\text{Il existe } x_\lambda \in \mathcal{O}_K \text{ non nul tel que } \sigma(x_\lambda) \in B_\lambda.$$

Autrement dit,

$$\forall i \in [\![1, r_1 + r_2]\!]\, |\sigma_i(x_\lambda)| \leq \lambda_i,$$

donc, puisqu'on a tous les conjugués,

$$\forall i \in [\![1, n]\!]\, |\sigma_i(x_\lambda)| \leq \lambda_i.$$

Reste à jouer avec les définitions. Comme $x_\lambda \in \mathcal{O}_K$ est non nul, on a $|N(x_\lambda)| \geq 1$ (rappelons que $N(x_\lambda) \in \mathbb{Z}$). Ainsi, en voyant qu'on compte deux fois les plongements complexes conjugués, on obtient

$$1 \leq |N(x_\lambda)| = \prod_{i=1}^{n} |\sigma_i(x_\lambda)| \leq \prod_{i=1}^{r_1} \lambda_i \prod_{i=r_1}^{r_1+r_2} {\lambda_i}^2 = \alpha. \tag{6}$$

On vient donc d'obtenir une borne des $|N(x_\lambda)|$.

- Or, pour un $i \in [\![1, n]\!]$ donné, on peut aussi écrire les équations dans l'autre sens, toujours en utilisant le fait que $N(x_\lambda) \geq 1$:

$$|\sigma_i(x_\lambda)| = |N(x_\lambda)| \prod_{j \neq i} \sigma_j(x_\lambda)|^{-1} \geq \prod_{j \neq i} |\lambda_j|^{-1} \geq \lambda_i \alpha^{-1}.$$

Finalement, on obtient

$$\lambda_i \alpha^{-1} \leq |\sigma_i(x_\lambda)| \leq \lambda_i.$$

On passe donc au logarithme, ce qui donne

$$0 \leq \ln(_i) - \ln(|\sigma_i(x_\lambda)|) \leq \ln(\alpha)$$
$$\text{d'où } 0 \leq |c_i| \Big(\ln(\lambda_i) - \ln(|\sigma_i(x_\lambda)|) \Big) \leq |c_i| \ln(\alpha).$$

On somme ensuite sur tous les i, puis on exploite l'inégalité triangulaire pour obtenir

$$\sum_{i=1}^{r_1+r_2} \Big(|c_i| (\ln(\lambda_i) - \ln(|\sigma_i(x_\lambda)|)) \Big) \leq \sum_{i=1}^{r_1+r_2} |c_i| \ln(\alpha)$$
$$\text{d'où } \left| \sum_{i=1}^{r_1+r_2} c_i (\ln(\lambda_i) - \ln(|\sigma_i(x_\lambda)|)) \right| \leq \sum_{i=1}^{r_1+r_2} |c_i| \ln(\alpha)$$
$$\text{d'où } \left| f(L(x_\lambda)) - \sum_{i=1}^{r_1+r_2} c_i \ln(\lambda_i) \right| \leq \sum_{i=1}^{r_1+r_2} |c_i| \ln(\alpha).$$

- Cela va nous permettre de construire une suite (x_n) telle que $f(L(x_n))$ tend vers ∞. Soit $n \in \mathbb{N}$. On cherche à s'assurer qu'il existe un vecteur $\lambda^n \in \mathbb{R}^{r_1+r_2}$ vérifiant

$$\prod_{i=1}^{r_1} \lambda_i \prod_{i=r_1}^{r_1+r_2} (\lambda_i^n)^2 = \alpha,$$
$$\text{c'est à dire } \sum_{i=1}^{r_1} \ln(\lambda_i^n) + \sum_{i=r_1}^{r_1+r_2} 2 \ln(\lambda_i^n) = \ln(\alpha),$$

ainsi que l'équation

$$\sum_{i=1}^{r_1+r_2} c_i \ln(\lambda_i^n) = n.$$

Ici le point déterminant est qu'on a pris $c = (c_1, ..., c_{r_1+r_2}) \neq (1, ..., 1, 2, ..., 2)$. Ainsi, l'ensemble des solutions des deux équations précédentes forment des hyperplans affines de $\mathbb{R}^{r_1+r_2}$ non parallèles, dont l'intersection est en conséquence non vide. On peut donc prendre un λ^n vérifiant ces deux équations. Mais alors, cela donne

$$|f(L(x_{\lambda^n})) - n| \leq \sum_{i=1}^{r_1+r_2} |c_i| \ln(\alpha),$$

que l'on peut réécrire,

$$f(L(x_{\lambda^n})) \geq n - \sum_{i=1}^{r_1+r_2} |c_i| \ln(\alpha).$$

Or, $\sum_{i=1}^{r_1+r_2} |c_i| \ln(\alpha)$ est une constante, on peut donc conclure que $f(L(x_{\lambda^n})) \longrightarrow \infty$.

- Reste alors à invoquer ce qu'on a dit plus haut : puisque $\forall n \in \mathbb{N}$ on a $N(x) \leq \alpha$ le principe des tiroirs permet d'affirmer qu'on a x_{n_1} et $x_{n_2} \in \mathcal{O}_K$ tels que
  (i) $x_{n_1}\mathcal{O}_K = x_{n_2}\mathcal{O}_K$,
  (ii) $f(L(x_{n_1})) \neq f(L(x_{n_2}))$.
  Mais alors on peut écrire $x_{n_1} = \zeta x_{n_2}$ avec $\zeta \in \mathcal{O}_K^\times$. En appliquant $f \circ L$, on obtient

$$f(L(\zeta)) = f(L(x_{n_1})) - f(L(x_{n_2})) \neq 0.$$

Ainsi, l'unité cherchée est trouvée.

On peut conclure :

$$\mathrm{Im}(L) = L(\mathcal{O}_K^\times) \cong \mathbb{Z}^{r_1+r_2-1}.$$

□

Pour résumer, on a obtenu :

- $L : \mathcal{O}_K^\times \to \mathbb{R}^{r_1+r_2}$ est un morphisme de groupes,
- $\mathrm{Ker}(L) = \mu(K)$ qui est un groupe cyclique,
- $\mathrm{Im}(L) \cong \mathbb{Z}^r$ où $r = r_1 + r_2 - 1$.

On peut donc affirmer que $\mathbb{Z}^r \cong \mathcal{O}_K^\times/\mu(K)$. On veut maintenant obtenir que $\mathcal{O}_K^\times \cong \mathbb{Z}^r \times \mu(K)$. Ce type de manipulation est en général faux, mais est ici valide car on est sur des $\mathbb{Z}$-modules, ce qu'on démontre au paragraphe suivant. Introduisons d'abord la notion de suite exacte.

Définition 4.1.2 (Suite exacte)**.** On dit qu'une suite de groupes et de morphismes de groupes

$$G_0 \xrightarrow{f_0} G_1 \xrightarrow{f_1} \ldots \xrightarrow{f_{n-1}} G_n$$

est exacte si, pour tout k, $\mathrm{Im}(f_k) = \mathrm{Ker}(f_{k+1})$.

Exemple 4.1.1. Dans notre cas, on a la suite exacte

$$1 \xrightarrow{i} \mu(K) \xrightarrow{j} \mathcal{O}_K^\times \xrightarrow{L} L(\mathcal{O}_K^\times) \xrightarrow{0} 0,$$

où i et j sont les injections canoniques, et 0 le morphisme constant nul. En effet,

- $\mathrm{Im}(i) = \mathrm{Ker}(j) = \{1\}$,
- $\mathrm{Im}(j) = \mathrm{Ker}(L) = \mu(K)$,
- $\mathrm{Im}(L) = \mathrm{Ker}(0) = L(\mathcal{O}_K^X)$.

On a alors la propriété générale suivante.

Proposition 4.1.6. *Soit une suite exacte de la forme*

$$0 \longrightarrow T \xrightarrow{p} A \xrightarrow{\phi} \mathbb{Z}^r \longrightarrow 0.$$

Alors,

$$A \cong \mathbb{Z}^r \times T.$$

On remarquera qu'on est dans ce cas, puisque 1 est l'élément neutre pour la multiplication et que $L(\mathcal{O}_K^\times) \cong \mathbb{Z}^r$.

Démonstration. L'idée de la preuve est de montrer qu'on peut construire des morphismes permettant de remonter la suite, c'est-à-dire qu'on a

$$T \xleftarrow{\psi} A \xleftarrow{j} \mathbb{Z}^r,$$

avec j injectif et ψ surjectif, puis de considérer le morphisme

$$\Phi \ : \left| \begin{array}{ccc} A & \to & T \times \mathbb{Z}^r \\ a & \mapsto & (\psi(a), \phi(a)), \end{array} \right.$$

qui sera alors bijectif.

- Étant donné qu'on a $\mathbb{Z}^r \longrightarrow 0$ dans la suite exacte $\mathrm{Im}(\phi) = \mathbb{Z}^r$. ϕ est donc surjectif, et on dispose d'une suite $a_1, ..., a_r$ de A telle que, en notant $e_1, ..., e_r$ la base canonique de $\mathbb{Z}^r$,

  $$\forall k \in [\![1, r]\!]\, \phi(a_k) = e_k.$$

  Considérons alors le morphisme

  $$j \ : \left| \begin{array}{ccc} \mathbb{Z}^r & \to & A \\ (\alpha_1, ..., \alpha_r) & \mapsto & \sum_{k=1}^r \alpha_k a_k. \end{array} \right.$$

  On remarque que j est injectif puisque $\phi \circ j = id_{\mathbb{Z}^r}$. On dit que j est un *scindage à droite.*
- Ensuite, on voit que comme $0 \longrightarrow T \xrightarrow{p} A$, p est injectif. Dès lors, $p : T \to \mathrm{Im}(p)$ est un isomorphisme, et on peut définir $p^{-1} : \mathrm{Im}(p) \to T$. On introduit alors le morphisme

  $$\psi \ : \left| \begin{array}{ccc} A & \to & T \\ a & \mapsto & p^{-1}(a - j \circ \phi(a)). \end{array} \right.$$

  On doit vérifier qu'il est bien défini, c'est-à-dire que pour $a \in A$ $a - j \circ \phi(a) \in \mathrm{Im}(p)$. Mais comme $T \xrightarrow{p} A \xrightarrow{\phi} \mathbb{Z}^r$ est exacte, on a $\mathrm{Im}(p) = \mathrm{Ker}(\phi)$.
  Or, pour $a \in A$, on a

  $$\phi(a - j \circ \phi(a)) = \phi(a) - \phi \circ j \circ \phi(a) = \phi(a) - id_{\mathbb{Z}_r} \circ \phi(a) = 0,$$

  donc pour $a \in A$, $a - j \circ \phi(a) \in \mathrm{Ker}(\phi) = \mathrm{Im}(p)$ et le morphisme ψ est bien défini.
  Enfin, on observe que pour tout $t \in T$, puisque l'on a $\mathrm{Im}(p) = \mathrm{Ker}(\phi)$,

  $$\psi \circ p(t) = p^{-1}(p(t) - j \circ \phi \circ p(t)) = t,$$

  donc $\psi \circ p = id_T$, et ψ est surjectif.

- Comme promis on pose alors le morphisme

$$\Phi \ : \left| \begin{array}{ccc} A & \to & T \times \mathbb{Z}^r \\ a & \mapsto & (\psi(a), \phi(a)). \end{array} \right.$$

On remarque alors qu'il admet l'inverse

$$\Phi^{-1} \ : \left| \begin{array}{ccc} T \times \mathbb{Z}^r & \to & A \\ (t, x) & \mapsto & p(t) + j(x) \end{array} \right.$$

En effet, d'une part, on a pour $a \in A$ que

$$\begin{aligned} \Phi^{-1} \circ \Phi(a) &= p(\psi(a)) + j(\phi(a)) \\ &= p(p^{-1}(a - j \circ \phi(a))) + j(\phi(a)) \\ &= a. \end{aligned}$$

Réciproquement, pour $(t, x) \in T \times \mathbb{Z}^r$,

$$\begin{aligned} \Phi \circ \Phi^{-1}(t, x) &= (\psi(p(t) + j(x)), \phi(p(t) + j(x))) \\ &= (t + \psi(j(x)), \phi(p(t)) + x) && (\text{car } \psi \circ p = id_T \text{ et } \phi \circ j = id_{\mathbb{Z}^r}) \\ &= (t, x), && (\text{car } \psi(j(x)) = 0 \text{ et } \mathrm{Im}(p) = \mathrm{Ker}(\phi)) \end{aligned}$$

où l'on rappelle pour le dernier point que $\psi(j(x)) = p^{-1}(j(x) - j \circ \phi \circ j(x) = p^{-1}(0) = 0$. Ainsi $\Phi : A \to T \times \mathbb{Z}^r$ est bien un isomorphisme, et on peut conclure que $A \cong T \times \mathbb{Z}^r$.

□

Revenons à notre cas. Comme on a montré que $L(\mathcal{O}_K^\times) \cong \mathbb{Z}^r$, on peut appliquer la proposition précédente. On vient donc de démontrer le théorème des unités de Dirichlet :

$$\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^r,$$

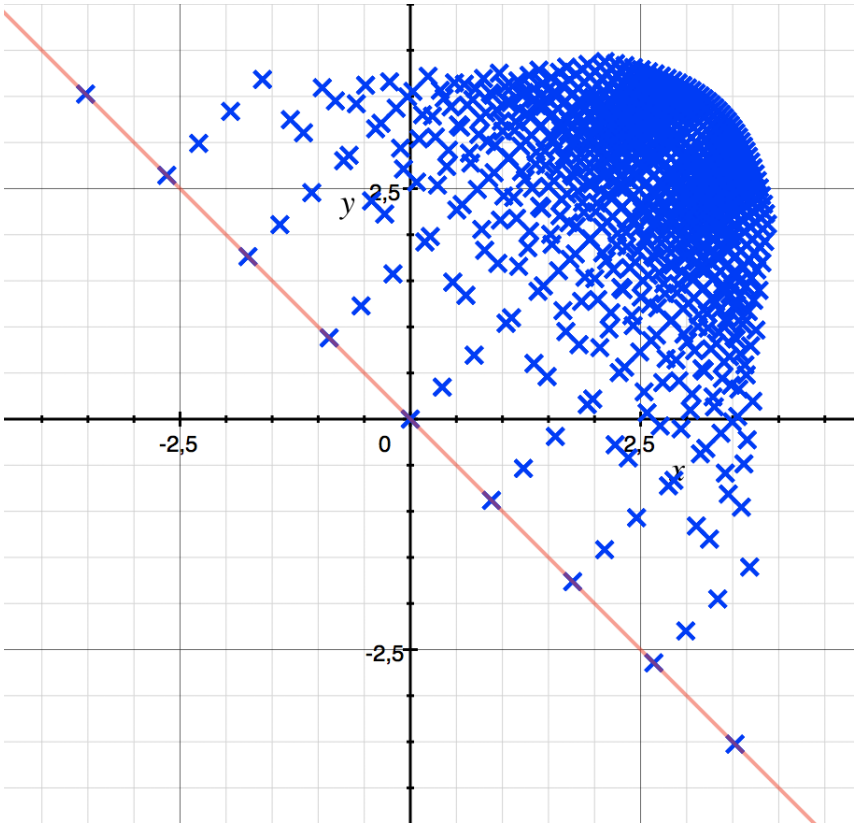
où $r = r_1 + r_2 - 1$, et $\mu(K)$ est le groupe cyclique des racines de l'unité de $\mathcal{O}_K$.

Illustrons de suite ce théorème dans un cas particulier.

Exemple 4.1.2 (Groupe des unités d'un anneau d'entiers quadratiques)**.** Regardons le théorème des unités dans le cas d'un anneau d'entiers d'un corps quadratique, par exemple $K = \mathbb{Q}(\sqrt{2})$. La figure suivante illustre la situation. On avait vu qu'on avait le plongement canonique

$$\sigma \ : \left| \begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \to & \mathbb{R}^2 \\ a + b\sqrt{2} & \mapsto & (a + b\sqrt{2}, a - b\sqrt{2}). \end{array} \right.$$

Ici, $n = 2, r_1 = 2, r_2 = 0$. L'hyperplan $\mathcal{H}$ est donc la droite d'équation $x + y = 0$. Le théorème de Dirichlet prévoit que $L(\mathcal{O}_K^\times)$ est un sous-réseau de rang 1. C'est bien ce qu'on observe sur la figure où on a représenté quelques valeurs de $L(x)$ pour $x \in \mathcal{O}_K$.



Comme prévu, on voit apparaître un sous-réseau de dimension 1 sur la droite $x+y=0$! Plus précisément :

- Comme $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ on a exactement deux racines de l'unité : 1 et -1.
- Pour trouver le générateur, il suffit de trouver une unité avec un a minimal dans l'écriture $a + b\sqrt{2}$. Un rapide calcul montre qu'il s'agit de $1 - 2\sqrt{2}$. En particulier, $L(1 - 2\sqrt{2}) \simeq (-0.9, 0.9)$, et c'est bien un générateur de notre sous-réseau.

4.2 Structure de $\mathcal{O}_{K,S}^\times$: le théorème des S-unités

On passe maintenant à la démonstration du théorème des S-unités, dont la démarche générale a été exposée en introduction. Rappelons le résultat.

Théorème (12). *Soit K un corps de nombres. Soit S un ensemble fini d'idéaux premiers de $\mathcal{O}_K$. On a l'isomorphisme de groupes*

$$\mathcal{O}_{K,S}^\times \cong \mu(K) \times \mathbb{Z}^{r+s},$$

où

- *$\mu(K)$ est le groupe cyclique fini des racines de l'unité de $\mathcal{O}_K^\times$,*
- *$r = r_1 + r_2 - 1$, où on note r_1 le nombre de plongements réels $K \to \mathbb{C}$ et $2r_2$ le nombre de plongements complexes,*
- *s est le cardinal de S.*

Démonstration. Comme on l'a vu, on se propose de montrer que $\mathcal{O}_{K,S}^\times \cong \mathcal{O}_K^\times \times \mathbb{Z}^s$.

Le fait que $\mathcal{O}_{K,S}^\times$ est un groupe multiplicatif ne fait aucun doute puisque c'est le groupe des unités d'un anneau.

Notons $S = \{\mathfrak{p}_1, ..., \mathfrak{p}_s\}$. Puisque $\mathcal{O}_{K,S}^\times$ est l'ensemble des S-unités, il contient $\mathcal{O}_K^\times$ (puisque la décomposition d'un (x) pour x une unité ne fait intervenir aucun idéal). On constate donc qu'on a la suite exacte

$$1 \longrightarrow \mathcal{O}_K^\times \hookrightarrow \mathcal{O}_{K,S}^\times \xrightarrow{\phi} \mathbb{Z}^s,$$

où l'on a introduit l'application

$$\phi \ : \left| \begin{array}{ccc} \mathcal{O}_{K,S}^\times & \to & \mathbb{Z}^s \\ x & \mapsto & (v_{\mathfrak{p}_1}(x), ..., v_{\mathfrak{p}_s}(x)). \end{array} \right.$$

Le caractère exact provient de la proposition 3.2.34 : les $x \in K$ qui vérifient pour tout $\mathfrak{p}$ que $v_\mathfrak{p}(x) = 0$ sont exactement les $x \in \mathcal{O}_K^\times$. Mais ici, ϕ part de l'ensemble $\mathcal{O}_{K,S}^\times$ des éléments de K dont la décomposition ne fait intervenir que des idéaux de S. Il s'ensuit que

$$\begin{aligned} \mathrm{Ker}(\phi) &= \left\{ x \in K \,\middle|\, \forall \mathfrak{p} \notin S \, v_\mathfrak{p}(x) = 0 \right\} \bigcap \left\{ x \in K \,\middle|\, \forall \mathfrak{p} \in S \, v_\mathfrak{p}(x) = 0 \right\} \\ &= \mathcal{O}_K^\times. \end{aligned}$$

Reste à déterminer la structure de $\mathrm{Im}(\phi)$. Soit $i \in [\![1, s]\!]$. On note e_i le i-ième vecteur de la base canonique de $\mathbb{Z}^r$. On voit alors qu'il existe un $x_i \in \mathcal{O}_{K,S}^\times$ et un $n_i \in \mathbb{Z}^*$ tels que

$$\phi(x_i) = n_i e_i.$$

En effet, on sait que le groupe des classes $Cl(\mathcal{O}_K)$ est fini, de cardinal noté h_K. En particulier, l'idéal $\mathfrak{p}_i^{h_k}$ est principal, disons égal à (x_i). Mais alors, la décomposition de (x_i) ne fait intervenir que $\mathfrak{p}_i$, donc $x_i \in \mathcal{O}_{K,S}^\times$, et en particulier

$$\phi(x_i) = h_K e_i.$$

On vient donc de se munir, pour tout $i \in [\![1, s]\!]$, de $n_i \in \mathbb{Z}^*$ et $x_i \in \mathcal{O}_{K,S}^\times$ tels que $\phi(x_i) = n_i e_i$. Mais alors :

- $Im(\phi)$ est un sous-groupe additif de $\mathbb{R}^s$.
- Il est inclus dans $\mathbb{Z}^s$, donc il est discret. En particulier c'est un sous-réseau de $\mathbb{R}^s$.
- Il contient les $n_i e_i$ pour $i \in [\![1, s]\!]$. Donc il engendre $\mathbb{R}^r$ sur $\mathbb{R}$. Ainsi, c'est un réseau de $\mathbb{R}^r$ et son rang est exactement r.

Dès lors,
$\mathrm{Im}(\phi) \cong \mathbb{Z}^s$. On peut ainsi compléter notre suite exacte :

$$1 \longrightarrow \mathcal{O}_K^\times \hookrightarrow \mathcal{O}_{K,S}^\times \xrightarrow{\phi} \mathbb{Z}^s \longrightarrow 1.$$

Cette suite a exactement de la forme de celle de la proposition 4.1.6. On peut donc affirmer que

$$\mathcal{O}_{K,S}^\times \cong \mathbb{Z}^s \times \mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{s+r},$$

où on utilise le théorème de Dirichlet pour dire que

$$\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^r.$$

□

5
CORPS VALUÉS

Nous sommes arrivés à la moitié de notre voyage. Arrêtons-nous un instant pour regarder le chemin parcouru, et vers où on se dirige.

Notre objectif final reste l'étude de l'équation $x + y = 1$ dans $\mathcal{O}_{K,S}^\times$, et plus précisément de borner son nombre de solutions.

- Dans le chapitre 1, on a généralisé la notion de nombres et d'entiers, en passant de $\mathbb{Q}$ et $\mathbb{Z}$ à K et $\mathcal{O}_K$.
- Dans le chapitre 2, on a commencé à faire de la géométrie discrète, ce qui nous a permis de géométriser $\mathcal{O}_K$ et de commencer à obtenir quelques résultats de finitude.
- Dans le chapitre 3, on a travaillé plus spécifiquement sur l'arithmétique de $\mathcal{O}_K$.

  Pour y retrouver l'arithmétique classique de $\mathbb{Z}$, il a été nécessaire de remplacer la notion de nombre premier p par la notion d'idéal premier $\mathfrak{p}$.

  En étudiant cette nouvelle arithmétique, on s'est intéressé au passage à la façon dont les $\mathfrak{p}$ de différents corps interagissent entre eux. Cela a fait apparaître naturellement la notion de localisé, et c'est là qu'on a rencontré $\mathcal{O}_{K,S}^\times$ pour la première fois : c'est en quelque sorte K restreint à seulement quelques $\mathfrak{p}$.
- Enfin, le chapitre 4 a montré les puissants théorèmes des unités de Dirichlet : $\mathcal{O}_K^\times$ et $\mathcal{O}_{K,S}^\times$ ont été géométrisés. En particulier, ces objets sont de type fini !

La preuve finale, présentée au chapitre 8, repose sur deux idées principales.

- $\mathcal{O}_{K,S}^\times$ est de type fini : c'est le théorème des S-unités de Dirichlet.
- La forme de l'équation impose des restrictions sur la complexité des interactions entre ses solutions : la bonne notion de complexité est celle de *hauteur*, que les deux prochains chapitres construisent.

En fait, on construira un espace, muni d'une distance issue de la hauteur. Le théorème des S-unités nous assurera que cet espace est de dimension finie, la forme de l'équation se traduira en relations géométriques grâce à la hauteur, et on conclura par des arguments de recouvrement de l'espace par des boules.

Voilà donc le concept qui nous manque : la mesure de la complexité des nombres !

- Dans ce chapitre, on regarde différentes manières de mesurer la complexité des nombres : les places d'un corps de nombre.
- Dans le chapitre suivant, on combinera toutes ces places pour construire la hauteur : comprendre les complétions des corps sera nécessaire pour le faire habilement. On obtiendra alors un puissant théorème de finitude : le théorème de Northcott.

Ce chapitre est donc consacré à l'étude des places d'un corps de nombre, et culmine par le théorème d'Ostrowski sur les corps de nombres.

- La partie 5.1 définit cette notion. On obtient une panoplie de géométries nouvelles, qui sont présentées et caractérisées.
- Ensuite, en 5.2, on s'intéresse à la notion de complétion : on ajoute toutes les limites de suites de Cauchy pour une place, et on obtient $\mathbb{R}$, $\mathbb{C}$, ou des nombres p-adiques.
- La dernière partie 5.3 fera la bilan du chapitre, en énonçant le théorème d'Ostrowski, qui classifie les places d'un corps de nombre K – et donc toutes les complétions de K.

On verra au passage qu'on peut classifier les valeurs absolues / places / complétions d'un corps de nombre en deux grandes familles : les *archimédiennes*, qui soulignent la structure « algébrique » de K, et les *ultramétriques*, qui en soulignent la structure « arithmétique ».

Le cours de théorie des nombres de Jean-François Dat [18] nous a beaucoup aidé à aborder la théorie des corps de nombres munis de valeurs absolues : de nombreuses preuves de ce chapitre s'inspirent largement de ses arguments.

5.1 Places

Dans cette partie, on introduit les notions de *place* et *valeurs absolues* pour mesurer la complexité des nombres.

- En 5.1.1, on constate que différentes notions de *valeur absolue* sur un corps permettent de caractériser différents aspects de la complexité des nombres. En fait, seule la topologie obtenue est importante : on arrive à la notion de *place*.
- En 5.1.2, on s'intéresse à des valeurs absolues qui respectent une inégalité plus forte que l'inégalité triangulaire. On traduit cela en propriétés géométriques remarquables.
- Enfin, en 5.1.3, on classifie toutes les places qui se comportent de cette manière : on dira qu'il y a correspondance entre places ultramétriques, valuations à proportionnalité près, et idéaux premiers.

5.1.1 • Comment mesurer la complexité des nombres ?

Intuitivement, il y a plusieurs manière de mesurer la complexité d'un nombre.

Par exemple $x = \frac{121}{67} = 11^2 \cdot 67^{-1}$ et $y = \frac{65}{36} = 2^{-2} \cdot 3^{-2} \cdot 5^1 \cdot 13^1$ sont très proches au sens de la valeur absolue usuelle sur $\mathbb{Q}$, puisque $|x - y| < \frac{1}{2000}$, mais semblent très différents d'un point de vue arithmétique.

- On formalise cette notion de « mesure de taille d'un nombre » par la notion de *valeur absolue*, introduite à la définition 5.1.1.
- Dans l'exemple 5.1.2, on construit la *valeur absolue p-adique*, qui vérifie une inégalité plus forte que l'inégalité triangulaire : *l'inégalité ultramétrique*.
- En fait, beaucoup de valeurs absolues sont similaires : on passe au quotient avec les *places* aux définitions 5.1.5 et 5.1.6.
- La propriété 5.1.3 vérifie que ces inégalités « plus que triangulaires » passent au quotient : on obtient une classification en places archimédiennes ou ultramétriques.

Voilà donc la définition de valeur absolue, qui formalise la notion de « mesure de taille d'un nombre ».

Définition 5.1.1 (Valeur absolue)**.** On appelle *valeur absolue* sur un corps de nombre K toute fonction $|\cdot| : K \to \mathbb{R}_+$, telle que

(i) $\forall x \in K\, |x| = 0 \iff x = 0$ (séparation),

(ii) $\forall x, y \in K\, |xy| = |x||y|$ (multiplicativité),

(iii) $\forall x, y \in K\, |x + y| \leq |x| + |y|$ (inégalité triangulaire).

L'exemple suivant, sur $\mathbb{Q}$, est bien connu.

Exemple 5.1.1. La valeur absolue usuelle sur $\mathbb{Q}$ est bien une valeur absolue au sens précédent, et sera notée $|\cdot|_\infty$ pour éviter toute confusion.

Exemple 5.1.2. Pour tout corps de nombre K, $\delta_0 : K \to \mathbb{R}_+$ est une valeur absolue, appelée *valeur absolue triviale* sur K, qu'on notera aussi $|\cdot|_0$.

Pour introduire des exemples plus originaux, faisons appel à la notion de valuation p-adique, introduite au chapitre 3 où nous faisions de l'arithmétique, et notée v_p.

Définition 5.1.2. Soit $p \in \mathcal{P}$. On définit la *valeur absolue p-adique*, dont on vérifie que c'est bien une valeur absolue, par

$$|\cdot|_p \ : \left| \begin{array}{ccc} \mathbb{Q} & \to & \mathbb{R}_+ \\ x & \mapsto & p^{-v_p(x)}. \end{array} \right.$$

Le fait suivant est remarquable. Pour p premier et pour tous $x, y \in \mathcal{P}$, on a mieux que l'inégalité triangulaire, qui affirme $|x + y|_p \leq |x|_p + |y|_p$. En fait, $|x + y|_p \leq \max(|x|_p, |y|_p)$.

Cela motive la définition suivante.

Définition 5.1.3. On appelle *valeur absolue ultramétrique* sur un corps K toute fonction $|\cdot| : K \to \mathbb{R}_+$, telle que

(i) $\forall x \in K\, |x| = 0 \iff x = 0$ (séparation),

(ii) $\forall x, y \in K\, |xy| = |x||y|$ (multiplicativité),

(iii) $\forall x, y \in K\, |x + y| \leq \max(|x|, |y|)$ (inégalité ultramétrique).

Toute valeur absolue ultramétrique est une valeur absolue mais la réciproque est en général fausse.

Définition 5.1.4. Si une valeur absolue ne vérifie pas partout l'inégalité ultramétrique, on dit que c'est une *valeur absolue archimédienne*.

De façon équivalente, on pourra dire d'une valeur absolue archimédienne qu'elle est *non ultramétrique*, et d'une valeur absolue ultramétrique qu'elle est *non archimédienne*.

Exemple 5.1.3. $|\cdot|_\infty$ est une valeur absolue archimédienne.
En effet, $|1+1|_\infty = 2 > 1 = \max(|1|_\infty, |1|_\infty)$.

Exemple 5.1.4. La valeur absolue triviale $|\cdot|_0$ est ultramétrique.

Exemple 5.1.5. Pour tout $p \in \mathcal{P}$, la valeur absolue p-adique $|\cdot|_p$ est ultramétrique.

Vérifier l'inégalité ultramétrique a des conséquences profondes ! On étudiera ceci plus en détail dans les prochaines parties.

On verra plus tard (c'est la théorème d'Ostrowski sur $\mathbb{Q}$) qu'on a en fait obtenu toutes les valeurs absolues sur $\mathbb{Q}$ à équivalence près, en un sens qu'on va maintenant définir.

Une construction assez simple nous permet d'obtenir de nouvelles valeurs absolues.

Proposition 5.1.1. *Soit $|\cdot|$ une valeur absolue. Pour tout $\alpha \in]0,1[$, $|\cdot|^\alpha : x \mapsto |x|^\alpha$ est également une valeur absolue.*

Démonstration. La séparation et la multiplicativité sont évidentes, et l'inégalité triangulaire est une conséquence de la croissance et concavité de la fonction $x \mapsto x^\alpha$ définie sur $\mathbb{R}_+$: en posant pour $x \in \mathbb{R}_+$

$$\lambda \ : \left| \begin{array}{ccc} \mathbb{R}_+ & \to & \mathbb{R} \\ y & \mapsto & (x+y)^\alpha - x^\alpha - y^\alpha, \end{array} \right.$$

on observe que $\lambda(0) = 0$ et

$$\forall y \geq 0 \, \lambda'(y) = \alpha((x+y)^{\alpha-1} - y^{\alpha-1}) \leq 0,$$

d'où on déduit l'inégalité triangulaire. □

Cependant, une valeur absolue obtenue par cette construction n'apporte pas grand chose de neuf. En effet, elle définit la même topologie que la v.a. source, au sens suivant.

Définition 5.1.5. Soit K un corps de nombre. On dit que deux valeurs absolues sur K $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes, et on note $|\cdot|_1 \sim |\cdot|_2$, si elles définissent la même topologie, c'est à dire si

$$\forall x \in K^{\mathbb{N}} \, |x_n|_1 \to 0 \iff |x_n|_2 \to 0.$$

En fait, comme le montre la reformulation suivante, toutes les valeurs absolues équivalentes apparaissent de cette façon.

Proposition 5.1.2. *Soient K un corps de nombre et $|\cdot|_1$, $|\cdot|_2$ deux de ses valeurs absolues. Les propriétés suivantes sont équivalentes.*

(i) $|\cdot|_1 \sim |\cdot|_2$ *i.e.* $\forall x \in K^{\mathbb{N}}\, |x|_1 \to 0 \iff |x|_2 \to 0$.

(ii) $\forall x \in K\, |x|_1 < 1 \iff |x|_2 < 1$.

(iii) $\forall x \in K\, |x|_1 > 1 \iff |x|_2 > 1$.

(iv) $\exists c \in \mathbb{R}_+\, |\cdot|_1 = |\cdot|_2^c$.

Démonstration.

- $(iv) \implies (i)$
  En effet, pour tout $c > 0$, l'application $\mathbb{R}_+ \to \mathbb{R}_+$, $x \mapsto x^c$ est continue.
- $(i) \implies (ii)$
  C'est une conséquence directe de la multiplicativité des valeurs absolues. En effet, pour tout $x \in K$,
  $$|x|_1 < 1 \iff |x^n|_1 \to 0 \iff |x^n|_2 \to 0 \iff |x|_2 < 1.$$
- $(ii) \implies (iii)$
  Il suffit de passer à l'inverse en utilisant la multiplicativité.
- $(iii) \implies (iv)$
  Soient $x, y \in K$ tels que $|x|_1, |y|_1 > 1$. On a aussi $|x|_2, |y|_2 > 1$.
  Supposons par l'absurde que $\frac{\ln|x|_1}{\ln|x|_2} \neq \frac{\ln|y|_1}{\ln|y|_2}$. On peut supposer sans perte de généralité que le premier rapport est le plus petit. Tous les logarithmes étant ici positifs, on peut réarranger l'inégalité, et on dispose alors de $\frac{m}{n} \in \mathbb{Q}_+^*$ tel que
  $$\frac{\ln|x|_1}{\ln|y|_1} < \frac{m}{n} < \frac{\ln|x|_2}{\ln|y|_2}.$$
  On en déduit que $\ln|x^n|_1 < \ln|y^m|_1$, puis que $|\frac{x^n}{y^m}|_1 < 1$, et de même que $|\frac{x^n}{y^m}|_2 > 1$, d'où une contradiction avec (iii).
  Ainsi, on dispose de $c > 0$ tel que $\forall x \in K\, |x|_1 > 1 \implies \ln|x|_1 = c \ln|x|_2$, i.e. $\forall x \in K\, |x|_1 > 1 \implies |x|_1 = |x|_2^c$.
  Par passage à l'inverse, puis en remarquant que l'égalité est triviale pour $|x|_1 \in \{0, 1\}$, on en déduit que
  $$\forall x \in K\, |x|_1 = |x|_2^c.$$

□

Exemple 5.1.6 (Contre-exemple)**.** Remarquons que la propriété n'affirme pas que pour toutes valeur absolue $|\cdot|$ et $c > 0$, $|\cdot|^c$ est une valeur absolue.

C'est d'ailleurs faux, puisque $|\cdot|_\infty^2$ ne vérifie pas l'inégalité triangulaire :

$$|1+1|_\infty^2 = 4 > 2 = |1|_\infty^2 + |1|_\infty^2.$$

Dans la suite, pour classifier les valeurs absolues, il suffira donc d'étudier l'ensemble de leurs classes d'équivalences.

Définition 5.1.6 (Places)**.** On appelle *place* une classe d'équivalence de valeurs absolues pour la relation $\sim$.

On notera $\mathcal{M}_K$ l'ensemble des places sur K.

La séparation en valeurs ultramétriques et archimédiennes est conservée par passage au quotient. On peut donc parler de *place ultramétrique* et de *place archimédienne*.

Proposition 5.1.3. *Soient $|\cdot|_1$ une valeur absolue ultramétrique, et $|\cdot|_2 \sim |\cdot|_1$. Alors, $|\cdot|_2$ est ultramétrique.*

Démonstration. Comme $|\cdot|_2 \sim |\cdot|_1$, on dispose de $c > 0$ tel que $|\cdot|_2 = |\cdot|_1^c$.

Soient $x, y \in K$.

$$|x+y|_2 = |x+y|_1^c \leq \max(|x|_1, |y|_1)^c = \max(|x|_1^c, |y|_1^c) = \max(|x|_2, |y|_2).$$

□

Définition 5.1.7. On note $\mathcal{M}_K^0$ l'ensemble des places ultramétriques sur K, et $\mathcal{M}_K^\infty$ l'ensemble des places archimédiennes.

Par définition, $\mathcal{M}_K = \mathcal{M}_K^0 \sqcup \mathcal{M}_K^\infty$.

On remarquera plus tard (c'est le théorème d'Ostrowski sur $\mathbb{Q}$), qu'avec $|\cdot|_\infty$, $|\cdot|_0$ et les $|\cdot|_p$, on a déjà obtenu toutes les places sur $\mathbb{Q}$.

On verra en 6.1.1 qu'on est même tombés sur un très bon ensemble de représentants !

5.1.2 • Géométries non archimédiennes

Comme nous le disions, les valeurs absolues qui vérifient l'inégalité ultramétrique ont des propriétés géométriques remarquables, qui sont contre-intuitives quand on n'y est pas habitués.

- On montre ainsi à la proposition 5.1.4 qu'une valeur absolue est ultramétrique si et seulement si $\mathbb{Z}$ est contenu dans sa boule unité.
- On en déduit à la proposition 5.1.5 que la classification en places ultramétriques et archimédiennes est stable par extension du corps.

- Enfin, la proposition 5.1.6 fournit une description du monde merveilleux de la géométrie non archimédienne, dont on fournit ensuite des représentations sous forme d'arbre et de boules empilées.

Comme remarque culturelle, notons que si ces résultats peuvent sembler de prime abord contre-intuitifs, beaucoup de choses se passent bien mieux dans le contexte ultramétrique que dans le contexte archimédien. On restera néanmoins vague sur ce point pour l'instant.

Il est de notoriété publique que $\mathbb{Z}$ n'est pas borné pour $|\cdot|_\infty$. C'est en fait une caractérisation des valeurs absolues archimédiennes.

Proposition 5.1.4. *Soit $|\cdot|$ une valeur absolue. Les propriétés suivantes s'équivalent.*

(i) $|\cdot|$ *est ultramétrique.*

(ii) $\forall n \in \mathbb{Z}\, |n| \leq 1$.

(iii) $\mathbb{Z}$ *est borné pour* $|\cdot|$.

Démonstration.

- $(i) \implies (ii)$
  Comme $|\cdot|$ est une valeur absolue, $|0| = 0$, $|\pm 1| = 1$. Ensuite, par récurrence immédiate, pour $n \in \mathbb{N}$, $|n| = |1 + \cdots + 1| \leq \max(|1|, ..., |1|) = 1$, et le résultat s'étend par multiplicativité à $\mathbb{Z}$.
- $(ii) \implies (iii)$
  Évident.
- $(iii) \implies (i)$
  Soit $M > 0$ tel que $\forall n \in \mathbb{Z}\, |n| \leq M$. Soient $x, y \in K$. Soit $n \in \mathbb{N}^*$.

$$|x+y|^n = |(x+y)^n| = \left|\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right| \leq \max_{k \in [\![0,n]\!]} \left|n \binom{n}{k} x^k y^{n-k}\right| \leq M \max(|x|, |y|)^n.$$

  En passant à la racine $n^{\text{ème}}$, on obtient $|x+y| \leq M^{\frac{1}{n}} \max(|x|, |y|)$, puis l'inégalité ultramétrique en faisant $n \to \infty$.

□

Corollaire 5.1.1. *On pourra remarquer que cela implique que, pour n'importe quel corps de nombre K muni d'une valeur absolue archimédienne $|\cdot|$, il existe $x \in \mathbb{Z} \subset \mathcal{O}_K$ tel que $|x| > 1$.*

De ce résultat, on déduit que la classification en places ultramétriques et archimédiennes est stable par extension du corps de base.

Proposition 5.1.5. *Soient K un corps de nombre, L une extension de K, et $|\cdot|_w$ une valeur absolue sur L. Alors*

(i) La restriction de $|\cdot|_w$ à K, notée $|\cdot|_v$, est une valeur absolue sur K,

(ii) $|\cdot|_w$ est ultramétrique si et seulement si $|\cdot|_v$ est ultramétrique.

Démonstration.
- Pour (i), il suffit de vérifier les axiomes d'une valeur absolue, qui, puisqu'ils sont vérifiés sur L, sont en particulier vérifiés sur K.
- Pour (ii), il suffit d'utiliser le fait qu'une valeur absolue est ultramétrique si et seulement si sa boule unité contient $\mathbb{Z}$, et que $\mathbb{Z} \subset K \subset L$.

□

On regardant l'exemple de $\mathbb{Q}$, on voit que la topologie induite par une norme ultramétrique est bien différente de la topologie usuelle. On vient par exemple de voir que $\mathbb{Z}$ est contenu dans la boule unité fermée de rayon 1.

Voici quelques autres résultats pour les normes p-adiques sur $\mathbb{Q}$.

Proposition 5.1.6. *Soit $p \in \mathbb{Z}$ un nombre premier. On se place dans $\mathbb{Q}$ muni de la norme p-adique.*

(i) $\lim_{n\to+\infty} p^n = 0$.

(ii) Pour toute suite bornée (a_n), $\sum_{n\in\mathbb{N}} a_n p^n$ est de Cauchy.

(iii) Toute boule de rayon strictement positif est à la fois ouverte et fermée.

(iv) Tout point d'une boule en est un centre.

(v) Toute boule non vide non réduite à un point est de la forme $x + p^k\mathbb{Z}_{(p)}$, où $x \in \mathbb{Q}$, $k \in \mathbb{Z}$, $\mathbb{Z}_{(p)} = \{z \in \mathbb{Q} \mid v_p(z) \geq 0\}$.

Rappelons que la boule $\mathbb{Z}_{(p)}$ a déjà été définie à l'exemple 3.2.16 : c'est le localisé de $\mathbb{Z}$ en $\mathbb{Z} \setminus p\mathbb{Z}$.

Démonstration.

(i) En effet, $|p^n|_p = p^{-v_p(p^n)} = p^{-n} \longrightarrow 0$.

(ii) Par l'inégalité ultramétrique, c'est un corollaire :

$$\left|\sum_{k=n}^{N} a_k p^k\right|_p \leq \sup(|a_k|_p)\left|\sum_{k=n}^{N} p^k\right|_p \leq \sup(|a_k|_p)|p^n|_p = \sup(|a_k|_p)p^{-n} \longrightarrow 0.$$

(iii) C'est une conséquence directe du fait que le seul point d'accumulation de $\{|x|_p \mid x \in \mathbb{Q}\}$ est 0.

(iv) Soient $x \in \mathbb{Q}, M \in \mathbb{R}_+^*$. Soit y tel que $|x - y|_p \leq M$.
Pour tout $z \in \mathbb{Q}$,

$$|x - z|_p = |x - y + y - z|_p \leq \max(x - y, y - z) \leq \max(M, y - z).$$

Ainsi, $|y-z| \leq M \implies |x-z| \leq M$, et de même $|x-z| \leq M \implies |y-z| \leq M$.
On en déduit

$$\overline{B}(x,M) = \overline{B}(y,M).$$

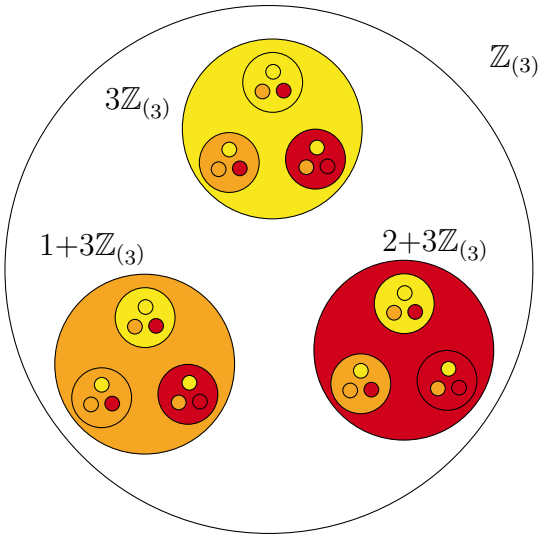
(v) Soient $x \in \mathbb{Q}, M \in \mathbb{R}_+^*$. On dispose de $k \in \mathbb{Z}$ tel que $B(x,M) = \{z \in \mathbb{Q} \,|\, v_p(x-z) \geq k\}$.
Pour tout $z \in \mathbb{Q}$,

$$z \in B(x,M) \iff v_p(x-z) \geq k \iff x - z \in p^k \mathbb{Z}_{(p)},$$

ce qui conclut.

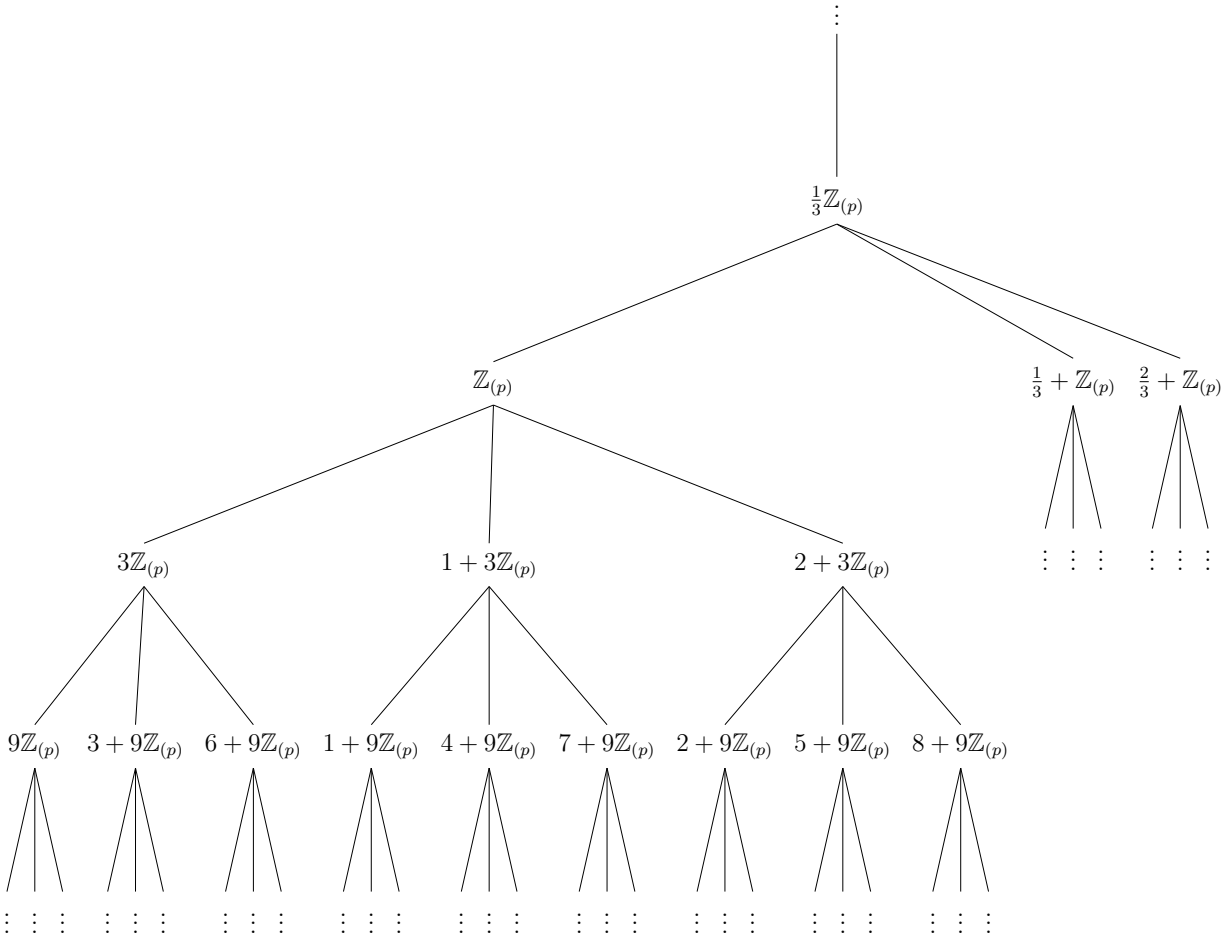
□

On peut s'amuser à essayer de représenter les inclusions entre les boules, par exemple ici dans $\mathbb{Q}$ pour la norme 3-adique.



Cette vision est inspirée de la vidéo « What does it feel like to invent math ? » de la chaîne YouTube 3Blue1Brown [19]. Profitons-en pour remercier son auteur.

On peut construire un graphe ayant pour sommets les boules de $(\mathbb{Q}, |\cdot|_p)$ et des arêtes correspondant à la relation d'inclusion. On obtient un arbre, pour lequel on peut définir une hauteur (en fixant $h(\mathbb{Z}_{(p)}) = 0$).



Les points de $\mathbb{Q}$ correspondent alors à des « feuilles à l'infini ».

Si l'on considère deux points $x, y \in \mathbb{Q}$, on voit alors apparaître leur « dernier ancêtre commun » (la plus petite boule qui les contient tous les deux).

La distance entre x et y s'exprime alors en fonction de la hauteur h de ce dernier ancêtre commun $|x-y|_p = p^{-h}$.

Enfin, on pourra remarquer que toutes les « feuilles à l'infini » n'atteignent pas toujours un point de $\mathbb{Q}$. Cela est dû au fait que $\mathbb{Q}$ n'est pas complet pour $|\cdot|_p$. On ajoutera ces dernières feuilles dans une prochaine partie, et on obtiendra le corps $\mathbb{Q}_p$ des *nombres p-adiques*.

Le sous-arbre prenant la place de $\mathbb{Z}_{(p)}$, c'est à dire le sous-arbre engendré par le dernier ancêtre commun des éléments de $\mathbb{Z}$, sera l'ensemble $\mathbb{Z}_p$ des *entiers p-adiques*.

On verra en 5.2.3 que les nombres p-adiques s'écrivent de façon similaire aux réels en développement décimal, mais avec un développement possiblement infini *à gauche*. Les chiffres qui apparaîtront dans ce développement (en partant vers la gauche) correspondent à des choix de branches en descendant dans l'arbre.

Parlons encore un peu des nombres p-adiques – les affirmations suivantes ne seront cependant pas démontrées, et servent uniquement à nourrir l'intuition du lecteur.

Par exemple, $x = \sum_{k\geq 0} 1 \times 3^k = ...111111$ et $y = \sum_{k\geq 0} 1 \times 3^k = ...222222$ sont des entiers 3-adiques (on rappelle que les séries associées sont bien convergentes pour $|\cdot|_3$).

Attention cependant ! Il ne suffit pas d'avoir un développement infini pour être en-dehors de $\mathbb{Q}$: on a ici $y = -1$ et $x = -\frac{1}{2}$ (pouvez-vous voir pourquoi ?).

En revanche il est vrai que $\mathbb{Q}$ n'est pas complet pour $|\cdot|_p$, et on a une caractérisation des rationnels similaire à celle de $\mathbb{R}$: un nombre p-adique x est rationnel si et seulement si le développement p-adique de x *en partant vers la gauche* est périodique à partir d'un certain rang.

On peut décrire certains des éléments de $\mathbb{Q}_p \setminus \mathbb{Q}$. Par exemple, $\sqrt{7} \in \mathbb{Q}_3$. En revanche, les $\mathbb{Q}_p$ sont loin d'être algébriquement clos. C'est même pire que ça : si on note $\overline{\mathbb{Q}_p}$ la clôture algébrique de $\mathbb{Q}_p$, alors $[\overline{\mathbb{Q}_p} : \mathbb{Q}_p] = \infty$. Rappelons que $[\mathbb{C} : \mathbb{R}] = 2$...

Laissons maintenant là ces remarques culturelles.

5.1.3 • Places ultramétriques, valuations, idéaux premiers

Sur $\mathbb{Q}$ nous avons construit les valeurs absolues p-adiques $|\cdot|_p$ à partir des valuations p-adiques v_p associées aux nombres premiers $p \in \mathcal{P}$ de $\mathbb{Z}$.

Nous allons maintenant montrer que c'est un phénomène général : pour tout corps de nombre K, il y a correspondance entre places ultramétriques, valuations à proportionnalité près, et idéaux premiers de $\mathcal{O}_K$. L'idée est d'utiliser les transformations $|\cdot|_\mathfrak{p} \longleftrightarrow v_\mathfrak{p} \longleftrightarrow \mathfrak{p}$.

- En 5.1.8, on définit de façon générale la notion de valuation sur un corps, puis en 5.1.9 l'équivalence de valuations.
- Aux propositions 5.1.8 et 5.1.9, on constate qu'on peut construire une valuation à partir de toute place ultramétrique, et réciproquement : on s'en sert pour construire la première moitié de la correspondance.
- On montre enfin à la proposition 5.1.13 que toute valuation est proportionnelle à la valuation $\mathfrak{p}$-adique pour un unique $\mathfrak{p}$, ce qui constitue la deuxième moitié de la correspondance.

Places et valuations On a déjà défini la notion de valuation p-adique, et même la valuation $\mathfrak{p}$-adique d'un idéal de $\mathcal{O}_K$ lors du chapitre d'arithmétique. La définition suivante généralise cette notion.

Définition 5.1.8 (Valuation)**.** Soit K un corps de nombre. On appelle *valuation* sur K toute application $v : K \to \mathbb{R} \cup \{\infty\}$ telle que

(i) $\forall x \in K\ v(x) = \infty \iff x = 0$,

(ii) $\forall x, y \in K\ v(xy) = v(x) + v(y)$,

(iii) $\forall x, y \in K\ v(x + y) \geq \min(v(x), v(y))$.

Les propriétés suivantes sont immédiates.

Proposition 5.1.7. *Soient K un corps de nombre et v une valuation sur K. On a*

(i) $v(1) = 0$,

(ii) $\forall x \in K\ v(x) = v(-x)$,

(iii) $\forall x \in K\, v(x) = -v(x^{-1})$.

Définition 5.1.9 (Valuations équivalentes)**.** Notons $\mathrm{val}(K)$ l'ensemble des valuations sur K quotienté par la relation d'équivalence définie par $v_1 \propto v_2 \iff \exists a > 0\, v_1 = a v_2$.

On remarque alors que toute valuation permet d'obtenir des valeurs absolues ultramétriques, et que toute valeur absolue ultramétrique s'obtient à partir d'une valuation.

Proposition 5.1.8. *Soient v une valuation et $b > 1$.*
Alors, $|\cdot|_{b,v} = b^{-v(\cdot)}$ est une valeur absolue ultramétrique.

Démonstration. La séparation correspond à l'axiome (i) des valuations et la multiplicativité à l'axiome (ii). Enfin, l'inégalité ultramétrique provient de l'axiome (iii). En effet, soient $x, y \in K$.

$$|x+y|_{b,v} = b^{-v(x+y)} \leq b^{-\min(v(x),v(y)))} = \max(b^{-v(x)}, b^{-v(y)}) = \max(|x|_{b,v}, |y|_{b,v}).$$

□

Proposition 5.1.9. *Soient $|\cdot|$ une valeur absolue ultramétrique et $b > 1$. Alors,*

$$v \;:\; \left|\begin{array}{ccc} K & \to & \mathbb{R} \cup \{\infty\} \\ x & \mapsto & -\ln_b |x| \quad si\ x \neq 0 \\ 0 & \mapsto & \infty \end{array}\right.$$

est une valuation, avec $|\cdot| = b^{-v(\cdot)}$.

Démonstration. Comme pour la proposition précédente, on récupère tous les axiomes des valuations directement à partir de ceux des valeurs absolues ultramétriques, et la dernière remarque est claire. □

Les constructions précédentes induisent une bijection entre $\mathcal{M}_K^0$ et $\mathrm{val}(K)$.

Proposition 5.1.10. *L'application suivante est bien définie et bijective :*

$$\begin{array}{ccc} \mathrm{val}(K) & \to & \mathcal{M}_K^0 \\ \overline{v} & \mapsto & |\cdot|_v, \end{array}$$

où pour toute valuation v, on note $\overline{v}$ sa classe dans $\mathrm{val}(K)$, et $|\cdot|_v = b^{-v}$ pour un $b > 1$ arbitraire.

Démonstration. Montrer que l'application est bien définie revient à montrer que pour toutes valuations $v_1 \propto v_2$ et $a, b > 1$, $|\cdot|_{a,v_1} \sim |\cdot|_{b,v_1} \sim |\cdot|_{b,v_2}$.

Cela provient du fait que si $v_1 = cv_2$, où $c > 0$, alors

$$|\cdot|_{b,v_1} = (|\cdot|_{b,v_2})^c = (|\cdot|_{a,v_1})^{\frac{\ln b}{\ln a}}.$$

Réciproquement, si $|\cdot|_1 \sim |\cdot|_2$, avec $|\cdot|_1 = |\cdot|_2^c$, si on fixe $b_1, b_2 > 0$, et qu'on pose $v_1 = -\ln_{b_1} |\cdot|_1$, $v_2 = -\ln_{b_2} |\cdot|_2$, alors

$$v_1 = c\frac{\ln b_2}{\ln b_1} v_2.$$

□

Il y a donc correspondance entre places ultramétriques et classes de valuations.

Exemple 5.1.7. La valuation associée à la valeur absolue triviale est $x \mapsto \infty \cdot \delta_0(x)$.

Exemple 5.1.8. Sur $\mathbb{Q}$, pour tout $p \in \mathcal{P}$, v_p est l'unique valuation v associée à la place de $|\cdot|_p$ telle que $v(p) = 1$.

Valuations et idéaux Établissons maintenant la correspondance entre valuations et idéaux premiers $\mathcal{O}_K$.

Dans la partie 3, on a défini en 3.2.7 la notion de valuation $\mathfrak{p}$-adique d'un idéal, qu'on peut transformer en une notion de valuation $\mathfrak{p}$-adique sur $\mathcal{O}_K$ puis sur K. Rappelons-en l'idée.

Définition 5.1.10 (Valuation $\mathfrak{p}$-adique)**.** Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$.

Pour tout $x \in \mathcal{O}_K$ non nul, on pose $v_\mathfrak{p}$ l'exposant de $\mathfrak{p}$ dans l'unique décomposition en idéaux premiers de l'idéal principal (x).

On étend alors $v_\mathfrak{p}$ à K en posant $v_\mathfrak{p}(0) = \infty$ et pour tout $x \in K \backslash \mathcal{O}_K$, $v_\mathfrak{p}(x) = v_\mathfrak{p}(a) - v_\mathfrak{p}(b)$ où $a, b \in \mathcal{O}_K$ et $x = \frac{a}{b}$.

On vérifie alors que $v_\mathfrak{p}$ est bien une valuation (proposition 3.2.33), qu'on appelle *valuation $\mathfrak{p}$-adique sur K*.

D'après ce qui précède, tout idéal premier $\mathfrak{p}$ définit donc une valuation $v_\mathfrak{p}$, puis une valeur absolue – ou plutôt une place – qu'on note $|\cdot|_\mathfrak{p}$.

Réciproquement, montrons que toute valuation sur K est soit triviale, soit équivalente à une valuation $\mathfrak{p}$-adique. Pour arriver à ce résultat, commençons par une remarque préliminaire.

Proposition 5.1.11. *Soit v une valuation sur K.*

Pour tout $x \in \mathcal{O}_K$, $v(x) \geq 0$.

Démonstration. Rappelons que pour tout entier $a \in \mathbb{Z}$, $|a| \leq 1$, où $|\cdot|$ est la valeur absolue associée à v, d'où $\forall a \in \mathbb{Z}\, v(a) \geq 0$.

Soient maintenant $x \in \mathcal{O}_k$, puis $n \geq 1$, $a_{n-1}, ..., a_0 \in \mathbb{Z}$ tels que

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

Supposons par l'absurde que $v(x) < 0$.

$$nv(x) = v(x^n) = v\Big(\sum_{k=0}^{n-1} a_k x^k\Big) \geq \min_{0\leq k\leq n-1}(v(a_k) + kv(x)) \geq (n-1)v(x),$$

d'où $v(x) \geq 0$: contradiction. □

Attention : on a seulement une inclusion.

Exemple 5.1.9. Soit $p \in \mathcal{P}$ un nombre premier. On a

$$\{x \in \mathbb{Q} \,|\, v_p(x) \geq 0\} = \left\{\frac{a}{b} \,\middle|\, a \in \mathbb{Z},\, b \in \mathbb{Z}^*,\, p \nmid b\right\} = \mathbb{Z}_{(p)}.$$

Cet exemple se généralise.

Proposition 5.1.12. *Soit v une valuation non triviale sur K.*
$\mathcal{O}_v = \{x \in K \,|\, v(x) \geq 0\}$ est un sous-anneau de K, et $\mathfrak{m} = \{x \in K \,|\, v(x) > 0\}$ est son unique idéal maximal.

Démonstration.

- Il est facile de vérifier que $\mathcal{O}_v$ est stable par addition, multiplication, et contient 0 et 1.
- De même, il est clair que $\mathfrak{m}$ est un idéal de $\mathcal{O}_v$. Montrons qu'il est maximal. Soit I un idéal de $\mathcal{O}_v$ tel que $\mathfrak{m} \subset I \subset \mathcal{O}_v$ avec $\mathfrak{m} \neq I$.
  On dispose de $x \in I \backslash \mathfrak{m}$. On a alors $v(x) = 0$ et $x \neq 0$, d'où $x^{-1} \in \mathcal{O}_v$. Ainsi, pour tout $y \in \mathcal{O}_v$, $y = (yx^{-1})x \in I$. On en déduit que $I = \mathcal{O}_v$, d'où $\mathfrak{m}$ maximal.
- La preuve de l'unicité est similaire. Soit I un idéal maximal de $\mathcal{O}_v$. Si $I \subset \mathfrak{m}$, alors par maximalité $I = \mathfrak{m}$.
  Supposons donc par l'absurde qu'il existe $x \in I \backslash \mathfrak{m}$, et soit un tel x. Comme précédemment, $\forall y \in \mathcal{O}_v\, (yx^{-1})x = y \in I$ d'où $I = \mathcal{O}_v$: contradiction.

□

Revenons au résultat qui nous intéresse.

Proposition 5.1.13. *Soient v une valuation sur K et $\mathfrak{p} = \{x \in \mathcal{O}_K \,|\, v(x) > 0\}$.*
Alors, $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_K$.
Si $\mathfrak{p}$ est réduit à $\{0\}$, cela signifie que v est la valuation triviale. Sinon, $v \propto v_{\mathfrak{p}}$.

Démonstration.

- D'après la proposition 5.1.11 et les axiomes des valuations, $\mathfrak{p}$ est un idéal de $\mathcal{O}_K$.
- De plus, soient $x, y \in \mathcal{O}_K$ tels que $xy \in \mathfrak{p}$. $v(x) + v(y) > 0$, donc $v(x) > 0$ ou $v(y) > 0$, i.e. $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$. $\mathfrak{p}$ est donc premier.
- Supposons $\mathfrak{p} \neq \{0\}$. Soit $\pi \in \mathfrak{p} \backslash \mathfrak{p}^2$. Il est clair qu'un tel π existe, puisque si $\mathfrak{p} = \mathfrak{p}^2$, on peut simplifier par $\mathfrak{p}$, puisque $\mathcal{O}_K$ est de Dedekind, et on en déduit que $\mathfrak{p} = \mathcal{O}_K$ ce qui est absurde.

  On a donc $v(\pi) > 0$ et $v_{\mathfrak{p}}(\pi) = 1$.

  Soit $\alpha \in K$ non nul. $v_{\mathfrak{p}}(\alpha \pi^{-v_{\mathfrak{p}}(\alpha)}) = 0$, donc d'après la proposition 3.2.39, on dispose de $a, b \in \mathcal{O}_K \backslash \mathfrak{p}$ tel que $\alpha \pi^{-v_{\mathfrak{p}}(\alpha)} = \frac{a}{b}$.

  Comme $v(a) = v(b) = 0$, on en déduit que $v(\alpha \pi^{-v_{\mathfrak{p}}(\alpha)}) = 0$, puis finalement que

$$v(\alpha) = v(\pi) v_{\mathfrak{p}}(\alpha).$$

  Ainsi, $v = v(\pi) v_{\mathfrak{p}}$, où $v(\pi) > 0$.

□

Remarquons que pour deux valuations équivalentes, on obtient le même $\mathfrak{p}$.
On a donc atteint notre objectif.

Proposition 5.1.14. *Soit K un corps de nombre. On a la correspondance suivante.*

$$\mathcal{M}_K^0 \longleftrightarrow \mathrm{val}(K) \longleftrightarrow \mathrm{Spec}(\mathcal{O}_K).$$

5.2 Complétion

Le lecteur a probablement déjà rencontré la notion de complétion : $\mathbb{R}$ peut par exemple se définir comme le complété de $(\mathbb{Q}, |\cdot|_\infty)$. Intuitivement $\mathbb{R}$ est donc ce qu'on obtient quand on ajoute à $\mathbb{Q}$ toutes les limites des suites qui sont de Cauchy au sens de la valeur absolue usuelle.

Il est intéressant d'étudier ce qu'on obtient pour d'autres corps de nombres et pour d'autres valeurs absolues : c'est l'objet de cette partie.

Notons que cette étude n'est pas gratuite, et aura son importance quand on voudra construire les hauteurs. En effet, c'est grâce à l'étude des complétions qu'on caractérise toutes les places archimédiennes de K, ce qui nous permet d'obtenir le théorème d'Ostrowski. De façon peut-être plus importante encore, c'est ce point de vue qui nous permettra de bien choisir les représentants des places au moment de construire la hauteur.

- En 5.2.1, on étudie la notion de complétion d'un corps valué, en la définissant par une propriété universelle.

- On utilise alors cette notion en 5.2.2 pour caractériser les places archimédiennes de K, le dernier élément qu'il nous manquait pour établir le théorème d'Ostrowski.
- Enfin, en 5.2.3, on étudie les complétions d'un corps de nombres pour ses places ultra-métriques, ce qui permet une petite escapade dans le monde merveilleux des nombres p-adiques et $\mathfrak{p}$-adiques.

5.2.1 • Quelques diagrammes

On va maintenant aborder la notion de complétion d'un corps valué.

- Tout d'abord, on définit les notions utiles, et ce qui nous permettra de dessiner des diagrammes.
- On définit ensuite le complété comme solution d'un problème universel à la définition 5.2.3, puis on montre à la proposition 5.2.2 que ce problème admet bien une solution (unique à unique isomorphisme près).
- Ceci étant fait, on montre à la proposition 5.2.4 que pour un corps de nombre, les opérations « compléter » et « ajouter α algébrique » commutent.
- On énonce enfin en 5.2.5 une proposition majeure, qu'on ne démontrera que dans le chapitre des hauteurs où en a besoin. C'est cette propriété des complétés qui permettra de choisir des bons représentants des places pour construire la hauteur.

Passons donc aux premières définitions.

Définition 5.2.1 (Corps valué complet)**.** Soient K un corps, et $|\cdot|$ une valeur absolue sur K. On dit alors que le couple $(K, |\cdot|)$ est un *corps valué*.

Si de plus les suites de Cauchy (au sens de $|\cdot|$) convergent dans K, on dit alors que c'est un *corps valué complet*.

Définition 5.2.2 (Morphisme de corps valué)**.** Soient $(K, |\cdot|_K)$, $(L, |\cdot|_L)$ deux corps valués.

On appelle *morphisme de corps valués* tout morphisme de corps $\sigma : K \hookrightarrow L$ tel que $|\cdot|_K = |\sigma(\cdot)|_L$.

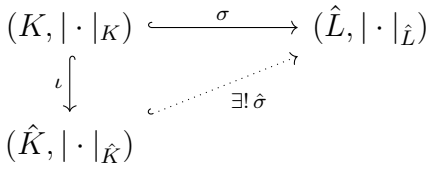
Le *complété* d'un corps valué est alors « le plus petit » corps valué complet qui le contient. On peut préciser cela sous la forme d'une propriété universelle.

Définition 5.2.3 (Complété d'un corps valué)**.** Soit $(K, |\cdot|)$ un corps valué. On appelle *complété* de K tout couple $((\hat{K}, |\cdot|), \iota)$ tel que

(i) $(\hat{K}, |\cdot|_{\hat{K}})$ est un corps valué complet,

(ii) $\iota : (K, |\cdot|) \hookrightarrow (\hat{K}, |\cdot|_{\hat{K}})$ est un morphisme de corps valués,

(iii) Pour tout corps valué complet $(\hat{L}, |\cdot|_{\hat{L}})$ et morphisme de corps valués σ, on a le diagramme commutatif ci-dessous.



On dit que ι est universel parmi les morphismes de K vers un corps valué complet.

Comme toute propriété universelle, cette définition nous fournit l'unicité à unique isomorphisme près, sous réserve d'existence d'un solution.

Proposition 5.2.1. *La propriété (iii) fournit l'unicité à (unique) isomorphisme près du complété d'un corps valué, sous réserve d'existence.*

Démonstration. En effet, soient $(\hat{K}_1, |\cdot|_1)$ et $(\hat{K}_2, |\cdot|_2)$ deux complétés de $(K, |\cdot|)$, et $\iota_1 : K \hookrightarrow K_1$, $\iota_2 : K \hookrightarrow K_2$ les plongements correspondants.

D'après la propriété (iii) il existe d'uniques $\sigma_1 : K_1 \hookrightarrow K_2$, $\sigma_2 : K_2 \hookrightarrow K_1$ tels que $\iota_1 = \sigma_1 \circ \iota_2$ et $\iota_2 = \sigma_2 \circ \iota_1$.

σ_1 et σ_2 sont donc des isomorphismes de corps valués, inverses l'un de l'autre. □

Montrons maintenant qu'il existe bien toujours une solution à ce problème universel.

Proposition 5.2.2. *Soit $(K, |\cdot|)$ un corps valué. Son complété existe et est unique à unique isomorphisme près.*

Démonstration.

- L'unicité à unique isomorphisme près est la proposition 5.2.1.
- Il s'agit donc de construire un complété, ce qui se fait de la même manière que pour $\mathbb{R}$: on considère l'ensemble des suites de Cauchy sur K, qu'on quotiente par la relation $u \sim v \iff (u - v)_n \underset{n\to\infty}{\to} 0$. Plus formellement, posons
  - $C(K) = \{a \in K^{\mathbb{N}} \,|\, \forall \epsilon > 0\, \exists N\, \forall n, m \geq N\, |a_n - a_m| < \epsilon\}$, l'ensemble des suites de Cauchy de K. C'est un anneau unitaire, d'unité la suite constante égale à 1.
  - $M(K) = \{a \in K^{\mathbb{N}} \,|\, a_n \to 0\}$, qui est un idéal de $C(K)$.
  - $\hat{K} = C(K)/M(K)$ l'anneau quotient.

  Montrons maintenant qu'on peut construire une valeur absolue $|\cdot|_{\hat{K}}$ et une injection ι telle que $(\hat{K}, |\cdot|_{\hat{K}}, \iota)$ soit une solution au problème universel.
  - Montrons que $\hat{K}$ est un corps. Soit $a \in C(K) \setminus M(K)$. $(|a_n|)_{n\in\mathbb{N}}$ est une suite de Cauchy dans $\mathbb{R}_+$, qui converge donc vers un certain $\alpha > 0$. On dispose alors de $N \in \mathbb{N}$ tel que $\forall n > N\, |a_n - \alpha| \leq |\frac{\alpha}{2}|$.

    Posons maintenant $b \in K^{\mathbb{N}}$ la suite définie par $b_n = 1$ pour $0 \leq n \leq N$, et $b_n = a_n$ pour $n > N$. b est de Cauchy, et $\hat{a} = \hat{b}$ (où $\hat{u}$ désigne la classe d'équivalence de u dans $\hat{K}$).

Maintenant que les zéros de a ont été supprimés, on peut définir la suite $c = (b_n^{-1})_{n\in\mathbb{N}}$. Dans $K^{\mathbb{N}}$, $bc = 1$. Il reste à montrer que $c \in C(K)$. Cela découle de

$$\forall n, m \in \mathbb{N}\, |b_n^{-1} - b_m^{-1}| = |b_n^{-1}||b_m^{-1}||b_m - b_n| \leq \frac{4}{\alpha^2}|b_m - b_n|.$$

On a donc obtenu $c \in C(K)$ tel que $\hat{a}\hat{c} = 1$, et ce pour tout $a \notin M(K)$: $\hat{K}$ est un corps.

- Étendons la valeur absolue de K à $\hat{K}$.
  On peut remarquer que pour tous $a \in C(K), b \in M(K)$ on a $\lim |a_n + b_n| = \lim |a_n|$. On en déduit que l'application $a \in C(K) \mapsto \lim |a_n|$ passe au quotient en une application $|\cdot|_{\hat{K}} : \hat{K} \to \mathbb{R}_+$. On vérifie alors que $|\cdot|_{\hat{K}}$ est bien une valeur absolue sur $\hat{K}$.
- Posons $\iota : K \to \hat{K}$ qui à x associe la classe d'équivalence de la suite constante $(x)_{n\in\mathbb{N}}$. C'est clairement un morphisme de corps valués.
  Remarquons que $\iota(K)$ est dense dans $\hat{K}$. En effet, soient $\hat{a} \in \hat{K}$ et $a \in C(K)$ un de ses représentants. Soit $\epsilon > 0$. On dispose de $N \in \mathbb{N}$ tel que $\forall n, m \geq N\, |a_n - a_m| < \epsilon$. Alors,
  $$|\iota(a_N) - \hat{a}|_{\hat{K}} = \lim_n |a_N - a_n| = 0.$$
- Montrons maintenant que $(\hat{K}, |\cdot|_{\hat{K}})$ est un corps valué complet. Soit $(\widehat{a^{(n)}})_{n\in\mathbb{N}}$ de Cauchy dans $\hat{K}$.
  Par densité de $\iota(K)$, pour tout $n \in \mathbb{N}$, on dispose de $b_n \in K$ tel que $|\iota(b_n) - \widehat{a^{(n)}}|_{\hat{K}} < 2^{-n}$.
  Soit $\epsilon > 0$. On dispose de N tel que $\forall n, m \geq N\, |\widehat{a^{(n)}} - \widehat{a^{(m)}}| < \frac{\epsilon}{2}$ et de M tel que $\forall n, m \geq M\, 2^{-n} + 2^{-m} < \frac{\epsilon}{2}$. Alors, pour tous $n, m \geq \max(N, M)$,
  $$|b_n - b_m| = |\iota(b_n) - \iota(b_m)|_{\hat{K}} < 2^{-n} + |\widehat{a^{(n)}} - \widehat{a^{(m)}}|_{\hat{K}} + 2^{-m} < \epsilon.$$
  (b_n) est donc de Cauchy dans K.
  De plus,
  $$\lim_n |\hat{b} - \widehat{a^{(n)}}|_{\hat{K}} \leq \lim_n |\hat{b} - \iota(b_n)|_{\hat{K}} + |\iota(b_n) - \widehat{a^{(n)}}|_{\hat{K}} \leq \lim_n \left(\lim_m |b_m - b_n| + 2^{-n} \right) = 0,$$
  c'est à dire que $\hat{b}$ est limite de $(\widehat{a^{(n)}})$. $(\hat{K}, |\cdot|_{\hat{K}})$ est donc complet.
- Maintenant que la structure de $(\hat{K}, |\cdot|_{\hat{K}}, \iota)$ est acquise, montrons enfin que c'est une solution au problème universel. Soient $(L, |\cdot|_L)$ complet et $\sigma : K \to L$ comme dans le diagramme (iii) en 5.2.3.
  Posons
  $$\hat{\sigma} \; : \left| \begin{array}{ccc} \hat{K} & \to & L \\ \hat{x} & \mapsto & \lim_n \sigma(x_n). \end{array} \right.$$
  $\hat{\sigma}$ est bien définie. En effet, pour toute suite $x \in C(K)$, $(\sigma(x_n))$ est de Cauchy dans L (qui est complet), donc converge. De plus, pour toute suite $y \in M(K)$, $\sigma(y_n) \to 0$, donc l'application ne dépend pas du représentant choisi.

On vérifie de plus que $\hat{\sigma}$ est bien un morphisme de corps valué, et on a bien $\sigma = \hat{\sigma} \circ \iota$.
Soit maintenant $\phi : \hat{K} \to L$ un morphisme de corps valué tel que $\sigma = \phi \circ \iota$. Montrons que $\phi = \hat{\sigma}$.
Soit $\hat{x} \in \hat{K}$. Par densité de $\iota(K)$, on dispose de deux suites $(x_n) \in K^{\mathbb{N}}$, $(\epsilon_n) \in \hat{K}^n$ telles que $\forall n \in \mathbb{N}\, \hat{x} = \iota(x_n) + \epsilon_n$, et $\epsilon_n \to 0$.
Alors, $\phi(\hat{x}) = \phi(\iota(x_n) + \epsilon_n) = \sigma(x_n) + \phi(\epsilon_n)$. En passant à la limite, comme $\lim_n \phi(\epsilon_n) = 0$, on obtient $\phi(\hat{x}) = \lim_n \sigma(x_n)$, d'où $\phi = \hat{\sigma}$.
On a donc bien l'existence et l'unicité de $\hat{\sigma}$ rendant le diagramme commutatif.

□

Exemple 5.2.1. On insiste un peu, cet exemple élémentaire étant fondamental : $\mathbb{R}$ muni de la valeur absolue usuelle est le complété de $(\mathbb{Q}, |\cdot|_\infty)$.

Corollaire 5.2.1. *On déduit immédiatement de la construction que $\hat{K}$ que K est dense dans sa complétion.*

Plus précisément, pour tout corps valué $(K, |\cdot|_K)$, complété à travers l'injection ι, le sous-corps $\iota(K)$ de $\hat{K}$ est dense dans $(\hat{K}, |\cdot|_{\hat{K}})$.

Proposition 5.2.3 (Extension de morphisme par complétion)**.** *Soient $(K, |\cdot|_K)$, $(L, |\cdot|_L)$ des corps valués, et $((\hat{K}, |\cdot|_{\hat{K}}), \iota_K)$, $((\hat{L}, |\cdot|_{\hat{L}}), \iota_L)$ leurs complétions respectives.*

Pour tout morphisme de corps valué $\sigma : K \to L$, il existe un unique morphisme de corps valué $\hat{\sigma}$ rendant le diagramme suivant commutatif.

$$\begin{array}{ccc} (K, |\cdot|_K) & \xhookrightarrow{\sigma} & (L, |\cdot|_L) \\ {\scriptstyle \iota_K}\downarrow & & \downarrow{\scriptstyle \iota_L} \\ (\hat{K}, |\cdot|_{\hat{K}}) & \xhookrightarrow{\exists! \hat{\sigma}} & (\hat{L}, |\cdot|_{\hat{L}}) \end{array}$$

Démonstration. Il suffit d'utiliser la définition du complété $(\hat{K}, |\cdot|_{\hat{K}})$ à l'aide de la propriété universelle, et de constater que $\iota_L \circ \sigma : K \to \hat{L}$ est un morphisme de corps valué vers un corps valué complet. □

Une autre opération utile sera de faire commuter « ajouter α algébrique » et « compléter ».

La démonstration s'appuie sur l'équivalence des normes sur un $\hat{K}$-ev de dimension finie, où $\hat{K}$ est un corps valué complet *quelconque*. La proposition suivante ne sera en fait utilisée que dans le cas des corps de nombres archimédiens, et on peut donc se reposer sur l'équivalence des normes d'un $\mathbb{R}$-ev, qui est bien connue. La démonstration complète de ce lemme se fait relativement bien par récurrence, et le lecteur intéressé pourra trouver les détails à la proposition 1.17 de ce cours de Pierre Colmez [20].

On reprend ici l'idée de la démonstration du théorème 4.1.5 de [18].

Proposition 5.2.4 (« Ajouter α » et « compléter » commutent)**.**
*Soient $(K, |\cdot|_K)$ et $L = K[\alpha]$ une extension **finie** munie de $|\cdot|_L$ qui étend $|\cdot|_K$. Alors,*

$$\hat{K}[\alpha] = \widehat{K[\alpha]}.$$

*On peut représenter ce fait en disant, de façon très informelle, que le diagramme commutatif suivant commute. **Attention** : les flèches ne représentent pas des morphismes mais des opérations d'extension de corps.*

$$\begin{array}{ccccc} K & & \xrightarrow{\cdot[\alpha]} & & K[\alpha] \\ \Big\downarrow{\scriptstyle \hat{\cdot}} & & & & \Big\downarrow{\scriptstyle \hat{\cdot}} \\ \hat{K} & & \xrightarrow{\cdot[\alpha]} & \hat{K}[\alpha] & = \widehat{K[\alpha]} \end{array}$$

Le point difficile est de montrer qu'on a bien une égalité en bas à droite, et non une simple inclusion.

Démonstration. On procède par double inclusion.

Pour simplifier les notations, on laisse implicites les injections $\iota_K : K \to \hat{K}$ et $\iota_L : L \to \hat{L}$.

La possibilité d'injecter $\hat{K}$ dans $\hat{L}$ au sens des corps valués, sans se poser de question, vient du fait que leurs valeurs absolues sont des normes d'espaces vectoriels, et de l'équivalence des normes sur les $\hat{K}$-ev de dimension finie :

$$(\hat{K}, |\cdot|_{\hat{K}}) \cong (\hat{K}, |\cdot|_{\hat{L}}).$$

- Comme $\hat{K} \subset \widehat{K[\alpha]}$ et $\alpha \in \widehat{K[\alpha]}$, il est clair que $\hat{K}[\alpha] \subset \widehat{K[\alpha]}$.
- Réciproquement, montrons que le sous-corps $\hat{K}[\alpha]$ de $\hat{L}$ est égal à $\hat{L}$ tout entier.
  - Remarquons tout d'abord que $\hat{K}[\alpha]/\hat{K}$ est algébrique. En effet, α est annulé par $\pi_{K,\alpha} \in K[X] \subset \hat{K}[X]$.
  - Remarquons que $|\cdot|_{\hat{L}}$ induit une valeur absolue sur $\hat{K}[\alpha]$ qui est aussi une norme de $\hat{K}$-espace vectoriel : $(\hat{K}[\alpha], |\cdot|_{\hat{L}})$ est un $\hat{K}$-espace vectoriel normé de dimension finie !
  - $\hat{K}[\alpha]$ est donc muni de l'unique topologie de $\hat{K}$-ev de dimension finie $[\hat{K}[\alpha] : \hat{K}]$. En conséquence, $\hat{K}[\alpha]$ est complet, et est donc fermé dans $\hat{L}$.
  - Ainsi, $\hat{K}[\alpha]$ contient $K[\alpha] = L$ qui est dense dans $\hat{L}$, et est également fermé dans $\hat{L}$:

$$\hat{K}[\alpha] = \hat{L}.$$

□

Exemple 5.2.2. En particulier, pour tout $\alpha \in \mathbb{C}$ algébrique sur $\mathbb{Q}$, au sens de $|\cdot|_\infty$,

$$\widehat{\mathbb{Q}[\alpha]} = \mathbb{R}[\alpha].$$

Avant de conclure ces remarques générales sur les complétions et de passer à l'étude des complétions de K pour chacune de ses places, énonçons le résultat global suivant, qui fait fonctionner la théorie de la hauteur, et qu'on démontrera au moment de l'aborder. Cette propriété motive également l'étude des complétions de K, puisqu'il est nécessaire de les comprendre pour la démontrer.

Définition 5.2.4 (Extension de valeur absolue)**.** Soient K un corps de nombre et L une extension finie de K.

Pour toutes valeurs absolues w de L et v de K, on dit que w *étend* v si w coïncide avec v sur K, ce que l'on note $w|v$.

Définition 5.2.5. Quand K est un corps de nombre et v une valeur absolue (ou une place de K, pour alléger les notations, on désignera parfois par K_v le complété de (K, v).

Proposition 5.2.5. *Soient K un corps de nombre et L une extension finie de K.*

Alors, pour toute valeur absolue v de K,

$$\sum_{w|v} [L_w : \mathbb{Q}_w] = [L : K][K_v : \mathbb{Q}_v],$$

où w parcourt l'ensemble des valeurs absolues de L qui étendent w.

Si l'on faisait de la géométrie algébrique, on pourrait interpréter ce résultat en disant que c'est un calcul de dimension sur le produit tensoriel

$$L \bigotimes_K K_v = \prod_{w|v} L_w,$$

ou

$$\mathcal{O}_L \bigotimes_{\mathcal{O}_K} (\mathcal{O}_K)_v = \prod_{w|v} (\mathcal{O}_L)_w,$$

qui s'interprète en disant qu'on regarde la fibre de $(\mathcal{O}_K)_v$ dans $\mathcal{O}_L$ qui vit au-dessus de $\mathcal{O}_K$...

Mais on n'aborde pas ici ce point de vue algébrique, plus profond, mais qui demande plus de pré-requis.

5.2.2 • Places archimédiennes et plongements

On va maintenant utiliser la théorie des complétions pour caractériser les places archimédiennes sur K, ce qui est le dernier ingrédient du théorème d'Ostrowski.

- On commence par montrer à la proposition 5.2.6 que $|\cdot|_\infty$ est, à équivalence près, la seule valeur absolue archimédienne de $\mathbb{Q}$. On aura ainsi démontré le théorème d'Ostrowski sur $\mathbb{Q}$.
- On donne ensuite à la définition 5.2.6 des exemples de valeurs absolues archimédiennes sur K. L'idée est de faire un détour par K en allant de $\mathbb{Q}$ à $\mathbb{C}$: on fait donc intervenir les plongements $\sigma \in \Sigma(K)$.
- Les dernières propositions s'appuient sur la théorie des complétions, et nous assurent que ces exemples fournissent une classification de toutes les places archimédiennes de K.

  On montre donc en 5.2.7 qu'il n'y a pas de cas d'équivalence non trivial entre les $|\cdot|_\sigma$ pour $\sigma \in \Sigma(K)$.

  La proposition 5.2.8 montre ensuite qu'il n'y a que deux façons de compléter K muni d'une place archimédienne : on tombe sur $\mathbb{R}$ ou $\mathbb{C}$.

  Enfin, la proposition 5.2.9 nous assure que toutes les places archimédiennes sont bien issues de $\sigma \in \Sigma(K)$.

On obtiendra ainsi les correspondances $\mathcal{M}_\mathbb{Q}^\infty \leftrightarrow \{\infty\}$ et $\mathcal{M}_K^\infty \leftrightarrow \Sigma(K)/(\text{C-conjugaison})$.
Commençons donc par l'ingrédient final du théorème d'Ostrowski de $\mathbb{Q}$.

Proposition 5.2.6. *Soit $|\cdot|$ une valeur absolue archimédienne sur $\mathbb{Q}$. Alors, $|\cdot| \sim |\cdot|_\infty$.*

Démonstration. En effet, soient $|\cdot|$ une telle valeur absolue et $b \in \mathbb{N}$ minimal tel que $|b| > 1$. Un tel b existe puisque $\mathbb{Z} \not\subset B(0,1)$ (cf proposition 5.1.4). De plus, $b \geq 2$ puisque $|0| = 0$ et $|1| = 1$.

Soit $e \in \mathbb{R}_+^*$ tel que $|b| = b^e$.

- Soit $n \in \mathbb{N}^*$. On dispose de $s \geq 0$, $a_0, ..., a_s \in [\![0, b-1]\!]$ tels que $n = \sum_{k=0}^s a_k b^k$. Remarquons que $\forall k\, |a_k| \leq 1$ par minimalité de b. On a alors

$$|n| \leq \sum_{k=0}^{s} |a_k||b|^k \leq \sum_{k=0}^{s} |b|^k \leq \frac{|b|^{s+1}-1}{|b|-1} \leq |b|^s \frac{1}{1-\frac{1}{|b|}} = Cb^e s \leq Cn^e,$$

  où l'on a posé $C = \frac{1}{1-\frac{1}{|b|}}$. Ainsi, $\forall n \in \mathbb{N}^*\, |n| \leq C|n|_\infty^e$.
- Pour $n \in \mathbb{N}^*$ fixé, on a alors, pour tout $r \in \mathbb{N}^*$, $|n|^r = |n^r| \leq C|n|_\infty^{re}$, puis $|n| \leq C^{\frac{1}{r}}|n|_\infty^e$, d'où finalement

$$|n| \leq |n|_\infty^e.$$

- Réciproquement, posons $n \in \mathbb{N}^*$ où $n = \sum_{k=0}^s a_k b^k$ comme précédemment. On a

$$b^{e(s+1)} = |b|^{s+1} = |b^{s+1} - n + n| \leq |b^{s+1} - n| + |n| \leq (b^{s+1} - n)^e + |n|.$$

Ainsi,

$$|n| \geq b^{e(s+1)} - (b^{s+1} - n)^e = b^{e(s+1)}\left(1 - (1 - \frac{n}{b^{s+1}})^e\right) \geq n^e\left(1 - (1 - \frac{1}{b^s})^e\right) = C'n^e,$$

où l'on a posé $C' = 1 - (1 - \frac{1}{b^s})^e$, donc $\forall n \in \mathbb{N}^* \, |n| \geq C'|n|_\infty^e$.

- Par le même argument que précédemment, on en déduit que

$$\forall n \in \mathbb{N}^* \, |n| \geq |n|_\infty^e.$$

- On a donc montré que $|\cdot| = |\cdot|_\infty^e$ sur $\mathbb{N}^*$, ce qui s'étend directement à $\mathbb{Z}$ puis $\mathbb{Q}$.

□

Le théorème d'Ostrowski de $\mathbb{Q}$ est démontré.

Donnons maintenant des exemples de valeurs absolues archimédiennes sur K. L'idée est de faire un détour par K en allant de $\mathbb{Q}$ à $\mathbb{C}$: il s'agit donc de faire intervenir $\Sigma(K)$.

Définition 5.2.6. Pour tout $\sigma \in \Sigma(K)$, on pose

$$|\cdot|_\sigma \; : \left| \begin{array}{ccc} K & \to & \mathbb{R}_+ \\ x & \mapsto & \|\sigma(x)\|, \end{array} \right.$$

où $\|\cdot\|$ représente le module complexe.

On vérifie que $|\cdot|_\sigma$ est une valeur absolue archimédienne, qui coïncide avec $|\cdot|_\infty$ sur $\mathbb{Q}$.

On peut remarquer que $|\cdot|_\sigma = |\cdot|_{\overline{\sigma}}$. Nous allons montrer que c'est en fait le seul cas cas d'équivalence parmi ces exemples, et que toutes les valeurs absolues archimédiennes (normalisées pour coïncider avec $|\cdot|_\infty$ sur $\mathbb{Q}$) sont de cette forme.

Tout d'abord, remarquons qu'il n'y a pas de cas d'équivalence non trivial.

Proposition 5.2.7. *Soient $\sigma, \rho \in \Sigma(K)$. Si $|\cdot|_\sigma \sim |\cdot|_\rho$, alors σ et ρ sont égaux ou conjugués.*

Démonstration. Soit $x \in K$ tel que $K = \mathbb{Q}[x]$. $\sigma \circ \rho^{-1}$ induit un isomorphisme de $\mathbb{Q}$-algèbres et de corps valués entre $(\mathbb{Q}[\rho(x)], \|\cdot\|_{\mathbb{C}})$ et $(\mathbb{Q}[\sigma(x)], \|\cdot\|_{\mathbb{C}})$.

Ce morphisme s'étend par complétion en un isomorphisme de $\mathbb{R}$-algèbres et de corps valués $\psi : (\mathbb{R}[\rho(x)], \|\cdot\|_{\mathbb{C}}) \to (\mathbb{R}[\rho(x)], \|\cdot\|_{\mathbb{C}})$.

On en déduit que $\mathbb{R}[\rho(x)] = \mathbb{R}[\sigma(x)] = \mathbb{R}$ ou $\mathbb{R}[\rho(x)] = \mathbb{R}[\sigma(x)] = \mathbb{C}$.

Ainsi, ψ est un isomorphisme du corps $\mathbb{R}$ ou $\mathbb{C}$ qui fixe $\mathbb{R}$. C'est donc soit l'identité, soit la conjugaison complexe.

Comme $\sigma = \psi \circ \rho$, on en déduit que $\sigma = \rho$ ou $\sigma = \overline{\rho}$. □

Pour vérifier qu'il est nécessaire d'aller jusqu'à $\mathbb{R}$ ou $\mathbb{C}$ quand on construit une place archimédiennes de K, on va montrer qu'il n'y a en fait que deux complétions possibles pour une telle place.

Proposition 5.2.8. *Soit $(K, |\cdot|)$ un corps de nombre valué, où $|\cdot|$ est archimédienne. Alors, une des deux situations suivantes se présente :*

(i) $(\hat{K}, |\cdot|_{\hat{K}}) \cong (\mathbb{R}, \|\cdot\|)$,

(ii) $(\hat{K}, |\cdot|_{\hat{K}}) \cong (\mathbb{C}, \|\cdot\|)$.

Commençons par un lemme.

Lemme 5.2.1. *La norme complexe $\|\cdot\|$ est la seule valeur absolue sur $\mathbb{C}$ qui étend la valeur absolue usuelle de $\mathbb{Q}$ à $\mathbb{C}$.*

Démonstration. Soit $|\cdot|$ une valeur absolue sur $\mathbb{C}$ telle que $\forall x \in \mathbb{R}\, |x| = \|x\|$.
Soit $x \in \mathbb{C}$.

- Supposons que x est une racine de l'unité.
  On dispose de $n \in \mathbb{N}$ tel que $x^n = 1$, d'où $|x|^n = |1| = 1$ puis $|x| = 1$.
- Supposons maintenant que $\|x\| = 1$.
  Soit $\epsilon > 0$. On dispose de ω racine de l'unité et de $\epsilon_1, \epsilon_2 \in [-\frac{\epsilon}{2}, \frac{\epsilon}{2}]$ tels que $x - \omega = \epsilon_1 + i\epsilon_2$.
  Alors, $|x - \omega| \leq |\epsilon_1| + |\epsilon_2| = \|\epsilon_1\| + \|\epsilon_2\| \leq \epsilon$.
  Ainsi,
  $$1 - \epsilon \leq |\omega| - |x - \omega| \leq |x| \leq |\omega| + |x - \omega| \leq 1 + \epsilon.$$
  Ce résultat étant vrai pour tout ϵ, on en déduit que $|x| = 1$.
- Plaçons nous enfin dans le cas général $x \in \mathbb{C}$.
  Si $x = 0$, $|x| = \|x\| = 0$. Sinon, on conclut par
  $$|x| = \left|\|x\| \frac{x}{\|x\|}\right| = |\|x\|| \cdot \left|\frac{x}{\|x\|}\right| = \|x\| \cdot 1 = \|x\|.$$

□

On a maintenant les outils pour conclure.

Démonstration de la proposition 5.2.8. Quitte à prendre une valeur absolue équivalente $|\cdot|$, on peut supposer que $|\cdot|$ étend $|\cdot|_\infty$ de $\mathbb{Q}$.
On a alors le diagramme commutatif suivant.

$$\begin{array}{ccc} (\mathbb{Q}, |\cdot|_\infty) & \hookrightarrow & (K, |\cdot|_K) \\ \downarrow & & \downarrow \sigma \\ (\mathbb{R}, \|\cdot\|) & \overset{\exists!}{\dashrightarrow} & (\hat{K}, |\cdot|_{\hat{K}}) \end{array}$$

Toutes les valeurs absolues peuvent donc être vues comme restrictions de $|\cdot|_{\hat{K}}$, et on peut voir tous les ensembles comme sous-ensembles de $\hat{K}$.

On dispose de $x \in \hat{K}$ algébrique sur $\mathbb{Q}$ tel que $K = \mathbb{Q}[x]$. Comme dans la proposition 5.2.4, on en déduit que

$$\hat{K} = \widehat{\mathbb{Q}[x]} = \hat{\mathbb{R}}[x] = \mathbb{R}[x].$$

Ainsi, $\hat{K}$ est un sur-corps de $\mathbb{R}$ de dimension finie : $\hat{K} = \mathbb{R}$ ou $\hat{K} = \mathbb{C}$.

Reste à montrer que $|\cdot|_{\hat{K}} = \|\cdot\|$, le module complexe. Puisque $|\cdot|_{\hat{K}}$ étend la valeur absolue usuelle sur $\mathbb{R}$, qui correspond à la restriction de $\|\cdot\|$, c'est évident si $\hat{K} = \mathbb{R}$, et c'est le lemme 5.2.1 dans le cas où $\hat{K} = \mathbb{C}$. □

On en déduit le résultat suivant de classification des places archimédiennes sur un corps de nombre.

Proposition 5.2.9. *Soit $(K, |\cdot|)$ un corps de nombre valué, où $|\cdot|$ est archimédienne. Il existe un plongement $\sigma \in \Sigma(K)$ tel que*

$$|\cdot| \sim \|\sigma(\cdot)\|.$$

Démonstration. Ce plongement est simplement le σ du diagramme commutatif de la preuve de la proposition précédente. □

D'après la propriété 5.2.7, cela conclut notre classification des places archimédiennes sur un corps de nombre.

Proposition 5.2.10. *Soit K un corps de nombre. On a la correspondance suivante.*

$$\mathcal{M}_K^\infty \longleftrightarrow \Sigma(K)/(\mathbb{C}\text{-}\textit{conjugaison}).$$

5.2.3 • Les nombres p-adiques

On peut se demander ce qu'on obtient quand on complète K pour une des ses places ultramétriques. Puisqu'on les a déjà obtenues, ce résultat ne nous est pas directement utile pour la classification de ces places. En revanche, cette question – intéressante en elle-même – se reposera au moment d'étudier la hauteur et ses propriétés. En particulier, on a en a besoin pour comprendre la propriété 5.2.5.

- On va commencer par introduire à la définition 5.2.7 les nombres p-adiques $\mathbb{Q}_p$. On montrera ensuite à la proposition 5.2.11 qu'ils admettent une écriture sous la forme de série : c'est la décomposition canonique de Hensel.
- Après cette construction analytique de $\mathbb{Q}_p$, on introduira la notion de limite projective pour présenter une autre construction équivalente, algébrique, de $\mathbb{Q}_p$.
- Ces constructions seront ensuite étendues aux nombres $\mathfrak{p}$-adiques $K_\mathfrak{p}$ à la proposition 5.2.15.

- Enfin, on utilise ces descriptions pour calculer les degrés $[K_\mathfrak{p} : \mathbb{Q}_p]$ et $[L_\mathfrak{P} : K_\mathfrak{p}]$ aux propositions 5.2.16 et 5.2.17. Ce résultat sera illustré sur trois exemples : 5.2.3, 5.2.4 et 5.2.5.

Pour étudier les nombres p-adiques et $\mathfrak{p}$-adiques, on s'est beaucoup appuyés sur les notes publiées par Mourad Abouzaid à propos de son exposé intitulé « Hauteurs de Weil et Application »[21].

Commençons par énoncer le résultat sur $\mathbb{Q}$: on construit les nombres p-adiques.

Définition 5.2.7. Soit $p \in \mathbb{Z}$ un nombre premier. On note $\mathbb{Q}_p$ le completé de $\mathbb{Q}$ pour la norme p-adique, et on l'appelle *corps des nombres p-adiques*.

On note $\mathbb{Z}_p$ son sous-anneau défini par

$$\left\{x \in \mathcal{O}_K \,\middle|\, v_p(x) \geq 0\right\}.$$

$\mathbb{Z}_p$ est appelé l'anneau des entiers de $\mathbb{Q}_p$.

Attention ! Cette définition ne coïncide pas avec l'anneau des entiers d'un corps de nombre. En effet, $\frac{1}{3} \in \mathbb{Z}_p$, mais $\frac{1}{3}$ n'est pas annulé par un polynôme unitaire de $\mathbb{Z}[X]$.

En particulier, on peut remarquer que $\mathbb{Z}_{(2)} \subset \mathbb{Z}_2$, où $\mathbb{Z}_{(2)} = \{x \in \mathbb{Q} \,|\, v_2(x) \geq 0\}$ est la boule définie à la proposition 5.1.6, qui correspond au localisé de la définition 3.2.16, et qui apparaît dans les arbres et empilements de boules qui la suivent. Comme on le disait, en complétant, on en fait « rajouté toutes les feuilles en bout de l'arbre » ! On pourrait par ailleurs montrer que $\mathbb{Z}_p$ est le complété de $\mathbb{Z}$ pour la norme p-adique.

Il est de plus clair par définition que $\mathrm{Frac}(\mathbb{Z}_p) = \mathbb{Q}_p$.

On peut représenter les nombres p-adiques grâce à des séries de Laurent.

Proposition 5.2.11 (Décomposition canonique de Hensel)**.** *Pour tout $x \in \mathbb{Q}_p$, il existe une unique suite $(a_k) \in [\![0, p-1]\!]^{[\![v_p(x), +\infty[\![}$, avec $a_{v_p(x)} \neq 0$ telle que*

$$x = \sum_{k=v_p(x)}^{+\infty} a_k p^k.$$

Pour obtenir ce résultat, nous passerons par quelques résultats intermédiaires.

Lemme 5.2.2. *Soit $x \in \mathbb{Z}_p$. Il existe une suite $(\alpha_n)_{n\in\mathbb{N}^*} \in \mathbb{Z}^{\mathbb{N}^*}$ telle que, au sens $|\cdot|_p$,*

$$x = \lim_{n\to\infty} \alpha_n,$$

et

$$\forall i \in \mathbb{N}^* \; \alpha_{i+1} \equiv \alpha_i [p^i].$$

Démonstration. Comme $\mathbb{Q}_p$ est la complétion $\mathbb{Q}$ pour $|\cdot|_p$, $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$ au sens de $|\cdot|_p$.

Soit $n \in \mathbb{N}^*$. D'après cette remarque, on dispose de $q \in \mathbb{Q}$ tel que $|x - q|_p \leq p^{-n}$.

Comme $|x|_p \leq 1$, $|q|_p = |x + (q - x)|_p \leq \max(1, p^{-n}) = 1$.

On dispose donc de $s, t \in \mathbb{Z}$ avec $p \not| t$ et $q = \frac{s}{t}$.

t étant premier avec p^n, on dispose d'après le lemme de Gauss de $\alpha_n \in [\![0, p^n - 1]\!]$ tel que $t\alpha_n \equiv s\,[p^n]$.

Puisqu'on a aussi $tx \equiv s\,[p^n]$, on en déduit que $x \equiv \alpha_n\,[p^n]$, c'est à dire $|x - \alpha_n|_p \leq p^{-n}$.

Ainsi, $\alpha_n \to x$. De plus, $\forall i \in \mathbb{N}\, \alpha_{i+1} \equiv \alpha_i [p^i]$. □

Lemme 5.2.3. *Pour tout $x \in \mathbb{Q}_p$, il existe une suite $(a_n) \in [\![0, p-1]\!]^{\mathbb{N}}$ telle que*

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

Démonstration. On prend une suite (α_n) comme dans le lemme précédent.

Il suffit alors de définir récursivement (a_n) de telle que sorte que pour tout $n \in \mathbb{N}^*$,

$$\alpha_n = \sum_{k=0}^{n-1} a_k p^k.$$

□

Lemme 5.2.4. *La suite (a_k) du lemme précédent est unique.*

Démonstration. Par l'absurde, soit $(a'_k) \in [\![0, p-1]\!]^{\mathbb{N}}$ une autre suite telle que $x = \sum_k a'_k p^k$.

Soient $n \in \mathbb{N}$ minimal tel que $a_n \neq a'_n$, $\alpha_{n+1} = \sum_{k=0}^{n} a_k p^k$ et $\alpha'_{n+1} = \sum_{k=0}^{n} a'_k p^k$.

On a $|\alpha'_{n+1} - \alpha_{n+1}|_p = |(a'_n - a_n)p^n|_p = p^{-n}$.

Or, en appliquant l'inégalité ultramétrique et par définition de (a_k) et (a'_k),

$$|\alpha'_{n+1} - \alpha_{n+1}|_p = |(\alpha'_{n+1} - x) + (x - \alpha_{n+1})|_p \leq \max(|\alpha'_{n+1} - x|_p, |\alpha_{n+1} - x|_p) < p^{-n},$$

d'où une contradiction. □

Remarquons que contrairement au développement décimal pour $|\cdot|_\infty$, il n'a pas été nécessaire de définir une notion de « développement propre »...

En mettant ces résultats ensemble, on démontre la proposition 5.2.11.

Démonstration – décomposition canonique de Hensel.

Il suffit de constater que $p^{-v_p(x)} x \in \mathbb{Z}_p$ et d'appliquer le résultat obtenu sur $\mathbb{Z}_p$. □

Ainsi,

$$\mathbb{Q}_p = \left\{ \sum_{k \geq n} b_k p^k \,\middle|\, n \in \mathbb{Z},\, \forall k \geq n\, b_k \in [\![0, p-1]\!],\, b_n \neq 0 \right\} \text{ et}$$

$$\mathbb{Z}_p = \left\{ \sum_{k \geq n} b_k p^k \,\middle|\, n \in \mathbb{N},\, \forall k \geq n\, b_k \in [\![0, p-1]\!],\, b_n \neq 0 \right\}.$$

On peut par ailleurs souligner que $\mathbb{Z}_p$ est la boule unité fermée de $\mathbb{Q}_p$, et qu'elle est compacte. La situation est donc très différente de celle sur $\mathbb{R}$.

On peut passer de cette vision analytique de $\mathbb{Q}_p$ et $\mathbb{Z}_p$ à une vision algébrique, sous forme de limite projective, dont on rappelle ici la définition.

Définition 5.2.8. Puisqu'on n'a pas encore discuté de la notion de catégories, considérons ici que « ananas » est une structure algébrique quelconque. On pourra remplacer « ananas » par « anneau » dans le rapport.

On appelle *système projectif d'ananas* une structure composée de

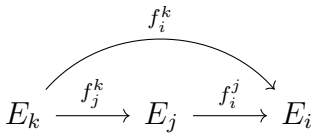
(i) $(I, \leq)$ un ensemble ordonné,

(ii) $(E_i)_{i\in I}$ une famille d'*ananas*,

(iii) $(f_i^j : E_j \to E_i)_{i,j\in I}$ une famille de morphismes d'*ananas* tels que

- $\forall i \in I\ f_i^i = \mathrm{Id}_{E_i}$,
- $\forall i \leq j \leq k \in I\ f_i^k = f_i^j \circ f_j^k$.

Le diagramme suivant est donc commutatif pour tous $i \leq j \leq k \in I$.



On appelle alors *limite projective* de ce système projectif l'ensemble suivant, dont on vérifie que c'est un *ananas*, comme sous-*ananas* de l'*ananas* produit.

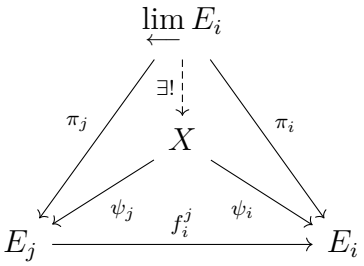
$$\varprojlim E_i = \left\{ (a) \in \prod_{i\in I} E_i \,\middle|\, \forall i \leq j \in I\ f_i^j(a_j) = a_i \right\}$$

La limite projective vérifie la propriété universelle suivante, qui peut également lui servir de définition, pour laquelle elle est unique à unique isomorphisme près.

Proposition 5.2.12. *Soit $I, (E_i)_{i\in I}, (f_i^j)_{i,j\in I}$ un système projectif d'*ananas.

$\varprojlim E_i$ est muni d'une famille de morphismes $\pi_i : \varprojlim E_k \to E_i$ tel que $\pi_i = f_i^j \circ \pi_j$ pour tous $i \leq j \in I$.

De plus, pour tout ananas *X muni d'une famille de morphismes $\psi_i : X \to E_i$ vérifiant $\psi_i = f_i^j \circ \pi_j$ pour tous $i \leq j \in I$, il existe un unique morphisme $u : X \to \varprojlim E_i$ rendant le diagramme suivant commutatif pour tous $i \leq j \in I$.*



L'écriture des éléments de $\mathbb{Z}_p$ sous forme de série nous permet d'avoir la réécriture suivante. Cela correspond simplement à la suite des projections des α_n dans $\mathbb{Z}/p^n\mathbb{Z}$, où les α_n sont définis

dans la preuve.

Proposition 5.2.13.

$$\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z},$$

où les projections sont les projections canoniques $\mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ *pour* $i \leq j \in \mathbb{N}^*$.

La construction algébrique de $\mathbb{Z}_p$ étant effectuée, on récupère $\mathbb{Q}_p$ en passant au corps des fractions.

Proposition 5.2.14. $\mathbb{Q}_p$ *est le corps des fractions de* $\mathbb{Z}_p$, *i.e.*

$$\mathbb{Q}_p \cong Frac\left(\varprojlim \mathbb{Z}/p^n\mathbb{Z}\right).$$

On aurait donc pu tout définir de façon équivalente sous un point de vue algébrique.
En passant à K, on obtient une structure similaire.

Proposition 5.2.15. *Soient* K *un corps de nombres,* $\mathfrak{p}$ *un idéal premier de* $\mathcal{O}_K$, $\pi \in \mathfrak{p}\backslash\mathfrak{p}^2$ *et* R *un système de représentant de* $\mathcal{O}_K/\mathfrak{p}$ *dans* $\mathcal{O}_K$.
On a alors

$$K_\mathfrak{p} = \left\{ \sum_{k\geq n} a_k \pi^k \,\middle|\, n \in \mathbb{Z},\ \forall k \geq n\, a_k \in R,\ a_n \notin \mathfrak{p} \right\} \cong Frac\left(\varprojlim \mathcal{O}_K/\mathfrak{p}^n\right).$$

Démonstration. Pour simplifier les notations, posons ici $p' := p^{\frac{1}{e_\mathfrak{p}}}$, où p est le premier $\mathbb{Z}$ vivant en-dessous de $\mathfrak{p}$ et où $e_\mathfrak{p}$ est le degré de ramification de p en $\mathfrak{p}$. On écrit alors $|\cdot|_\mathfrak{p} := p'^{-v_\mathfrak{p}(\cdot)}$ le représentant de la place $\mathfrak{p}$-adique sur K qui coïncide avec $|\cdot|_p$ sur $\mathbb{Q}$.

On peut faire le même raisonnement que pour $\mathbb{Q}_p$. Nous allons le détailler pour mettre en évidence le fait que tout fonctionne bien ainsi que les propriétés utilisées. Posons $\mathbb{Z}_\mathfrak{p} = \mathcal{O}_{K_\mathfrak{p}}$.

- Remarquons tout d'abord que l'existence de $\pi \in \mathfrak{p}\backslash\mathfrak{p}^2$ est claire : si par l'absurde $\mathfrak{p} = \mathfrak{p}^2$, on peut simplifier par $\mathfrak{p}$ puisque $\mathcal{O}_K$ est de Dedekind, et on en déduit $\mathfrak{p} = \mathcal{O}_K$: contradiction.
- Pour tout $x \in \mathbb{Z}_\mathfrak{p}$ il existe une suite (α_n) d'éléments de $\mathcal{O}_K$ qui converge vers x au sens de $|\cdot|_\mathfrak{p}$ telle que $\forall i \in \mathbb{N}\, \alpha_{i+1} \equiv \alpha_i[\mathfrak{p}^i]$.
  En effet, par densité de K dans $K_\mathfrak{p}$, pour un tel x et pour $n \in \mathbb{N}^*$, on dispose de $q \in K$ tel que $|x-q|_\mathfrak{p} \leq p^{-n}$.
  Comme $|x|_\mathfrak{p} \leq 1$, $|q|_\mathfrak{p} = |x + (q-x)| \leq \max(1, p^{-n}) = 1$, i.e. $v_\mathfrak{p}(q) \geq 0$.
  D'après la proposition 3.2.39, on dispose donc de $s, t \in \mathcal{O}_K$ tels que $t \notin \mathfrak{p}$ et $q = \frac{s}{t}$.
  Comme (t) et $\mathfrak{p}$ sont premiers entre eux, d'après la proposition 3.2.21, one en déduit que (t) et $\mathfrak{p}^n$ sont premiers entre eux.
  Par le lemme de Gauss, on dispose donc de $\alpha_n \in \mathcal{O}_K$ tel que $t\alpha_n - s \in \mathfrak{p}^n$, i.e. $t\alpha_n \equiv s[\mathfrak{p}^n]$.
  Par ailleurs, $tx - s = 0 \in \mathfrak{p}^n$, donc $tx \equiv t\alpha_n[\mathfrak{p}^n]$, d'où $x \equiv \alpha_n[\mathfrak{p}^n]$.
  La suite (α_n) vérifie alors les deux propriétés requises.

- Notons que dans le cas sur $\mathbb{Q}$, on avait $\alpha_n \in [\![0, p^n - 1]\!]$. Il faut donc retrouver ici un analogue de cette propriété, qui correspond à $\alpha_n \in \sum_{k=0}^{n-1} \pi^k R$.
  Fixons a_0 un représentant de α_0 dans R modulo $\mathfrak{p}$.
  Ensuite, pour $n \in \mathbb{N}^*$, on a $\alpha_{n+1} \equiv \alpha_n [\mathfrak{p}^n]$, et on aimerait trouver $a_n \in R$ tel que $a_n \pi^n \equiv \alpha_{n+1} - \alpha_n [\mathfrak{p}^{n+1}]$.
  Comme $R\pi^n \subset \mathfrak{p}^n$, que c'est un ensemble de cardinal fini $|R| = |\mathcal{O}_K/\mathfrak{p}| = |\mathfrak{p}^n/\mathfrak{p}^{n+1}| = p^{f_\mathfrak{p}}$ et que les éléments de R sont tous distincts modulo $\mathfrak{p}$, on a $\overline{R\pi^n} = \mathfrak{p}^n/\mathfrak{p}^{n+1}$ où $\overline{R\pi^n}$ désigne la projection de $R\pi^n$ dans $\mathfrak{p}^n/\mathfrak{p}^{n+1}$.
  Ainsi, il existe bien $a_n \in R$ tel que $a_n \pi^n \equiv \alpha_{n+1} - \alpha_n [\mathfrak{p}^{n+1}]$.
  En posant alors, pour tout $n \in \mathbb{N}^*$,

$$\alpha'_n = \sum_{k=0}^{n-1} a_k \pi^k,$$

  on constate que (α'_n) est une suite d'éléments de $\mathcal{O}_K$ qui converge vers x telle que

$$\forall n \in \mathbb{N}^* \; \alpha'_{n+1} \equiv \alpha'_n [\mathfrak{p}^n] \text{ et } \alpha'_n \in \sum_{k=0}^{n-1} \pi^k R.$$

  En particulier,

$$\sum_{k=0}^{n-1} a_k \pi^k \underset{n\to\infty}{\longrightarrow} x.$$

- L'unicité de la suite (a_k) se fait de la même manière que pour $\mathbb{Q}$. Soit par l'absurde une autre suite (b_k) d'éléments de R tels que

$$\sum_{k=0}^{n-1} b_k \pi^k \underset{n\to\infty}{\to} x.$$

  Soient $n \in \mathbb{N}$ minimal tel que $a_n \neq b_n$, $\alpha'_{n+1} = \sum_{k=0}^{n} a_k \pi^k$ et $\beta'_{n+1} = \sum_{k=0}^{n} b_k \pi^k$.
  On a $|\alpha'_{n+1} - \beta'_{n+1}|_\mathfrak{p} = |(a_n - b_n)\pi^n|_\mathfrak{p} = p'^{-n}$.
  Or, en appliquant l'inégalité ultramétrique et par définition de (a_k) et (b_k),

$$|\alpha'_{n+1} - \beta'_{n+1}|_\mathfrak{p} = |(\alpha'_{n+1} - x) + (x - \beta'_{n+1})|_\mathfrak{p} \leq \max(|\alpha'_{n+1} - x|_\mathfrak{p}, |\beta'_{n+1} - x|_\mathfrak{p}) < p'^{-n},$$

  d'où une contradiction.

- On va maintenant passer à $K_\mathfrak{p}$ tout entier, et plus précisément retrouver l'écriture avec les indices démarrant à $v_\mathfrak{p}(x)$ qu'on annonce dans le lemme.
  Soit $x \in K_\mathfrak{p}$.
  On $v_\mathfrak{p}(\pi^{-v_\mathfrak{p}(x)} x) = 0$. Ainsi, $\pi^{-v_\mathfrak{p}(x)} x \in \mathbb{Z}_\mathfrak{p}$, et on peut lui appliquer le résultat précédant.
  On dispose donc de $(a_k)_{k\geq 0}$ une suite d'éléments de R tels que

$$\pi^{-v_\mathfrak{p}(x)} x = \sum_{k=0}^{\infty} a_k \pi^k.$$

De plus, comme $v_\mathfrak{p}(\pi^{-v_\mathfrak{p}(x)}x) = 0$, on a nécessairement $a_0 \notin \mathfrak{p}$.
Il n'y a plus qu'à multiplier par $\pi^{v_\mathfrak{p}(x)}$ pour translater l'écriture et se ramener à l'énoncé de la proposition.

$$x = \sum_{k=0}^{\infty} a_k \pi^{k+v_\mathfrak{p}(x)},$$

où $a_0 \notin \mathfrak{p}$.

- On retrouve la limite projective en faisant la transformation $(a_n) \longleftrightarrow (\alpha'_n)$.

□

Corollaire 5.2.2 (De la preuve)**.** *Soient K un corps de nombres, $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$, R un système de représentant de $\mathcal{O}_K/\mathfrak{p}$ dans $\mathcal{O}_K$, et $(\pi_m) \in \mathcal{O}_K^{\mathbb{N}}$ telle que pour tout $m \in \mathbb{N}$, $\pi_m \in \mathfrak{p}^m \backslash \mathfrak{p}^{m+1}$, i.e. $v_\mathfrak{p}(\pi_m) = m$.*
On a alors

$$\mathbb{Z}_\mathfrak{p} = \left\{ \sum_{k\geq 0} a_k \pi_k \,\middle|\, \forall k \geq 0\, a_k \in R \right\}.$$

Corollaire 5.2.3. *Soient K un corps de nombres, $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$, R un système de représentant de $\mathcal{O}_K/\mathfrak{p}$ dans $\mathcal{O}_K$, et $(\pi_m) \in K^{\mathbb{Z}}$ telle que pour tout $m \in \mathbb{Z}$, $\pi_m \in \mathfrak{p}^m \backslash \mathfrak{p}^{m+1}$, i.e. $v_\mathfrak{p}(\pi_m) = m$.*
On impose de plus qu'on peut translater pour se ramener à $x \in \mathcal{O}_K$ avec $v_\mathfrak{p}(x) = 0$:

$$\forall m \in \mathbb{Z}\, \exists \Pi_m \in K \left(v_\mathfrak{p}(\Pi_m) = -m \text{ et } \forall m' \geq m\, \pi'_m \Pi_m \in \mathcal{O}_K \right).$$

On a alors

$$K_\mathfrak{p} = \left\{ \sum_{k\geq n} a_k \pi_k \,\middle|\, n \in \mathbb{Z},\, \forall k \geq n\, a_k \in R,\, a_n \notin \mathfrak{p} \right\}.$$

En utilisant cette écriture, on obtient le résultat suivant, utile pour la théorie des hauteurs. Remarquons que le voit apparaître le degré de ramification $e_\mathfrak{p}$ et le degré résiduel (ou d'inertie) $f_\mathfrak{p}$ qui ont été définis dans la sous-partie 3.2.5.

Proposition 5.2.16. *Soient K un corps de nombre et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ vivant au-dessus de $p \in \mathbb{Z}$. Alors,*

$$[K_\mathfrak{p} : \mathbb{Q}_p] = e_\mathfrak{p} f_\mathfrak{p}.$$

Démonstration. Soient R un système de représentants de $\mathcal{O}_K/\mathfrak{p}$ dans $\mathcal{O}_K$, et π tel que $v_\mathfrak{p}(\pi) = 1$.

- **Ramification**

  Pour tout $m \in \mathbb{Z}$ posons $\pi_m = p^q \pi^r$, où q, r sont respectivement le quotient et le reste de la division euclidienne de m par le degré de ramification $e_\mathfrak{p}$.

  Pour $m \in \mathbb{Z}$, on a $v_\mathfrak{p}(\pi_m) = q v_\mathfrak{p}(p) + r v_\mathfrak{p}(\pi) = q e_\mathfrak{p} + r = m$.

  De plus, pour chaque $m \in \mathbb{Z}$, on peut simplement choisir l'élément $\Pi_m = \pi_{-m}$ qui fait bien fonctionner les translations.

  Ainsi, pour tout $x \in K_\mathfrak{p}$, il existe une unique suite $(a_k) \in R^\mathbb{Z}$, dont les termes sont nuls en-dessous d'un certain rang, telle que

$$x = \sum_{k \in \mathbb{Z}} a_k \pi_m.$$

  Remarquons que cela se réécrit, l'absolue convergence des séries étant claire pour $|.|_\mathfrak{p}$,

$$\begin{aligned} x &= \sum_{q \in \mathbb{Z}} \sum_{r=0}^{e_\mathfrak{p}-1} p^q a_{qe_\mathfrak{p}+r} \pi^r \\ &= \sum_{r=0}^{e_\mathfrak{p}-1} \Big(\sum_{q \in \mathbb{Z}} p^q a_{qe_\mathfrak{p}+r} \Big) \pi^r. \end{aligned}$$

- **Degré résiduel**

  On a maintenant presque des nombres p-adique dans la somme interne, mais les $a_{qe_\mathfrak{p}+r}$ ne sont pas dans $[\![0, p-1]\!]$.

  Soient donc $\overline{\epsilon_1}, ..., \overline{\epsilon_{f_\mathfrak{p}}}$ une base de $\mathcal{O}_K/\mathfrak{p}$ en tant que $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel puis $\epsilon_1, ..., \epsilon_{f_\mathfrak{p}}$ des représentants de ces éléments dans $\mathcal{O}_K$.

  Pour tout élément $\alpha \in \mathcal{O}_K/\mathfrak{p}$, on écrit la décomposition de α dans la base $(\overline{\epsilon_j})$ sous la forme $\alpha = \sum_{j=1}^{f_\mathfrak{p}} \alpha^{(j)} \overline{\epsilon_j}$, où les α_j sont dans $[\![0, p-1]\!]$.

  On peut alors définir

$$R' := \Big\{ \sum_{j=1}^{f_\mathfrak{p}} \alpha^{(j)} \epsilon_j \,\Big|\, \alpha \in \mathcal{O}_K/\mathfrak{p} \Big\},$$

  qui est bien sûr un système de représentants de $\mathcal{O}_K/\mathfrak{p}$ dans $\mathcal{O}_K$.

  D'après le point précédent, pour tout $x \in K_\mathfrak{p}$, il existe alors une unique suite $(a_k) \in R'^\mathbb{Z}$, qui est nulle en-dessous d'un certain rang, telle que

$$\begin{aligned} x &= \sum_{r=0}^{e_\mathfrak{p}-1} \Big(\sum_{q \in \mathbb{Z}} p^q a_{qe_\mathfrak{p}+r} \Big) \pi^r \\ &= \sum_{r=0}^{e_\mathfrak{p}-1} \sum_{j=1}^{f_\mathfrak{p}} \Big(\sum_{q \in \mathbb{Z}} p^q a^{(j)}_{qe_\mathfrak{p}+r} \Big) \epsilon_j \pi^r. \end{aligned}$$

  Remarquons que

$$\forall r, j, \ \sum_{q \in \mathbb{Z}} p^q a^{(j)}_{qe_\mathfrak{p}+r} \in \mathbb{Q}_p.$$

On a donc obtenu $(x_r^{(j)}) \in \mathbb{Q}_p^{[\![0,e_\mathfrak{p}-1]\!]\times[\![1,f_\mathfrak{p}]\!]}$ tel que $x = \sum_{r,j} x_r^{(j)} \epsilon_j \pi^r$.
Réciproquement, par construction, pour tout $x \in K_\mathfrak{p}$, il existe une unique écriture $(x_r^{(j)}) \in \mathbb{Q}_p^{[\![0,e_\mathfrak{p}-1]\!]\times[\![1,f_\mathfrak{p}]\!]}$ telle que $x = \sum_{r,j} x_r^{(j)} \epsilon_j \pi^r$.
$(\epsilon_j \pi^r)_{j,r}$ est donc une base de $K_\mathfrak{p}$ en tant $\mathbb{Q}_p$-espace vectoriel :

$$[K_\mathfrak{p} : \mathbb{Q}_p] = e_\mathfrak{p} f_\mathfrak{p}.$$

□

Plus généralement, avec la même démonstration, on pourrait obtenir le résultat suivant.

Proposition 5.2.17. *Soient K, L deux corps de nombres, où L est un sur-corps de K. Soit $\mathfrak{P}$ un idéal premier de $\mathcal{O}_L$ vivant au-dessus de $\mathfrak{p}$, un idéal premier de $\mathcal{O}_K$. Notons ici $e_\mathfrak{P} := v_\mathfrak{P}(\mathfrak{p})$ et $f_\mathfrak{P} := [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$. Alors,*

$$[L_\mathfrak{P} : K_\mathfrak{p}] = e_\mathfrak{P} f_\mathfrak{P}.$$

Avant de passer au bilan de notre classification des places sur un corps de nombre, montrons ce passage de $K_\mathfrak{p}$ à $\mathbb{Q}_p$ sur quelques exemples concrets.

Cela nous permettra de voir à quoi peuvent ressembler les nombres $\mathfrak{p}$-adiques, et comment interviennent les degrés de ramification et résiduels.

Exemple 5.2.3 (Ramification seule)**.** Posons $K = \mathbb{Q}[i]$. On a $\mathcal{O}_K = \mathbb{Z}[i]$.
Soit $p = 2$. En tant qu'idéaux de $\mathcal{O}_K$,

$$(2) = (1+i)^2.$$

Soient donc $\pi = 1 + i$ et $\mathfrak{p} = (\pi)$. On a $e_\mathfrak{p} = 2$ et $f_\mathfrak{p} = 1$.
$R = \{0, 1\}$ est un système de représentants de $\mathcal{O}_K/\mathfrak{p}$ dans $\mathcal{O}_K$.
Soit $x \in K_\mathfrak{p}$. On dispose d'une unique suite $(a_k) \in \{0,1\}^\mathbb{Z}$ dont les termes sont nuls en-dessous d'un certain rang telle que

$$x = \sum_{k\in\mathbb{Z}} a_k \pi^k.$$

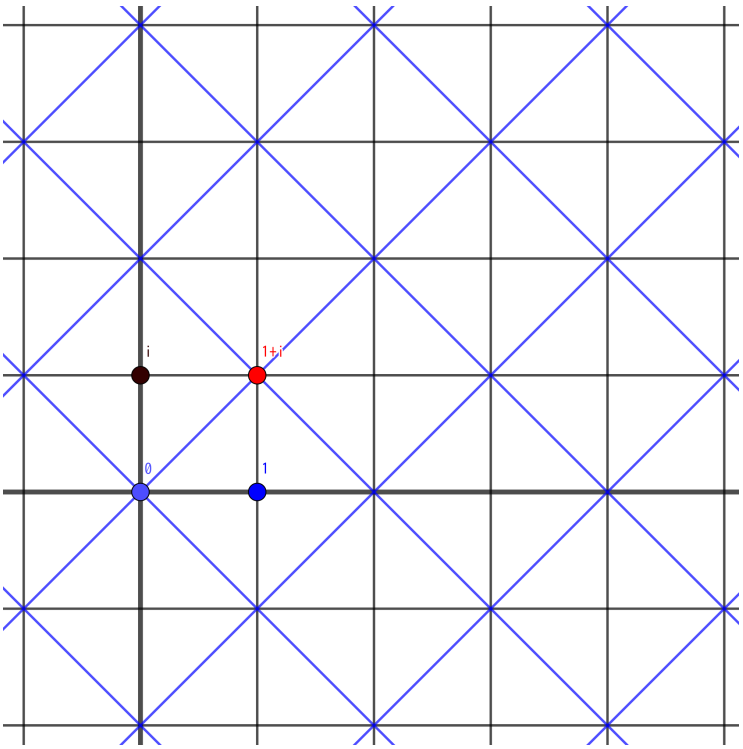
On obtient

$$\begin{aligned} x &= \sum_{q\in\mathbb{Z}} (\pi^2)^q (a_{2q+1}\pi + a_{2q}1) \\ &= \sum_{q\in\mathbb{Z}} (-2i)^q (a_{2q+1}\pi + a_{2q}1) \\ &= \sum_{q\in\mathbb{Z}} 2^q (b_q^{(1)}\pi + b_q^{(0)}1) \\ &= b^{(1)}\pi + b^{(0)}1, \end{aligned}$$

où $(b_q^{(1)})_q, (b_q^{(0)})_q$ sont deux suites à valeurs dans $\{0,1\}$ obtenues en réarrangeant les termes (multiplication globale par $-i$) et où $b^{(1)}, b^{(0)} \in \mathbb{Q}_2$. De plus, une telle écriture est unique.

On retrouve donc bien

$$[K_\mathfrak{p} : \mathbb{Q}_2] = 2 = e_\mathfrak{p} f_\mathfrak{p}.$$



$\mathcal{O}_K$ se trouve à l'intersection des droites noires, $\mathfrak{p}$ à l'intersection des droites bleues. On voit 0 et 1 servant de représentants de $\mathcal{O}_K/\mathfrak{p}$ qui correspond à la cellule élémentaire.

Exemple 5.2.4 (Degré résiduel seul)**.** Posons $K = \mathbb{Q}[\zeta_7]$, où ζ_7 est une racine septième de l'unité. On a $\mathcal{O}_K = \mathbb{Z}[\zeta_7]$.

Soit $p = 2$. On a

$$2\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2,$$

où $\mathfrak{p}_1 = (2, \zeta_7^3 + \zeta_7^2 + 1)$ et $\mathfrak{p}_2 = (2, \zeta_7^3 + \zeta_7 + 1)$ sont deux idéaux premiers distincts de $\mathcal{O}_K$.

Puisque $v_{\mathfrak{p}_1}(2) = 1$, on peut choisir $\pi = 2$. On a de plus $e_{\mathfrak{p}_1} = 1$ et $f_{\mathfrak{p}_1} = 3$.

$R = \{0, 1, \zeta_7, \zeta_7 + 1, \zeta_7^2, \zeta_7^2 + 1, \zeta_7^2 + \zeta_7 + 1\}$ est un système de représentants de $\mathcal{O}_K/\mathfrak{p}_1$ dans $\mathcal{O}_K$. Remarquons qu'on peut voir R sous la forme

$$R = \left\{ \sum_{i=0}^{2} \epsilon_i \zeta_7^i \,\middle|\, \epsilon_0, \epsilon_1, \epsilon_2 \in \{0,1\} \right\}.$$

Soit $x \in K_{\mathfrak{p}_1}$. On dispose d'une unique suite $(a_k) \in R^\mathbb{Z}$ dont les termes sont nuls

en-dessous d'un certain rang telle que

$$x = \sum_{k\in\mathbb{Z}} 2^k a_k.$$

On obtient

$$\begin{aligned} x &= \sum_{k\in\mathbb{Z}} 2^k (a_k^{(2)}\zeta_7^2 + a_k^{(1)}\zeta_7 + a_k^{(0)}1) \\ &= x^{(2)}\zeta_7^2 + x^{(1)}\zeta_7 + x^{(0)}1, \end{aligned}$$

où les $(a_k^{(j)})_k$ sont des suites à valeurs dans $\{0,1\}$ et où $x^{(2)}, x^{(1)}, x^{(0)} \in \mathbb{Q}_2$. De plus, une telle écriture est unique.

On retrouve donc bien

$$[K_{\mathfrak{p}_1} : \mathbb{Q}_2] = 3 = e_{\mathfrak{p}_1} f_{\mathfrak{p}_1}.$$

Exemple 5.2.5 (Ramification et degré résiduel)**.** Posons $K = \mathbb{Q}[\sqrt{\varphi}]$, où $\varphi = \frac{1+\sqrt{5}}{2}$ est le nombre d'or. On peut montrer que $\mathcal{O}_K = \mathbb{Z}[\sqrt{\varphi}]$.

Soit $p = 2$. On a

$$2\mathcal{O}_K = \mathfrak{p}^2,$$

où $\mathfrak{p} = (2, \varphi + \sqrt{\varphi} + 1)$ est un idéal premier de $\mathcal{O}_K$.

Posons $\pi = \varphi + \sqrt{\varphi} + 1$. On a $v_{\mathfrak{p}}(\pi) = 1$, $e_{\mathfrak{p}} = 2$ et $f_{\mathfrak{p}} = 2$.

$R = \{0, 1, \sqrt{\varphi}, \sqrt{\varphi}+1\}$ est un système de représentants de $\mathcal{O}_K/\mathfrak{p}$ dans $\mathcal{O}_K$. Remarquons qu'on peut voir R sous la forme

$$R = \left\{ \sum_{i=0}^{1} \epsilon_i (\sqrt{\varphi})^i \,\middle|\, \epsilon_0, \epsilon_1 \in \{0,1\} \right\}.$$

Soit $x \in K_{\mathfrak{p}}$. On dispose d'une unique suite $(a_k) \in R^{\mathbb{Z}}$ dont les termes sont nuls en-dessous d'un certain rang telle que

$$x = \sum_{k\in\mathbb{Z}} a_k \pi^k.$$

On obtient

$$\begin{aligned} x &= \sum_{q\in\mathbb{Z}} (\pi^2)^q (a_{2q+1}\pi + a_{2q}1) \\ &= \sum_{q\in\mathbb{Z}} (2(\varphi+1)(\sqrt{\varphi}+1))^q (a_{2q+1}\pi + a_{2q}1) \\ &= \sum_{q\in\mathbb{Z}} 2^q (b_q^{(1)}\pi + b_q^{(0)}1) \\ &= \sum_{q\in\mathbb{Z}} 2^q (x_q^{(11)}\sqrt{\varphi}\pi + x_q^{(10)}\pi + x_q^{(01)}\sqrt{\varphi} + x_q^{(00)}1) \\ &= x^{(11)}\sqrt{\varphi}\pi + x^{(10)}\pi + x^{(01)}\sqrt{\varphi} + x^{(00)}1, \end{aligned}$$

où les $(b_q^{(r)})_q$ sont des suites à valeurs dans R obtenues en réarrangeant les termes, les $(x_q^{(r,j)})_q$ sont des suites à valeurs dans $\{0,1\}$ obtenues en décomposants les $b_q^{(r)}$ sur une $\mathbb{Z}/2\mathbb{Z}$-base, et où $x^{(11)}, x^{(10)}, x^{(01)}, x^{(00)} \in \mathbb{Q}_2$. De plus, une telle écriture est unique.

On retrouve donc bien

$$[K_\mathfrak{p} : \mathbb{Q}_2] = 4 = e_\mathfrak{p} f_\mathfrak{p}.$$

5.3 Les théorèmes d'Ostrowski

On peut maintenant faire le bilan de le classification des places obtenue ! C'est le théorème d'Ostrowski.

Nous n'avons pas seulement obtenu la liste $\mathcal{M}_K$ des places d'un corps de nombre. Nous avons également construit des correspondances, qui permettent d'interpréter quelles sont les informations qu'on obtient quand on regarde une de ces places. Ainsi, en un certain sens, les places archimédiennes $\mathcal{M}_K^\infty$ permettent de regarder une partie de l'information algébrique, alors que les places ultramétriques $\mathcal{M}_K^0$ permettent d'observer des phénomènes arithmétiques.

Enfin, puisque classifier les places est la même chose que classifier les complétions, nous avons décrit toutes les complétions des corps de nombres.

- Sur $\mathbb{Q}$, les arguments de 5.1.3 ont permis de classifier les places ultramétriques. Ensuite, un simple argument analytique a permis de donner l'autre moitié du théorème d'Ostrowski, en vérifiant que la seule valeur absolue archimédienne de $\mathbb{Q}$ est la valeur absolue usuelle.
- Pour passer à K, la théorie des complétions a été nécessaire, et a permis d'obtenir à la fois le théorème d'Ostrowski et une meilleure compréhension des complétions de K.
- En ouverture, pour clore ce chapitre, on présentera en 5.3.3 des théorèmes d'Ostrowski au-delà et en dehors des corps de nombres.

5.3.1 • Classification des places sur $\mathbb{Q}$

Théorème 14 (Théorème d'Ostrowski sur $\mathbb{Q}$)**.**

$$\mathcal{M}_{\mathbb{Q}} = \mathcal{M}_{\mathbb{Q}}^0 \sqcup \mathcal{M}_{\mathbb{Q}}^\infty$$
$$\mathcal{M}_{\mathbb{Q}}^0 \longleftrightarrow \mathrm{val}(\mathbb{Q}) \longleftrightarrow \mathrm{Spec}(\mathbb{Z}) = \{0\} \cup \mathcal{P}.$$
$$\mathcal{M}_{\mathbb{Q}}^\infty \longleftrightarrow \{\infty\}$$

5.3.2 • Classification des places sur K

Théorème 15 (Théorème d'Ostrowski sur K)**.**

$$\mathcal{M}_K = \mathcal{M}_K^0 \sqcup \mathcal{M}_K^\infty$$
$$\mathcal{M}_K^0 \longleftrightarrow \mathrm{val}(K) \longleftrightarrow \mathrm{Spec}(\mathcal{O}_K)$$
$$\mathcal{M}_K^\infty \longleftrightarrow \Sigma(K)/\textit{conjugaison complexe.}$$

D'une certaine manière, les places archimédiennes d'un corps semblent donc contenir l'information *algébrique* de ce corps, tandis que les places ultramétriques en contiennent l'information *arithmétique*.

5.3.3 • D'autres Ostrowski

Pour le plaisir, donnons sans démonstration (mais avec références) quelques autres résultats de classification de places sur un corps. La fin de cette peut être sautée, et n'est pas nécessaire à la compréhension de le preuve de l'équation aux S-unités.

Si l'on souhaite se placer en caractéristique $p > 0$, une idée naturelle serait de regarder ce qu'il se passe sur des corps finis $\mathbb{F}_q$. Ce cas n'est cependant pas très intéressant, et vérifier la propriété suivante est un exercice facile.

Proposition 5.3.1. *Soit $\mathbb{F}_q$ un corps fini. La seule place sur $\mathbb{F}_q$ est la place triviale, i.e.*

$$\mathcal{M}_{\mathbb{F}_q}^\infty = \emptyset$$
$$\mathcal{M}_{\mathbb{F}_q}^0 \longleftrightarrow \{0\}$$

Il ne faudrait pas abandonner dès maintenant : il faut considérer des corps infinie pour trouver la richesse de la situation en caractéristique finie.

En fait, il y a beaucoup de similarités entre les *corps de nombres*, extensions finies de $\mathbb{Q}$, et les *corps de fonctions globaux*, c'est à dire les extensions finies du corps $\mathbb{F}_q(t)$ de fractions rationnelles sur $\mathbb{F}_q$. Un dictionnaire présentant quelques-uns de ces parallèles peut être trouvé dans ce cours de Bjorn Poonen [22].

Par exemple, on y trouve des analogies entre $\mathbb{Q}$ et $\mathbb{F}_q(t)$, $\mathbb{Z}$ et $\mathbb{F}_q[t]$, $\mathbb{Q}_p$ et $\mathbb{F}_q((t))$, K et les fonctions rationnelles sur X une $\mathbb{F}_q$-courbe algébrique... On retrouve des classifications des places, un théorème des S-unités de Dirichlet, une formule du produit...

Pour ce qui est des places sur $\mathbb{F}_q(t)$, on obtient le résultat suivant, présenté dans ces notes de Keith Conrad [23].

Proposition 5.3.2. *Soit $\mathbb{F}_q$ un corps fini. et $\mathbb{F}_q(t)$ son corps des fractions rationnelles.*

$$\mathcal{M}^{\infty}_{\mathbb{F}_q(t)} = \emptyset,$$

$$\begin{aligned}\mathcal{M}^{0}_{\mathbb{F}_q(t)} &\longleftrightarrow \mathrm{val}(\mathbb{F}_q(t)) \\ &\longleftrightarrow \mathrm{Spec}(\mathbb{F}_q[t]) \cup \{\deg\} = \{0\} \cup \{\Pi \in \mathbb{F}_q[t] \,|\, \Pi \textit{ irréductible unitaire}\} \cup \{\infty\} \\ &\longleftrightarrow \{0\} \cup \mathbb{P}^1(\mathbb{F}_q),\end{aligned}$$

où $\mathbb{P}^1(\mathbb{F}_q)$ désigne la droite projective sur $\mathbb{F}_q$.
De plus, toute valuation sur $\mathbb{F}_q(t)$ s'annule sur $\mathbb{F}_q$.

Il y a une analogie claire avec le cas sur $\mathbb{Q}$: on a une place triviale, une place à l'infinie, et des irréductibles/premiers.

En fait, le résultat est même plus simple ici ! On peut facilement faire de la géométrie sur $\mathbb{P}^1(\mathbb{F}_q)$, alors que c'est bien compliqué pour $\mathcal{P}$ et $\mathrm{Spec}(\mathcal{O}_K)$: il faudrait aborder la topologie de Zariski... Notons tout de même que de nouvelles difficultés apparaissent du fait de la caractéristique finie.

Sans en dire plus, notons que l'équation aux S-unités est également étudié dans ce cas de caractéristique p, par exemple par José Felipe Voloch dans cet article de 1998 [24].

Plus généralement, pour tout corps de fonctions, on a le résultat suivant.

Proposition 5.3.3. *Soient F un corps (pas nécessairement fini), et $F(t)$ son corps des fractions rationnelles.*

Alors, l'ensemble des valuations ***qui s'annulent sur*** *F est en correspondance avec*

$$\{0\} \cup \{\Pi \in F[t] \,|\, \Pi \textit{ irréductible unitaire}\} \cup \{\infty\}.$$

Dans le cas de $\mathbb{C}$, on retrouve le résultat suivant.

Proposition 5.3.4. *Considérons le corps $\mathbb{C}(t)$ des fractions rationnelles sur $\mathbb{C}$.*

$$\mathcal{M}^{\infty}_{\mathbb{C}(t)} = \emptyset,$$

$$\begin{aligned}\mathcal{M}^0_{\mathbb{C}(t)} &\longleftrightarrow \mathrm{val}(\mathbb{C}(t)) \\ &\longleftrightarrow \mathrm{Spec}(\mathbb{C}[t]) \cup \{\infty\} = \{0\} \cup \mathbb{C} \cup \{\infty\} \\ &\longleftrightarrow \{0\} \cup \mathbb{P}^1(\mathbb{C}),\end{aligned}$$

où $\mathbb{P}^1(\mathbb{C})$ *désigne la droite projective complexe.*

6
HAUTEURS DE NOMBRES

Dans le chapitre précédent, à travers les théorèmes d'Ostrowski et l'étude des complétions, on a obtenu diverses mesures de complexité algébrique et arithmétique sur K, qui s'expriment sous la forme de *places*.

Dans ce chapitre, on va les combiner pour construire la *hauteur* : une mesure globale de la complexité de nombres.

Pour obtenir quelque chose de numérique, il est nécessaire de choisir un système de représentants de ces places. En choisissant bien ce système, on pourra obtenir de bonnes propriétés qui donneront toute sa force à la hauteur.

On veut construire cette hauteur de façon à obtenir des résultats forts de finitude : il faut que les nombres de « faible complexité » soient peu communs. C'est l'énoncé informel du théorème de Northcott, qui est l'aboutissement de cette partie.

- On commence par réaliser dans la partie 6.1 que le système de représentant qu'on a déjà sur $\mathbb{Q}$ a des propriétés remarquables : en particulier, toutes ses valeurs absolues se compensent exactement ! On tirera partie de ce phénomène pour construire la hauteur de $\mathbb{Q}$, puis on en déduira le théorème de finitude de Northcott sur $\mathbb{Q}$.
- Il y a plus de travail à faire dans la partie 6.2 : pour choisir un bon système de représentants de $\mathcal{M}_K$, il faut utiliser les résultats de la théorie des complétions. On construit alors la hauteur sur K puis sur $\overline{\mathbb{Q}}$ tout entier, et on étudie ses propriétés.
- Enfin, ce chapitre se clôt sur la partie 6.3, qui démontre le puissant théorème de Northcott.

Encore une fois, on s'est beaucoup appuyés sur les notes de Mourad Abouzaid intitulées « Hauteurs et équations diophantiennes »[21] pour étudier la hauteur sur les nombres, et de nombreux arguments de ce chapitre en sont issus ou adaptés.

6.1 Le théorème de Northcott sur $\mathbb{Q}$

Cette partie construit la hauteur sur $\mathbb{Q}$ et en déduit un résultat de finitude. Les résultats obtenus ici, sans être surprenants en eux-mêmes, sont très importants : c'est l'intuition de ces phénomènes qu'on va vouloir transposer à K dans le reste de ce chapitre.

- La définition 6.1.1 nous rappelle qu'on a un système de représentants naturels des places de $\mathbb{Q}$: on le notera $M_{\mathbb{Q}}$. Il a de plus des propriétés remarquables : toutes ces valeurs absolues se compensent exactement ! C'est la formule du produit, énoncée à la proposition 6.1.1.
- On pourrait croire que ce phénomène empêche de construire une mesure de complexité globale. Tout au contraire ! C'est ce qui nous permettra d'avoir de bonnes propriétés dans les prochaines parties, et on contourne sans problème l'obstacle : il suffit d'introduire un max, ce qu'on fait en définissant la hauteur de $\mathbb{Q}$ en 6.1.2.

- Enfin, le théorème 16 est le théorème de Northcott sur $\mathbb{Q}$, première pierre du théorème de Northcott qui sera l'aboutissement de ce chapitre.

Rappelons quelles sont les valeurs absolues qu'on a trouvées sur $\mathbb{Q}$.

Définition 6.1.1 (Valeurs absolues standard sur $\mathbb{Q}$)**.** On note $M_{\mathbb{Q}} = \{|\cdot|_x \,|\, x \in \mathcal{P} \cup \{\infty\}\}$ l'ensemble des *valeurs absolues standard sur* $\mathbb{Q}$. Remarquons que pour chaque place de $\mathcal{M}_{\mathbb{Q}}$ (sauf la place triviale), on a choisi un unique représentant.

Pour rappel, $|\cdot|_\infty$ est la valeur absolue usuelle sur $\mathbb{Q}$, et $|\cdot|_p = p^{-v_p(\cdot)}$.

Comme nous le disions, il y a ici un phénomène remarquable : ces valeurs absolues se compensent exactement !

Considérons par exemple $2 \in \mathbb{Q}$: on a $|2|_\infty = 2$, $|2|_2 = 2^{-1}$, et $|2|_p = 1$ sur tous les autres p. Le produit de tout ceci fait exactement 1.

On peut regarder un cas compliqué, par exemple $x = \frac{57}{11}$. On a $|x|_\infty = 11^{-1} \cdot 57$, $|x|_3 = 3^{-1}$, $|x|_{11} = 11$, $|x|_{19} = 19^{-1}$, et $|x|_p = 1$ partout ailleurs. Encore une fois, tout ceci se compense.

Ce phénomène est général, et on lui donne un nom : la *formule du produit*.

Proposition 6.1.1 (Formule du produit)**.** *Soit $x \in \mathbb{Q}^*$. Alors*

$$\prod_{v \in \mathcal{P} \cup \{\infty\}} |x|_v = 1.$$

Démonstration. En effet,

$$\prod_{v \in \mathcal{P} \cup \{\infty\}} |x|_v = |x|_\infty \prod_{p \in \mathcal{P}} |x|_p = \prod_{p \in \mathcal{P}} p^{v_p(x)} \cdot \prod_{p \in \mathcal{P}} p^{-v_p(x)} = 1.$$

□

En ajoutant un max pour éliminer cette compensation, et mesurer malgré tout sur toutes les places, on peut maintenant définir la hauteur sur $\mathbb{Q}$.

Définition 6.1.2 (Hauteur)**.** On appelle *hauteur* sur $\mathbb{Q}$ la fonction

$$H(\cdot) = \prod_{v \in \mathcal{P} \cup \{\infty\}} \max(1, |x|_v).$$

On peut alors calculer facilement la hauteur d'un rationnel, ce qui nous donne immédiatement le théorème de Northcott dans ce cas.

Proposition 6.1.2. *Soit $\frac{a}{b} \in \mathbb{Q}$, où $a \wedge b = 1$. Alors,*

$$H\left(\frac{a}{b}\right) = \max(|a|_\infty, |b|_\infty).$$

Démonstration. On calcule

$$H\left(\frac{a}{b}\right) = \max\left(1, \left|\frac{a}{b}\right|_\infty\right) \prod_{p\in\mathcal{P}} p^{v_p(b)} = \max\left(1, \left|\frac{a}{b}\right|_\infty\right)|b|_\infty = \max(|a|_\infty, |b|_\infty).$$

□

Théorème 16 (Théorème de Northcott sur $\mathbb{Q}$)**.** *Soit $M \in \mathbb{N}$.*

$$\textit{L'ensemble } \left\{x \in \mathbb{Q} \,\middle|\, H(x) \leq M\right\} \textit{ est fini}$$

Démonstration. En effet,

$$\left\{x \in \mathbb{Q} \,\middle|\, H(x) \leq M\right\} = \left\{\frac{a}{b} \,\middle|\, a \in [\![-M, M]\!],\, b \in [\![1, M]\!]\right\},$$

qui est fini. On peut d'ailleurs borner son cardinal par $M(2M+1)$, ou même le calculer à l'aide de l'indicatrice d'Euler φ, et obtenir le résultat asymptotique [25]

$$\left|\left\{x \in \mathbb{Q} \,\middle|\, H(x) \leq M\right\}\right| = 1 + 2\sum_{b=1}^{M} \varphi(b) \underset{M\to\infty}{\sim} \frac{3}{\pi^2} M^2.$$

□

6.2 Mesure de la complexité des nombres

On a maintenant une bonne manière de mesure la complexité des nombres rationnels. À présent l'objectif est d'étendre cette construction, pour obtenir une hauteur sur tout corps de nombre K, puis de rendre cette construction indépendante du corps de nombre choisi.

- Dans la sous-partie 6.2.1, on travaille pour bien choisir un système de représentants de $\mathcal{M}_K$. Il s'agit tout d'abord de retrouver la formule du produit : pour bien choisir nos normalisations, on s'appuie sur la théorie des complétions, étudiée au chapitre précédent.
- Ceci étant fait, on construit la formule sur K dans la sous-partie 6.2.2, et on commence à la manipuler dans la sous-partie 6.2.3, en vérifiant qu'elle a de bonnes propriétés.
- Enfin, dans la sous-partie 6.2.4, on étend la hauteur à $\overline{\mathbb{Q}}$ tout entier, pour obtenir la *hauteur absolue* : c'est le fait de s'être appuyé sur les complétions qui fait fonctionner tout ça.

6.2.1 • La formule du produit

On veut choisir un bon système de représentants de $\mathcal{M}_K$. En particulier, on souhaite retrouver la formule du produit.

La première idée qui vient à l'esprit naturellement est de simplement choisir les valeurs absolues standard de $\mathbb{Q}$. On peut bien faire ceci : rappelons une propriété qui se déduit immédiatement des constructions du chapitre précédent.

Proposition 6.2.1. *Soient K un corps de nombre, L une extension finie de K, et w une place de L.*

Il existe une unique place v sur K correspondant à la restriction de w à K (on travaille ici à équivalence près sur les valeurs absolues).

De plus, pour tout représentant $|\cdot|_v$ de v, il existe une unique représentant $|\cdot|_w$ de w dont la restriction à K soit égale *à $|\cdot|_v$.*

On peut donc définir l'ensemble des *valeurs absolues standard de K*.

Définition 6.2.1. Soit K un corps de nombre.

On note M_K l'unique système de représentants de $\mathcal{M}(K)$ (privé de la place triviale) dont toutes les valeurs absolues sont des extensions d'éléments de $M_{\mathbb{Q}}$, les valeurs absolues standard de $\mathbb{Q}$.

On appelle M_K l'ensemble des *valeurs absolues standard de K*.

On notera M_K^∞ le sous-ensemble de M_K composé des valeurs absolues archimédiennes, et M_K^0 celui composé des valeurs absolues ultramétriques.

On a en fait déjà caractérisé M_K au chapitre précédent ! Insistons sur le fait qu'on voit apparaître un degré de ramification sur les valeurs absolues ultramétriques.

Proposition 6.2.2. *Soit K un corps de nombre. On a*

$$M_K = \left\{ |\cdot|_\sigma \,\middle|\, \sigma \in \Sigma(K)/\textit{conjugaison} \right\} \cup \left\{ |\cdot|_{\mathfrak{p}}^{e_{\mathfrak{p}}} \,\middle|\, \mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K) \right\}.$$

Démonstration. En effet, on a déjà montré que cet ensemble M_K contient un unique représentant de chaque place de $\mathcal{M}_K$, à l'exception de la place triviale.

Il n'y a donc plus qu'à montrer que M_K est bien une extension de $M_{\mathbb{Q}}$.

- **Places archimédiennes**

  Soit $\sigma \in \Sigma(K)$. Comme σ est un morphisme de $\mathbb{Q}$-algèbre de K dans $\mathbb{C}$,

  $$\forall x \in \mathbb{Q}\, |x|_\sigma := \|\sigma(x)\| = \|x\| = |x|_\infty.$$

  $|\cdot|_\sigma$ est donc bien une extension de $|\cdot|_\infty$.

- **Places ultramétriques**
  Soit $\mathfrak{p}$ un idéal premier de K, et $p \in \mathbb{Z}$ le nombre premier au-dessus du quel il vit.
  Remarquons que par définition du degré de ramification,

$$\forall x \in \mathbb{Q}\, v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(p)v_p(x) = e_{\mathfrak{p}}v_p(x).$$

  Ainsi, $\forall x \in \mathbb{Q}\, |x|_p = |x|_{\mathfrak{p}}^{e_{\mathfrak{p}}}$, donc $|\cdot|_{\mathfrak{p}}^{e_{\mathfrak{p}}}$ est une extension de $|\cdot|_p$.

□

Malheureusement, ce système de représentants n'est pas le bon...

Exemple 6.2.1 (Contre-exemple)**.** Calculons ce qu'on obtient en faisant le produit pour $x = 3$.

$$\prod_{|\cdot| \in M_K} |3| = (|3|_\infty)^{|M_K^\infty|} \cdot \prod_{p \in \mathcal{P}} \prod_{\mathfrak{p}|(p)} |3|_p = 3^{|\Sigma_{\mathbb{R}}|+|\Sigma_{\mathbb{C}}|} \cdot 3^{-s_3},$$

où s_3 désigne le nombre de terme apparaissant dans la décomposition canonique de 3 en idéaux premiers. Cela ne se réduit pas à 1 en général.

Si on considère simplement $K = \mathbb{Q}[i]$, on peut voir que $s_3 = 1$: c'est un premier de Gauss. Or, $|\Sigma_{\mathbb{R}}| = 0$ et $|\Sigma_{\mathbb{C}}| = 2$. Dans ce cas,

$$\prod_{|\cdot| \in M_K} |3| = 9 \cdot 3^{-1} = 3 \neq 1.$$

Pour retrouver la formule du produit, il nous faut donc encore introduire des coefficients de normalisation. Ce qui fait tout fonctionner est d'utiliser les $n_v = [K_v : \mathbb{Q}_v]$ qui ont été introduits lors de l'étude des complétions.

On démontre ici qu'on retrouve la formule du produit. On obtiendra dans la sous-partie 6.2.4 une autre conséquence très heureuse de ce choix, qui est en fait la traduction de la propriété 5.2.5.

La preuve de ce résultat s'inspire de celle sur $\mathbb{Q}$, en utilisant de plus la notion de norme d'idéaux introduite au chapitre 3.

Démonstration. Comme pour $\mathbb{Q}$, on sépare sur M_K^∞ et M_K^0.

- **Sur** M_K^∞
  Rappelons que l'on peut écrire $\Sigma(K) = \Sigma_{\mathbb{R}} \sqcup \Sigma_{\mathbb{C}} \sqcup \overline{\Sigma_{\mathbb{C}}}$, où $\Sigma_{\mathbb{R}}$ est l'ensemble des plongements de K dans $\mathbb{R}$.
  Ainsi,

$$\begin{aligned}\prod_{|\cdot|_v \in M_K^\infty} |x|_v^{n_v} &= \prod_{\sigma \in \Sigma_{\mathbb{R}}} \|\sigma(x)\| \cdot \prod_{\sigma \in \Sigma_{\mathbb{C}}} \|\sigma(x)\|^2 = \prod_{\sigma \in \Sigma(K)} \|\sigma(x)\| \\ &= |N_{K/\mathbb{Q}}(x)|_\infty.\end{aligned}$$

- **Sur M_K^0**
  Rappelons que pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$, $n_\mathfrak{p} = e_\mathfrak{p} f_\mathfrak{p}$ d'après la proposition 5.2.16. De plus, $\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}) = p^{f_\mathfrak{p}}$, puisque $\mathcal{O}_K/\mathfrak{p} \cong (\mathbb{Z}/p\mathbb{Z})^{f_\mathfrak{p}}$ en tant qu'espace vectoriel.
  Ainsi,

$$\begin{aligned}\prod_{|\cdot|_v \in M_K^0} |x|_v^{n_v} &= \prod_p \prod_{\mathfrak{p}|p} (p^{f_\mathfrak{p}})^{-v_\mathfrak{p}(x)} = \prod_p \prod_{\mathfrak{p}|p} (\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}))^{-v_\mathfrak{p}(x)} \\ &= \prod_\mathfrak{p} (\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}))^{-v_\mathfrak{p}(x)} = \mathcal{N}_{K/\mathbb{Q}}\Big(\prod_\mathfrak{p} \mathfrak{p}^{-v_\mathfrak{p}(x)}\Big) = \mathcal{N}_{K/\mathbb{Q}}((x)^{-1}) \\ &= |N_{K/\mathbb{Q}}(x)|_\infty^{-1}.\end{aligned}$$

La conclusion est alors immédiate :

$$\prod_{|\cdot|_v \in M_K} |x|_v^{n_v} = |N_{K/\mathbb{Q}}(x)|_\infty \cdot |N_{K/\mathbb{Q}}(x)|_\infty^{-1} = 1.$$

□

6.2.2 • Hauteur sur K

Maintenant qu'on a bon système de représentants, bien normalisés grâce aux n_v de façon à obtenir la formule du produit, on peut définir la hauteur de K, en s'inspirant de la construction déjà effectuée sur $\mathbb{Q}$.

Définition 6.2.2. Soit K un corps de nombres. On pose

$$H_K \ : \left| \begin{array}{ccc} K & \to & \mathbb{R}_+ \\ x & \mapsto & \displaystyle\prod_{|\cdot|_v \in M_K} \max(1, |x|_v)^{n_v}, \end{array} \right.$$

et on appelle H_K la *hauteur sur* K.

Remarquons que cette définition coïncide avec la hauteur sur $\mathbb{Q}$, pour laquelle on avait obtenu que

$$H_\mathbb{Q}\left(\frac{a}{b}\right) = \max(|a|_\infty, |b|_\infty), \text{ où } a \wedge b = 1.$$

Pour simplifier les notations, il est souvent pratique de travailler dans un univers additif, en passant au logarithme.

Définition 6.2.3. Soit K un corps de nombres. On pose $\ln^+(\cdot) := \max(0, \ln(\cdot))$, puis

$$h_K \ : \left| \begin{array}{ccc} K & \to & \mathbb{R} \\ x & \mapsto & \displaystyle\sum_{|\cdot|_v \in M_K} n_v \ln^+ |x|_v, \end{array} \right.$$

et on appelle h_K la *hauteur logarithmique sur* K.

6.2.3 • Manipuler les hauteurs

Étudions maintenant les « bonnes propriétés » de cette hauteur, dont on parle dans le vague depuis le début de ce chapitre.

On va successivement établir les résultats suivants.

(i) Invariance de la hauteur par passage à l'opposé, à l'inverse et conjugaisons. Cela découle de la définition, de la formule du produit, et du théorème d'Ostrowski.

(ii) Inégalités sur les hauteurs de sommes ou de produits : ce sont des propriétés liées aux valeurs absolues et aux degrés des complétions.

(iii) Multiplication globale de la hauteur (logarithmique) lors d'une extension de corps : c'est une conséquence de la propriété 5.2.5 des complétions, qu'on démontre maintenant.

Commençons par les invariances. On l'exprime sur H_K par commodité, mais le résultat est évidemment vrai pour h_K.

Proposition 6.2.3 (Invariances de H_K)**.**
Soient K un corps de nombre, $x \in K$ et $\sigma \in \Sigma(K)$. On a

$$H_K(x) = H_K(-x) = H_K(x^{-1}) = H_K(\sigma(x)).$$

Démonstration. Soient K un corps de nombre et $x \in K$. Rappelons que

$$H_K(x) = \prod_{|\cdot|_v \in M_K} \max(1, |x|_v)^{n_v}.$$

- Comme $\forall |\cdot|_v \in M_K \, |x|_v = |-x|_v$, on a $H_K(x) = H_K(-x)$.
- Le fait $H_K(x) = H_K(x^{-1})$ provient de la formule du produit. En effet,

$$\begin{aligned} H_K(x) = 1^{-1} \cdot \prod_{\substack{|\cdot|_v \in M_K \\ |x|_v > 1}} |x|_v^{n_v} &= \left(\prod_{\substack{|\cdot|_v \in M_K \\ |x|_v \leq 1}} |x|_v^{n_v} \right)^{-1} \\ &= \left(\prod_{\substack{|\cdot|_v \in M_K \\ |x|_v < 1}} |x|_v^{n_v} \right)^{-1} = \prod_{\substack{|\cdot|_v \in M_K \\ |x^{-1}|_v > 1}} |x^{-1}|_v^{n_v} \\ &= H_K(x^{-1}). \end{aligned}$$

- Pour montrer $H_K(x) = H_K(\sigma(x))$, il est suffisant de montrer que

$$\sigma(M_K) := \left\{ |\sigma(\cdot)| \,\middle|\, |\cdot| \in M_K \right\} = M_K.$$

Remarquons tout d'abord que σ induit une bijection entre les deux ensembles de valeurs absolues que sont M_K et $\sigma(M_K)$, puisque qu'on peut inverser avec σ^{-1}.

En passant au quotient par la relation d'équivalence définissant les places, on observe que l'on a de même une bijection entre les places admettant un représentant dans M_K et celles en admettant un dans $\sigma(M_K)$. On a donc deux ensemble de même cardinal fini $|\mathcal{M}_K|$ inclus dans dans $\mathcal{M}_K$: ils sont donc identiques. $\sigma(M_K)$ est donc un système de représentants de $\mathcal{M}_K$.
Comme de plus, pour tout $|\cdot| \in M_K$, $|\sigma(\cdot)|_{|\mathbb{Q}} = |\cdot|_{|\mathbb{Q}} \in M_{\mathbb{Q}}$, $\sigma(M_K)$ est un système de représentants de $\mathcal{M}_K$ qui étend $M_{\mathbb{Q}}$, donc d'après la proposition 6.2.2, on en déduit que $\sigma(M_K) = M_K$.

□

Remarquons au passage que la stabilité par passage à l'inverse nous fournit une méthode alternative pour calculer h_K, en cachant le max.

Proposition 6.2.4. *Soit K un corps de nombres. Pour tout $x \in K$,*

$$h_K(x) = \frac{1}{2} \sum_{|\cdot|_v \in M_K} n_v |\ln(|x|_v)|.$$

Démonstration. Soit $x \in K$.

$$\begin{aligned} 2h_K(x) &= h_K(x) + h_K(x^{-1}) \\ &= \sum_{|\cdot|_v \in M_K} n_v \Big(\max(0, \ln(|x|_v)) + \max(0, -\ln(|x|_v)) \Big) \\ &= \sum_{|\cdot|_v \in M_K} n_v |\ln(|x|_v)|. \end{aligned}$$

□

En plus de ces égalités, on a quelques inégalités utiles pour notre résultat de finitude.
On utilise ici la propriété

$$\sum_{v \in M_K^\infty} n_v = n.$$

Proposition 6.2.5. *Soient $x_1, ..., x_r \in K$. Alors*

- $h_K(\prod_{i=1}^r x_i) \leq \sum_{i=1}^r h_K(x_i)$,
- $h_K(\sum_{i=1}^r x_i) \leq n \ln(r) + \sum_{i=1}^r h_K(x_i)$,

où $n = [K : \mathbb{Q}]$.

Démonstration. On rappelle que pour tout $x \in K$,

$$h_K(x) = \sum_{v \in M_K} n_v \ln^+ |x|_v = \frac{1}{2} \sum_{v \in M_K} n_v \Big| \ln |x|_v \Big|.$$

- En appliquant l'inégalité triangulaire (pour la valeur absolue usuelle $|\cdot|$) et la multiplicativité pour les $|\cdot|_v$, on obtient

$$\begin{aligned} h_K\Big(\prod_{i=1}^r x_i\Big) &= \frac{1}{2}\sum_{v\in M_K} n_v \Big|\ln\Big|\prod_{i=1}^r x_i\Big|_v\Big| = \frac{1}{2}\sum_{v\in M_K} n_v\Big|\sum_{i=1}^r \ln|x_i|_v\Big| \\ &\leq \frac{1}{2}\sum_{v\in M_K} n_v \sum_{i=1}^r \ln|x_i|_v = \sum_{i=1}^r h_K(x_i). \end{aligned}$$

- Pour la somme, remarquons que
  - Si $v\in M_K^0$, d'après l'inégalité ultramétrique,

$$\Big|\sum_{i=1}^r x_i\Big|_v \leq \max_{1\leq i\leq r}|x_i|_v \leq \prod_{i=1}^r \max(1,|x_i|_v).$$

    Ainsi,

$$\ln^+\Big|\sum_{i=1}^r x_i\Big|_v \leq \sum_{i=1}^r \ln^+|x_i|_v.$$

  - Si $v\in M_K^\infty$, on n'a que l'inégalité triangulaire, donc

$$\Big|\sum_{i=1}^r x_i\Big|_v \leq r\max_{1\leq i\leq r}|x_i|_v \leq r\prod_{i=1}^r \max(1,|x_i|_v).$$

    Ainsi,

$$\ln^+\Big|\sum_{i=1}^r x_i\Big|_v \leq \ln(r) + \sum_{i=1}^r \ln^+|x_i|_v.$$

  Grâce à ces inégalités, on obtient

$$\begin{aligned} h_K\Big(\prod_{i=1}^r x_i\Big) &= \sum_{v\in M_K} n_v \ln^+\Big|\prod_{i=1}^r x_i\Big|_v \\ &= \sum_{v\in M_K^0} n_v \ln^+\Big|\prod_{i=1}^r x_i\Big|_v + \sum_{v\in M_K^\infty} n_v \ln^+\Big|\prod_{i=1}^r x_i\Big|_v \\ &\leq \sum_{v\in M_K^0} n_v \sum_{i=1}^r \ln^+|x_i|_v + \sum_{v\in M_K^\infty} n_v\Big(\ln(r) + \sum_{i=1}^r \ln^+|x_i|_v\Big) \\ &= \sum_{i=1}^r h_K(x_i) + \sum_{v\in M_K^\infty} n_v \ln(r) \\ &= \sum_{i=1}^r h_K(x_i) + n\ln(r). \end{aligned}$$

□

Le n obtenu dans l'inégalité sur la somme est quelque peu inélégant... On explique sa présence grâce au fait suivant.

Proposition 6.2.6. *Soient K, L deux corps de nombre, où L est un sur-corps de K. Alors,*

$$\forall x \in K\, h_L(x) = [L : K] h_K(x).$$

C'est une conséquence de la propriété 5.2.5, qu'on rappelle puis démontre maintenant.

Proposition (5.2.5)**.** *Soient K un corps de nombre et L/K une extension finie. Soit v une place de K. Alors*

$$\sum_{w|v} [L_w : \mathbb{Q}_w] = [L : K][K_v : \mathbb{Q}_v],$$

où l'indice w parcourt l'ensemble des places de L qui étendent v.

Démonstration. Séparons le cas ultramétrique et archimédien.

- **Supposons $v \in \mathcal{M}_K^0$.**
  On dispose d'un idéal premier $\mathfrak{p} \subset \mathcal{O}_K$ associé à v.
  D'après la proposition 5.2.17 puis le théorème 11, on sommant sur les idéaux premiers $\mathfrak{P} \subset \mathcal{O}_L$ qui divisent $\mathfrak{p}$,

$$\begin{aligned}\sum_{w|v} [L_w : \mathbb{Q}_w] &= \Big(\sum_{w|v} [L_w : K_w]\Big)[K_w : \mathbb{Q}_w] = \Big(\sum_{w|v} [L_w : K_w]\Big)[K_v : \mathbb{Q}_v] \\ &= \Big(\sum_{\mathfrak{P}|\mathfrak{p}} [L_\mathfrak{P} : K_\mathfrak{p}]\Big)[K_v : \mathbb{Q}_v] = \Big(\sum_{\mathfrak{P}|\mathfrak{p}} e_\mathfrak{P} f_\mathfrak{P}\Big)[K_v : \mathbb{Q}_v] \\ &= [L : K][K_v : \mathbb{Q}_v].\end{aligned}$$

- **Supposons maintenant $v \in \mathcal{M}_K^\infty$.**
  On dispose d'un plongement $\sigma : K \hookrightarrow \mathbb{C}$ associé à v.
  À conjugaison près, les places $w|v$ correspondent aux $\mathbb{Q}$-plongement $\tilde{\sigma} : L \hookrightarrow \mathbb{C}$ qui étendent σ, qui ne sont autres que les K-plongements de $L \hookrightarrow \mathbb{C}$ où $\mathbb{C}$ est muni de la structure de K-algèbre induite par σ.

  - Si σ est un plongement réel, notons r_1 le nombre de K-plongements réels de L dans $\mathbb{C}$, et r_2 le nombre de couples de K-plongements complexes conjugués de L dans $\mathbb{C}$. On obtient

$$\begin{aligned}\sum_{w|v} [L_w : \mathbb{Q}_w] &= \Big(\sum_{w|v} [L_w : K_w]\Big)[K_v : \mathbb{Q}_v] \\ &= (r_1[\mathbb{R} : \mathbb{R}] + r_2[\mathbb{C} : \mathbb{R}])[K_v : \mathbb{Q}_v] = [L : K][K_v : \mathbb{Q}_v].\end{aligned}$$

  - Sinon, il y a $[L : K]$ K-plongements de L dans $\mathbb{C}$. Comme $\sigma \neq \overline{\sigma}$ et que ces $\tilde{\sigma}$ étendent σ, il n'y a ici aucun couple de morphismes conjugués au sens complexe.

Ainsi, dans ce cas également,

$$\begin{aligned}\sum_{w|v}[L_w:\mathbb{Q}_w] &= \Big(\sum_{w|v}[L_w:K_w]\Big)[K_v:\mathbb{Q}_v] \\ &= [L:K][\mathbb{C}:\mathbb{C}][K_v:\mathbb{Q}_v] = [L:K][K_v:\mathbb{Q}_v].\end{aligned}$$

□

On en déduit le lien entre les deux hauteurs logarithmiques.

Démonstration de la propriété 6.2.6. Soit $x \in K$. On a

$$\begin{aligned}h_L(x) &= \sum_{|\cdot|_w \in M_L} n_w \ln^+ |x|_w = \sum_{|\cdot|_v \in M_K} \sum_{w|v} n_w \ln^+ |x|_w \\ &= \sum_{|\cdot|_v \in M_K} \Big(\ln^+ |x|_v \sum_{w|v} n_w\Big) = \sum_{|\cdot|_v \in M_K} [L:K] n_v \ln^+ |x|_v \\ &= [L:K] h_K(x).\end{aligned}$$

□

6.2.4 • Hauteur absolue

Comme on aurait pu le voir sur un exemple, la hauteur d'un nombre algébrique, telle qu'on l'a définie, dépend du corps ambiant.

En revanche, on a montré qu'elle le faisait de façon très régulière : cela nous invite à définir la hauteur de façon indépendante du corps sous-jacent.

Définition 6.2.4 (Hauteur absolue)**.** On définit la *hauteur absolue* h par

$$h \ : \left| \begin{array}{ccc} \overline{\mathbb{Q}} & \to & \mathbb{R} \\ x & \mapsto & \dfrac{h_{\mathbb{Q}[x]}(x)}{[\mathbb{Q}[x]:\mathbb{Q}]}. \end{array} \right.$$

Cette définition est une généralisation de la hauteur logarithmique sur un corps de nombre, au sens suivant.

Proposition 6.2.7. *Soit K un corps de nombre. Alors, pour tout $x \in K$,*

$$h(x) = \frac{h_K(x)}{[K:\mathbb{Q}]}.$$

Démonstration. Puisque $x \in K$, K est un sur-corps de $\mathbb{Q}[x]$, donc

$$\begin{aligned}\frac{h_K(x)}{[K:\mathbb{Q}]} &= \frac{[K:\mathbb{Q}[x]] \cdot h_{\mathbb{Q}[x]}(x)}{[K:\mathbb{Q}[x]] \cdot [\mathbb{Q}[x]:\mathbb{Q}]} \\ &= \frac{h_{\mathbb{Q}[x]}(x)}{[\mathbb{Q}[x]:\mathbb{Q}]} = h(x).\end{aligned}$$

□

Pour certaines manipulations, on pourra utiliser la hauteur absolue sous forme non-logarithmique.

Définition 6.2.5 (Hauteur absolue non-logarithmique)**.** On définit la *hauteur absolue non logarithmique* H en passant h à l'exponentielle. Autrement dit

$$\begin{array}{rcl|ll} H & : & \overline{\mathbb{Q}} & \to & \mathbb{R}_+ \\ & & x & \mapsto & \displaystyle\prod_{v\in M_K} \max\left(1, |x|_v\right)^{\frac{n_v}{n}}, \end{array}$$

où K est un corps de nombre contenant x, M_K l'ensemble de ses valeurs absolues standard, $n = [K:\mathbb{Q}]$ et $n_v = [K_v:\mathbb{Q}_v]$.

On peut vérifier que les invariances et inégalité obtenues pour H_K et h_K se traduisent bien sur H et h. De plus, on est s'est maintenant libéré du degré $[K:\mathbb{Q}]$.

6.3 Théorème de Northcott

On a maintenant tous les ingrédients pour démontrer le théorème de Northcott, non seulement sur K, mais sur $\overline{\mathbb{Q}}$ tout entier.

C'est l'aboutissement de ce chapitre : h est une excellente mesure de la complexité des nombres, qui se manipule bien, et qui permet de plus de montrer des résultats de finitude.

Théorème 17 (Théorème de Northcott sur $\overline{\mathbb{Q}}$)**.** *Soient $M, D \geq 0$.*

$$\{x \in \overline{\mathbb{Q}} \mid \deg \mu_x \leq D,\ h(x) \leq M\} \quad \textit{est fini.}$$

Démonstration. En effet, soient $M, D \geq 0$. Soit $x \in \overline{\mathbb{Q}}$ tel que $\deg \mu_x \leq D$, $h(x) \leq M$.

D'après la propriété 6.2.3, la hauteur de tout $\mathbb{Q}$-conjugué de x est bornée par M.

Or, les coefficients de $\mu_x \in \mathbb{Q}[X]$ s'expriment en une fonction polynomiale en les $\mathbb{Q}$-conjugués de x, donc d'après la propriété 6.2.5, ces coefficients ont une hauteur bornée.

D'après le théorème de Northcott sur $\mathbb{Q}$ appliqué à ces coefficients, on en déduit la finitude de

$$\{\mu_x \in \mathbb{Q}[X] \mid x \in \overline{\mathbb{Q}},\ \deg \mu_x \leq D,\ h(x) \leq M\}.$$

Comme ces polynômes ont au plus D racines, l'ensemble de l'union de leurs racines est bien fini. Cet ensemble n'est autre que

$$\{x \in \overline{\mathbb{Q}} \mid \deg \mu_x \leq D,\ h(x) \leq M\}.$$

□

On obtient immédiatement le corollaire suivant en se restreignant à un corps de nombre K, puisque $[K : \mathbb{Q}] < \infty$.

Corollaire 6.3.1 (Théorème de Northcott sur K)**.**
Soient K un corps de nombres et $M > 0$.

$$\textit{L'ensemble } \left\{x \in K \,\middle|\, h(x) \leq M\right\} \textit{ est fini.}$$

7
RAPPELS PRÉLIMINAIRES À LA PREUVE

Les éléments de la preuve commencent à s'accumuler. On reconnaît les idées clés qui la composent, notamment la structure de $\mathcal{O}_{K,S}^{\times}$ comme réseau et la notion de hauteur qui mesure la complexité des nombres. Cependant, quelques outils mathématiques supplémentaires sont nécessaires pour faire le lien entre ces idées. L'exploration de ces outils nous amène à exposer de nouveaux concepts mathématiques.

- L'analyse complexe. C'est un domaine fondé sur l'étude des "fonctions polynomiales de degré infini" à une variable complexe. L'étude de ces fonctions nous permet de quantifier de façon assez fidèle la complexité de nombres à partir de certaines propriétés facilement accessibles.
- L'extension des scalaires. Comme son nom l'indique, cette technique étend les scalaires qui ont une action sur notre structure (un module ou un espace vectoriel). En effet, souvent, manipuler des espaces continus (l'ensemble des scalaires contient $\mathbb{R}$) permet d'avoir plus de résultats que de manipuler des espaces discrets. C'est pour cela qu'on va être amené à transformer $\mathcal{O}_{K,S}^{\times}$ d'un $\mathbb{Z}$-module à un espace vectoriel réel

7.1 Des notions d'analyse complexe

L'analyse complexe est un domaine étendu des mathématiques. En s'y plongeant, on se retrouve rapidement à faire du calcul différentiel sur des variétés et des formes géométriques assez complexes. Certains résultats d'analyse complexe vont nous être utile pour mettre en avant les propriétés qu'on veut obtenir sur les hauteurs. On va également être amenés à manipuler des fonctions pour optimiser les inégalités escomptées. Et c'est le caractère *holomorphe* de ces fonctions qui va nous être très utile. Ce caractère sera par exemple la clé permettant l'usage du puissant principe du maximum 7.1.17. Nous introduisons donc d'abord quelques notions élémentaires d'analyse complexe sans donner les preuves pour ne pas alourdir le document.
Nous démontrons ensuite le théorème de Puiseux. Ce théorème garantit la clôture algébrique du corps de fractions des séries entières de Puiseux. Les séries entières de Puiseux sont des séries entières où l'on a ajouté les racines n-éme de z. Nous nous appuyons sur le livre de cours d'Analyse complexe de deuxième année de l'école Polytechnique [26], ainsi que sur un article écrit par J.N.Krzysztof où il démontre le théorème de Puiseux [27].

7.1.1 • Fonctions holomorphes

On commence par définir les fonction holomorphes et énoncer les propriétés de la dérivation sur $\mathbb{C}$. Ces propriétés ressemblent fortement à la dérivation réelle et le lecteur peut donc survoler le début de cette partie s'il est familier avec ces notions.

Définition 7.1.1 (ℂ-dérivabilité)**.** Soient Ω un ouvert de $\mathbb{C}$ et f une fonction complexe continue de Ω vers $\mathbb{C}$. On dit que f est $\mathbb{C}$-dérivable en $z \in \mathbb{C}$ si la limite suivante existe :

$$\lim_{w \to 0} \frac{f(z+w) - f(z)}{w}.$$

Si c'est le cas, on note $f'(z)$ cette limite, et on l'appelle la *dérivée au sens complexe* de f au point z.

Définition 7.1.2 (Fonction holomorphe)**.** Soient Ω un ouvert de $\mathbb{C}$ et f une fonction complexe continue de Ω vers $\mathbb{C}$. On dit que f est *holomorphe* si elle est $\mathbb{C}$-dérivable en tout point de Ω et si sa dérivée est une fonction continue. On note $\mathrm{Hol}(\Omega)$ l'espace vectoriel (sur $\mathbb{C}$) des fonctions holomorphes sur Ω.

Définition 7.1.3 (Différentiabilité)**.** Soient $n, p \in \mathbb{N}$, f une fonction d'un ouvert U de $\mathbb{R}^n$ à valeurs dans $\mathbb{R}^p$ et a un point de U. On dit que f est *différentiable* en a s'il existe $L : \mathbb{R}^n \to \mathbb{R}^p$ linéaire telle que

$$f(a+h) = f(a) + L(h) + o(\|h\|).$$

L'application L, si elle existe, est unique et s'appelle *différentielle* de f en a. On la note df_a.

Notons que le choix de la norme n'est pas important puisque toute les normes sont équivalentes sur un $\mathbb{R}$-espace vectoriel de dimensions finie.

Vous pouvez peut-être déjà le voir, lorsque $n = p = 2$, les notions de $\mathbb{C}$-dérivabilité et de différentiabilité sont reliées.

Identifions $\mathbb{C}$ à $\mathbb{R}^2$ par l'application $p : z \mapsto (x, y)$ où $z = x + iy$. Ainsi, une fonction $f : \Omega \to \mathbb{C}$ peut être vue comme une fonction d'un ouvert Ω de $\mathbb{R}^2$ à valeurs dans $\mathbb{R}^2$. Au lieu de voir df_a comme une application linéaire de $\mathbb{R}^2$ on peut la voir comme une application $\mathbb{R}$-linéaire de $\mathbb{C}$. C'est à dire que pour $z = x + iy$, $df_z(w) = df_{(x,y)}((x_w, y_w))$.

Proposition 7.1.1. *Soit f une fonction d'un ouvert Ω de $\mathbb{C}$ (ou de $\mathbb{R}^2$) à valeurs dans $\mathbb{C}$ (ou $\mathbb{R}^2$). Alors les assertions suivantes sont équivalentes.*

(i) f est différentiable au point z et df_z est $\mathbb{C}$-linéaire.

(ii) f est $\mathbb{C}$-dérivable en z.

Démonstration.

Supposons que f est différentiable au point z et df_z est $\mathbb{C}$-linéaire. Par définition de la différentiabilité et après identification de $\mathbb{R}^2$ avec $\mathbb{C}$, $|f(z+w) - f(z) - df_z(w)| = o(|w|)$. Or,

puisque df_z est $\mathbb{C}$-linéaire on peut diviser par w et obtenir

$$\left|\frac{f(z+w)-f(z)}{w} - df_z(1)\right| = o\left(\frac{|w|}{w}\right) = o(1),$$

donc f est $\mathbb{C}$-dérivable en z.

Supposons maintenant que f est $\mathbb{C}$-dérivable en z, et soit $L : z \mapsto \lambda z$ avec $\lambda = f'(z)$ une fonction $\mathbb{C}$-linéaire de Ω dans $\mathbb{C}$. On vérifie facilement que $|f(z+w) - f(z) - \lambda w| = o(|w|)$, donc f est différentiable au point z et df_z est $\mathbb{C}$-linéaire. □

Définition 7.1.4 (Opérateurs différentiels)**.** On définit les opérateurs différentiels

$$\frac{\partial}{\partial z} = \frac{1}{2}\left(\frac{\partial}{\partial x} - i\frac{\partial}{\partial y}\right) \quad \text{et} \quad \frac{\partial}{\partial \overline{z}} = \frac{1}{2}\left(\frac{\partial}{\partial x} + i\frac{\partial}{\partial y}\right).$$

Proposition 7.1.2 (Conditions de Cauchy réelles)**.** *Soit f une fonction d'un ouvert Ω de $\mathbb{C}$ (ou de $\mathbb{R}^2$) à valeurs dans $\mathbb{C}$. Supposons en plus qu'elle soit différentiable. Alors f est $\mathbb{C}$-dérivable en z si et seulement si $\frac{\partial f}{\partial z}(z) = 0$. Dans ce cas on a $f'(z) = \frac{\partial f}{\partial \overline{z}}(z)$.*

Démonstration. $df_{(x,y)}$ est une application linéaire de $\mathbb{R}^2$ vers $\mathbb{R}^2$. Écrivons sa matrice :

$$\begin{pmatrix} \frac{\partial f_1}{\partial x} & \frac{\partial f_1}{\partial y} \\ \frac{\partial f_2}{\partial x} & \frac{\partial f_2}{\partial y} \end{pmatrix}.$$

Or, d'après la proposition 7.1.1, f est $\mathbb{C}$-dérivable en z si et seulement si cette matrice est la matrice d'une multiplication par un nombre complexe qu'on note $\alpha + i\beta$, c'est-à-dire si et seulement si la matrice en question s'écrit $\begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$, ce qui revient à notre condition sur $\frac{\partial f}{\partial z}(z)$.

De plus, dans le cas où ces propriétés sont vérifiées, on a $\frac{\partial f}{\partial \overline{z}}(z) = \alpha + i\beta = f'(z)$. □

Écrivons maintenant quelques propriétés sur les dérivées complexes en utilisant ces opérateurs.

Proposition 7.1.3. *Soient f, g deux fonctions de classe C^1 comme fonctions de deux variables réelles. Alors,*

$$\frac{\overline{\partial f}}{\partial z} = \frac{\partial \overline{f}}{\partial \overline{z}}, \qquad \frac{\partial(f+g)}{\partial z} = \frac{\partial f}{\partial z} + \frac{\partial g}{\partial z},$$
$$\frac{\partial(fg)}{\partial z} = \frac{\partial f}{\partial z}g + f\frac{\partial g}{\partial z}, \qquad \frac{\partial(1/f)}{\partial z} = -\frac{1}{f^2}\frac{\partial f}{\partial z}.$$

Démonstration. Ces propriétés s'obtiennent par linéarité et en utilisant les propriétés équivalentes avec les dérivées partielles réelles. □

Proposition 7.1.4 (Dérivée de la composée)**.** *Avec les mêmes notations (et des ensembles de départ qui permettent la composition) on a*

$$\frac{\partial(f\circ g)}{\partial z} = \left(\frac{\partial f}{z}\circ g\right)(z)\times\frac{\partial g}{\partial z}(z) + \left(\frac{\partial f}{\overline{z}}\circ g\right)(z)\times\frac{\partial \overline{g}}{\partial z}(z).$$

Démonstration. Il suffit d'écrire $f\circ g = \tilde{f}\left(\frac{g+\overline{g}}{2}, \frac{g-\overline{g}}{2i}\right)$ et d'appliquer les dérivées partielles en x et en y pour recomposer les opérateurs de la définition 7.1.4. □

Cela nous permet de construire de nouvelles fonctions holomorphes.

Proposition 7.1.5. *Les combinaisons linéaires et produits de fonctions holomorphes sur un même ouvert donnent des fonctions holomorphes.*

De plus si f est holomorphe *alors $1/f$ est* holomorphe *sur l'ouvert où f ne s'annule pas.*

Enfin, les composées de fonctions holomorphes sont égalements holomorphes.

On va maintenant définir une certaine classe de fonctions *holomorphe*. C'est les séries entières. On va voir ensuite une généralisation de cette classe dans ce qu'on appelle fonction *analytique*. Et on va voir que les notions de fonctions *analytique* et *holomorphe* sont équivalentes.

Proposition 7.1.6 (Classe de fonctions holomorphes particulière)**.** *Une série entière*

$$f(z) = \sum_{n\geq 0} a_n z^n$$

à coefficients complexes, de rayon de convergence $R>0$ définit une fonction holomorphe *sur son disque ouvert de convergence admet des dérivées complexes données par la formule*

$$f^{(k)}(z) = \sum_{n\geq k} n(n-1)\cdots(n-k+1)a_n z^{n-k}.$$

Démonstration. On rappelle que le rayon de convergence R d'une série entière $f(z)=\sum_{n\geq 0} a_n z^n$ est le sup des $\rho\geq 0$ tels que la série est normalement convergente sur le disque fermé de rayon ρ. C'est aussi le sup des ρ tels que la suite $(|a_n|\rho^n)_{n\geq 0}$ est bornée. On en déduit donc facilement que la série $\sum_{n\geq 1} n a_n z^{n-1}$ a le même rayon de convergence que f. On a donc le droit de faire le calcul pour arriver à notre résultat. Il faut vérifier que f' comme on l'a définie garantit bien une limite nulle à $|\frac{f(z+w)-f(z)}{w} - f'(z)|$. Le raisonnement pour $k\in\mathbb{N}$ quelconque ne diffère pas beaucoup. □

Définition 7.1.5 (Fonction biholomorphe)**.** Une fonction *holomorphe*$h:\Omega_1\to\Omega_2$ est dite biholomorphe si h est une bijection dont la réciproque h^{-1} est *holomorphe* sur Ω_2.

Proposition 7.1.7 (Corollaire du theorème d'inversion locale)**.** *Soient $f \in Hol(\Omega)$ et $z_0 \in \Omega$ tels que $f'(z_0) \neq 0$. Alors, il existe un ouvert $\Omega_1 \subset \Omega$ contenant z_0 tel que :*

- *Le sous ensemble $\Omega_2 = f(\Omega_1)$ est un ouvert de $\mathbb{C}$,*
- *La restriction de f à Ω_1 est une application biholomorphe de Ω_1 sur Ω_2.*

Pour continuer à explorer les fonctions holomorphes, il faut que nous introduisons un outil très souvent sollicité en analyse complexe : l'intégrale sur un chemin donné.

Définition 7.1.6 (Chemin)**.** Soit Ω un ouvert non vide de $\mathbb{C}$. Un chemin γ (orienté) de Ω est une application continue de classe C^1 par morceaux

$$\gamma : [a, b] \to \Omega,$$

où $a < b$.

On appelle $\gamma^{\text{opp}}(t) := \gamma(a + b - t)$ le chemin opposé de γ.

Si de plus $\gamma(a) = \gamma(b)$, on dira que γ est un *lacet*.

On suppose évidemment que γ admet des dérivées à droite et à gauche en tout point de discontinuité. En particulier, cette dérivée reste bornée.

Définition 7.1.7 (Intégrale sur un chemin)**.** Si $f : \Omega \to \mathbb{C}$ est une fonction continue et si $\gamma : [a, b] \to \Omega$ est un chemin, on définit l'intégrale de f le long du chemin γ par la formule

$$\int_\gamma f(z)dz := \int_a^b f(\gamma(t))\gamma'(t)dt.$$

L'intégrale est bien définie puisque γ' reste borné (car γ admet des dérivées à droite et à gauche).

On va énoncer quelques propriétés naturelles sur l'intégration le long d'un chemin. Les démonstrations de ces propriétés sont immédiates et ne seront pas détaillées.

Proposition 7.1.8. *Soient f une fonction définie sur Ω, $\gamma : [a, b] \to \Omega$ un chemin et $\phi : [a', b'] \to [a, b]$ un C^1-difféomorphisme croissant. Alors, en notant $\tilde{\gamma} = \gamma \circ \phi$,*

$$\int_\gamma f(z)dz = \int_{\tilde{\gamma}} f(z)dz.$$

Proposition 7.1.9. *Soient f une fonction définie sur Ω et $\gamma : [a, b] \to \Omega$ un chemin.*

Alors,

$$\int_\gamma f(z)dz = -\int_{\gamma^{opp}} f(z)dz.$$

Définition 7.1.8 (Chemins composables)**.** Soient $\gamma_1 : [a_1, b_1] \to \Omega$ et $\gamma_2 : [a_2, b_2] \to \Omega$ deux chemins. On dit qu'ils sont composables si $\gamma_1(b_1) = \gamma_2(a_2)$.

On appelle alors chemin composé, qu'on note $\gamma_1 \vee \gamma_2 : [a_1, b_1 + b_2 - a_2] \to \Omega$, le chemin défini par $\gamma_1(t)$ pour $t \in [a_1, b_1]$ et par $\gamma_2(t + a_2 - b_1)$ sinon.

Proposition 7.1.10.

Soient f une fonction définie sur Ω et $\gamma_1 : [a_1, b_1] \to \Omega$, $\gamma_2 : [a_2, b_2] \to \Omega$ deux chemins composables. Alors,

$$\int_{\gamma_1 \vee \gamma_2} f(z)dz = \int_{\gamma_1} f(z)dz + \int_{\gamma_2} f(z)dz.$$

Proposition 7.1.11. *Soient $f \in \mathrm{Hol}(\Omega)$ et $\gamma : [a, b] \to \Omega$ un chemin. On suppose que f admet une primitive* holomorphe *F sur Ω. Alors,*

$$\int_\gamma f(z)dz = F(\gamma(b)) - F(\gamma(a)).$$

En particulier, si γ est un lacet alors l'intégrale sera nulle.

On arrive maintenant à une propriété importante : la formule intégrale de Cauchy. On peut voir dans le résultat une forme de rigidité des fonctions *holomorphes*. En effet, la valeur de cette fonction sur un cercle autour d'un point donné permet de fixer sa valeur en ce point.

Proposition 7.1.12 (Formule Intégrale de Cauchy)**.** *Soient $z_0 \in \Omega$ et $r > 0$. On suppose que $\overline{D}(z_0, r) \subset \Omega$ et l'on note $\Gamma := C(z_0, r)$ le bord de ce disque (que l'on suppose orienté positivement). Soit $f \in \mathrm{Hol}(\Omega)$. Alors, pour tout $z \in D(z_0, r)$,*

$$f(z) = \frac{1}{2i\pi} \int_\Gamma \frac{f(w)}{w - z} dw.$$

Donnons à présent une nouvelle description des fonctions holomorphes, qui illustre leur rigidité, à l'origine de la force de l'analyse complexe : sur $\mathbb{C}$, « être dérivable » est identique à « être développable en série entière et donc C^∞ ».

Définition 7.1.9 (Fonction analytique)**.** Une fonction est dite *analytique* sur Ω si, pour tout $z_0 \in \Omega$, la fonction f admet un développement en série entière de la forme

$$f(z) = \sum_{n \geq 0} a_n (z - z_0)^n$$

qui est convergente dans un voisinage de z_0.

Proposition 7.1.13 (Analytique vs. Holomorphe)**.**
Une fonction est holomorphe *sur Ω si et seulement si elle est analytique sur Ω.*

Démonstration. Une preuve de ce résultat peut être trouvée dans la page 110 du livre [26]. □

En nous aidant de cette nouvelle vision des fonction holomorphes, on va montrer une autre de leurs propriétés.

Proposition 7.1.14 (Principe des zéros isolés)**.** *Soit Ω un ouvert connexe et f une fonction* holomorphe *sur Ω non identiquement nulle. Alors, les zéros de f sont isolés.*
Autrement dit, si $f(z_0) = 0$, il existe $\epsilon > 0$ tel que $\forall z \in \Omega \cap (D(z_0, \epsilon) \setminus \{z_0\}), f(z) \neq 0$.

Un résultat qui découle directement de ce principe est le principe de prolongement analytique.

Proposition 7.1.15 (Principe du prolongement analytique)**.** *Deux fonctions holomorphes, définies sur un ouvert connexe et qui coïncident sur un ouvert ou sur un arc non constant sont égales.*

On a désormais tous les outils pour démontrer le principe du maximum et la formule de la moyenne sur les fonctions holomorphes.

Proposition 7.1.16 (Formule de la moyenne)**.** *Soient f une fonction* holomorphe *sur un ouvert Ω et $\overline{D}(z, r)$ un disque fermé contenu dans Ω, avec $r > 0$. Alors,*

$$f(z) = \frac{1}{2\pi} \int_0^{2\pi} f(z + re^{i\theta}) d\theta.$$

Démonstration. Grâce à la formule intégrale de Cauchy 7.1.12, en posant $w = z + re^{i\theta}$, on obtient

$$f(z) = \frac{1}{2\pi} \int_{C(z,r)} \frac{f(w)}{w - z} dw = \frac{1}{2\pi} \int_0^{2\pi} f(z + re^{i\theta}) d\theta.$$

□

Proposition 7.1.17 (Principe du maximum)**.** *Soit f une fonction* holomorphe *sur un ouvert Ω. Si $z \mapsto |f(z)|$ admet un maximum local en $z_0 \in \Omega$, alors f est constante sur Ω.*

Démonstration. Supposons que $|f|$ ait un maximum local en $z_0 \in \Omega$, i.e qu'il existe un disque fermé $\overline{D}(z_0, r) \subset \Omega$ tel que $|f(z)| \leq |f(z_0|$ pour tout $z \in \overline{D}(z_0, r)$. On va montrer qu'il existe un voisinage de z_0, où f est constante. L'ouvert Ω étant connexe, le principe du prolongement analytique nous dit alors que f est constante sur Ω.
La fonction f est développable en série entière au voisonage de z_0 et l'on peut écrire

$$f(z) = f(z_0) + \sum_{n \geq 1} a_n (z - z_0)^n$$

On suppose que f n'est pas constante au voisinage de z_0, donc il existe au moins un $a_n \neq 0$. Soit N le plus petit entier non nul tel que $a_n \neq 0$. Écrivons

$$f(z) = f(z_0) + (z - z_0)^N \sum_{n \geq N} a_n (z - z_0)^{n-N}$$

On note $g(z) = \sum_{n \geq N} a_n (z - z_0)^{n-N}$ et l'on développe

$$\begin{aligned} |f(z)|^2 &= |f(z_0) + (z - z_0)^N g(z)|^2 \\ &= |f(z_0)|^2 + 2\mathbb{R}\Big((z - z_0)^N g(z)\overline{f(z_0)}\Big) + |z - z_0|^{2N}|g(z)|^2 \end{aligned}$$

Ensuite on fixe $z = z_0 + te^{i\beta}$ où $t, \beta \in \mathbb{R}$. On ne détaille pas la suite de la preuve qui ne présente pas de difficulté particulière : on cherche β et t tel que $|f(z)| > |f(z_0)|$, ce qui donne une contradiction, et donc le résultat voulu. □

7.1.2 • Théorème de Puiseux.

Dans cette sous-partie, nous démontrons un résultat d'algèbre sur les polynômes à coefficients dans le corps de fractions de l'anneau des séries entières. C'est le théorème de Puiseux. Le corps de fractions des séries entières n'est pas algébriquement clos, mais il le devient en rajoutant les racines n-iémes de z pour tout entier n. C'est ce qu'on appelle le corps de fractions des séries entières de Puiseux. Clarifions notre description de ce théorème avant de se lancer dans l'écriture de l'énoncé : tout polynôme à coefficients dans le corps de fractions de l'anneau des séries entières de Puiseux est produit de polynômes de degré 1 à coefficients dans ce même corps.

Définition 7.1.10 (Série entière de Puiseux)**.** Soit $f(z)$ une série entière, on appelle série entière de Puiseux toute série qui s'écrit sous la forme $f(z^{1/r})$ pour $r \in \mathbb{N}^*$.

Exemple 7.1.1. $r \in \mathbb{N}^*$, $(a_k)_{k\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$.

$$\sum_{k=0}^{\infty} a_k z^{k/r}$$

est une série de Puiseux.
Remarquons que cette écriture n'est pas unique notamment quant au choix de r, en effet une autre écriture est obtenue en remplaçant r par $2r$ et $(a_k)_{k\in\mathbb{N}}$ par $(b_k)_{k\in\mathbb{N}}$ vérifiant $b_{2k} = a_k$ et $b_{2k+1} = 0$:

$$\sum_{k=0}^{\infty} b_k z^{k/2r} = \sum_{k=0}^{\infty} a_k z^{2k/2r}$$

On pourrait faire de même avec tout multiple de r.

Définition 7.1.11 (Notations)**.** On va adopter les notations suivantes :

- On note $\mathbb{C}\{z\}$ l'anneau des séries entières à rayon de convergence strictement positif.
- On note $\mathbb{C}[[z]]$ l'anneau des séries entières formelles.
- On note $\mathbb{C}(\{z\})$ le corps de fractions de $\mathbb{C}\{z\}$.
- On note $\mathbb{C}((z))$ le corps de fractions de $\mathbb{C}[[z]]$.
- On note $\mathbb{C}[[z^*]]$ l'anneau des séries entières de Puiseux formelles.
- On note et $\mathbb{C}\{z^*\}$ l'anneau des séries entières de Puiseux à rayon de convergence strictement positif.
- On note $\mathbb{C}((z^*))$ les corps de fractions de $\mathbb{C}[[z^*]]$.
- On note $\mathbb{C}(\{z^*\})$ les corps de fractions de $\mathbb{C}\{z^*\}$.

Définition 7.1.12 (Ordre)**.** Tout élément $\Phi \in \mathbb{C}((z^*))$ peut être écrit sous la forme $\sum_{k=n}^{\infty} a_k z^{k/r}$ avec $n \in \mathbb{Z}$. Lorsque Φ est écrite sous cette forme et que $a_n \neq 0$, on appelle *ordre* de Φ $ord\Phi = \frac{n}{r}$.

Démonstration. Montrons que n/r est unique même si le choix de r change.
Soit $\Phi \in \mathbb{C}((z^*))$. Soient n_1, n_2, r_1, r_2 et des coefficients complexes $(a_k)_{k\geq n_1}$ et $(b_k)_{k\geq n_2}$ tels que :

$$\Phi(z) = \sum_{k=n_1}^{\infty} a_k z^{k/r_1} = \sum_{k=n_2}^{\infty} b_k z^{k/r_2}$$

On en déduit avec le changement de variable $z \mapsto z^{r_1 r_2}$ que :

$$\begin{aligned} \textstyle\sum_{k=n_1}^{\infty} a_k (z^{r_1 r_2})^{k/r_1} &= \textstyle\sum_{k=n_2}^{\infty} b_k (z^{r_1 r_2})^{k/r_2} \\ \textstyle\sum_{k=n_1}^{\infty} a_k z^{k r_2} &= \textstyle\sum_{k=n_2}^{\infty} b_k z^{k r_1} \end{aligned}$$

Et en utilisant l'identification terme à terme, on trouve en particulier que $n_2 r_1 = n_1 r_2$ d'où l'unicité de la définition ci-dessus. □

Proposition 7.1.18. *Les inversibles de $\mathbb{C}\{z\}, \mathbb{C}\{z^*\}, \mathbb{C}[[z]], \mathbb{C}[[z^*]]$ sont exactement les éléments d'ordre 0.*

Démonstration. Le résultat pour $\mathbb{C}\{z\}$ vient du fait qu'une fonction f *holomorphe* au voisinage de 0 qui ne s'annule pas pas en 0 a son inverse $1/f$ qui est également *holomorphe* sur un voisinage de 0.
Démontrons le résultat pour $\mathbb{C}\{z^*\}$. Soit $\Phi \in \mathbb{C}\{z^*\}$. Prenons $r \in \mathbb{N}$ et $f \in \mathbb{C}\{z\}$ telle que $\Phi = f(z^{1/r})$. Alors $1/f(z^{1/r})$ est clairement un inverse de Φ et est dans $\mathbb{C}(\{z\})$.
En ce qui concerne les séries formelles, ça revient à résoudre un système d'équation triangulaire (infini). Ce qui est toujours possible.

□

Dans le cours de la démonstration du théorème de Pusieux, on aura besoin du lemme de Hensel. Introduisons pour ce lemme la notion de topologie I-adique.

Définition 7.1.13 (Topologie I-adique)**.** Soit A un anneau commutatif, I un idéal de A. La topologie I-adique de de A est définie par la base de voisinages en chaque point a de A de la forme $a + I^n$, $n \in \mathbb{N}$.

A est alors topologique (i.e. muni d'une topologie). Il est séparé (i.e. c'est un espace de Hausdorff) pour cette topologie si et seulement si $\cap_{n\in\mathbb{N}} I^n = 0$. On pourrait alors définir une distance sur A.
On remarque également que cette définition est cohérente avec les topologies correspondantes aux normes $\mathfrak{p}$-adiques définies plus tôt.
On rappelle la définition des suites de Cauchy pour un groupe topologique, car le lemme de Hensel repose en effet sur une hypothèse de complétude.

Définition 7.1.14. Soit G un groupe muni d'une topologie.
On dit qu'une suite $(g_n)_{n\in\mathbb{N}}$ est de Cauchy si pour tout voisinage V de l'élément neutre, il existe $N \in \mathbb{N}$ tel que

$$\forall n, m \geq N,\ g_n g_m^{-1} \in V.$$

Proposition 7.1.19 (Lemme d'Hensel)**.** *Soit A un anneau commutatif local (i.e.qui possède un unique idéal maximal).*
Soit I son idéal maximal, on suppose que A est complet pour sa topologie I-adique. On suppose de plus que $\cap_{s_in} I^s = 0$ (i.e. que A muni de cette topologie est un espace de Hausdorff).
Soit f un polynôme unitaire de $A[X]$ de degré $n \geq 1$.
Supposons enfin que l'on dispose de deux polynômes premiers entre eux G et H dans

$(A/I)[X]$, *de degrés respectifs* r *et* $n-r$ $(n > r > 0)$ *tels que*

$$\overline{f} = GH$$

avec $\overline{f}$ *la classe de* f *dans* $(A/I)[X]$ *par projection canonique.*
Alors, il existe deux polynômes unitaires g *et* h *dans* $A[X]$*, de degrés respectifs* r *et* $n-r$*, tels que*

$$\overline{g} = G \ ; \ \overline{h} = H \ ; \ f = gh.$$

Remarque : les cas $r = 0$ et $r = n$ sont triviaux par le caractère unitaire des différents polynômes.

Démonstration. Nous nous appuyons pour cette preuve sur le travail de Daniel Murfet exposé dans son article *Hensel's Lemma* [28].

- Nous construisons d'abord par récurrence $g_k, h_k \in A[X]$ unitaires tels que $f \equiv g_k h_k \pmod{I^k[X]}$ pour tout $k \geq 1$, avec $\overline{g_k} = G$ et $\overline{h_k} = H$, et g_k et h_k uniques modulo $I^k[X]$.

  - En choisissant des représentants dans A pour les coefficients non nuls de G et H (en prenant bien 1 pour $1 + I$), on définit deux polynômes unitaires $g_1, h_1 \in A[X]$ de degrés r et $n-r$ avec $\overline{g_1} = G$ et $\overline{h_1} = H$. Comme

    $$\overline{f} = GH = \overline{g_1 h_1}$$

    on a bien $f \equiv g_1 h_1 \pmod{I[X]}$. Et g_1 et h_1 sont uniques modulo $I[X]$ par définition.

  - Soit $k \geq 1$, on suppose maintenant construits g_k et h_k comme souhaités. Construisons g_{k+1} et h_{k+1}.
    Nous allons pour cela trouver δ et ϵ dans $I^k[X]$ de degrés respectivement strictement inférieurs à r et $n-r$ tels que $g_{k+1} = g_k + \delta$, $h_{k+1} = h_k + \epsilon$ satisfassent les propriétés nécessaires.
    Comme G et H sont premiers entre eux, on dispose de α et β dans $A[X]$ tels que

    $$1 \equiv \alpha g_k + \beta h_k \mod I[X].$$

    Par hypothèse de récurrence, $\Delta = f - g_k h_k \in I^k[X]$. Donc $\Delta \equiv \Delta\alpha g_k + \Delta\beta h_k \pmod{I^{k+1}[X]}$.
    On cherche des polynômes de degrés strictement inférieurs respectivement à r et $n-r$. Comme h_k est unitaire, on peut faire la division euclidienne de $\Delta\alpha$ par h_k pour obtenir $\gamma, \epsilon \in A[X]$ tels que $deg(\epsilon) < n-r$ et $\Delta\alpha = \gamma h_k + \epsilon$. Or, $\Delta\alpha \in I^k[X]$ donc $\gamma h_k + \epsilon \equiv 0 \pmod{I^k[X]}$. Comme h_k est unitaire, il est de degré $n-r$ modulo $I^k[X]$ aussi. Par unicité de la division euclidienne dans $(A/I^k)[X]$, $\gamma, \epsilon \in I^k[X]$. Il vient la congruence suivante $(*)$:

    $$\Delta \equiv \epsilon g_k + \delta h_k \mod I^{k+1}[X]$$

avec $\delta = \gamma g_k + \Delta\beta \in I^k[X]$, car $\gamma, \Delta \in I^k[X]$. Comme Δ et ϵg_k sont tous deux de degré strictement inférieur à n, δh_k aussi, donc $deg(\delta) < r$. Etant donnés les degrés de δ, ϵ, les polynômes $g_{k+1} = g_k + \delta$ et $h_{k+1} = h_k + \epsilon$ sont unitaires et de degrés respectifs r et $n - r$. Comme $\delta\epsilon \in I^{2k}$ et $2k \geq k + 1$, modulo $I^{k+1}[X]$:

$$\begin{aligned} g_{k+1}h_{k+1} &\equiv g_k h_k + \epsilon g_k + \delta h_k + \delta\epsilon \\ &\equiv g_k h_k + \Delta \\ &\equiv f. \end{aligned}$$

De plus comme δ et ϵ sont dans $I^k[X]$ et par hypothèse de récurrence, $\overline{g_{k+1}} = G$ et $\overline{h_{k+1}} = H$.

- Reste à prouver l'unicité.
  Soient g' et h' des polynômes unitaires de degrés r et $n - r$ tels que $\overline{g'} = G$, $\overline{h'} = H$ et $f \equiv g'h' \pmod{I^{k+1}[X]}$. Alors, $deg(\epsilon' = h' - h_k) < n - r$ et $deg(\delta' = g' - g_k) < r$. Par hypothèse de récurrence, g_k et h_k sont uniques modulo $I^k[X]$ donc ϵ' et δ' sont dans $I^k[X]$ puis $\epsilon'\delta' \in I^{k+1}[X]$. Ainsi, modulo $I^{k+1}[X]$,

$$\begin{aligned} 0 &\equiv f - g'h' \equiv f - g_k h_k - \delta' h_k - \epsilon' g_k - \epsilon'\delta' \\ &\equiv \Delta - (\epsilon' g_k + \delta' h_k). \end{aligned}$$

  En soustrayant ce résultat à la congruence $(*)$, on a :

$$0 \equiv \mu g_k + \nu h_k \mod I^{k+1}[X]$$

  avec $deg(\mu = \epsilon - \epsilon') < n - r$ et $deg(\nu = \delta - \delta') < r$. En multipliant par α et comme $\alpha g_k + \beta h_k - 1 = i \in I[X]$, on a

$$\mu \equiv (\mu\beta - \alpha\nu)h_k - \mu i \mod I^{k+1}[X].$$

  Or $\mu \in I^k[X]$ et $i \in I[X]$, donc μ est un multiple de h_k dans $(A/I^{k+1})[X]$. Mais dans $(A/I^{k+1})[X]$, $deg(\mu) < n - r$ et $deg(h_k) = n - r$, d'où $\mu \equiv 0 \pmod{I^{k+1}}$. De même $\nu \equiv 0$. D'où modulo I^{k+1}

$$h' \equiv h_k + \epsilon' \equiv h_k + \epsilon \equiv h_{k+1}$$

  et de même $g' \equiv g_{k+1}$. On a bien unicité.

Par le principe de récurrence, on a donc construit nos deux suites comme souhaitées.

- Définissons maintenant g et h.
  Pour $1 \leq i \leq j$, $f - g_j h_j \in I^j[X] \subset I^i[X]$ donc $f \equiv g_j h_j \pmod{I^i[X]}$ d'où par unicité $g_i \equiv g_j$ et $h_i \equiv h_j \pmod{I^i[X]}$. Il vient que les suites des coefficients sont de Cauchy dans A muni de la topologie I-adique et donc convergent vers $a_0, ..., a_{r-1}$ (pour g_i) et $b_0, ..., b_{n-r-1}$ (pour h_i). On pose alors

$$g = a_0 + a_1 X + \cdots + a_{r-1}X^{r-1} + X^r$$

et

$$h = b_0 + b_1 X + \cdots + b_{n-r-1} X^{n-r-1} + X^{n-r}.$$

Comme pour tout $k \geq 1$, $\overline{g_k} = G$ et $\overline{h_k} = H$, on obtient en conidérant la convergence des coefficients $\overline{g} = G$ et $\overline{h} = H$.

- Montrons enfin que $f = gh$.
  On remarque d'abord que pour $0 \leq i \leq n-1$

$$\begin{aligned}(gh)_i - (g_k h_k)_i &= \sum_{j=0}^{i} (g_j h_{i-j} - g_{k,j} h_{k,i-j}) \\ &= \sum_{j=0}^{i} (g_j - g_{k,j}) h_{i-j} + \sum_{j=0}^{i} g_{k,j} (h_{i-j} - h_{k,i-j})\end{aligned}$$

Par la définition topologique de la convergence, pour tout $l \in \mathbb{N}$, on dispose de $N \in \mathbb{N}$ tel que pour tout $k \geq N$, $(gh)_i - (g_k h_k)_i \in I^l$. Or,

$$f_i - (gh)_i = f_i - (g_k h_k)_i + (g_k h_k)_i - (gh)_i$$

et $f_i - (g_k h_k)_i \in I^k$ par construction. D'où, par ces deux remarques, $f_i - (gh)_i \in \cap_s I^s$. Or par hypothèse du lemme $\cap_s I^s = 0$. Donc $f = gh$.

□

Le lemme d'Hensel est démontré, mais avant de passer au théorème de Puiseux on va préparer le terrain. On définit une terminologie qui permet de parler, de façon légère, de la classe d'un polynôme dans l'espace quotient A/I.

Définition 7.1.15 (Réduction d'un polynôme)**.** Soit $P(z,T) \in \mathbb{C}[[z]][T]$. On appelle la réduction en polynôme complexe de $P(z,T)$ le polynôme $P(0,T) \in \mathbb{C}[T]$. Ce polynôme est l'image de $P(z,T)$ dans l'anneau des polynômes à coefficients dans le quotient de l'anneau $\mathbb{C}[[z]]$ par l'idéal $\{a \in \mathbb{C}[[z]], ord\ a \geq 1\}$.

On exhibe ici une version "prête à appliquer" du lemme d'Hensel dans notre cas. Ainsi, on peut distinguer la structure de la preuve du théorème de Puiseux plus facilement.

Corollaire 7.1.1 (Lemme d'Hensel appliqué)**.** *Soit $P(z,T) \in \mathbb{C}[[z]][T]$ de degré n. Si l'on dispose de $G, H \in \mathbb{C}[T]$ premiers entre eux de degrés $1 \leq r, n-r \leq n-1$ tels que $P(0,T) = G(T)H(T)$.*
Alors il existe $g, h \in \mathbb{C}[[z]][T]$ premiers entre eux de degrés $1 \leq r, n-r \leq n-1$ tels que $P(z,T) = h(z,T)g(z,T)$
Le résultat reste vrai si on remplace $\mathbb{C}[[z]]$ par $\mathbb{C}\{z\}$.

Démonstration. Ce corollaire est une application directe du lemme d'Hensel 7.1.19 dès qu'on a montré que $\mathbb{C}[[z]]$ vérifie ses hypothèses. En ce qui concerne $\mathbb{C}\{z\}$, même s'il ne vérifie pas les conditions qu'on utilise (en particulier la complétude) on peut montrer qu'il vérifie le lemme d'Hensel. On dit qu'il est Hensélien (Voir la partie "Examples" de cette page Wikipédia `https://en.wikipedia.org/wiki/Henselian_ring`.
Montrons donc que $\mathbb{C}[[z]]$ est local en explicitant son unique idéal maximal I, qu'il est complet pour la topologie issue de I, et que $\cap_{s=1}^{\infty} I^s = 0$:

- Soit $I = \{a \in \mathbb{C}[[z]], ord\ a \geq 1\}$. Montrons que I est un idéal, maximal, unique (le seul idéal maximal) :
  - soit $a \in I$ et $b \in \mathbb{C}[[z]]$. On a $ord\ ab \geq ord\ a = 1$ et donc $ab \in I$. et I est clairement un groupe additif. Donc I est un idéal.
  - Montrons que I est maximal. Soit J un idéal contenant strictement I. On dispose donc de $b \in J$ vérifiant $ord\ b = 0$. Soit $c(z) \in \mathbb{C}[[z]]$, montrons que $c \in J$.

    $$c(z) = \left(c(z) - \frac{c(0)}{b(0)}b(z)\right) + \frac{c(0)}{b(0)}b(z)$$

    On a $\left(c(z) - \frac{c(0)}{b(0)}b(z)\right) \in I \subset J$ car son terme d'ordre 0 s'annule. Et $\frac{c(0)}{b(0)}b(z) \in J$ car $b \in J$. Ainsi $c \in J$ et $J = \mathbb{C}[[z]]$. Donc I est maximal.
  - Passons maintenant à l'unicité. Soit J un idéal maximal. En particulier $I \backslash J \neq \emptyset$. Soit donc $c \in J \backslash I$, on sait que $ordc = 0$ et donc on dispose d'une série formelle $1/c$ et ainsi $c \in \mathbb{C}[[z]]^{\times}$ et donc $J = \mathbb{C}[[z]]$. Et I est l'unique idéal maximal de $\mathbb{C}[[z]]$.
- Montrons que $\mathbb{C}[[z]]$ est un anneau complet pour la topologie issue de I. Soit $(f_n(z))_{n\geq 0}$ une suite de Cauchy de séries entières, $f_n(z)$ ayant pour coefficients $(a_{k,n})_{k\geq 0}$.
  - Montrons que pour tout $k \in \mathbb{N}$, $(a_{k,n})_{n\geq 0}$ est un suite stationnaire à partir d'un certain rang.

    Soit $k \in \mathbb{N}$. Soit N_0 le rang à partir duquel $(f_p - f_q) \in I^k$ un voisinage de 0. $\forall p, q \geq N_0, a_{k,p} = a_{k,q}$ puisque le plus petit coefficient non nul de $(f_p - f_q)$ est de rang supérieur à k (puisqu'il est dans le voisinage I^k). Ainsi à partir de N_0 $(a_{k,n})_{n\geq 0}$ est stationnaire.
  - Montrons que f est la limite des f_n

    $$f(z) = \sum_{k=0}^{\infty} \left(\lim_{m\mapsto\infty} a_{k,m}\right) z^k$$

    Soit V un voisinage de 0. On veut trouver un rang à partir duquel les premiers coefficients deviennent stationnaires. Identifions d'abord ce que veut dire "les premiers coefficients". On dispose de $N_1 \in \mathbb{N}$ tel que $I^{N_1} \subset V$. Les « premiers coefficients » vont donc être ceux antérieurs à ce rang N_1. Or on dispose de $N_2 \in \mathbb{N}$ tel que $\forall 0 \leq j \leq N_1, (a_{j,n})_{n\geq 0}$ est stationnaire à partir du rang N_2.

    On a $\forall n \geq N_2, \left(f - f_n\right) \in I^{N_1} \subset V$ et donc f est bien la limite des f_n. Et elle est évidemment dans l'espace des séries entières formelles.

- Montrons finalement que $\cap_{s=1}^{\infty} I^s = 0$.
  On a clairement que pour $k \in \mathbb{N}, (f(z) \in I^k) \implies f(z) = \sum_{n \geq k} a_n z^n$. Une conséquence immédiate est que si $f(z) \in \cap_{s=1}^{\infty} I^s$ alors $f = 0$. Et donc $\cap_{s=1}^{\infty} I^s = \{0\}$

On a montré toutes le conditions nécessaires sur $\mathbb{C}[[z]]$ et on obtient notre corollaire en appliquant le lemme d'Hensel 7.1.19. □

Théorème 18 (Théorème de Puiseux)**.** *Les corps* $\mathbb{C}(\{z^*\})$ *et* $\mathbb{C}((z^*))$ *sont algébriquement clos.*

Démonstration. En admettant que le lemme d'Hensel 7.1.1 est applicable pour les séries entières convergentes et non seulement les séries formelles, cette propriété se démontre exactement de la même manière pour les deux espaces. Nos raisonnements vont donc porter uniquement sur $\mathbb{C}\{z\}$.
On va plutôt montrer que tout polynôme irréductible est forcément de degré $= 1$, ce qui est équivalent. Puisqu'on travaille dans un corps, il suffit de prouver ce résultat sur les polynômes unitaires, quitte à diviser par le coefficient dominant.
Les polynômes de degré 1 sont bien irréductibles. Il suffit donc de prouver qu'un polynôme de degré supérieur à 1 n'est pas irréductible. Prenons donc le polynôme $P \in \mathbb{C}(\{z^*\})[X]$ de degré $n > 1$ suivant :

$$P(z, T) = T^n + a_{n-1}(z)T^{n-1} + \cdots + a_0(z)$$

Supposons que P ne s'écrit pas $P(z, T) = (T - c(z))^n$ (sinon P est clairement factorisable). Cette condition est essentielle car le lemme d'Hensel 7.1.19 porte sur les factorisations en polynômes non constants premiers entre eux. Il faut maintenant se ramener à un polynôme à coefficients dans $\mathbb{C}\{z\}$ pour pouvoir appliquer le lemme 7.1.19.
Néanmoins, le lemme d'Hensel est une simple implication. On se doute donc qu'il est possible d'obtenir, après réduction, un polynôme complexe qui n'est pas produit de deux polynômes premiers entre eux même si le polynôme de départ l'est. Si c'est le cas, on ne peut pas appliquer le lemme.

Exemple 7.1.2. $P(z, T) = T^2 + zT = T(T + z)$ est un polynôme qui s'écrit comme produit de deux polynômes premiers entre eux. Néanmoins sa réduction :

$$P(0, T) = T^2$$

ne s'écrit pas comme produit de deux polynômes complexes premiers entre eux.

Pour éviter cette situation, on procède en deux étapes.
Tout d'abord on se ramène au cas d'un polynôme ayant 0 pour coefficient de rang $n - 1$. Cette adaptation nous garantit un argument simple pour obtenir que la réduction de notre polynôme donne un polynôme complexe soit produit de deux polynômes premiers entre eux, soit égal à T^n (c'est à dire qu'il ne peut pas être écrit sous la forme $(T - c)^n$ avec $c \neq 0$).

La deuxième étape est simplement d'éviter que les séries entières coefficients de notre polynôme ne s'annulent toutes en 0 (sinon la réduction serait égale à T^n).

Pour la première étape sus-mentionnée on va faire un changement de variable sur T :

$$\begin{aligned}
Q(z,T) &= P(z, T - \frac{a_{n-1}(z)}{n}) \\
&= \Big(T - \frac{a_{n-1}(z)}{n}\Big)^n + a_{n-1}(z)\Big(T - \frac{a_{n-1}(z)}{n}\Big)^{n-1} + \cdots + a_0(z) \\
&= T^n - n\frac{a_{n-1}(z)}{n}T^{n-1} + a_{n-1}(z)T^{n-1} + R(z,T) \\
&\text{avec } R(z,T) \text{ un polynôme de degré inférieur à } n-2 \\
&= T^n + R(z,T) \\
&= T^n + b_{n-2}(z)T^{n-2} + \cdots + b_0(z)
\end{aligned}$$

et on a bien évidemment que P est irréductible si et seulement si Q l'est.
On a également que $Q(z,t) = T^n \implies P(z,T) = (T - \frac{a_{n-1}(z)}{n})^n$ et donc par contraposée $P(z,T) \neq (T - \frac{a_{n-1}(z)}{n})^n \implies (Q(z,t) \neq T^n) \iff \Big(\exists k \in [\![0; n-2]\!], \exists z \in \mathbb{C}, b_k(z) \neq 0\Big)$.
On peut donc tout simplement supposer que (quitte à prendre Q à la place de P) :

$$P(z,T) = T^n + a_{n-2}(z)T^{n-2} + \cdots + a_0(z)$$

Avec un des $a_i(z)$ non identiquement nul.
La première étape est accomplie. Notre objectif est désormais de se ramener à un polynôme à coefficients dans $\mathbb{C}\{z\}$. Travaillons sur l'ensemble $I = \{k \in [\![0; n-2]\!] | \exists z \in \mathbb{C}, a_k(z) \neq 0\}$. I est non vide. Pour tout $k \in I$ on pose :

- $r_k = ord\ a_k(z)$
- $r = \min\{\frac{r_k}{k}\}$
- q_k tel que $a_k(z) = f(z^{1/q_k})$ avec $f(z) \in \mathbb{C}(\{z\})$
- $q = k! \prod_k q_k$

Montrons qu'on peut écrire $r = \frac{p}{q}$ avec $p \in \mathbb{Z}$, un résultat qui servira à rendre toutes les puissances entières, moyennant un changement de variable. Ceci nous permettra d'ailleurs de comprendre pourquoi q a été défini ainsi.
On a $\forall k \in I, \frac{r_k}{k} \cdot kq_k \in \mathbb{Z}$ par définition de q_k.
Ainsi, $r \prod_k kq_k \in \mathbb{Z}$
Donc pour $p = rq \in \mathbb{Z}$ on a bien $r = \frac{p}{q}$.
Nous nous ramenons maintenant à un polynôme à coefficients dans $\mathbb{C}\{z\}$.
Appliquons les transformations de variables suivantes :

- $z \mapsto w^q$
- $T \mapsto U \cdot w^p$
- $P(z,T) \mapsto w^{np} \cdot Q(w,U)$

Déterminons l'écriture de Q :

$$\begin{aligned} P(z,T) &= T^n + a_{n-2}(z)T^{n-2} + \cdots + a_0(z) \\ P(w,T) &= T^n + a_{n-2}(w^q)T^{n-2} + \cdots + a_0(w^q) \\ P(w,U) &= (Uw^p)^n + a_{n-2}(w^q)(Uw^p)^{n-2} + \cdots + a_0(w^q) \\ &= w^{pn}\left(U^n + \frac{a_{n-2}(w^q)}{w^{2p}}U^{n-2} + \cdots + \frac{a_0}{w^{np}}\right) \end{aligned}$$

Ainsi,

$$Q(w,U) = U^n + \frac{a_{n-2}(w^q)}{w^{2p}}U^{n-2} + \cdots + \frac{a_0}{w^{np}}$$

Montrons que $b_k(z) = \frac{a_k(w^q)}{w^{kp}} \in \mathbb{C}\{z\}$.

$$\begin{aligned} a_k(w^q) &= \sum_{j=qr_k}^{\infty} c_j (w^q)^{j/q} \\ &\quad \text{L'écriture ci-dessus découle} \\ &\quad \text{de la définition des séries de Puiseux} \\ &= \sum_{j=qr_k} c_j w^j \\ &= \left(\sum_{j=qr_k} c_j w^{j-kp}\right) w^{kp} \\ &= \left(\sum_{j=qr_k-kp} c_j w^j\right) w^{kp} \end{aligned}$$

Ensuite, on divise par w^{kp} pour obtenir $b_k(z)$
On a donc clairement que $ord\ b_k = qr_k - kp \in \mathbb{Z}$ puisque $qr_k q \in \mathbb{Z}$ et $k, p \in \mathbb{Z}$. Regardons maintenant son signe.
On sait que $0 \leq \frac{r_k}{k} - r = \frac{1}{kq}(r_k q - kp)$ et donc $ordb_k \in \mathbb{N}$ c'est à dire entier et positif. De plus, l'ordre d'un des b_k est égal à 0 (par définition de r comme minimum sur I qui est non vide et fini). C'est à dire que au moins l'un des b_k ne s'annule pas en 0.
Ainsi $Q(w,U) \in \mathbb{C}\{z\}$. Maintenant qu'on s'est placé dans un anneau adéquat, où l'on pourra appliquer le lemme d'Hensel. Regardons donc la réduction de Q en polynôme complexe comme dans la définition 7.1.15 .

$$Q(0,U) = U^n + b_{n-2}(0)U^{n-2} + \cdots + b_0(0)$$

Notre but est de montrer que $Q(0,U) \in \mathbb{C}[U]$ s'écrit comme produit de deux polynômes premiers entre eux. Or dans $\mathbb{C}$ ceci équivaut à dire qu'il ne s'écrit pas sous la forme $(U-c)^n$.

- Traitons le cas $c \neq 0$: il faut se rappeler qu'on s'est mis dans le cas où $b_{n-1}(0) = 0$. Ainsi si $Q(0,U) = (X-c)^n$ alors $-nc = b_{n-1}(0) = 0$ ce qui contredit $c \neq 0$.
- Pour le cas $c = 0$: $Q(0,U) \neq U^n$ puisque au moins un des b_k admet 0 comme ordre et donc $b_k(0) \neq 0$.

- Remarquons que le changement de variable qui a garantit le premier point devait être fait au tout début pour pouvoir obtenir la bonne définition des b_k qui permet d'avoir le deuxième point.

Or $\mathbb{C}$ est algébriquement clos et donc ce polynôme se factorise en produit de deux polynômes non constants premiers entre eux. Or d'après le corollaire 7.1.1, on déduit que $Q(w,U)$ s'écrit comme produit de deux polynômes non constants (car leurs image comme polynômes complexes n'est pas constante) à coefficients dans $\mathbb{C}\{z\}$ premiers entre eux $Q_1(w,U), Q_2(w,U)$.
Ceci nous donne le résultat voulu :

$$P(z,T) = z^{nr} Q_1(z^{1/q}, z^{-r}T) Q_2(z^{1/q}, z^{-r}T)$$

Ainsi tout polynôme à coefficient dans $\mathbb{C}((z^*))$ de degré supérieur à 1 n'est pas irréductible, et seuls les polynômes de degré 1 le sont. Et donc le corps $\mathbb{C}(\{z^*\})$ est algébriquement clos. □

7.2 Produit tensoriel

L'extension des scalaires est une opération de théorie des modules qui permet de changer l'anneau de base au moyen d'un produit tensoriel et d'un morphisme d'anneaux. Nous nous appuyons dans cette sous-section principalement sur le chapitre 9 du cours *Algèbre et théorie de Galois* de 2005-2006 dispensé par Patrick Polo à l'Université Paris VI [29].

Qu'est-ce qu'un produit tensoriel ?

7.2.1 • Propriété universelle

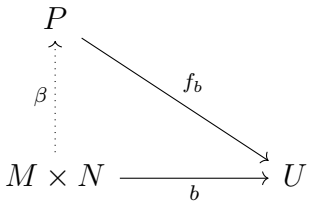
On se donne A un anneau commutatif. Soient M et N deux A-modules. On cherche à construire un module $M \bigotimes N$ tel que la donnée d'une forme A-bilinéaire b sur $M \times N$ équivale à celle d'une forme A-linéaire f_b sur $M \bigotimes N$. Plus généralement, on étudie le problème suivant.

Existe-t-il un couple (P, β) formé d'un A-module P et d'une application A-bilinéaire $\beta : M \times N \to P$ vérifiant que pour toute application bilinéaire b de $M \times N$ vers un A-module U quelconque, il existe une unique application linéaire $f = f_b : P \to U$ telle que

$$\forall (m,n) \in M \times N \; b(m,n) = f_b(\beta(m,n)),$$

ou autrement dit, telle que $b = f_b \circ \beta$?

Autrement dit, on cherche $\beta : M \times N \to P$ tel que le diagramme suivant commute.



Cela revient à « oublier » le caractère bilinéaire de b pour se ramener à un f_b linéaire.

Ce problème admet une unique solution (dans un certain sens), c'est ce qui définit la notion de produit tensoriel.

Théorème 19 (Propriété universelle du produit tensoriel, version 1)**.** *Soient M et N deux modules sur A. Il existe*

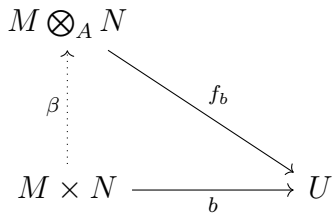
- *un A-module noté $M \bigotimes_A N$, unique à isomorphisme de A-modules près,*
- *une application A-linéaire $\beta : M \times N \to M \bigotimes_A N$, unique à isomorphisme de A-modules près*

tels que

- *pour tout A-module U,*
- *pour toute application A-bilinéaire $b : M \times N \to U$*

il existe une unique $f_b \in \mathrm{Hom}_A(M \bigotimes_A N, U)$ telle que $b = f_b \circ \beta$.

Autrement dit, le diagramme suivant commute.



Lorsque dans le contexte, l'anneau A est évident, on notera simplement $M \bigotimes N$.

Donnons une autre façon de voir la propriété universelle, qui est simplement une réécriture de ce qu'on vient de dire en termes d'espaces d'homomorphismes.

Proposition 7.2.1 (Propriété universelle du produit tensoriel version 2)**.** *Soient A un anneau, M et N des A-modules.*

Pour tout A-module U, on a une bijection

$$\begin{array}{ccc} \mathrm{Bil}_A(M \times N, U) & \xrightarrow{\sim} & \mathrm{Hom}_A(M \bigotimes_A N, U) \\ b & \mapsto & f_b \\ f \circ \beta & \leftarrow\!\shortmid & f. \end{array}$$

On peut aussi écrire

$$\mathrm{Hom}_A(M \bigotimes_A N, U) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, U)).$$

Définition 7.2.1.

Comme β est unique, on note, pour tout $(m,n) \in M \times N$, $\beta(m,n) = m \otimes n$.

La démonstration de ce théorème ne nous intéresse pas en tant que telle, mais il est instructif de regarder une idée de construction possible. On veut donc pour ce « produit » deux propriétés qui traduisent la bilinéarité de β recherché.

(i) bi-additivité : $\begin{cases} (m+m') \otimes n &= m \otimes n + m' \otimes n \\ m \otimes (n+n') &= m \otimes n + m \otimes n'. \end{cases}$

(ii) unicité de l'action de A :

$$a(m \otimes n) = (am) \otimes n = m \otimes (an).$$

À cette fin, on pose C le A-module des applications de $M \times N$ dans A nulles en dehors d'un sous-ensemble fini de $M \times N$. C est libre et admet pour base $\{e_{(m,n)}, (m,n) \in M \times N\}$ où e_x désigne la fonction de Dirac relative au point x.

On considère le sous-module D de C engendré par les éléments de la forme

$$\begin{aligned} e_{(m,n+n')} - e_{(m,n)} - e_{(m,n')} \\ e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)}, \\ e_{(\lambda m,n)} - \lambda e_{(m,n)}, \\ e_{(m,\lambda n)} - \lambda e_{(m,n)}, \end{aligned}$$

puis le module quotient $P = C/D$. On définit alors

$$\beta \ : \left| \begin{array}{ccc} M \times N & \to & P \\ (m,n) & \mapsto & \overline{e_{(m,n)}}, \end{array} \right.$$

avec $\overline{e_{(m,n)}}$ la classe de $e_{(m,n)}$ dans P. β est bilinéaire et son image engendre P tout entier. De plus, pour toute application $b : M \times N \to U$, l'application $\tilde{f}_b : P \to U$ qui attache à un élément $\sum_{(m,n) \in E \subset M \times N, Efini} \lambda_{(m,n)} e_{(m,n)}$ de P l'élément $\sum_{(m,n) \in E \subset M \times N, Efini} \lambda_{(m,n)} b(m,n)$ de U est bien définie (car les $e_{(m,n)}$ forment une base de P), et est linéaire. Si b est de plus bilinéaire, $\tilde{f}_b$ s'annule sur D, et définit donc par passage au quotient par D une application linéaire $f_b : P \to U$, qui vérifie bien $f_b \circ \beta = b$. Enfin, f_b est la seule application linéaire de P dans U vérifiant cette propriété, puisque l'image de β engendre P tout entier.

Cette construction permet de retomber sur le produit tensoriel défini plus haut.

Définition 7.2.2 (Produit tensoriel)**.** Avec les notations définie ci-dessus, on peut poser $M \bigotimes_A N = C/D$ et on note $m \otimes n$ la classe de $e_{(m,n)}$ dans $M \bigotimes_A N$, c'est à dire $\beta(m,n)$.

7.2.2 • Manipulation

Proposition 7.2.2. *Soient $(e_i)_{i \in I}$, respectivement $(f_j)_{j \in J}$, un système de générateurs de M, respectivement N, comme A-module.*

Alors, $M \bigotimes_A N$ est engendré comme A-module par les $e_i \otimes f_j$, pour $i \in I$, $j \in J$.

Démonstration. Cette propriété découle des propriétés de bi-additivité et de l'unicité de l'action de A que l'on a obtenu par notre construction par quotient. Ainsi pour

$$m = a_{i_1} e_{i_1} + ... + a_{i_r} e_{i_r}, \quad n = b_{j_1} f_{j_1} + ... + b_{j_r} f_{j_s},$$

on a

$$m \otimes n = \sum_{t=1}^{r} \sum_{u=1}^{s} a_{i_t} b_{j_u} e_{i_t} \otimes f_{j_u}.$$

Puisque tout élément de $M \bigotimes_A N$ est une somme finie d'éléments $m \otimes n$, il en résulte que les $e_i \otimes f_j$ engendrent $M \bigotimes_A N$ comme A-module. □

Malgré toute la pertinence de cette proposition explicite, il est souvent plus efficace de manipuler la propriété universelle. Regardons ce que cela donne sur un exemple.

Exemple 7.2.1. Prenons a et b deux entiers relatifs non nuls, et essayons de calculer le produit tensoriel

$$\mathbb{Z}/a\mathbb{Z} \bigotimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z}.$$

La propriété universelle invite à considérer l'application bilinéaire

$$F \quad : \left| \begin{array}{ccc} (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z}) & \to & \mathbb{Z}/(a \wedge b)\mathbb{Z} \\ (x + a\mathbb{Z}, y + b\mathbb{Z}) & \mapsto & (x + a\mathbb{Z})(y + b\mathbb{Z}). \end{array} \right.$$

On vérifie que F est bien définie. On a bien, pour x et y des entiers,

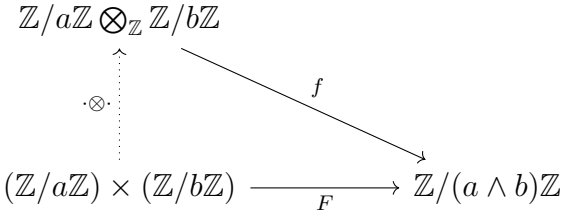
$$\begin{aligned} F(x + a\mathbb{Z}, y + b\mathbb{Z}) &= xy + ay\mathbb{Z} + bx\mathbb{Z} + ab\mathbb{Z} \\ &= xy + a\mathbb{Z} + b\mathbb{Z} \\ &= xy + (a \wedge b)\mathbb{Z}, \end{aligned}$$

et F est bien $\mathbb{Z}$-bilinéaire.

Par définition, on dispose d'une application $\mathbb{Z}$-linéaire

$$f : \mathbb{Z}/a\mathbb{Z} \bigotimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/(a \wedge b)\mathbb{Z}$$

telle que le diagramme suivant commute.



Ainsi, pour tous x et y entiers

$$f((x+a\mathbb{Z})\otimes(y+b\mathbb{Z}))=xy+(a\wedge b)\mathbb{Z}.$$

Reste à montrer que f est un isomorphisme. La surjectivité est automatique puisque

$$f((1+a\mathbb{Z})\otimes(1+b\mathbb{Z}))=1+(a\wedge b)\mathbb{Z}.$$

Pour l'injectivité, on a l'équivalence

$$f((x+a\mathbb{Z})\otimes(y+b\mathbb{Z}))=(a\wedge b)\mathbb{Z}\iff(a\wedge b)|xy.$$

Soit donc $(x+a\mathbb{Z})\otimes(y+b\mathbb{Z})\in\mathrm{Ker}(f)$. Par définition, on dispose de s et $r\in\mathbb{Z}$ tels que

$$a\wedge b=ra+sb.$$

On peut donc affirmer, quitte à changer les s et r, que

$$xy=ra+sb.$$

On peut alors faire disparaître les termes dans le produit, en remarquant que $y+b\mathbb{Z}$ est y fois la classe de 1 dans $\mathbb{Z}/b\mathbb{Z}$:

$$\begin{aligned}(x+a\mathbb{Z})\otimes(y+b\mathbb{Z})&=(xy+a\mathbb{Z})\otimes(1+b\mathbb{Z})\\&=(ra+sb+a\mathbb{Z})\otimes(1+b\mathbb{Z})\\&=s\cdot\Big((1+a\mathbb{Z})\otimes(b+b\mathbb{Z})\Big)\\&=0,\end{aligned}$$

donc f est un isomorphisme, et on peut affirmer que

$$\mathbb{Z}/a\mathbb{Z}\bigotimes_{\mathbb{Z}}\mathbb{Z}/b\mathbb{Z}\cong_{\mathbb{Z}-\text{modules}}\mathbb{Z}/(a\wedge b)\mathbb{Z}.$$

Le produit tensoriel est associatif et commutatif. On n'en fera pas la démonstration ici, mais le lecteur y arrivera sans peine.

Proposition 7.2.3 (associativité, commutativité)**.** *Soient A un anneau, M, N et P des modules, on a*

(i) associativité : $(M\otimes N)\otimes P\cong M\otimes(N\otimes P)$,

(ii) commutativité : $M\otimes N\cong N\otimes M$.

Une autre propriété immédiate, mais remarquable.

Proposition 7.2.4. *Soient A un anneau, M un A-module. On a*

$$A \bigotimes_A M \cong M.$$

On déduit de la propriété universelle la propriété suivante.

Proposition 7.2.5. *Soient A un anneau, I, J deux ensembles, et M, respectivement N, le A-module libre de base $(e_i)_{i\in I}$, respectivement $(f_j)_{j\in J}$.*
Alors, $M \bigotimes_A N$ est un A-module libre de base $(e_i \otimes f_j)_{(i,j)\in I\times J}$.

Démonstration. On se donne le A-module libre $V = A^{(I\times J)}$ dont les fonctions de Dirac $(v_{(i\times j)})_{(i,j)\in I\times J}$ forment clairement une base. On dispose d'une unique application linéaire $\phi : V \to M \bigotimes N$ telle que

$$\forall (i,j) \in I \times J \, \phi(v_{(i,j)}) = e_i \otimes f_j.$$

D'autre part, il existe une unique application A-bilinéaire $\theta : M \times N \to V$ telle que

$$\forall (i,j) \in I \times J \, \theta(e_i, f_j) = v_{(i,j)}.$$

Par la propriété universelle énoncée ci-dessus, il existe une unique application linéaire $\psi : M \bigotimes N \to V$ telle que

$$\forall (i,j) \in I \times J \, \psi(e_i \otimes f_j) = v_{(i,j)}.$$

On a clairement $\phi \circ \psi = id$ et $\psi \circ \phi = id$. □

Sans trop s'étendre sur le sujet, on peut définir un produit tensoriel à $n > 2$ facteurs en établissant une correspondance entre les applications n-linéaires sur le produit cartésien et les applications linéaires sur le produit tensoriel, de façon analogue à notre construction à deux modules. En outre et naturellement, le produit tensoriel défini ainsi est l'itération du produit tensoriel à deux facteurs donnent les mêmes objets. On obtiendrait alors la propriété suivante.

Proposition 7.2.6 (Propriété universelle de $M_1 \bigotimes_A \cdots \bigotimes_A M_s$)**.** *Soient A un anneau, $M_1, ..., M_s$ des modules.*
Pour tout A-module U, on a une bijection

$$\mathrm{Hom}_A(M_1 \bigotimes_A \cdots \bigotimes_A M_s, U) \cong \mathrm{Mult}_A(M_1 \times \cdots \times M_s, U).$$

7.2.3 • Extension des scalaires

On en vient désormais au sujet qui nous intéresse : l'extension des scalaires.

Proposition 7.2.7 (Extension des scalaires)**.** *Soient A et B deux anneaux commutatifs et ϕ un morphisme d'anneaux de A dans B. Soit M un A-module. Alors sur le A-module $B \bigotimes_A M$, il existe une unique structure de B-module telle que*

$$\forall b, b' \in B \, \forall m \in M \; b(b' \otimes m) = bb' \otimes m.$$

On l'appelle le module obtenu par extension des scalaires (ou changement de base) de A à B.

Démonstration. Par hypothèse, B et M sont des A-modules (B est même une A-algèbre), et on peut former le A-module $B \bigotimes_A M$, où l'action de A est définie par

$$a \cdot (b \otimes m) = \phi(a)b \otimes m = b \otimes am.$$

On dispose de l'application

$$\begin{array}{ccc} B \times B \times M & \to & B \bigotimes_A M \\ (b, b', m) & \mapsto & bb' \otimes m \end{array}$$

A-trilinéaire. Elle induit donc par la propriété universelle de $B \bigotimes_A B \bigotimes_A M$ une application A-linéaire

$$\begin{array}{ccc} B \bigotimes_A B \bigotimes_A M & \to & B \bigotimes_A M \\ b \otimes b' \otimes m & \mapsto & bb' \otimes m \end{array},$$

puis une application A-bilinéaire

$$\begin{array}{ccc} B \times (B \bigotimes_A M) & \to & B \bigotimes_A M \\ b \cdot (b' \bigotimes m) & \mapsto & bb' \bigotimes m \end{array}.$$

Comme tout élément w de $B \bigotimes_A M$ est une somme de tenseurs $b' \otimes m$, on obtient aisément $1 \cdot w = w$ et $b \cdot (c \cdot w) = bc \cdot w$ pour tous $b, c \in B$. Ainsi, $B \bigotimes_A M$ est bien un B-module. □

La construction de l'extension des scalaires telle qu'on vient de la faire permet de préserver la structure des groupes d'homomorphismes.

Proposition 7.2.8. *Soient A et B deux anneaux commutatifs, où l'on suppose par commodité $A \subset B$. Soit M un A-module.*

Pour tout B-module N, on a l'isomorphisme de B-modules

$$\mathrm{Hom}_B(M \bigotimes_A B, N) \cong_{B-modules} \mathrm{Hom}_A(M, N).$$

Démonstration. Avant de commencer la preuve, il faut bien voir que $\mathrm{Hom}_A(M, N)$ n'est a priori qu'un A-module. On peut néanmoins le munir d'un produit par des éléments de B de la façon suivante.

$$(b \cdot \phi) \; : \left| \begin{array}{ccc} M & \to & N \\ m & \mapsto & b\phi(m), \end{array} \right.$$

où $b \in B$, $\phi \in \mathrm{Hom}_A(M,N)$. Bien évidemment, ce produit est justifié car N est un B-module. On peut ensuite considérer les isomorphismes de B-modules suivants.

$$\begin{array}{ccc} \mathrm{Hom}_B(M \bigotimes_A B, N) & \xrightarrow{\sim} & \mathrm{Hom}_A(M,N) \\ \phi & \mapsto & \left(\begin{array}{ccc} M & \to & N \\ m & \mapsto & \phi(m \otimes 1) \end{array} \right) \\ \left(\begin{array}{ccc} M \bigotimes_A B & \to & N \\ m \otimes b & \mapsto & b\psi(m) \end{array} \right) & \mapsto & \psi \end{array}$$

où on vérifie aisément qu'on a bien affaire à des isomorphismes de B-modules réciproques. Ainsi on a bien l'isomorphisme souhaité :

$$\mathrm{Hom}_B(M \bigotimes_A B, N) \cong_{B-modules} \mathrm{Hom}_A(M,N).$$

□

Exemple 7.2.2 (Complexification)**.** Que le lecteur n'ayant jamais rencontré le produit tensoriel ne s'inquiète pas ! L'extension des scalaires est en fait un processus très courant et naturel, auquel la notion de produit tensoriel permet simplement de donner un cadre commode. Regardons l'exemple le plus commun : celui de la complexification.

On regarde le $\mathbb{R}$-espace vectoriel $\mathbb{R}$, et on veut le complexifier, donc faire une extension de scalaires $\mathbb{R} \to \mathbb{C}$. On s'attend donc à tomber le $\mathbb{C}$-espace vectoriel $\mathbb{C}$. La proposition 7.2.7 affirme que $\mathbb{C} \bigotimes_{\mathbb{R}} \mathbb{R}$ convient. Quelle est la structure de cet espace ? On exploite la proposition sur les bases 7.2.5 :

- (1) génère le $\mathbb{R}$-module $\mathbb{R}$,
- $(1, i)$ génère le $\mathbb{R}$-module $\mathbb{C}$,

donc $(1 \otimes 1, 1 \otimes i)$ génère $\mathbb{R} \bigotimes_{\mathbb{R}} \mathbb{C}$ comme $\mathbb{R}$-module. Mais on peut écrire

$$\begin{aligned} \mathbb{R} \bigotimes_{\mathbb{R}} \mathbb{C} &= \Big\{ a(1 \otimes 1) + b(1 \otimes i) \Big| a, b \in \mathbb{R} \Big\} \\ &= \Big\{ 1 \otimes z \Big| z \in \mathbb{C} \Big\}. \end{aligned}$$

La dernière expression fait clairement apparaître la structure de $\mathbb{C}$-module de $\mathbb{R} \bigotimes_{\mathbb{R}} \mathbb{C}$, et on a bien l'isomorphisme de $\mathbb{C}$-modules

$$\begin{array}{ccc} \mathbb{R} \bigotimes_{\mathbb{R}} \mathbb{C} & \xrightarrow{\sim} & \mathbb{C} \\ 1 \otimes z & \mapsto & z \\ 1 \otimes z & \mapsto & z. \end{array}$$

Dans cas, l'isomorphisme de la proposition précédente est simplement, pour E un $\mathbb{C}$-

espace vectoriel

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{C}}(\mathbb{C}, E) & \xrightarrow{\sim} & \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}, E) \\ \phi & \mapsto & \phi_{|\mathbb{R}} \\ \left(\begin{array}{c|ccc} z & \mapsto & z\psi(1) \\ \mathbb{C} & \to & E \end{array}\right) & \mapsto & \psi. \end{array}$$

Une question naturelle qu'on se pose avec l'extension des scalaires est celle de la dimension de l'espace obtenu. Dans le cas de la complexification qu'on vient de voir, on est parti d'un $\mathbb{R}$-espace de dimension 1 pour arriver sur un $\mathbb{C}$-espace de dimension 1. C'est en fait un résultat très général : l'extension des scalaires préserve la dimension.

Proposition 7.2.9. *Soit A un anneau commutatif. Soit M un A-module libre de rang d. Soit B un sur-anneau commutatif de A.*

Alors, le B-module $M \bigotimes_A B$ est encore libre et de rang d. Autrement dit,

$$\mathrm{rg}_B(M \bigotimes_A B) = \mathrm{rg}_A(M).$$

Démonstration. Par la proposition 7.2.8 on a l'isomorphisme de B-modules

$$\mathrm{Hom}_B(M \bigotimes_A B, B) \cong_{B-module} \mathrm{Hom}_A(M, B),$$

où on voit B comme un B-module. Comme les modules sont libres, on obtient

$$\mathrm{rg}_B(M \bigotimes_A B) = \mathrm{rg}_B(\mathrm{Hom}_A(M, B)).$$

Reste à calculer $\mathrm{rg}_B(\mathrm{Hom}_A(M, B))$. On peut expliciter une base de ce B-module libre. Notons $n = \mathrm{rg}_A(M)$ et $(e_1, ..., e_n)$ une base du A-module M. On se donne alors une base β du A-module libre $\mathrm{Hom}_A(M, A)$ avec la famille

$$\beta = (\delta_1, ..., \delta_n),$$

où pour tous i, j on a $\delta_i(e_j) = 1_{i=j}$. Mais β peut aussi être vue comme une famille du B-module $\mathrm{Hom}_A(M, B)$ puisque $A \subset B$, et elle en est même une base.

- La liberté de β s'obtient aisément en évaluant en les e_i une combinaison linéaire nulle.
- β est génératrice. En effet, pour $\phi \in \mathrm{Hom}_A(M, B)$, on écrit $\phi = \sum_{i=1}^n \phi(e_i)\delta_i$, qui est bien une combinaison linéaire avec des scalaires dans B.

Ainsi, $\mathrm{rg}_B(\mathrm{Hom}_A(M, B)) = n = \mathrm{rg}_A(M)$. On peut donc conclure que

$$\mathrm{rg}_B(M \bigotimes_A B) = \mathrm{rg}_A(M).$$

□

Enfin, pour conclure cette partie, on donne un exemple un peu plus intéressant et inhabituel : considérons le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\sqrt{2}]$. Quel serait l'espace vectoriel obtenu en étendant ses scalaires à $\mathbb{R}$? Comme une base de $\mathbb{Q}(\sqrt{2})$ est $(1, \sqrt{2})$, on aurait envie de dire que $\mathbb{Q}[\sqrt{2}] \bigotimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}$ puisque l'ensemble des combinaisons $x + y\sqrt{2}$ avec $x, y \in \mathbb{R}$ permet d'obtenir tous les réels. Mais il y a une contradiction avec la proposition précédente, car on perd en dimension.

En fait cette démarche est trompeuse : dans $\mathbb{Q}[\sqrt{2}]$, $\sqrt{2}$ ne peut pas être envisagé comme un élément de $\mathbb{R}$. Il vaut mieux considérer la construction $\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[X]/(X^2 - 2)$, ainsi que la proposition suivante.

Proposition 7.2.10. *Soient L/K une extension de corps et $P \in K[X]$. Alors, on a l'isomorphisme de $L[X]$-modules*

$$(K[X]/P) \bigotimes_K L \cong L[X]/P.$$

Cette proposition peut se démontrer en exploitant le fait que le produit tensoriel distribue les sommes directes et respecte les quotients (sous certaines hypothèses). On propose ici une démonstration « avec les mains » qui exploite la propriété universelle.

Démonstration. Pour alléger les notations, on note $I = (P)$ dans l'anneau $K[X]$ et $\tilde{I} = (P)$ dans l'anneau $L[X]$. Ainsi les éléments de $(K[X]/P)$ seront notés $Q(X)+I$ par exemple. Notons de plus $n+1$ le degré de P.

On commence par justifier que $(K[X]/P) \bigotimes_K L$ a bien une structure de $L[X]$-module, via le produit

$$\left(\sum_{i=0}^{d} s_i X^i\right) \cdot (Q(X) + I \otimes s) = \sum_{i=0}^{d} (X^i Q(x) + I) \otimes (s s_i)$$

où $\sum_{i=0}^{d} s_i X^i \in L[X]$, $Q(X) + I \in K[X]/P$, $s \in L$. De plus, par la proposition 7.2.5, $(K[X]/P) \bigotimes_K L$ est engendré par les $(X^i + I \otimes s)_{i \in \{0,\dots,n\},\, s \in L}$. En fait on a même une écriture finie puisque tout élément de $(K[X]/P) \otimes_K L$ s'écrit, avec les $t_{i,s} \in K$ sont tous nuls sauf un nombre fini, sous la forme

$$\sum_{i=0}^{n} \sum_{s \in L} t_{i,s}(X^i + I \otimes s) = \sum_{i=0}^{n} (X^i + I) \otimes s_i,$$

où les s_i valent chacun $\sum_{s \in L} s t_{i,s}$.

Dès lors, on pose l'application

$$F \ : \left| \begin{array}{ccc} K[X]/P \times L & \to & L[X]/P \\ (Q(X) + I, S) & \mapsto & sQ(X) + \tilde{I}. \end{array} \right.$$

Notre F est bien bilinéaire, et on a une factorisation par

$$f : (K[X]/P) \bigotimes_K L \to L[X]/P,$$

avec pour tout $Q(X)+I \in K[X]/P$ et tout $s \in L$

$$f(Q(X)+I\otimes s) = sQ(x)+\tilde{I}.$$

Cette application est bien surjective, puisque pour un $Q(X)=\sum_{i=0}^{d} s_i X^i \in L[X]$ on a

$$\begin{aligned} f\left(\sum_{i=0}^{d})(X^i+I\otimes s_i)\right) &= \sum_{i=0}^{d} f(X^i+I\otimes s_i) \\ &= \sum_{i=0}^{d} F(X^i+I, s_i) \\ &= \sum_{i=0}^{d} (s_i X^i+\tilde{I}) \\ &= Q(X)+\tilde{I}. \end{aligned}$$

L'injectivité demande un peu plus de travail. D'après ce qu'on a dit plus haut, tous les éléments de $(K[X]/P)\bigotimes_K L$ ont une écriture de la forme $\sum_{i=0}^{n}(X^i+I)\otimes s_i$. Supposons donc qu'on a $s_0,...,s_n \in L$ avec

$$f\left(\sum_{i=0}^{n}(X^i+I)\otimes s_i\right) \in \tilde{I} \iff \sum_{i=0}^{n} s_i X^i \in \tilde{I}.$$

C'est le cas si et seulement si on a une écriture $\sum_{i=0}^{n} s_i X^i = Q(X)P(X)$ où $Q(X)\in L[X]$. On note alors $Q(X)=\sum_j u_i X^J$, et $P(X)=\sum_l a_l X^l$ (on exclut les degrés pour alléger). Alors,

$$\sum_{i=0}^{n} s_i X^i = Q(X)P(X) \iff \forall i\ s_i = \sum_{j+l=i} u_j a_l,$$

et on peut donc écrire

$$\begin{aligned} \sum_{i=0}^{n}(X^i+I)\otimes s_i &= \sum_{i=0}^{n}(X^i+I)\otimes \sum_{j+l=i} u_j a_l \\ &= \sum_{j,l}(X^{j+l}+I)\otimes(u_j a_l) \\ &= \sum_{j,l}(a_l X^{j+l}+I)\otimes(u_j) && \text{(car les } a_l \text{ sont dans } K) \\ &= \sum_{j}(P(X)X^j+I)\otimes u_j \\ &= 0. \end{aligned}$$

Ainsi, f est injective, et on a l'isomorphisme de K-modules

$$(K[X]/P)\bigotimes_K L \cong L[X]/P.$$

On vérifie alors sans peine que f est en fait un morphisme de $L[X]$-modules avec la définition donnée plus haut, et on obtient l'isomorphisme souhaité. □

Autrement dit, on résout le problème de $\mathbb{Q}[\sqrt{2}]\cong\mathbb{Q}[X]/(X^2-2)$ de la façon suivante.

Exemple 7.2.3. D'après ce qu'on vient de voir, on a $(\mathbb{Q}[X]/X^2-2) \bigotimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}[X]/(X^2-2)$. On retombe donc bien sur un espace vectoriel de dimension 2.

Terminons cette section par une remarque importante : l'extension des scalaires ne permet pas en général de conserver toutes les propriétés qu'on veut de l'espace vectoriel de départ. Un exemple fondamental est celui de la norme. Reprenons ce qu'on vient de voir.

Exemple 7.2.4. Le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\sqrt{2}]$ peut être muni de la norme induite par valeur absolue (en voyant ses éléments comme des réels) :

$$\left\|a + b\sqrt{2}\right\|_{\mathbb{Q}[\sqrt{2}]} = |a + b\sqrt{2}|.$$

En effet, il est bien connu que $\sqrt{2}$ est irrationnel, ce qui garantit le caractère défini positif de notre norme.

Comme on l'a vu plus haut, $(\mathbb{Q}[X]/X^2-2) \bigotimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}[X]/(X^2-2)$. L'extension naturelle de notre norme serait donc, en notant I l'idéal $(X^2 - 2)$ dans $\mathbb{R}[X]$,

$$\left\|a + bX + I\right\|_{\mathbb{R}[X]/(X^2-2)} = |a + b\sqrt{2}|.$$

Mais on perdrait alors le caractère défini positif de notre norme, puisque a et b sont réels !

Dans la partie suivante, on partira d'un $\mathbb{Q}$-espace vectoriel normé, sur lequel on voudra faire une extension de scalaires pour passer à un $\mathbb{R}$-espace vectoriel. Il faudra donc s'assurer que la norme obtenue soit encore définie positive. Ce point utilisera de façon cruciale le théorème de Northcott.

8
FINITUDE ET BORNE POUR L'ÉQUATION AUX S-UNITÉS

Les dernières briques de la preuve seront posées dans cette partie. En effet après qu'on a préparé tous les outils indispensables au traitement des solutions de notre équation $x + y = 1$, il faut les mettre en oeuvre.

Une première sous-partie 8.1 va plonger les groupes de type fini, comme le sont $\mathcal{O}_{K,S}^{\times}$ et donc $(\mathcal{O}_{K,S}^{\times})^2$, dans un $\mathbb{R}$-espace vectoriel normé. Cette étape permet non seulement d'utiliser des propriétés géométriques sur des espaces vectoriels réels, mais en plus la norme de cet espace est très fortement liée à la hauteur de ses coordonnées.

C'est là où intervient la deuxième sous-partie 8.2 qui établit des inégalités sur la hauteur des solutions de l'équation aux S-unités. Dans cette partie on va exploiter à maintes reprises les résultats d'analyse complexe établis dans la partie 7.1.

Pour finir, la troisième partie 8.3 introduira brièvement des résultats géométriques visuels. Il s'agit plus précisément de résultats de recouvrement de certains domaines d'un espace vectoriel réel par des boules. Ensuite, dans la même partie on retrouve la démonstration finale du théorème de finitude des solutions.

8.1 Géométrisation hauteur-compatible des objets de type fini

Le premier outil qu'on va utiliser du chapitre précédent est l'extension des scalaires 7.2. La mise à profit de cette technique permet de géométriser l'espace de travail et de passer de l'étude de solutions dans un $\mathbb{Z}$-module à l'étude de solutions dans un $\mathbb{R}$-espace vectoriel. Cette nouvelle vision du problème nous est très bénéfique puisqu'on peut profiter des propriétés de volume et de recouvrement sur les $\mathbb{R}$-espaces vectoriels.

Mais ce n'est pas tout. La géométrisation vient avec une norme, qui elle-même est très fortement reliée à la hauteur.

On va procéder en trois étapes. D'abord, on va construire un $\mathbb{Q}$-espace vectoriel à partir de notre groupe H qui est de type fini, en introduisant la $\mathbb{Q}$-*clôture* G de H. Cet espace sera présenté de deux manières différentes : G/T et $G \otimes_{\mathbb{Z}} \mathbb{Q}$. La première construction est plus commode à utiliser pour des démonstrations. En particulier, on utilise cette vision dans la deuxième partie pour établir la norme associée à la hauteur. La seconde construction permet de passer à la troisième étape qui consiste au passage vers un $\mathbb{R}$-espace vectoriel.

8.1.1 • Construction d'un $\mathbb{Q}$-espace vectoriel

Définition 8.1.1 (ℚ-clôture)**.** Soit H un sous-groupe de type fini de $(\mathbb{C}^*)^m$, $m \in \mathbb{N}^*$.

On appelle ℚ-clôture de H le groupe G obtenu en prenant toutes les racines d'éléments de H.

Plus précisément, on pose

$$G = \left\{ a = (a_1, ..., a_m) \in (\mathbb{C}^*)^m \;\middle|\; \exists N \in \mathbb{N}\, a^N = (a_1^N, ..., a_m^N) \in H \right\}.$$

On cherche à obtenir la finitude de l'ensemble des solutions $(x, y) \in G$ (avec borne explicite) pour l'équation

$$x + y = 1.$$

L'intérêt de travailler sur G est qu'en le quotientant par son groupe de torsion, on obtient une structure naturelle de ℚ-espace vectoriel, sur laquelle on peut de plus construire une norme $\|\cdot\|$ issue de la hauteur. Ensuite, on pourra étendre notre corps des scalaires pour passer d'un ℚ-espace vectoriel à un ℝ-espace vectoriel, tout en conservant notre norme. On verra qu'en général l'extension des scalaires n'a aucune raison de conserver la norme (prolongée par continuité), mais que c'est ici le cas. Enfin, nos inégalités numériques sur les hauteurs se réécriront naturellement avec notre norme $\|\cdot\|$. On se sera donc ramené d'un problème sur un groupe à un problème de dénombrement dans un ℝ-espace vectoriel normé, ce qui simplifie grandement la question.

Grâce au théorème des S-unités de Dirichlet, on pourra ensuite prendre pour H le groupe $(\mathcal{O}_{K,S}^\times)^2$ pour K un corps de nombre et obtenir le résultat annoncé en introduction.

Définition 8.1.2. Soient H un sous-groupe de type fini du groupe multiplicatif $(\overline{\mathbb{Q}}^*)^m$, et G sa ℚ-clôture. On peut définir une loi de multiplication externe de $\mathbb{Z}$ sur G :

$$\begin{aligned} \mathbb{Z} \times G &\longrightarrow G \\ (n, g) &\longmapsto g^n. \end{aligned}$$

On notera cette loi simplement ng. On peut la distinguer du produit de G par le fait que l'élément de gauche est un entier qui n'a pas été pris dans G.

Proposition 8.1.1. *Soient H un sous-groupe de type fini de $(\overline{\mathbb{Q}}^*)^m$. On note r son rang sans torsion, et G sa ℚ-clôture.*

Alors, $G \otimes_{\mathbb{Z}} \mathbb{Q}$ est un ℚ-ev de dimension r.

Démonstration. Montrons d'abord que G est un $\mathbb{Z}$-module.

(i) $(G, +_{\mathbb{Z}})$ est un groupe abélien. Ici on note $+_{\mathbb{Z}}$ la loi de composition interne de G pour ne pas la confondre avec la multiplication externe.

(ii) La loi de multiplication externe définie ci-dessus vérifie les propriétés qu'il faut. En effet, soient $x, y \in G$ et $a, b \in \mathbb{Z}$. On a

$$\begin{aligned} a(x +_{\mathbb{Z}} y) &= a(x \cdot_G y) \\ &= (x \cdot_G y)^a \\ &= x^a \cdot_G y^a \\ &= ax +_{\mathbb{Z}} ay \\ (a+b)x &= x^{a+b} \\ &= x^a +_{\mathbb{Z}} x^b \\ &= ax +_{\mathbb{Z}} bx \\ (a \cdot b)x &= x^{ab} \\ &= (x^a)^b \\ &= b(ax) \\ 1x &= x^1 = x. \end{aligned}$$

Puisque G est un $\mathbb{Z}$-module, le produit tensoriel est bien défini.

$G \bigotimes_{\mathbb{Z}} \mathbb{Q}$ est un $\mathbb{Q}$-ev. On note $(h_1, \cdots, h_r)$ une famille de H indépendante sur $\mathbb{Z}$ maximale. Montrons que cette famille génère « quasiment » tous les élèments de H.

Soit $x \in H$. la famille $(x, h_1, \cdots, h_r)$ n'est pas indépendante on dispose donc de $\alpha \in \mathbb{Z}$ et $(\beta_1, \cdots, \beta_r)$ tels que

$$\prod_i h_i^{\beta_i} = x^{\alpha}.$$

- Montrons que $(h_1 \otimes 1, \cdots, h_r \otimes 1)$ génère les éléments de la forme $g \otimes q$ pour $g \in G$ et $q \in \mathbb{Q}$, qui eux génèrent $G \bigotimes_{\mathbb{Z}} \mathbb{Q}$.
  Soit $N \in \mathbb{N}$ tel que $g^N \in H$. On va passer dans $G \bigotimes_{\mathbb{Z}} \mathbb{Q}$ et on va donc utiliser la loi de multiplication externe qu'on a définie. Alors $g \otimes q = g^N \otimes \frac{q}{N}$.
  Soient donc $M \in \mathbb{Z}$ et les coefficients $(\alpha_1, \cdots, \alpha_r)$ tels que $\prod_i h_i^{\alpha_i} = (g^N)^M$.
  Ainsi $g \otimes q = \frac{q}{MN} \sum_i h_i^{\alpha_i} \otimes 1$.
  La famille $(h_1 \otimes 1, \cdots, h_r \otimes 1)$ est donc une famille génératrice de $G \bigotimes_{\mathbb{Z}} \mathbb{Q}$.
- Montrons que $(h_1 \otimes 1, \cdots, h_r \otimes 1)$ es libre dans $G \bigotimes_{\mathbb{Z}} \mathbb{Q}$.
  Soit $(\alpha_1, \cdots, \alpha_r)$ tels que $\sum_i h_i^{\alpha_i} \otimes 1 = 1$.
  Passons dans H : $\prod_i h_i^{\alpha_i} = e_H$ et donc tous les α_i sont nuls par hypothèse d'indépendance de la famille considérée.

On déduit donc que $G \bigotimes_{\mathbb{Z}} \mathbb{Q}$ est un $\mathbb{Q}$-ev de dimension r. □

Définition 8.1.3. Soient G un groupe et $x \in G$.
On dit que x est de torsion lorsque x est d'ordre fini dans G.

Définition 8.1.4. Soit G un groupe.

On appelle *groupe de torsion* de G le sous-groupe de G composé des éléments de torsion.

Si cet ensemble est réduit à l'identité de G, on dit que G est *sans torsion*, ou de manière équivalente que G est *libre*.

Proposition 8.1.2. *Soient H un sous-groupe de type fini de $(\overline{\mathbb{Q}}^*)^m$ et r son rang sans torsion. Soient G la $\mathbb{Q}$-clôture de H et T le groupe torsion de G.*

Alors, G/T a une structure de $\mathbb{Q}$-espace vectoriel de dimension r.

Ainsi, on a $G/T \cong G \bigotimes_{\mathbb{Z}} \mathbb{Q}$.

Démonstration. L'opération $+_{\mathbb{Q}}$ est définie dans comme l'opération $\cdot$ de G/T, et $a._{\mathbb{Q}} g := g^a$. Notons que les puissances rationnelles ont un sens puisqu'on a quotienté par le sous-groupe T des racines de l'unité et que G est une $\mathbb{Q}$-clôture. On va indiquer au début en indice à quel espace correspond chaque opération. Mais on ne va pas garder cette notation longtemps pour éviter d'alourdir le passage.

(i) $(G/T, +_{\mathbb{Q}}) = (G/T, \cdot_{G/T})$ est un groupe abélien (puisque G est un groupe abélien et T est un sous-groupe).

(ii) Le neutre $e_{G/T}$ fait office de neutre pour l'addition : $\forall g \in G/T, g + e = g \cdot e = g$,

(iii) $\forall a \in \mathbb{Q}\, \forall g_1, g_2 \in G/T\; a.g_1 + a.g_2 = g_1^a \cdot g_2^a = a.(g_1 + g_2)$,

(iv) $\forall a, b \in \mathbb{Q}\, \forall g \in G/T\; a.g + b.g = g^a \cdot g^b = g^{a+b} = (a+b).g$,

(v) $\forall a, b \in \mathbb{Q}\, \forall g \in G/T\; a.(b.g) = (g^b)^a = (a.b).g$,

(vi) $\forall g \in G/T\; 1.g = g^1 = g$,

donc G/T est bien un $\mathbb{Q}$-espace vectoriel. Trouvons la dimension de cet espace.
Soit $(h_1, \cdots, h_r)$ une famille de représentants d'une famille de H indépendante sur $\mathbb{Z}$ maximale.
Montrons que cette famille génère « quasiment » tous les éléments de H.
Soit $x \in H$. la famille $(x, h_1, \cdots, h_r)$ n'est pas indépendante on dispose donc de $\alpha \in \mathbb{Z}$ et $(\beta_1, \cdots, \beta_r)$ tels que :

$$\prod_i h_i^{\beta_i} = x^\alpha$$

C'est ce qu'on appelle donc générer « quasiment » les éléments de H.

Montrons que cette famille est génératrice de G/T comme $\mathbb{Q}$-ev :
Soient $g \in G$ et $N, M \in \mathbb{N}$ tel que $g^N \in H$ et $(g^N)^M$ qui s'écrit comme puissances entières des h_i.
On dispose de $(\alpha_1, \cdots, \alpha_r)$ tels que $\sum_i \alpha_i h_i = NMg$ Et donc $\sum_i \frac{\alpha_i}{MN} h_i = g$.
Montrons maintenant que cette famille est libre :
Soit $(\alpha_1, \cdots, \alpha_r) \in \mathbb{Q}^r$ tels que $\sum_i \alpha_i h_i = e$
En multipliant par le ppcm des dénominateurs on obtient $(\beta_1, \cdots, \beta_r) \in \mathbb{Z}^r$ tels que $\sum_i \alpha_i h_i = e$
Et donc en passant dans G : $\prod_i h_i^{\beta_i} \in T$. On dispose donc de $N_0 \in \mathbb{N}^*$ tel que

$$\prod_i h_i^{N_0 \beta_i} = e$$

Et donc par liberté de la famille $(h_1, \cdots, h_r)$ dans H(On confond ici la famille avec son système de représentants), on déduit que $(\alpha_1, \cdots, \alpha_r) = (0, \cdots, 0)$.
Et donc la famille $(h_1, \cdots, h_r)$ est libre dans G/T.
Ainsi, G/T est un $\mathbb{Q}$-ev de dimension r. □

8.1.2 • Une norme issue de la hauteur

Pour construire notre norme, on va utiliser l'expression de la hauteur logarithmique. Pour montrer que notre norme est bien séparante, on aura besoin du lemme suivant :

Proposition 8.1.3. *Soit K un corps de nombres. Soit $x \in K$.*
x est une racine de l'unité si et seulement si $\forall v \in \mathcal{M}_K$, $|x|_v = 1$.

Démonstration.
Le sens direct est facile. Soit x une racine de l'unité, disons $x^m = 1$. Notons $\sigma_1, ..., \sigma_n$ les plongements $K \hookrightarrow \mathbb{C}$. Alors :

- Pour tout $i \in \{1, ..., n\}$, $|\sigma_i(x)|^m = |\sigma_i(x^m)| = 1$, donc $|\sigma_i(x)| = 1$. Cela garantit que $|x|_v = 1$ pour les places archimédiennes.
- En vertu de 3.2.34, on sait que pour tout $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ on a $v_\mathfrak{p}(x) = 0$. Cela garantit que $|x|_v = 1$ pour les places ultramétriques.

Réciproquement soit $x \in K$ avec $\forall v \in \mathcal{M}_K$, $|x|_v = 1$.

- On sait en regardant les places ultramétriques que pour tout $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ on a $v_\mathfrak{p}(x) = 0$. Par la proposition 3.2.34, on sait donc que $x \in \mathcal{O}_K^\times$.
- Pour vérifier que x est une racine de l'unité, on pose $E = \{1, x, x^2, ...\}$. En regardant les places archimédiennes, on peut affirmer que pour tout i, $|\sigma_i(x)| = 1$. En particulier, pour tout $j \in \mathbb{N}$ on a $|\sigma_i(x^j)| = 1$. On peut donc appliquer la proposition 2.2.5 à $E \subset \mathcal{O}_K$ et obtenir qu'il est fini. En particulier, cela dit qu'on a $n > m$ tels que $x^n = x^m$. Or x est inversible, et on obtient $x^{n-m} = 1$. Ainsi x est bien une racine de l'unité.

□

Proposition 8.1.4 (Norme sur $G \otimes_\mathbb{Z} \mathbb{Q}$)**.**
Soit G la $\mathbb{Q}$-clôture d'un groupe de type fini $H \subset (\overline{\mathbb{Q}}^*)^m$.
On note $h(x) = \ln H(x)$ la hauteur logarithmique, et r le rang sans torsion de H.
Alors, $\|(x_1, ..., x_m)\| = \max_{i=1}^m h(x_i)$ induit une norme sur $G \otimes_\mathbb{Z} \mathbb{Q}$ en tant que $\mathbb{Q}$-ev.

Démonstration.
Écrivons la formule explicite pour la norme d'un élément.
On dispose d'une $\mathbb{Q}$-base de $G/T \cong \otimes_\mathbb{Z} \mathbb{Q}$, composée des $a_i = (a_{i,1}, ..., a_{i,m})$ pour $i \in [\![1, r]\!]$.
Tout élément de G s'écrit donc, modulo des racines de l'unité, sous la forme

$$x = (x_1, ..., x_m) = \left(\prod_{i=1}^r a_{i,j}^{e_i} \right)_{1 \leq j \leq m},$$

avec les $e_i \in \mathbb{Q}$.
Rappelons une expression de la théorie des hauteurs. Comme on l'a vu à la proposition 6.2.4 puis en généralisant aux hauteurs absolues, pour tout $a \in \overline{\mathbb{Q}}$ et pour tout corps de nombre K contenant a, en notant $n = [K : \mathbb{Q}]$ puis, pour tout $v \in \mathcal{M}_K$, $n_v = [K_v : \mathbb{Q}_v]$, on a

$$h(a) = \frac{1}{2n} \sum_{v \in \mathcal{M}_K} n_v \Big| \ln |a|_v \Big|.$$

Pour utiliser cette formule de la hauteur pour un élément $x \in G$, on prend un corps de nombre K contenant toutes les coordonnées $x_j \in \overline{\mathbb{Q}}$ de x. Avec les n, n_v associés à K, on a alors

$$\|x\| = \max_{1 \leq j \leq m} \frac{1}{2n} \sum_{v \in \mathcal{M}_K} n_v \Big| \sum_{i=1}^{r} e_i \ln |a_{i,j}|_v \Big|.$$

- Remarquons que $\|\cdot\|$ passe au quotient sur G/T : en effet, un élément $x \in G/T$ est défini à une racine de l'unité près, et ses représentants ont donc tous la même hauteur.
- Montrons maintenant que $\|\cdot\|$ induit bien une norme sur G/T.
  - Pour tout $x \in G/T$, on a bien $\|x\| \geq 0$.
  - Soient $x, y \in G/T$.
    On choisit deux représentants quelconques de x et y de coordonnées $\prod_j a_{i,j}^{e_{x,i}}$ et $\prod_j a_{i,j}^{e_{y,i}}$, avec $1 \leq j \leq m$ et les exposants dans $\mathbb{Q}$.
    On se munit de plus d'un corps de nombre K contenant toutes ces coordonnées, et on écrit n et n_v les degrés associés à K. On a alors

$$\begin{aligned}
\|x+y\| &= \max_{1 \leq j \leq m} \frac{1}{2n} \sum_{v \in \mathcal{M}_K} n_v \Big| \sum_{i=1}^{r} (e_{x,i} + e_{y,i}) \ln |a_{i,j}|_v \Big| \\
&\leq \max_{1 \leq j \leq m} \frac{1}{2n} \sum_{v \in \mathcal{M}_K} n_v \Big| \sum_{i=1}^{r} (e_{x,i}) \ln |a_{i,j}|_v \Big| + \frac{1}{2n} \sum_{v \in \mathcal{M}_K} \Big| \sum_{i=1}^{r} (e_{y,i}) \ln |a_{i,j}|_v \Big| \\
&\leq \max_{1 \leq j \leq m} \frac{1}{2n} \sum_{v \in \mathcal{M}_K} n_v \Big| \sum_{i=1}^{r} (e_{x,i}) \ln |a_{i,j}|_v \Big| + \max_{1 \leq j \leq m} \frac{1}{2n} \sum_{v \in \mathcal{M}_K} n_v \Big| \sum_{i=1}^{r} (e_{y,i}) \ln |a_{i,j}|_v \Big| \\
&\leq \|x\| + \|y\|.
\end{aligned}$$

  - Soit $x \in G/T$.
    Encore une fois, on se donne un représentant de x de coordonnées $x_j = \prod_j a_{i,j}^{e_i} \in \overline{\mathbb{Q}}$, avec $1 \leq j \leq m$ et les exposants dans $\mathbb{Q}$.
    On se munit d'un corps de nombre K contenant toutes ces coordonnées, et on écrit n et n_v les degrés associés à K. On a alors les implications

$$\begin{aligned}
\|x\| = 0 &\implies \forall v \in \mathcal{M}_K \, \forall j \in [\![1, m]\!], \ \sum_{i=1}^{r} e_i \ln |a_{i,j}|_v = 0 \\
&\implies \forall v \in \mathcal{M}_K \, \forall j \in [\![1, m]\!], \ \ln |x_j|_v = 0 \\
&\implies \forall j \in [\![1, m]\!] \, \forall v \in \mathcal{M}_K, \ |x_j|_v = 1 \\
&\implies \forall j \in [\![1, m]\!], \ x_j \text{ est une racine de l'unité} \quad \text{en vertu de la proposition 8.1.3} \\
&\implies x = 1_{G/T}.
\end{aligned}$$

$\|\cdot\|$ est donc bien une norme sur $G \bigotimes_{\mathbb{Z}} \mathbb{Q}$.

□

8.1.3 • Complétion en un $\mathbb{R}$-espace vectoriel

Il s'agit maintenant d'étendre notre espace en un $\mathbb{R}$-ev. Pour ce faire, il suffit d'étendre les scalaires à $\mathbb{R}$ comme expliqué plus haut. Il faut néanmoins vérifier qu'on peut prolonger notre norme sur cet espace.

Proposition 8.1.5. *$\|\cdot\|$ peut être prolongée en une norme sur $G \bigotimes_{\mathbb{Z}} \mathbb{R}$.*

Démonstration.

- Commençons par définir $\|\cdot\|$ sur $G \bigotimes_{\mathbb{Z}} \mathbb{R}$.
  On se munit à nouveau d'une base du $\mathbb{Q}$-espace vectoriel $G \bigotimes_{\mathbb{Z}} \mathbb{Q}$, composée des r éléments $a_i \otimes 1 = (a_{i,1}, ..., a_{i,m}) \otimes 1$. Cette famille est clairement une $\mathbb{R}$-base de $G \bigotimes_{\mathbb{Z}} \mathbb{R}$.
  Tout élément de $x \in G \bigotimes_{\mathbb{Z}} \mathbb{R}$ s'écrit donc sous la forme $x = \sum_{i=1}^{r} (a_{i,1}, ..., a_{i,m}) \otimes e_i$, avec les $e_i \in \mathbb{R}$.
  En posant $K = \mathbb{Q}[(a_{i,j})]$ le corps de nombres engendré par tous les $a_{i,j}$, et en notant n, n_v les degrés associés à K, on a déjà démontré l'expression

$$\|x\| = \max_{1 \le j \le m} \frac{1}{2n} \sum_{v \in \mathcal{M}_K} n_v \Big| \sum_{i=1}^{r} e_i \ln |a_{i,j}|_v \Big|$$

  dans le cas où les $e_i \in \mathbb{Q}$.
  On peut définir $\|\cdot\|$ sur $G \bigotimes_{\mathbb{Z}} \mathbb{R}$ par cette expression, de sorte qu'elle reste vérifiée (par définition) avec les $e_i \in \mathbb{R}$.
- Montrons maintenant que $\|\cdot\|$ reste une norme après avoir été étendue.
  Elle reste positive et vérifie l'inégalité triangulaire. Il n'y a donc qu'à montrer que $\|\cdot\|$ reste définie positive.
  Pour cela on s'appuie sur le lemme suivant, qui utilise le théorème de Northcott (17).

  Lemme 8.1.1. *Soit*

$$X = \left\{ \sum_{i=1}^{r} (a_{i,1}, ..., a_{i,m}) \otimes e_i \,\middle|\, \forall i \, e_i \in \mathbb{Z} \right\}$$

  l'ensemble des éléments de $G \bigotimes_{\mathbb{Z}} \mathbb{R}$ qui s'exprime avec des e_i dans $\mathbb{Z}$.
  Autrement dit, si on pose $K = \mathbb{Q}[(a_{i,j})]$ le corps de nombre engendré par tous les $a_{i,j}$, alors X est l'ensemble des éléments de $G \bigotimes_{\mathbb{Z}} \mathbb{Q} \cong G/T$ qui admettent un représentant dont toutes les coordonnées sont dans K.
  On dit qu'un élément $x \in G \bigotimes_{\mathbb{Z}} \mathbb{R}$ est non trivial s'il est non nul ***dans le groupe additif*** *$G \bigotimes_{\mathbb{Z}} \mathbb{R}$.*
  Ces notations étant posées, le résultat est ce qui suit.
  On dispose d'une constante *$\mu > 0$* ***telle que*** *$\forall x \in X$* ***non trivial,*** *$\|x\| \ge \mu$.*

Démonstration du lemme.

- Comme dans l'énoncé, on pose $K = \mathbb{Q}[(a_{i,j})]$ et n, n_v les degrés associés.
  Soit $a_0 \in K$ tel que $h(a_0) \neq 0$, (par exemple $a_0 = 2$). Notons $M = h(a_0)$.
  D'après le théorème de Northcott, l'ensemble

$$\left\{a \in K \,\|\, 0 < h(a) \leq M\right\}$$

  est fini. Comme il contient a_0, il est de plus non-vide.
  On note μ le minimum des hauteurs des éléments de cet ensemble fini non vide, et on a $\mu > 0$.
- Soit maintenant $x \in X \subset G/T$ non trivial, et $x_1, ..., x_m \in K$ les coordonnées d'un de ses représentants dans G.
  Supposons par l'absurde que $\|x\| < \mu$.
  Cela implique que

$$\forall j \in [\![1, m]\!]\ h(x_j) < \mu,$$

  puis par minimalité que

$$\forall j \in [\![1, m]\!]\ h(x_j) = 0.$$

  Par un raisonnement qu'on a déjà fait dans la partie précédente, cela implique que tous les x_j sont des racines de l'unité.
  Autrement dit, $(x_1, ..., x_m) \in T$, d'où x trivial dans G/T : **contradiction**.

On dispose donc bien de $\mu > 0$ tel que $\forall x \in X$ non trivial, $\|x\| \geq \mu$.

□

- On peut maintenant appliquer ce lemme pour vérifier que $\|\cdot\|$ est toujours définie positive.
  Supposons par l'absurde que la norme ne soit pas définie positive et soit donc $e \in \mathbb{R}^r$ tel que $x := \sum a_i \otimes e_i \neq 0$ avec $\|x\| = 0$. En particulier, on a $e \neq 0$.
  Comme plus tôt, on pose $K = [(a_{i,j}]$ et n, n_v les degrés associés.
  Comme $\|x\| = 0$, on a

$$\max_{1 \leq j \leq m} \frac{1}{2n} \sum_{v \in \mathcal{M}_K} n_v \Big| \sum_{i=1}^{r} e_i \ln |a_{i,j}|_v \Big| = 0,$$

  d'où

$$\forall v\, \forall j \in [\![1, m]\!] \sum_{i=1}^{r} e_i \ln |a_{i,j}|_v = 0.$$

  De plus, on peut écrire la même égalité pour tous les $x^n = 1$ avec $n \in \mathbb{N}$, et donc pour toute famille $(ne_1, ..., ne_r)$ pour $n \in \mathbb{N}$.
  On va maintenant tirer partie du fait que cette relation est vérifiée pour une infinité de familles, pour exhiber une famille de coefficients entiers qui contredit la minoration obtenue dans le lemme précédent.

Soit $\delta > 0$ tel que

$$\forall j \ \frac{\delta}{2n} \sum_v n_v \Big| \sum_{i=1}^{r} \ln |a_{i,j}|_v \Big| < \mu.$$

On peut imposer que $\delta \in]0,1[$.

Le principe des tiroirs de Dirichlet nous fournit l'existence de $e', e'' \in e\mathbb{Z}^* \subset \mathbb{R}^r$ distincts tels que

$$\forall i \in [\![1, r]\!] \ \Big|(\mathrm{Id} - E)(e'_i - e''_i)\Big| \leq \delta,$$

où E est la fonction partie entière. $(\mathrm{Id} - E)$ est la fonction qui renvoie la partie décimale d'un nombre, à valeurs dans $[0,1[$.

Pour voir ça, il suffit subdiviser le cube $[0,1]^r$ en petit cubes de côtés plus petit que δ chacun. Il y a un nombre fini de tels cubes. Or, pour vérifier cette propriété, il suffit de trouver deux vecteurs e', e'' distincts tels que les vecteurs $((\mathrm{Id} - E)(e'_i))$ et $((\mathrm{Id} - E)(e'_i))$ soient dans le même cube. Le principe des tiroirs permet de conclure : on dispose de tels vecteurs $e', e'' \in e\mathbb{Z}^*$ distincts.

Puisque $\| \sum_i a_i \otimes e'_i \| = \| \sum_i a_i \otimes e''_i \| = 0$, en notant $d = e' - e'' \in e\mathbb{Z}^*$, on a $\| \sum_i a_i \otimes d_i \| = 0$.

En fait, quitte à prendre $e' = n' \cdot e$ et $e'' = n'' \cdot e$ avec $n'' \gg n'$, on peut imposer qu'un des $E(d_i)$ soit non nul (puisque un des e_i est non nul).

On en déduit que

$$\begin{aligned}
\frac{1}{2n} \sum_v n_v \Big| \sum_{i=1}^{r} E(d_i) \ln |a_{i,j}|_v \Big| &\leq \frac{1}{2n} \sum_v n_v \left(\Big| \sum_{i=1}^{r} d_i \ln |a_{i,j}|_v \Big| + \Big| \sum_{i=1}^{r} (Id - E)(d_i) \ln |a_{i,j}|_v \Big| \right) \\
&\leq \frac{1}{2n} \left(0 + \delta \sum_v n_v \sum_{i=1}^{r} \Big| \ln |a_{i,j}|_v \Big| \right) \\
&< \mu.
\end{aligned}$$

D'après le lemme précédent, cela implique que

$$\sum_i a_i \otimes E(d_i) = 0_{G \bigotimes \mathbb{Q}}.$$

Comme le produit tensoriel se fait sur $\mathbb{Z}$, on peut réécrire ceci sous la forme

$$\sum_i E(d_i) \cdot (a_i \otimes 1) = 0_{G \bigotimes \mathbb{Q}}.$$

Or, la famille des $(a_i \otimes 1)$ est une base de $G \bigotimes_{\mathbb{Z}} \mathbb{Q}$. Cela implique que $\forall i \, E(d_i) = 0$.

On a pourtant construit le vecteur $(E(d_i))$ pour qu'il soit non nul : **contradiction**.

On peut conclure : la norme prolongée sur $\mathbb{R}$ reste définie positive, et reste donc bien une norme. □

8.2 Analyse par la hauteur de la forme de l'équation

Le problème ayant maintenant été géométrisé de façon compatible avec la hauteur, on va ici analyser la structure de l'équation aux S-unités sous l'angle de la hauteur. On va procéder en deux temps.

Tout d'abord on commence par expliciter des inégalités numériques sur la hauteur des solutions. Cette sous-partie est assez longue et s'appuie sur des résultats d'analyse complexe 7.1, dont le très puissant théorème de Puiseux 18. À la fin de cette étape on aura obtenu trois inégalités sur les hauteurs.

Ensuite on va simplement traduire les inégalités obtenues sur les hauteurs en terme de la distance associée à l'espace vectoriel qu'on a déjà construit.

On s'appuie principalement sur l'article de F.Beukers et H.P.Schlickewei [2].

8.2.1 • Inégalités numériques

Cette sous-partie s'attèle à obtenir des inégalités numériques, qui seront ensuite interprétées géométriquement dans la sous-partie suivante (8.2.2). Présentons rapidement ces résultats.

- Pour pouvoir étudier la « complexité » des solutions d'une équation en plusieurs variables, on commence par étendre en 8.2.1 notre définition de la hauteur à $(\overline{\mathbb{Q}}^*)^N$.
- Dans les propositions 8.2.3 et 8.2.4, on analyse la structure d'équations similaires à celle qui nous intéresse.

  Les propositions 8.2.8 et 8.2.9 traduiront ceci géométriquement, en estimant le rapport des normes de deux solutions « assez éloignées » et « dans un même cône ».
- La proposition 8.2.5 est la plus importante : elle sera interprétée à la proposition 8.2.10 comme exprimant le fait que deux solutions ne peuvent pas être « trop proches ».

  C'est donc sur elle que reposent le résultat de finitude et la borne obtenue, destinations finale de cet ouvrage.
- Cette proposition est en fait un beau corollaire du théorème 20, qui est issu d'un article de Beukers et D.Zagier [7].

  Après avoir nommé les hypothèses utiles aux définitions 8.2.3 et 8.2.4, on énonce ce théorème très fort : les zéros « non-singuliers » d'un polynôme « multihomogène » ont une « complexité » (au sens de la hauteur) *minorée* par la « complexité » (en un sens que le théorème introduit) de ce polynôme.

Comme nous le disions, nous allons avoir besoin d'une hauteur à plusieurs variables pour analyser nos équations.

Définition 8.2.1 (Hauteur à plusieurs variables)**.** Pour tous $N \in \mathbb{N}^*$ et $x_0, ..., x_N \in \overline{\mathbb{Q}}^*$, on pose

$$H(x_0, ..., x_N) = \prod_{v \in M_K} \max\left(|x_0|_v, ..., |x_N|_v\right)^{\frac{n_v}{n}},$$

où K est un corps de nombre contenant les $x_0, ..., x_N$, M_K est l'ensemble de ses valeurs absolues standard, $n = [K : \mathbb{Q}]$ et $n_v = [K_v : \mathbb{Q}_v]$.

On peut remarquer que cette définition est très similaire à celle de 6.2.5, et on montre de la même manière (par la propriété 5.2.5) que H est bien définie et indépendante du corps de base.

En fait, on vient de définir une extension à cette définition.

Proposition 8.2.1. *Soit $\alpha \in \overline{\mathbb{Q}}^*$. Alors,*

$$H(1, \alpha) = H(\alpha).$$

On peut par ailleurs remarquer une conséquence de la formule du produit.

Proposition 8.2.2. *Soient $N \in \mathbb{N}^*$ un entier et K un corps de nombre.*
Pour tous $x_0, ..., x_N \in K^*$ et $\lambda \in K^*$, on a

$$H(\lambda x_0, ..., \lambda x_N) = H(x_0, ..., x_N).$$

Ainsi, H définit en fait une hauteur sur l'espace projectif $\mathbb{P}^N(K)$ (mais on n'aura pas besoin ici de ce point de vue).

Cet outil étant introduit, on peut commencer à analyser la forme de l'équation aux S-unités sous l'angle de la hauteur, à travers l'étude d'équations analogues.

La prochaine proposition permettra plus tard de montrer que des points « assez éloignés » d'un « même cône » ont des normes « suffisamment différentes ».

Proposition 8.2.3. *Soient $a, a', b, b', A, B \in \overline{\mathbb{Q}^*}$ et $c, c' \in \overline{\mathbb{Q}}$ tels que $ab' \neq a'b$ et*

$$aA + bB = c, \quad a'A + b'B = c'.$$

Alors,

$$H(A, B, 1) \leq 2H(a, b, c)H(a', b', c').$$

Dans le cas particulier où $a' = b' = c' = c = 1$, c'est à dire où

$$aA + bB = 1, \quad A + B = 1,$$

on obtient

$$H(A, B, 1) \leq 2H(a, b, 1).$$

Démonstration. Soit K un corps de nombre contenant a, a', b, b', A, B.

Pour chaque valeur absolue standard v de K, on pose

$$r_v = \begin{cases} 2 & \text{si } v \text{ est archimédienne,} \\ 1 & \text{si } v \text{ est ultramétrique.} \end{cases}$$

On vérifie alors que, avec $\Delta = a'b - ab'$, on a $A = \frac{bc'-b'c}{\Delta}$ et $B = \frac{a'c-ac'}{\Delta}$. En effet,

$$bc' - b'c = b(a'A + b'B) - b'(aA + bB) = A(ba' - b'a) = A\Delta,$$

puis on en déduit le résultat pour B par symétrie de a, a', A et b, b', B.

Ainsi,

$$\begin{aligned} H(A, B, 1) &= H(bc' - b'c, a'c - ac', a'b - ab') \\ &= \prod_v \max\left(|bc' - b'c|_v, |a'c - ac'|_v, |a'b - ab'|_v\right)^{n_v/n}, \end{aligned}$$

ce qui donne avec les inégalités triangulaires et ultramétriques que

$$\begin{aligned} H(A, B, 1) &\leq \prod_v \left(r_v \max(|bc'|_v, |b'c|_v, |a'c|_v, |ac'|_v, |a'b|_v, |ab'|_v)\right)^{n_v/n} \\ &\leq \prod_v \left(r_v \max(|a|_v, |b|_v, |c|_v) \max(|a'|_v, |b'|_v, |c'|_v)\right)^{n_v/n} \\ &= 2H(a, b, c)H(a', b', c'), \end{aligned}$$

où l'on a utilisé $\sum_{v \in M_K^\infty} n_v = n$ pour faire apparaître le 2 à la dernière ligne. □

Au contraire, la prochaine proposition servira plus tard à montrer que des points « assez éloignés » d'un « même cône » ont des normes « plutôt similaires ».

Proposition 8.2.4. *Soient $a, b, A, B \in \overline{\mathbb{Q}^*}$ et $\rho \in \mathbb{N}$ tels que*

$$A + B = 1, \quad aA^{2\rho} + bB^{2\rho} = 1.$$

Alors,

$$H(A, B, 1) \leq 2^{1/\rho} c H(a, b, 1)^{1/\rho},$$

où $c = 6\sqrt{3}$.

La preuve de cette proposition repose sur l'existence de 3 polynômes vérifiant certaines propriétés. Leur construction se fait par le calcul et n'est pas très éclairante : on laisse le lecteur intéressé lire leur construction aux lemmes 1 à 6 de l'article de F.Beukers et R.Tijdeman [30]. Nous admettons ici qu'on peut faire cette construction.

Démonstration. On admet qu'on peut se munir de trois polynômes Q_ρ, P_ρ, R_ρ de degré inférieur à ρ tels que

- $\forall z \in \mathbb{C}\ z^{2\rho}P_\rho(z) + (1-z)^{2\rho}Q_\rho(z) = R_\rho(z)$,
- $bP_\rho(A) \neq aQ_\rho(A)$,
- $H(P_\rho(A), Q_\rho(A), R_\rho(A)) \leq (6\sqrt{3})^\rho H(A)^\rho$.

Remplaçons z par A dans l'égalité entre les polynômes. Cela nous donne

$$A^{2\rho}P_\rho(A) + B^{2\rho}Q_\rho(A) = R_\rho(A).$$

Or, par hypothèse

$$aA^{2\rho} + bB^{2\rho} = 1,$$

donc en appliquant la propriété 8.2.3 avec $A^{2\rho}, B^{2\rho}$ au lieu de A, B et $c = 1, a' = P_\rho(A), b' = Q_\rho(A), c' = R_\rho(A)$, on obtient

$$\begin{aligned} H(A,B,1)^{2\rho} &\leq 2H(a,b,1)H(P_\rho(A), Q_\rho(A), R_\rho(A)) \\ &\leq 2c^\rho H(a,b,1)H(A)^\rho \\ &\leq 2c^\rho H(a,b,1)H(A,B,1)^\rho. \end{aligned}$$

Il ne reste alors plus qu'à diviser par $H(A,B,1)^\rho$ puis prendre la racine ρ-ème. □

On va maintenant aboutir au puissant théorème de cette partie, issue de l'article de F. Beukers et D. Zagier [7], et qui fournit le corollaire qui fait tenir toute la preuve de Buekers et Schlikewei [2].

Avant de l'énoncé, il nous faut en définir les termes.

Définition 8.2.2. Soient N et M deux entiers. On note $\mathbb{Z}[X_{i,j}]$ l'ensemble des polynômes à coefficients dans $\mathbb{Z}$ en les indéterminées $X_{i,j}$ où $0 \leq i \leq N$ et $0 \leq j \leq M$.

Pour un polynôme $F \in \mathbb{Z}[X_{i,j}]$ et pour tout (i,j), on note $d_{i,j}$ le degré de F en l'indéterminée $X_{i,j}$.

De plus, si on se donne un vecteur $(x_{i,j})$, on notera x_i le vecteur $(x_{i,0}, ..., x_{i,M})$. On s'autorisera aussi à noter $F(X_0, ..., X_N)$ notre polynôme, avec donc les vecteurs d'indéterminées $X_i = (X_{i,0}, ..., X_{i,M})$.

Dans ce contexte où certaines variables sont regroupées, on généralise la notion de polynôme homogène.

Définition 8.2.3 (Polynôme multihomogène)**.** Soit F un polynôme de $\mathbb{Z}[X_{i,j}]$. On dit que F est multihomogène s'il existe $d_0, d_1, ..., d_N \in \mathbb{N}$ tels que pour tout $i \in [\![0, N]\!]$

$$\forall \lambda \in \mathbb{R}\ F(X_0, ..., X_{i-1}, \lambda X_i, X_{i+1}, ..., X_N) = \lambda^{d_i} F(X_0, ..., X_N),$$

où on insiste sur le fait que X_i est le vecteur d'indéterminées $(X_{i,0}, ..., X_{i,M})$. On dira alors que F est multihomogène de multidegrés $d_0, ..., d_N$ en $X_0, ..., X_N$.

Exemple 8.2.1. Le polynôme $P(X,Y,Z,T) = X^2YZ + XY^2Z + X^3T$ est multihomogène de multidegré 3 en (X,Y) et multidegré 1 en (Z,T).

On donne maintenant un nom à l'hypothèse nécessaire à l'application du théorème. Notons que ce vocabulaire est personnel et non standard.

Définition 8.2.4 (Zéro inversible)**.** Soient $N, M \in \mathbb{N}^*$, $F \in \mathbb{Z}[X_{i,j}]$ et $x \in \overline{\mathbb{Q}}^{N\times M}$. On dit que x est un *zéro inversible de* F si

(i) x est un zéro de F : $F(x) = F\Big((x_{i,j})_{(i,j)\in[\![1,N]\!]\times[\![1,M]\!]}\Big) = 0$,

(ii) Toutes les coordonnées de x sont non nulles : $\forall i,j\ x_{i,j} \neq 0$,

(iii) F ne s'annule pas en x^{-1} : $F(x^{-1}) = F\Big((x_{i,j}^{-1})_{(i,j)\in[\![1,N]\!]\times[\![1,M]\!]}\Big) \neq 0$.

Passons enfin au théorème lui-même. Il s'énonce pour trois points ayants trois coordonnées chacun : $N = M = 2$.

On en a réduit l'énoncé, en omettant la notion d'espace projectif et en imposant cette restriction $N = M = 2$. On y gagne un théorème plus proche de son corollaire et une démonstration plus élémentaire, au prix d'une perte en généralité et d'un moindre recul conceptuel.

Intuitivement, tout zéro inversible du polynôme multihomogène est au moins aussi complexe que ce polynôme. Exprimons ceci plus précisément.

Théorème 20. *Soit $F \in \mathbb{Z}[X_{i,j}]$ un polynôme* multihomogène *où $0 \leq i,j \leq 2$ (il s'exprime donc en 9 indéterminées).*

Alors, pour tout $x = (x_0, x_1, x_2) \in \overline{\mathbb{Q}}^{3\times 3}$ zéro inversible *de F,*

$$H(x_0)^3 H(x_1)^3 H(x_2)^3 \geq \rho,$$

où ρ est l'unique racine réelle supérieure à 1 de l'équation

$$\rho^{-2} + c_F^{-1}\rho^{-\delta} = 1,$$

$$\text{où } c_F = \max_{i,j} \left\| \frac{\partial F}{\partial X_{i,j}} \right\| \text{ et } \delta = \max_i \frac{-d_i + \sum_j d_{i,j}}{3} = \max_i \frac{\tilde{d}_i}{3},$$

$\|\cdot\|$ *étant la somme des valeurs absolues des coefficients du polynôme.*

Démonstration. La démonstration de ce théorème s'appuie sur trois lemmes.

- Au lemme 8.2.1, on montre tout d'abord un résultat plus fort : étant donnée une famille pondérée de polynômes $(v^{(k)}, G^{(k)})$ qui n'annulent pas x, on peut minorer une « hauteur pondérée » de x par la quantité $\exp(-\max \Phi(x'))$, où Φ est une quantité qui ne dépend que de la famille $(v^{(k)}, G^{(k)})$, et où x' parcourt les « petits zéros complexes de F ».

- Ensuite, au lemme 8.2.2, par un argument d'analyse complexe, on constate que Φ atteint bien son max, et le fait sur les « presque-coins » du cube unité.
- Enfin, le lemme 8.2.3 est calculatoire : il nous permettra d'optimiser la borne recherchée et de caractériser ce qu'on obtient.

Ceci étant fait,

- On choisira comme famille $(G^{(k)})$ les monômes $X_{i,j}$ ainsi qu'un polynôme $\tilde{F}$ issu de F,
- On tachera de choisir une bonne pondération de cette famille pour appliquer le premier lemme,
- On étudiera le max de Φ sur les différents « presque-coins » du cube unité grâce au deuxième lemme,
- On finira enfin d'optimiser notre pondération grâce au troisième lemme.

Lemme 8.2.1 (Minoration de la complexité d'un zéro x de F grâce à une famille pondérée de polynômes ne l'annulant pas)**.**

Soient $F \in Z[X_{i,j}]$ un polynôme multihomogène comme dans l'énoncé du théorème, et notons de plus $X(\mathbb{C})$ l'ensemble des zéros de F à coordonnées complexes, ainsi que $X(\mathbb{C})_1$ l'intersection de $X(\mathbb{C})$ avec le cube unité.

Autrement dit,

$$X(\mathbb{C}) = \left\{ x \in \mathbb{C}^{3\times 3} \,\middle|\, F(x) = 0 \right\},$$
$$X(\mathbb{C})_1 = X(\mathbb{C}) \cap \left\{ x \in \mathbb{C}^{3\times 3} \,\middle|\, \forall i,j \ \|x_{i,j}\| \leq 1 \right\}.$$

On pose de même $X(\overline{\mathbb{Q}}) \subset \overline{\mathbb{Q}}^{3\times 3}$ l'ensemble des zéros de F à coordonnées algébriques.

Soient $x = (x_0, x_1, x_2) \in X(\overline{\mathbb{Q}})$, $N \in \mathbb{N}^*$ et $(\nu^{(k)}, G^{(k)})_{k\in[\![1,N]\!]} \in (\mathbb{R}_+^* \times \mathbb{Z}[X_{i,j}])^N$ une famille pondérée de N polynômes multihomogènes n'annulant pas x. Pour tout k, on note de plus $(d_0^{(k)}, d_1^{(k)}, d_2^{(k)})$ les multidegrés de $G^{(k)}$ en (X_0, X_1, X_2).

Alors,

$$\prod_{i=0}^{2} H(x_i)^{w_i} \geq e^{-\lambda},$$

avec

$$\forall i \ w_i = \sum_k \nu^{(k)} d_i^{(k)},$$
$$\lambda = \max_{x' \in X(\mathbb{C})_1} \Phi(x'),$$
$$\Phi : x' \mapsto \sum_k \nu^{(k)} \ln \|G^{(k)}(x')\|,$$

où l'on rappelle que $\|\cdot\|$ désigne le module complexe.

Notons que dans ce lemme, on n'impose pas que x soit un zéro inversible de F.

Démonstration. L'inégalité étant évidente si l'un des vecteurs x_i est nul, on peut supposer que ce n'est pas le cas.

Pour démontrer ce premier lemme, on va séparer l'inégalité qu'on veut obtenir sur chaque place, puis tout recombiner pour obtenir la hauteur.

Soit donc K un corps de nombre contenant tous les $x_{i,j}$.

On note comme d'habitude $n = [K : \mathbb{Q}]$ et $n_v = [K_v : \mathbb{Q}_v]$ pour toute place v de K.

Montrons que pour toute valeur absolue standard v de K,

$$\sum_{i=0}^{2} w_i \ln\left(\max_j |x_{i,j}|_v\right) \geq \sum_k \nu^{(k)} \ln|G^{(k)}(x)|_v - \lambda \mathbb{1}_{v \text{ archimédienne}}.$$

Soit v une valeur absolue standard de K.

- Dans un premier temps, on montre qu'on peut se ramener au cas où $\forall i \ \max_j |x_{i,j}|_v = 1$.
  En effet, s'il existe un i tel que ça n'est pas le cas, on peut écrire

$$\begin{aligned} w_i \ln\left(\max_j |x_{i,j}|_v\right) &= \sum_k \nu^{(k)} d_i^{(k)} \ln\left(\max_j |x_{i,j}|_v\right) \\ &= \sum_k \nu^{(k)} \left(\ln|G^{(k)}(x)|_v - \ln\left|G^{(k)}\left(\frac{x}{\max_j |x_{i,j}|_v}\right)\right|_v\right), \end{aligned}$$

  puis soustraire cette égalité à l'inégalité ci-dessus, ce qui nous ramène à $\max_j |x_{i,j}|_v = 1$.
  Quitte à faire ça trois fois, on obtient donc la simplification annoncée.
  On se ramène donc à montrer que, sachant que $\forall i \max_j |x_{i,j}|_v = 1$,

$$\lambda \mathbb{1}_{v \text{ archimédienne}} \geq \sum_k \nu^{(k)} \ln|G^{(k)}(x)|_v.$$

- **Supposons v ultramétrique.**
  Grâce à l'inégalité ultramétrique, on sait que la boule $B_v(0,1) = \{z \in K \,|\, |z|_v \leq 1\}$ est un sous-anneau de K.
  Or, par hypothèse (grâce à notre réduction), tous les $x_{i,j}$ sont dans $B_v(0,1)$. De plus, tous les coefficients de tous les $G^{(k)}$ sont dans $\mathbb{Z} \subset B_v(0,1)$.
  On en déduit que pour tout k, $G^{(k)}(x)$ est aussi dans $B_v(0,1)$.
  On peut reformuler ce résultat en disant que pour tout k, $\ln|G^{(k)}(x)|_v \leq 0$, ce qui conclut.
- **Supposons v archimédienne.**
  Il s'agit de montrer l'existence de $x' \in X(\mathbb{C})_1$ tel que

$$\sum_k \nu^{(k)} \ln\|G^{(k)}(x')\| \geq \sum_k \nu^{(k)} \ln|G^{(k)}(x)|_v,$$

  ce qui se réécrit, en choisissant $\sigma \in \Sigma(K)$ associée à v, sous la forme

$$\sum_k \nu^{(k)} \ln\|G^{(k)}(x')\| \geq \sum_k \nu^{(k)} \ln\left\|\sigma\left(G^{(k)}(x)\right)\right\|.$$

Puisque les $G^{(k)}$ sont à coefficients dans $\mathbb{Z}$, on a pour tout k que

$$\sigma\Big(G^{(k)}(x)\Big) = G^{(k)}\Big(\sigma(x)\Big) := G^{(k)}\Big(\big((\sigma(x_{i,j})\big)_{0\leq i,j\leq 2}\Big).$$

Or, par hypothèse (grâce à notre réduction), $\forall i,j\ \|\sigma(x_{i,j})\| = |x_{i,j}|_v \geq 1 : \sigma(x)$ est dans le cube unité !

Comme de plus $F(\sigma(x)) = \sigma(F(x)) = \sigma(0) = 0$, on a donc $\sigma(x) \in X(\mathbb{C})_1$, ce qui implique que le choix $x' = \sigma(x)$ convient.

L'inégalité désirée étant obtenue pour chaque valeur absolue, il ne plus qu'à sommer pour retrouver la hauteur.

Sommons sur les trois termes de l'inégalité obtenue.

- Par définition de la hauteur, pour tout i,

$$\sum_v \frac{n_v}{n} w_i \ln\Big(\max_j |x_{i,j}|_v\Big) = w_i \ln H(x_i),$$

donc

$$\sum_i \sum_v \frac{n_v}{n} w_i \ln\Big(\max_j |x_{i,j}|_v\Big) = \ln\Big(\prod_i H(x_i)^{w_i}\Big).$$

- Par la formule du produit, pour tout k,

$$\sum_v \frac{n_v}{n} \ln |G^{(k)}(x)|_v = \ln\Big(\prod_v |G^{(k)}(x)|_v^{\frac{n_v}{n}}\Big) = \ln(1) = 0,$$

donc

$$\sum_k \nu^{(k)} \sum_v \frac{n_v}{n} \ln |G^{(k)}(x)|_v = 0.$$

- Enfin, en sommant sur les n_v, on obtient

$$\sum_v \frac{n_v}{n} \lambda \mathbb{1}_{v \text{ archimédienne}} = \lambda \sum_{v\in M_K^\infty} \frac{n_v}{n} = \lambda.$$

On a montré que pour toute v,

$$\sum_{i=0}^{2} w_i \ln\Big(\max_j |x_{i,j}|_v\Big) \geq \sum_k \nu^{(k)} \ln |G^{(k)}(x)|_v - \lambda \mathbb{1}_{v \text{ archimédienne}},$$

on en déduit donc que

$$\ln\Big(\prod_i H(x_i)^{w_i}\Big) \geq -\lambda,$$

ce qui se traduit en la conclusion :

$$\prod_i H(x_i)^{w_i} \geq \exp(-\lambda).$$

□

Nous avons donc obtenu une minoration sur une « hauteur pondérée » de x par $\exp(-\lambda)$, où $\lambda = \max \Phi$.

Ainsi, plus λ est petit, plus l'inégalité est bonne.

Pour pouvoir utiliser ce lemme, puis optimiser la famille qui définit Φ, on aimerait calculer $\lambda = \max \Phi$. En s'appuyant sur des raisonnements d'analyse complexe appliqués aux fonctions harmoniques, et plus spécifiquement sur le théorème de Puiseux 18, le lemme suivant nous dit que $\max \Phi$ existe, et où le chercher.

Définition 8.2.5 (Presque-coin)**.** Notons C l'ensemble des points de $\mathbb{C}^{3\times 3}$ dont toutes les coordonnées ont pour module 1, avec au plus une exception, dont le module est inférieur ou égal à 1.

On appelle C l'ensemble des « presque-coins du cube unité » : c'est une réunion de segments de dimension 1.

Lemme 8.2.2.

Avec les mêmes notations que précédemment, la fonction

$$\Phi : x' \mapsto \sum_k \nu^{(k)} \ln \|G^{(k)}(x')\|$$

admet un maximum dans $X(\mathbb{C})_1$, qui est de plus atteint en un presque-coin du cube unité.

Démonstration. Montrons d'abord que Φ admet un maximum. Φ n'est pas définie sur $X(\mathbb{C})_1$ entier, mais unique là où les polynôme $G(k)$ ne s'annulent pas. Le maximum de Φ sur $X(\mathbb{C})_1$ veut donc dire le maximum sur son domaine de définition à l'intérieur de $X(\mathbb{C})_1$. On va donc travailler sur $e^{\Phi(x')}$ qui se prolonge par continuité sur tout $X(\mathbb{C})_1$. Et évidemment $\Phi(z)$ est maximale si et seulement si $e^{\Phi(z)}$ l'est. Comme il est plus facile de travailler sur un compact, on va donc se ramener à ce cas. Puisque les $\nu^{(k)}$ sont positifs, alors $e^{\Phi(x')}$ est majorée sur le cube unité et donc sur $X(\mathbb{C})_1$. Notons M cette borne supérieure .Nous nous restreignons, pour ϵ assez petit à $\{y \in X(\mathbb{C})_1 | e^{\Phi(y)} \geq \epsilon\}$ qui est non vide (pour ϵ assez petit) et compact (il est fermé comme image réciproque du fermé $[\epsilon; M]$ par une fonction continue et est borné).
Or puisque e^{Φ} est continue, elle admet un maximum sur $X(\mathbb{C})_1$. Et donc Φ admet un maximum sur $X(\mathbb{C})_1$. Et on peut parler de façon interchangeable de maximum de Φ ou de e^{Φ}
Supposons maintenant par l'absurde que Φ admet un maximum appelé M_Φ en un point $\tilde{x}$ ayant au moins deux coordonnées $\tilde{x}_{i_0,j_0}, \tilde{x}_{i_1,j_1}$ de module < 1. Notons ces deux coordonnées ξ, η. On va rajouter des contraintes supplémentaires sur ce point qui peuvent paraître « parachutées », on va donc essayer de les justifier. Tout d'abord c'est quoi ces contraintes ? Pour les expliciter on va utiliser la notion de *point paramétré* :

Définition 8.2.6 (Un point paramétré)**.** Soient $c_1, c_2 \in \mathbb{C}^2$ On appelle un point paramétré $x'(c_1, c_2) \in \mathbb{C}^{3\times 3}$ le point qui a $x_{i,j}$ pour coordonnées lorsque $x_{i,j} \notin (\xi, \eta)$. Et dont les coordonnées (ξ, η) valent (c_1, c_2).
Cette définition induit naturellement une fonction $\mathbb{C}^2 \to \mathbb{C}^{3\times 3}$ qui à (c_1, c_2) associe $x'(c_1, c_2)$.
Nous définissons l'ensemble $Y(\mathbb{C})_1 = \{(c_1, c_2) | x(c_1, c_2) \in X(\mathbb{C})_1\}$

- $Y(\mathbb{C})_1$ est l'intersection de l'ensemble $[(c_1, c_2) \in \mathbb{C}^2 | \|c_1\| \leq 1, \|c_2\| \leq 1]$. Avec l'ensemble $F(x'(\cdot,\cdot))^{-1}(0)$ qui est l'image réciproque de $\{0\}$ un fermé par un polynôme à deux variables complexes. (Le fait que cette fonction est un polynôme sera traité plus en détail ensuite). $Y(\mathbb{C})_1$ est donc un fermé. Or il est borné. Il est donc compacte.
- Soit l'ensemble suivant $E = [(c_1, c_2) \in Y(\mathbb{C})_1 | \Phi(x'(c_1, c_2)) = M_\Phi]$. E est donc un fermé de $\mathbb{C}^2$ comme intersection de deux fermés ($Y(\mathbb{C})_1$ et $\Phi(x'(\cdot,\cdot))^{-1}(\{M_\Phi)\}$), borné, donc compacte.
- L'application $(a, b) \in E \mapsto \max(\|a\|, \|b\|)$ atteint donc un maximum sur E. Soit α ce maximum. Soit un point $(a_0, b_0) \in E$ où c'est atteint. Supposons sans perte de généralités que $\|a_0\| = \alpha$.
  On pose $E_{\max} = \{(c_1, c_2) \in E | \|c_1\| = \alpha\}$. Cet ensemble est également un compact parce qu'on a intersecté E par un autre fermé. On peut donc trouver un couple qui a le module de sa deuxième coordonnée maximal. Notons ce maximum β et notons un couple où c'est atteint $(\xi_0, \eta_0) \in E_{\max}$.
  On a donc $\forall c_1, c_2 \in E, (\|c_1\| < \|\xi_0\| = \alpha)$ ou $(\|c_1\| = \|\xi_0\| = \alpha$ et $\|c_2\| \leq \|\eta_0\| = \beta)$.

Appelons donc $x = x'(\xi_0, \eta_0)$.
En fait les contraintes rajoutées font de $x = x'(\xi_0, \eta_0)$ et plus précisément de (ξ_0, η_0) un couple maximal sur E pour un certain ordre partiel. Et le but de la preuve est de trouver $x'(\xi_0', \eta_0')$ un nouveau point paramétré avec $(\xi_0', \eta_0') \in E$ strictement plus grand que (ξ_0, η_0) pour cet ordre partiel si $\alpha < 1$. Et on conclut ainsi que $\alpha = 1$ par maximalité de (ξ_0, η_0). Or cela contredit notre première supposition.

On va maintenant trouver un « paramétrage » de $X(\mathbb{C})_1$ au voisinage de ce point. C'est à dire des fonctions (qu'on veut analytiques) qui donnent une possibilité de variation des deux coordonnées qui nous intéressent tout en restant dans $X(\mathbb{C})_1$ et en gardant Φ maximale.

Remplaçons dans l'équation $F = 0$ les valeurs de toutes les coordonnées au point x sauf celles de ξ, η. Ceci nous donne une équation polynomiale en ξ, η :

$$g(\xi, \eta) = 0 \tag{7}$$

On veut donc des trouver $\xi(z), \eta(z)$ vérifiant :

- $\xi(0) = \xi_0$
- $\eta(0) = \eta_0$
- $\xi(z), \eta(z)$ des fonctions holomorphes au voisinage de (0,0).

Avec un changement de variable, on simplifie la situation pour avoir $(0, 0)$ comme point de départ. C'est à dire, on considère l'équation polynomiale :

$$f(U, T) = g(U + \xi_0, T + \eta_0)$$

Et donc il suffit de trouver un couple de séries entières convergentes en 0 solutions de $f = 0$ pour avoir des fonctions analytiques solutions de $g = 0$.
En vue d'appliquer le théorème de Puiseux 18, on va « fixer » U, la première variable de $f(U, T)$ à la série entière identité $z \mapsto z$. Ce choix peut paraître très restrictif mais il ne l'est pas et on

verra pourquoi à la suite.
On a donc une équation polynomiale à coefficients dans $\mathbb{C}(\{z^*\})$

$$f(z,T)=0 \tag{8}$$

vérifiant $f(0,0)=0$.
Si le polynôme $f(U,T)$ est divisible par U alors il suffit de prendre la série nulle pour U (et donc $\xi(z)=\xi_0$) et $z\mapsto z$ pour T (et donc $\eta(z)=\eta_0+z$). Supposons que $f(U,T)$ n'est pas divisible par U.
De même supposons qu'il n'est pas divisible par T.
Puisque $\mathbb{C}(\{z^*\})$ est algébriquement clos alors on peut écrire l'équation 8 en factorisant le polynôme :

$$f(z,T)=g_0(z)(T-g_1(z))\cdots(T-g_n(z))$$

Tel que les $g_i(z)\in\mathbb{C}(\{z^*\})$. On dispose donc de $r\in\mathbb{N}$ tel que les $g_i(z^r)\in\mathbb{C}(\{z\})$. Et ainsi en changeant de variable :

$$f(w^r,T)=f_0(w)(T-f_1(w))\cdots(T-f_n(w))$$

Avec les $f_i(w)\in\mathbb{C}(\{w\})$. Aucune des $f_i(w)$ n'est identiquement nulle, sinon T divise le polynôme. On cherche maintenant à ne garder que des séries entières d'ordre ≥ 0 dans les parenthèses. Appelons $a_0=-ord\ f_0\in\mathbb{Z}$ et pour $i\geq 1$, $a_i=-\min(0,ord\ f_i)\in\mathbb{N}$, la multiplicité éventuelle de 0 comme pôle. Et $b=-\sum_i a_i$. Ainsi :

$$\begin{aligned}f(w^r,T)&=w^bw^{a_0}f_0(w)(w^{a_1}T-w^{a_1}f_1(w))\cdot\dot{\cdot}(w^{a_n}T-w^{a_n}f_n(w))\\&=w^bh_0(w)(w^{a_1}T-h_1(w))\cdots(w^{a_n}T-h_n(w))\end{aligned}$$

Avec $\forall i\geq 1, h_i(w)\in\mathbb{C}\{w\}$ et si elle s'annule en 0 alors $a_i=0$. Et pour $h_0(w)\in\mathbb{C}\{w\}$ elle est d'ordre 0 (0 n'est ni pôle ni racine). Or $f(z,T)$ était un polynôme en z. Regardons le terme avec la plus petite puissance de z. Ce terme est le produit de w^b par le terme constant dans chaque parenthèse (T si $a_i=0$ ou le terme constant de h_i qui existe puisque $a_i>0$ (par contraposée)). Puisque $f(U,T)$ est un polynôme en U implique que $f(z,T)$ n'a aucune puissance négative en z (qui a pris le rôle de U). Il doit avoir une puissance positive de w^r (qui a pris ensuite le rôle de z et donc de U) alors $b\geq 0$. De plus $f(U,T)$ était un polynôme non divisible par U et donc pour la même raison $b=0$. Ainsi :

$$f(0,0)=(-1)^n\prod_{i=0}^{n}h_i(0)=0$$

Et donc au moins une des $h_i(w)$ s'annule en 0. Appelons i_0 son indice. On prend cette fonction comme solution à notre polynôme. On revient à l'utilisation de la variable muette z qui bien plus naturelle pour les complexes. On pose $\phi(z)=z^r$ et $\psi(z)=f_{i_0}(z)$. $\phi,\psi\in\mathbb{C}\{z\}$ sont solutions de $f(x,y)=0$ et tels que $(\phi(0),\psi(0))=(0,0)$.
En posant :

$$\begin{aligned}\xi(z)&=\phi(z)+\xi_0\\\eta(z)&=\psi(z)+\eta_0\end{aligned}$$

on obtient le paramètrage voulu. C'est à dire deux fonctions analytiques vérifiant l'équation (7) et passant par le point (ξ_0, η_0). On remarque que par construction au moins l'une de ces fonctions s'écrit sous la forme $z \mapsto z^r + c$ pour $r \in \mathbb{N}^*$
Revenons à l'expression de Φ. Et plus précisément e^{Φ} :

$$e^{\Phi(x')} = \prod_k \|G^{(k)}(x')^{v^{(k)}}\|$$

On va montrer que cette fonction est constante (en un sens à définir) et qu'on peut donc trouver notre point paramétré annoncé au début en faisant varier les paramètres.
En injectant les valeurs de toutes les coordonnées sauf de ξ, η comme on a fait pour le polynôme F au départ, on a la fonction suivante :

$$\phi(c_1, c_2) = e^{\Phi(x'(c_1,c_2))}$$

Et en remplaçant c_1, c_2 par $\xi(z), \eta(z)$ on obtient une fonction analytique (c'est un polynôme en deux séries entières convergentes en 0) :

$$z \to \phi(\xi(z), \eta(z)) = e^{\Phi(x'(\xi(z),\eta(z)))}$$

dont le module atteint un maximum au point $z = 0$. Cette fonction est donc forcément constante d'après le principe du maximum. Et donc $(\xi(z), \eta(z)) \in E$ pour tout z dans leur domaine de convergence.
Maintenant, procédons à l'obtention de notre contradiction. On a un point $x = x'(\xi_0, \eta_0)$ tel que $\Phi(x) = M_\Phi$ et qu'il est maximal au sens suivant :

$$\forall c_1, c_2 \in E, (\|c_1\| < \|\xi_0\| = \alpha) \text{ ou } (\|c_1\| = \|\xi_0\| = \alpha \text{ et } \|c_2\| \leq \|\eta_0\| = \beta).$$

Distinguons donc deux cas pour atteindre notre objectif

- Si $\xi(z)$ est non constante alors elle ne peut pas atteindre un module maximal en $z = 0$ par le principe du maximum, et on peut donc trouver un point $((\xi_0', \eta_0') \in E)$ tel que $\|\xi_0'\| > \alpha$ et c'est absurde.
- Sinon si $\xi(z)$ est constante, alors nécessairement $\eta(z)$ est non constante. Par le principe du maximum, on peut donc trouver un point $((\xi_0, \eta_0') \in E)$ tel que $\|\xi_0\| = \alpha$ puisque la première coordonnée n'a pas changé et de plus $\|\eta_0'\| > \beta$ ce qui contredit notre hypothèse de maximalité. Remarquons que le nouveau couple garde la première valeur ξ_0 constante puisque la fonction correspondante est constante.

Ainsi on a réussi à trouver un point où le maximum est atteint et où ξ ou η a pour module 1. On peut répéter toute cette procédure à partir de ce point qu'on vient de trouver sur le nombre fini de coordonnées de module inférieur à 1 et ainsi obtenir le lemme. □

Une fois qu'on aura calculé $\max \Phi$ (et en fait perdu un peu en le majorant), il ne restera plus que l'optimisation finale.

Pour cette optimisation, on utilisera ce dernier lemme calculatoire, où l'on reconnaît la forme du théorème escompté.

Lemme 8.2.3. *Soient $\alpha, \beta, \gamma > 0$.*

On pose

$$m = \min_{\substack{u,v\geq 0 \\ \alpha u+\beta v=1}} u \ln \frac{\gamma u}{u+v} + v \ln \frac{v}{u+v}.$$

Alors, e^{-m} est l'unique solution réelle supérieure à 1 de

$$\gamma^{-1} t^{-\alpha} + t^{-\beta} = 1.$$

Démonstration. Il s'agit d'un problème d'optimisation sur deux variables avec une contrainte d'égalité : on travaille à une dimension.

α, β, γ sont fixés, et on optimise sur $u, v \geq 0$ tout en respectant la contrainte.

Posons $y = \frac{v}{u+v}$. On a donc $1 - y = \frac{u}{u+v}$,

$$u = \frac{1-y}{\beta y + \alpha(1-y)}, \quad v = \frac{y}{\beta y + \alpha(1-y)},$$

où $y \in [0,1]$. On doit donc minimiser

$$f(y) = \frac{(1-y)\ln(\gamma(1-y)) + y \ln y}{\beta y + \alpha(1-y)}$$

dans $[0,1]$. Dérivons donc par rapport à y :

$$f'(y) = \frac{-\beta \ln(\gamma(1-y)) + \alpha \ln y}{(\beta y + \alpha(1-y))^2},$$

qui s'annule lorsque $(\gamma(1-y))^\beta = y^\alpha$.

Cette égalité n'est vérifiée que seulement une fois sur $y_0 \in]0,1[$, puisque les deux fonctions sont strictement monotones et leur différence change de signe entre 0 et 1.

Soit $\rho > 0$ tel que $y_0 = \rho^{-\beta}$. Alors $\gamma(1-y) = y_0^{\alpha/\beta} = \rho^{-\alpha}$. On a donc bien $1 - \rho^{-\beta} = \gamma^{-1}\rho^{-\alpha}$. Il nous reste donc simplement à vérifier que $f(y_0) = -\ln \rho$, ce qui est immédiat. □

Nous allons assembler ces 3 lemmes pour obtenir le théorème à proprement parler, de la façon dont on l'a annoncé.

Soient donc F comme dans l'énoncé et x un zéro non inversible de F.

- Pour utiliser la borne trouvée au premier lemme, commençons par choisir la famille pondérée.
  - Comme famille $(G^{(k)})$, on choisit l'ensemble des monômes $X_{i,j}$ où $0 \leq i, j \leq 2$, auquels on ajoute $\tilde{F}$, défini par

    $$\tilde{F} = F\Big((X_{i,j}^{-1})_{0\leq i,j\leq 2}\Big) \prod_{i,j} X_{i,j}^{d_{i,j}},$$

    dont on vérifie que c'est bien un polynôme de $\mathbb{Z}[X_{i,j}]$, par définition des $d_{i,j}$ comme degré de F en $X_{i,j}$.

- On vérifie de plus que ces 10 polynômes sont bien multihomogènes.

  Chaque monôme $X_{i,j}$ a un multidegré 1 en i et 0 ailleurs.

  Pour tout i, on note de plus $\tilde{d}_i$ le multidegré de $\tilde{F}$ en i, qui s'exprime en fonction des multidegrés et degrés de F sous la forme

$$\tilde{d}_i = -d_i + \sum_j d_{i,j}.$$

- Pour chaque monôme $X_{i,j}$, on note $\nu^{(i,j)} \geq 0$ la pondération associée.

  On note de plus $\mu \geq 0$ la pondération associée à $\tilde{F}$.

- Ainsi, avec les notations du premier lemme,

$$\Phi : x' \mapsto \mu \ln|\tilde{F}(x')| + \sum_{i,j} \nu^{(i,j)} \ln|x'_{i,j}|,$$
$$w_i = \mu\tilde{d}_i + \sum_j \nu^{(i,j)}, \qquad \lambda = \max_{x \in X(\mathbb{C})_1} \Phi(x).$$

  On a alors, x étant choisi zéro non inversible de F,

$$\prod_{i=0}^{2} H(x_i)^{w_i} \geq e^{-\lambda}$$

- On choisit d'imposer $w_0 = w_1 = w_2 = 3$. Seule la variable μ reste alors libre. En effet, on a alors, pour tous i, j,

$$\nu^{(i,j)} = 1 - \frac{\tilde{d}_i}{3}\mu.$$

- Il s'agit maintenant d'étudier $\max_{X(\mathbb{C})_1} \Phi$. D'après le deuxième lemme, Φ atteint son maximum sur un presque-bord.

  On va estimer (majorer) le maximum de Φ sur chaque segment qui compose ces presque-bords, puis majorer l'ensemble de ces maxima locaux. On aura donc obtenu une majoration de $\lambda = \max \Phi$: on perd en particulier quelque chose en sortant de $X(\mathbb{C})_1$ (on arrête d'imposer $F(x') = 0$ pour pouvoir optimiser).

  - C'est ici qu'apparaît la norme $\|\cdot\|$ pour polynômes présentée dans l'énoncé du théorème. On va en effet avoir besoin, pour $P \in C[X]$, $a, b \in \mathbb{C}$, de majorer $\|P(a) - P(b)\|$ à l'aide de $\|P'\|$.

    Attention à bien distinguer les deux définitions de $\|\cdot\|$ pour un complexe ou pour un polynôme ! On rappelle que pour un polynôme $P \in \mathbb{C}[X]$, $\|P\|$ désigne la somme des modules de ses coefficients.

Commençons par prendre c_0T^k un monôme, $d \geq k$ (qui désignera le degré du polynôme en T où apparaît c_0T^k), et $a, b \in \mathbb{C}$. On a

$$\begin{aligned}
\|c_0a^k - c_0b^k\| &= \|c_0\|\|a-b\| \cdot \|a^{k-1} + \cdots + b^{k-1}\| \\
&\leq \|c_0\|\|a-b\| \cdot k \max(\|a\|, \|b\|, 1)^{k-1} \\
&= k\|c_0\|\|a-b\| \max(\|a\|, \|b\|, 1)^{k-1} \\
&= \left\|\frac{dc_0T^k}{dT}\right\| \|a-b\| \max(\|a\|, \|b\|, 1)^{k-1} \\
&\leq \left\|\frac{dc_0T^k}{dT}\right\| \|a-b\| \max(\|a\|, \|b\|, 1)^{d-1}.
\end{aligned}$$

Ainsi, pour tous $P \in \mathbb{C}[T]$ de degré d et $a, b \in \mathbb{C}$, en sommant sur tous les monômes, on obtient

$$\|P(a) - P(b)\| \leq \left\|\frac{dP(T)}{dT}\right\| \|a-b\| \max(\|a\|, \|b\|, 1)^{d-1}.$$

- Choisissons donc (i_0, j_0) et $x' \in C$ tel que $\|x'_{i_0,j_0}\| \leq 1$ et $\forall (i,j) \neq (i_0,j_0)\ \|x'_{i,j}\| = 1$. Le terme de droite de Φ étant très simple (il y a un seul terme non nul), regardons ce qui se passe à gauche. On introduit la notation $\overline{x'} := \left((\overline{x'_{i,j}})_{0 \leq i,j \leq 2}\right)$.

$$\begin{aligned}
\|\tilde{F}(x')\| &= \|F(x'^{-1})\| \cdot \|\prod_{i,j} {x'_{i,j}}^{d_{i,j}}\| \\
&= \|F({x'_{i_0,j_0}}^{-1}, \overline{x'_{i,j}})\| \cdot \|x'_{i_0,j_0}\|^{d_{i_0,j_0}} && \text{car si } \|z\| = 1, \text{ alors } z^{-1} = \overline{z} \\
&= \|F({x'_{i_0,j_0}}^{-1}, \overline{x'_{i,j}}) - F(\overline{x'})\| \cdot \|x'_{i_0,j_0}\|^{d_{i_0,j_0}} && \text{car } F(\overline{x'}) = \overline{F(x')} = 0.
\end{aligned}$$

On applique alors le point précédent. En effet, on peut ici voir F comme un polynôme ne dépendant que de X_{i_0,j_0}, qu'on évalue ici en x_{i_0,j_0}^{-1} et $\overline{x_{i_0,j_0}}$, les autres $X_{i,j}$ étant fixés à $\overline{x_{i,j}}$.

$$\begin{aligned}
\|\tilde{F}(x')\| &\leq \left\|\frac{\partial F}{\partial X_{i_0,j_0}}\right\| \|{x'_{i_0,j_0}}^{-1} - \overline{x'_{i_0,j_0}}\| \max\left(\|{x'_{i_0,j_0}}^{-1}\|, \|x'_{i_0,j_0}\|\right)^{d_{i_0,j_0}-1} \cdot \|x'_{i_0,j_0}\|^{d_{i_0,j_0}} \\
&\leq \left\|\frac{\partial F}{\partial X_{i_0,j_0}}\right\| \|{x'_{i_0,j_0}}^{-1} - \overline{x'_{i_0,j_0}}\| \cdot \|x'_{i_0,j_0}\|^{1-d_{i_0,j_0}} \cdot \|x'_{i_0,j_0}\|^{d_{i_0,j_0}} \\
&= \left\|\frac{\partial F}{\partial X_{i_0,j_0}}\right\| \left(1 - \|{x'_{i_0,j_0}}^2\|\right).
\end{aligned}$$

En posant $c_{i_0,j_0} = \left\|\frac{\partial F}{\partial X_{i_0,j_0}}\right\|$, cela se réécrit

$$\|\tilde{F}(x')\| \leq c_{i_0,j_0}\left(1 - \|{x'_{i_0,j_0}}^2\|\right).$$

- Cherchons le maximum de Φ sur ce segment (identifié par (i_0, j_0)). En écrivant $\chi = \|{x'_{i_0,j_0}}^2\|$, on constate que, **sur ce segment**,

$$\max \Phi \leq \max_{\chi \in [0,1]} \mu \ln(c_{i_0,j_0}(1-\chi)) + \frac{\nu^{(i_0,j_0)}}{2} \ln \chi.$$

  Le maximum de cette fonction est atteint pour $\chi = \frac{\nu^{i_0,j_0}}{\nu^{i_0,j_0}+2\mu}$ qu'on trouve par simple calcul (rassembler les termes en χ). En réinjectant, on obtient que, **sur ce segment**,

$$\max \Phi \leq \mu \ln \frac{2\mu c_{i_0,j_0}}{\nu^{(i_0,j_0)}+2\mu} + \frac{\nu^{(i_0,j_0)}}{2} \ln \frac{\nu^{(i_0,j_0)}}{\nu^{(i_0,j_0)}+2\mu}.$$

- Grâce à ces majorations de maxima locaux, on passe à la majoration globale.
  En posant $\delta = \max_i \frac{\tilde{d}_i}{3}$, pour tous i, j, on a par définition $\nu^{(i,j)} \geq 1 - \delta\mu$.
  En vérifiant la décroissance de la fonction appropriée, par le point précédent, et d'après le lemme 2 qui nous permet de se restreindre aux presque-bords, on obtient

$$\lambda = \max_{x' \in X(\mathbb{C})_1} \Phi(x') \leq \mu \ln \frac{2\mu c_F}{(1-\delta\mu)+2\mu} + \frac{1-\delta\mu}{2} \ln \frac{1-\delta\mu}{(1-\delta\mu)+2\mu},$$

  où

$$c_F = \max_{i,j} \left\| \frac{\partial F}{\partial X_{i,j}} \right\|.$$

- Le difficile travail d'étude de Φ étant fait, il ne nous reste plus qu'à optimiser sur μ pour obtenir la meilleure majoration possible de λ.
  C'est là qu'intervient le dernier lemme dans notre arsenal.
  On pose $u = \mu, v = (1-\delta\mu)/2, \gamma = c_F, \alpha = \delta, \beta = 2$, où on vérifie bien sûr que $\alpha u + \beta v = 1$.
  En posant ρ réelle supérieur à 1 tel que $c_F^{-1}\rho^{-\delta} + \rho^{-2} = 1$, on obtient donc que $\lambda \leq -\ln \rho$.
  En reprenant l'application de notre premier lemme, on peut finalement conclure :

$$\prod_i H(x_i)^3 \geq e^{-\lambda} \geq \rho.$$

□

On va maintenant appliquer ce théorème sur les hauteurs pour analyser la structure de l'équation aux S-unités.

Pour pouvoir utiliser le théorème de façon agréable, il va falloir ramener la forme de l'équation à quelque chose sur lequel on pourra faire apparaître un polynôme multihomogène.

Ainsi, pour étudier les interactions de solutions de l'équation

$$x + y = 1, \quad \text{en } x, y \in \overline{\mathbb{Q}}^*,$$

on va démontrer la proposition suivante, qui s'applique à l'équation

$$\lambda p + \mu q = 1, \quad \text{en } p, q \in \overline{\mathbb{Q}}^*, \quad \text{où } \lambda, \mu \in \overline{\mathbb{Q}}^*,\ \lambda + \mu = 1.$$

Dans la preuve de cette proposition, on va voir cette équation comme un cas particulier d'une équation plus générale, définie par

$$\lambda x + \mu y + \nu z = 0, \quad \text{en } x, y, z \in \overline{\mathbb{Q}}^*, \quad \text{où } \lambda, \mu, \nu \in \overline{\mathbb{Q}}^*.$$

On géométrisera cette équation, qui définit un plan plongé dans un espace à trois dimensions (sur le corps $\mathbb{C}$). Trois solutions distinctes de l'équation annulent ainsi un déterminant (3×3) : voilà notre polynôme multihomogène !

Proposition 8.2.5. *Soient $\lambda, \mu \in \overline{\mathbb{Q}}^*$ et supposons que $\lambda + \mu = 1$. Soit (p_i, q_i) pour $i = 1, 2$ deux solutions de $\lambda p + \mu q = 1$ dans $\overline{\mathbb{Q}}^*$ telles que $(p_1, q_1), (p_2, q_2), (1, 1)$ soient distincts. Alors*

$$H(p_1, q_1, 1)H(p_2, q_2, 1) \geq \rho \approx 1.0942711...$$

où ρ est l'unique réel ≥ 1 tel que

$$\rho^{-6} + \frac{1}{2}\rho^{-2} = 1.$$

Démonstration. Cette proposition est un joli corollaire du théorème 20. On va réussir à se ramener à la propriété géométrique suivante : il y a au plus deux points dans l'intersection d'une droite et d'une conique (définies sur le corps des complexes).

On va d'abord faire un peu de géométrie algébrique pour voir comment appliquer le théorème 20 à des équations de forme similaire à celle de la proposition (mais plus adaptée à ce théorème).

Au deuxième point, on va ensuite montrer la proposition en transformant l'équation de l'énoncé pour la rendre adaptée au théorème, et appliquer le premier.

- Soient $\lambda, \mu, \nu \in \overline{\mathbb{Q}}^*$. On considère l'équation

  $$(L) : \lambda X + \mu Y + \nu Z = 0,$$

  qui fait de (L) un plan vectoriel.

  Soient P_1, P_2, P_3 trois points distincts de (L), avec des coordonnées toutes non nulles, qu'on note $P_i = (x_i, y_i, z_i)$.

  On suppose de plus que $z_1 = z_2 = z_3 \neq 0$. On note z cette coordonnée commune, et T_z le plan affine associé :

  $$(T_z) : Z = z.$$

  - Faisons apparaître un polynôme multihomogène.

    Puisque ces trois points appartiennent à un même plan, on a la relation

    $$\Delta = \begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} = 0,$$

    (P_1, P_2, P_3) est donc un zéro du déterminant ! On prend pour F le déterminant (3×3), qui est bien un polynôme multihomogène en 3×3 variables.

- Pour appliquer le théorème, vérifions que (P_1, P_2, P_3) est un zéro inversible de F : on va utiliser un argument géométrique.
  - Il s'agit de vérifier que
  $$\tilde{\Delta} = \begin{vmatrix} x_1^{-1} & y_1^{-1} & z_1^{-1} \\ x_2^{-1} & y_2^{-1} & z_2^{-1} \\ x_3^{-1} & y_3^{-1} & z_3^{-1} \end{vmatrix} \neq 0.$$
  Supposons par l'absurde que $\tilde{\Delta} = 0$.
  On dispose alors de $\alpha, \beta, \gamma \in \overline{\mathbb{Q}}$ non tous nuls tels que
  $$\forall i \; \alpha x_i^{-1} + \beta y_i^{-1} + \gamma z_i^{-1} = 0.$$
  - Puisque tous les $x_i y_i z_i$ sont non nuls, on en déduit que tous les P_i sont des zéros de
  $$(C) : \alpha YZ + \beta XZ + \gamma XY = 0,$$
  dont on va montrer que c'est l'équation d'une conique.
  Pour cela, il faut montrer que $\alpha YZ + \beta XZ + \gamma XY$ n'est pas factorisable de façon non triviale. On vérifie aisément que c'est équivalent à montrer que les α, β, γ sont tous non nuls.
  Supposons par l'absurde que ce n'est pas le cas. Sans perte de généralité, on suppose $\gamma = 0$.
  On a alors
  $$(C) : (\alpha Y + \beta X)Z = 0.$$
  Puisque tous les z_i sont non nuls (de la même manière dans les deux autres cas on utiliserait le fait que tous les x_i sont non nuls ou de même pour les y_i – la situation est bien symétrique), les points P_1, P_2, P_3 appartiennent au plan vectoriel
  $$(L') : \alpha Y + \beta X = 0.$$
  Ainsi les P_1, P_2, P_3 sont dans l'intersection $(L) \cap (L') \cap (T_z)$.
  Puisque $\nu \neq 0$ (on aurait de même $\lambda \neq 0$ et $\mu \neq 0$ dans les deux autres cas), (L) et (L') sont distincts. Leur intersection est donc réduite à une droite vectorielle.
  Or, (T_z) est un plan *affine* (non vectoriel). Son intersection avec une telle droite est donc réduite à un point. On en déduit que $P_1 = P_2 = P_3$: **contradiction**.
  Ainsi, (C) est bien une conique, qui contient les trois points P_1, P_2, P_3.
  - Ainsi, si (P_1, P_2, P_3) est un zéro non-inversible de F, alors P_1, P_2, P_3 sont trois points distincts de $(L) \cap (T_Z) \cap (C)$, où (L) est le plan vectoriel défini plus haut, (T_z) est le plan affine $Z = z$, et (C) est la conique qu'on vient de définir.
  Or, $(L) \cap (T_z)$ est au plus une droite (affine). Plus précisément, $(L) \cap (T_z)$ est contenu dans une droite affine.
  Ainsi, P_1, P_2, P_3 sont trois points distincts dans l'intersection d'une droite (affine) avec une conique. Pourtant, une telle intersection est faite d'au plus deux points : c'est donc **absurde**.

- On peut conclure : (P_1, P_2, P_3) est un zéro inversible de F.
  On peut donc appliquer le théorème 20, en vérifiant qu'on a dans notre cas $c_F = 2$ et $\delta = 2/3$.
  Ainsi, si on pose ρ_1 l'unique réel ≥ 1 tel que $\rho_1^{-2} + (1/2)\rho_1^{-2/3} = 1$, on obtient
  $$H(P_1)^3 H(P_2)^3 H(P_3)^3 \geq \rho_1,$$
  ce qui se réécrit avec nos hypothèses
  $$H(x_1, y_1, 1)^3 H(x_2, y_2, 1)^3 H(x_3, y_3, 1)^3 \geq \rho_1.$$

- Appliquons maintenant ce résultat à notre problème. Comme dans l'énoncé de la proposition, on choisit $\lambda, \mu \in \overline{\mathbb{Q}^*}$ tels que que $\lambda + \mu = 1$, et (p_i, q_i) pour $i = 1, 2$ deux solutions de $\lambda p + \mu q = 1$ dans $\overline{\mathbb{Q}}^*$ telles que $(p_1, q_1), (p_2, q_2), (1, 1)$ soient distincts.
  On pose $\nu = -1$, $P_1 = (p_1, q_1, 1)$, $P_2 = (p_2, q_2, 1)$ et $P_3 = (1, 1, 1)$.
  De cette manière, maintenant qu'on a artificiellement introduit une troisième dimension, on vérifie toutes les hypothèses du point précédent. Notons que ce phénomène vient du fait que la démonstration originale se déroule dans des espaces projectifs, ce qu'on a dissimulé ici.
  On applique donc le point précédent, et on en déduit que
  $$H(p_1, q_1, 1)^3 H(p_2, q_2, 1)^3 \cdot 1 \geq \rho_1,$$
  ρ_1 étant défini de la même manière.
  En passant à la racine troisième, on pose $\rho = \rho_1^{1/3}$, qui est l'unique réel ≥ 1 tel que
  $$\rho^{-6} + \frac{1}{2}\rho^{-2} = 1,$$
  et on obtient
  $$H(p_1, q_1, 1) H(p_2, q_2, 1) \geq \rho,$$
  où la valeur numérique de ρ est
  $$\rho \approx 1.0942711...$$

□

On peut maintenant redescendre à la forme de notre équation aux S-unités et en déduit l'inégalité qui permet de mesurer précisément les interactions entre les solutions pour obtenir plus tard notre résultat de finitude.

Proposition 8.2.6.
Soient $(x_0, y_0), (x_1, y_1) et (x_2, y_2)$ trois solutions distinctes de
$$x + y = 1 \quad x, y \in \overline{\mathbb{Q}^*}$$
Alors,
$$\max_{i=1,2} \left(\max(H(x_i/x_0), H(y_i/y_0))\right) \geq \sqrt[4]{\rho} \approx 1.022777...,$$

où ρ est l'unique réel ≥ 1 tel que

$$\rho^{-6} + \frac{1}{2}\rho^{-2} = 1.$$

Démonstration. On applique le lemme précédent avec $\lambda = x_0, \mu = y_0$ et $p_i = x_i/x_0, q_i = y_i/y_0$.

Cela nous donne

$$H(x_1/x_0, y_1/y_0, 1)H(x_2/x_0, y_2/y_0, 1) \geq \rho,$$

dont on déduit

$$\max\Big(H(x_1/x_0, y_1/y_0, 1), H(x_2/x_0, y_2/y_0, 1)\Big) \geq \sqrt{\rho}.$$

De plus, on remarque que

$$\max\Big(H(a,1), H(b,1)\Big) \geq \sqrt{H(a,b,1)}$$

On peut donc conclure que

$$\max_{i=1,2}\left(\max(H(x_i/x_0), H(y_i/y_0))\right) \geq \sqrt[4]{\rho} \approx 1.022777...$$

□

8.2.2 • Conséquences géométriques

Comme prévu, on va travailler sur $V_G = G \otimes_{\mathbb{Z}} \mathbb{R}$ pour montrer la finitude des solutions qui y sont incluses. Il nous faut donc tout d'abord montrer que ce résultat implique un nombre de résultats fini dans G.

Proposition 8.2.7. *On note $V_G = G \otimes_{\mathbb{Z}} \mathbb{R}$, $p : G \to V_G$ la projection canonique, et S l'ensemble des solutions de $x + y = 1, (x, y) \in G$.*

On a alors

$$|S| \leq 2|p(S)|.$$

Démonstration. Soient (x_0, y_0), (x_1, y_1) et (x_2, y_2) trois solutions distinctes, et supposons par l'absurde que leurs images par p sont toutes égales. $\frac{x_i}{x_0}$ et $\frac{y_i}{y_0}$, pour $i = 1, 2$, sont alors des racines de l'unité, ce qui contredit la proposition 8.2.6. □

Établissons maintenant des résultats sur les distances relatives entre les différentes solutions dans V_G. On note $\mathcal{S} = p(S)$ la projection sur V_G des solutions dans G.

Cette première propriété sera utilisée pour montrer que le ratio de deux normes de certains points qui sont « assez loin » et qui sont « dans le même cône » ne peut pas être très proche de 1. Les notions de « assez loin » et « dans le même cône » seront définies pendant la preuve finale du théorème.

Proposition 8.2.8. *Soient w_1, w_2 deux points distincts de $\mathcal{S}$. Alors,*

$$\|w_1\| \leq \ln(2) + 2\|w_2 - w_1\|.$$

Démonstration. Pour $i = 1, 2$, on note (x_i, y_i) les coordonnées du point w_i. La proposition 8.2.3 nous donne le résultat $H(A, B, 1) \leq 2H(a, b, 1)$ qu'on va donc appliquer avec

$$a = \frac{x_2}{x_1}, b = \frac{y_2}{y_1}, A = x_1, B = y_1.$$

On a

$$\begin{aligned}
\|w_1\| &= \max\left(h\left(x_1\right), h\left(y_1\right)\right) \\
&\leq h(x_1, y_1, 1) \\
&\leq \ln\left(2\right) + h\left(\frac{x_2}{x_1}, \frac{y_2}{y_1}, 1\right) \\
&\leq \ln\left(2\right) + 2\max\left(h\left(\frac{x_2}{x_1}\right), h\left(\frac{y_2}{y_1}\right)\right) \\
&= \ln(2) + 2\|w_2 - w_1\|,
\end{aligned}$$

où l'on a utilisé la propriété suivante sur la hauteur, qui découle de la définition comme produit de maximaux :

$$\max\left(H(a), H(b)\right) \leq H(a, b, 1) \leq \max\left(H(a), H(b)\right)^2.$$

On remarque que les coordonnées de $w_2 - w_1$ sont $\frac{x_2}{x_1}, \frac{y_2}{y_1}$ en raison du choix des lois de G en tant qu'espace vectoriel réel. □

Cette deuxième propriété sera utilisée pour montrer que le ratio de deux normes est majoré, pour des points vérifiant les mêmes conditions quand dans la propriété précédente.

Proposition 8.2.9. *Soient w_1, w_2 deux points distincts de $\mathcal{S}$ et $\rho \in \mathbb{N}$. On a alors*

$$\|w_1\| \leq \ln(c) + \frac{1}{\rho}\Big(\ln(2) + 2\|w_2 - \rho w_1\|\Big),$$

où $c = 6\sqrt{3}$.

Démonstration. Pour $i = 1, 2$, on note (x_i, y_i) les coordonnées du point w_i. La proposition 8.2.4 nous donne le résultat $H(A, B, 1) \leq 2^{1/\rho} c H(a, b, 1)^{1/\rho}$ qu'on va donc appliquer avec

$$a = \frac{x_2}{x_1^{2\rho}}, b = \frac{y_2}{y_1^{2\rho}}, A = x_1, B = y_1.$$

On a alors

$$\begin{aligned}\|w_1\| &= \max\left(h\left(x_1\right), h\left(y_1\right)\right)\\ &\leq h(x_1, y_1, 1)\\ &\leq \ln\left(c\right) + \frac{\ln\left(2\right)}{\rho} + \frac{1}{\rho} h\left(\frac{x_2}{x_1^{2\rho}}, \frac{y_2}{y_1^{2\rho}}, 1\right)\\ &\leq \ln\left(c\right) + \frac{\ln\left(2\right)}{\rho} + \frac{2}{\rho}\max\left(h\left(\frac{x_2}{x_1^{2\rho}}\right), h\left(\frac{y_2}{y_1^{2\rho}}\right)\right)\\ &= \ln\left(c\right) + \frac{1}{\rho}\Big(\ln\left(2\right) + \|w_2 - 2\rho w_1\|\Big),\end{aligned}$$

où l'on a de nouveau utilisé la propriété suivante sur la hauteur, qui découle de la définition comme produit de maximaux :

$$\max\left(H(a), H(b)\right) \leq H(a, b, 1) \leq \max\left(H(a), H(b)\right)^2.$$

□

Cette dernière propriété sera utilisée pour contrôler le nombre des points qui ne sont pas « assez loin ».

Proposition 8.2.10. *Soient w_0, w_1, w_2 trois points distincts de $\mathcal{S}$. Alors,*

$$\max(\|w_2 - w_0\|, \|w_1 - w_0\|) \geq \frac{1}{4}\log\rho \approx 0.022522...$$

où ρ est l'unique réel ≥ 1 tel que

$$\rho^{-6} + \frac{1}{2}\rho^{-2} = 1.$$

Démonstration. Pour $i = 1, 2, 3$, on note (x_i, y_i) les coordonnées du point w_i. La proposition 8.2.6 nous donne le résultat suivant :

$$\max_{i=1,2}\left(\max(H(x_i/x_0), H(y_i/y_0))\right) \geq \rho^4 \approx 1.022777...\,.$$

En passant au logarithme, on en déduit que

$$\max(\|w_2 - w_0\|, \|w_1 - w_0\|) \geq \frac{1}{4}\log\rho 0.022522...$$

□

8.3 Démonstration finale

8.3.1 • Reformulation du problème

Grâce à tout ce qui a été fait dans les chapitres précédents, on s'est ramené à un problème géométrique.

On va donc maintenant démontrer un théorème *géométrique* qui, si il utilise des hypothèses assez spécifiques puisqu'ici de notre analyse de l'équation $x+y=1$ par la théorie des hauteurs, pourrait très s'appliquer hors de ce contexte.

Les arguments qu'on va construire dans la sous-partie 8.3.2 sont par ailleurs tout à fait indépendants de ce qui a été fait ailleurs.

Énonçons donc maintenant ce théorème purement géométrique. La toute fin de ce chapitre se chargera de redescendre dans le monde de l'équation $x+y=1$ et d'appliquer ce théorème géométrique à des objets de type fini très généraux, puis à $\mathcal{O}_{K,S}^{\times}$.

Théorème 21 (Théorème de Beukers et Schlickewei, version géométrique)**.** *Soit Σ un sous-ensemble d'un espace vectoriel normé V qui satisfait les conditions suivantes.*

(i) $\|w_1\| \leq \ln(2) + 2\|w_2 - w_1\|$ *pour tous* $w_1, w_2 \in \Sigma$ *distincts.*

(ii) Il existe $c_1 \in \mathbb{R}$ *tel que pour tous* $\rho \in \mathbb{N}$ *et* $w_1, w_2 \in \Sigma$ *distincts on a*

$$\|w_1\| \leq c_1 + \frac{1}{\rho}\Big(\ln(2) + 2\|w_2 - 2\rho w_1\|\Big).$$

(iii) Il existe $c_0 \in \mathbb{R}_+^*$ *tel que pour tous* $w_0, w_1, w_2 \in \Sigma$ *distincts,*

$$\max(\|w_2 - w_0\|, \|w_1 - w_0\|) \geq c_0.$$

Alors, en notant $c_2 = \max\left(2\ln(2), c_1 + \frac{\ln(2)}{20}\right)$ *et* r *la dimension de* V*, on peut garantir que*

$$|\Sigma| \leq \frac{1}{2}\left(44 + 2\frac{c_2}{c_0}\right)^{r+1}.$$

8.3.2 • Recouvrir l'espace avec des boules

Comme expliqué dans la partie 8.3.1, on va se retrouver face à des propriétés géométriques. Afin de les exploiter au mieux pour borner le nombre de solutions, on va se munir de résultats de recouvrement par des boules ou par des cônes de certains domaines de l'espace vectoriel réel.

Ce sont des résultats très visuels et intuitifs, mais dont la démonstration peut être un peu technique.

Définition 8.3.1 (Recouvrement de l'espace)**.** Soient E un $\mathbb{R}$-espace vectoriel normé de dimension r et Φ une partie non vide de E. On appelle recouvrement par translations de E par Φ un ensemble Δ_Φ de points de E tels que

$$\bigcup_{x\in\Delta_\Phi}\Big(\Phi+x\Big)=E.$$

Cette définition se généralise à n'importe quel recouvrement d'une partie A de E.

Définition 8.3.2 (Recouvrement d'une partie)**.** Soient E un $\mathbb{R}$-espace vectoriel normé de dimension r et Φ une partie non vide de E. On appelle recouvrement par translations de A par Φ un ensemble Δ_Φ de points de E tels que :

$$A\subset\bigcup_{x\in\Delta_\Phi}\Big(\Phi+x\Big)$$

Comme on peut l'imaginer, il y a de nombreuses façons de recouvrir une partie A de E par une autre partie Φ. Un exemple déjà rencontré est le cas des réseaux dans $\mathbb{R}^n$, où on avait vu qu'il était possible de recouvrir l'espace tout entier par les translatés du domaine fondamental (voir proposition 2.1.7). Sur cet exemple, nos translatés ne s'intersectaient pas.

Néanmoins, dans la plupart des cas, on est obligé d'accepter que nos translatés de Φ se recouvrent partiellement mutuellement afin d'obtenir une couverture totale de A : on peut par exemple penser au cas du recouvrement d'un carré par un petit cercle dans le plan.

Il est alors intéressant de regarder la densité d'un recouvrement donné, c'est-à-dire d'évaluer à quel point nos Φ translatés se chevauchent. Pour cela on introduit une fonction de comptage.

Définition 8.3.3 (Fonction de comptage)**.** Pour un recouvrement par translations Δ_Φ de E par Φ, on introduit la fonction de comptage $\mathbf{v}$ définie par

$$\forall e\in E\ \ \mathbf{v}(e)=\Big|\{x\in\Delta_\Phi\,|\,e\in(\Phi+x)\}\Big|.$$

Ainsi, $\mathbf{v}$ compte, pour chaque e, le nombre de translatés de Φ auxquels appartient e (il y en a au moins 1).

La fonction de comptage est souvent utilisée dans les problèmes de recouvrement pour estimer la finesse du pavage. Il est par exemple courant de s'intéresser, pour des parties de A fixées, à la quantité

$$\frac{\int_A\mathbf{v}(x)dx}{\int_A dx},$$

qui évalue la densité du recouvrement. Ces considérations sont ici purement culturelles, et on se contentera du fait suivant.

Proposition 8.3.1. *Soit $R > 0$. Il existe un recouvrement par translations Δ_R de E par $B(0,R)$ qui vérifie*

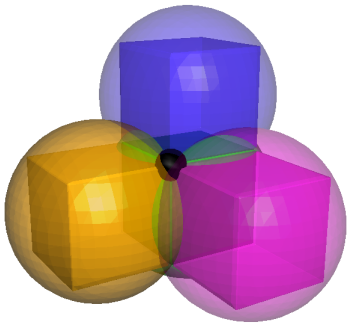
$$\forall x \in E \;\; \mathbf{v}(x) \leq 2^r.$$

Démonstration. Une possibilité consiste à regarder les hypercubes inscrits dans les boules, et à les empiler. Une telle construction constitue bien un recouvrement de E par des translatés de $B(0,R)$. La fonction de comptage est maximale sur les coins des hypercubes, en lesquels se rejoignent 2^r hypercubes, donc 2^r boules. Pour ces points, $\mathbf{v}(x) = 2^r$, et partout ailleurs c'est moins. Finalement, on a bien

$$\forall x \in E \;\; \mathbf{v}(x) \leq 2^r.$$

□

On représente cette construction sur le dessin suivant. L'idée est simple : plutôt que d'empiler les sphères, on empile les hypercubes, ce qui garantit qu'il n'y a pas de trous. On observe bien que les coins sont les points en lesquels le plus de sphères se chevauchent, et qu'il y en a 2^r.



On en déduit le théorème suivant, qui nous sera très utile.

Proposition 8.3.2. *Soit B la boule unité, soit $R > 0$. On peut recouvrir B avec au plus $(4 + \frac{2}{R})^r$ translatés de la boule $B(0,R)$.*

Démonstration. L'idée est d'extraire d'un recouvrement de l'espace E tout entier par $B(0,R)$ un recouvrement de B de cardinal plus petit que $(4 + \frac{2}{R})^r$. Dans la suite, on note $V(R)$ le volume pour la norme sur E de la boule $B(0,R)$.

Soit donc Δ_R un recouvrement de E par $B(0,R)$ vérifiant la propriété de 8.3.1. Alors en particulier, on voit que

$$\int_{B(0,1+2R)} \mathbf{v}(x)dx \leq 2^r V(1+2R).$$

Notons Δ' le recouvrement de $B(0,1)$ par $B(0,R)$ issu de Δ_R. Autrement dit,

$$\Delta' = \{x \in \Delta_R \,|\, (x + B(0,R)) \cap B \neq \emptyset\}.$$

On note N son cardinal. En particulier tous ces $x + B(0, R)$ sont inclus dans $B(0, 1 + 2R)$ par inégalité triangulaire. On a donc l'inégalité

$$\int_{B(0,1+2R)} \mathbf{v}(x)dx \geq \sum_{x\in\Delta'} V(R) = N(R),$$

d'où finalement

$$N \cdot V(R) \leq 2^r \cdot V(1 + 2R).$$

Or, $B(0, 1 + 2R) = (2 + \frac{1}{R})B(0, R)$, et donc $V(1 + 2R) = (2 + \frac{1}{R})^r V(R)$. Ainsi,

$$N \leq 2^r\Big(2 + \frac{1}{R}\Big)^r = \Big(4 + \frac{2}{R}\Big)^r,$$

ce qui est exactement ce qu'on voulait. □

On vient donc d'obtenir une majoration du nombre de petites boules nécessaires pour recouvrir une grosse boule. On obtient maintenant une inégalité qui est dans quelque sorte dans l'autre sens : on ne cherche maintenant plus à obtenir un pavage, mais plutôt à faire rentrer un nombre maximum de petites boules dans la grosse. On peut obtenir une majoration de cette quantité par un banal argument de volume.

Proposition 8.3.3. *On est toujours dans notre $\mathbb{R}$-espace vectoriel normé de dimension r. Soient $R > \delta > 0$. Soit B la boule de centre l'origine et de rayon R. On suppose que B contient un ensemble U de points qui vérifient :*

$$\forall u_1, u_2 \in U,\ u_1 \neq u_2 \implies ||u_1 - u_2|| \geq \delta$$

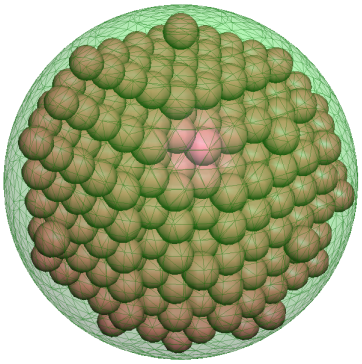
Alors $|U| \leq \Big(1 + 2\frac{R}{\delta}\Big)^r$

Démonstration. Notons V le volume de la boule unité. La propriété qui définit U signifie qu'autour de chaque point u de U on peut placer une boule ouverte B_u de rayon $\frac{\delta}{2}$, et que les boules B_u sont disjointes. Leur volume est $\Big(\frac{\delta}{2}\Big)^r V$. Mais toutes ces boules sont contenues dans une grosse boule de centre l'origine et de rayon $R + \frac{\delta}{2}$ puisque $U \subset B$. Le volume de cette boule est $\Big(R + \frac{\delta}{2}\Big)^r V$. En passant au volume, il vient :

$$|U|\Big(\frac{\delta}{2}\Big)^r V \leq \Big(R + \frac{\delta}{2}\Big)^r V$$

Cela donne bien $|U| \leq \Big(1 + 2\frac{R}{\delta}\Big)^r$ □

L'argument utilisé ici peut paraître peu raffiné. Après tout regarder les petites boules peuvent laisser beaucoup de volume libre, surtout lorsqu'elles ont un grand rayon. Dans le cas où elles sont nombreuses et petites (comme sur le dessin qui suit), l'approximation est meilleure.



On en déduit la propriété suivante, qui revient à recouvrir l'espace entier par des cônes d'origine 0.

Proposition 8.3.4. *Soient V un $\mathbb{R}$-espace vectoriel de dimension r doté d'une norme $\|\cdot\|$ et $\epsilon > 0$.*

Il existe alors un ensemble $E \subset V$ fini de vecteurs unitaires tel que tout $v \in V$ puisse s'écrire $v = \|v\|e + v'$ avec $e \in E$ et $\|v'\| \leq \epsilon\|v\|$.

De plus, E peut être choisi tel que son cardinal est plus petit que $\left(4 + \frac{4}{\epsilon}\right)^r$.

Démonstration. Prenons $\epsilon < 1$. Soit B la boule unité, et C le cercle unité. D'après la proposition 8.3.2, avec $R = \frac{\epsilon}{2}$, on dispose de $x_1, ...x_q \in V$, où $q = \lceil (4 + \frac{4}{\epsilon})^r \rceil$ tels que B soit recouverte par les $B(x_i, \frac{\epsilon}{2})$.

On regarde alors l'ensemble des boules qui intersectent la frontière de B, c'est-à-dire C.

$$I = \left\{ i \in [\![1, q]\!] \,\middle|\, B(x_i, \frac{\epsilon}{2}) \cap C \neq \emptyset \right\} = \left\{ i \in [\![1, q]\!] \,\middle|\, 1 - \frac{\epsilon}{2} \leq \|x_i\| \leq 1 + \frac{\epsilon}{2} \right\},$$

et on définit alors

$$E = \left\{ \frac{x_i}{\|x_i\|} \,\middle|\, i \in I \right\}.$$

E est bien défini car s'il existe i tel que $x_i = 0$, alors $i \notin I$.

De plus, on sait que $0 \in B$, donc on dispose de j_0 tel que $0 \in B(x_{j_0}, \frac{\epsilon}{2})$. On a $\|x_{j_0}\| \leq \frac{\epsilon}{2}$ donc $j_0 \notin I$. Ainsi,

$$|E| = |I| < \left(4 + \frac{4}{\epsilon}\right)^r.$$

Soit $v \in V$ un vecteur quelconque non nul. $\frac{v}{\|v\|} \in C$ donc on dispose de $j \in I$ tel que $\frac{v}{\|v\|} \in B(x_j, \frac{\epsilon}{2})$. On pose $e = \frac{x_j}{\|x_j\|}$. e et x_j sont colinéaires et $j \in I$, d'où

$$\|x_j - e\| = |1 - \|x_j\|| \leq \frac{\epsilon}{2}.$$

On pose $v' = v - \|v\|e$. On a

$$\frac{v'}{\|v\|} \leq \left\| \frac{v}{\|v\|} - x_j \right\| + \|x_j - e\| \leq \epsilon,$$

d'où le résultat voulu. □

8.3.3 • Un théorème général

Grâce à la sous-partie précédente, on va maintenant démontrer le théorème de Beukers et Schlickewei dans sa version géométrique, qu'on rappelle ici.

Ensuite, grâce aux raisonnements du reste de ce chapitre, et plus généralement à la majorité de ce livre, on va redescendre sur ce qui nous intéresse vraiment, et démontrer le théorème de Beukers et Schlickewei pour l'équation $x + y = 1$, dans un cas très général pour des objets de type fini. C'est le théorème 22.

La sous-section 8.3.4 redescendra encore un peu pour appliquer ce résultat au cas de l'équation aux S-unités dans $\mathcal{O}_{K,S}^{\times}$ (théorème 3).

Théorème (Théorème géométrique 21)**.** *Soit Σ un sous-ensemble d'un espace vectoriel normé V qui satisfait les conditions suivantes.*

(i) $\|w_1\| \leq \ln(2) + 2\|w_2 - w_1\|$ *pour tous $w_1, w_2 \in \Sigma$ distincts.*

(ii) Il existe $c_1 \in \mathbb{R}$ tel que pour tous $\rho \in \mathbb{N}$ et $w_1, w_2 \in \Sigma$ distincts on a

$$\|w_1\| \leq c_1 + \frac{1}{\rho}\Big(\ln(2) + 2\|w_2 - 2\rho w_1\| \Big).$$

(iii) Il existe $c_0 \in \mathbb{R}_+^*$ tel que pour tous $w_0, w_1, w_2 \in \Sigma$ distincts,

$$\max(\|w_2 - w_0\|, \|w_1 - w_0\|) \geq c_0.$$

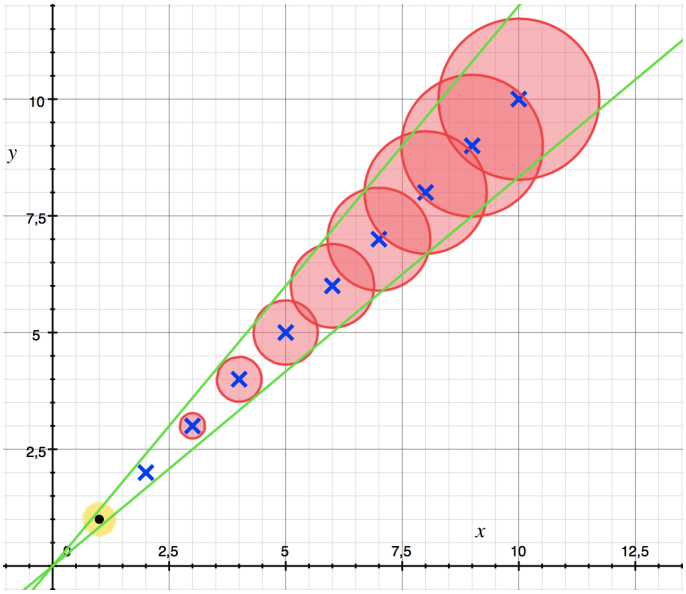
Alors, en notant $c_2 = \max\left(2\ln(2), c_1 + \frac{\ln(2)}{20}\right)$ et r la dimension de V, on peut garantir que

$$|\Sigma| \leq \frac{1}{2}\left(44 + 2\frac{c_2}{c_0}\right)^{r+1}.$$

Démonstration. Commençons par donner sommairement une interprétation géométrique des deux premières inégalités.

- L'inégalité (i) dit que si on a un point $w_1 \in \Sigma$ tel qu'il existe un point w_2 proche de lui, alors w_1 est petit. En particulier, cela signifie que la densité de nos points diminue au fur et à mesure qu'on s'éloigne de l'origine.
- L'inégalité (ii) est plus compliquée à interpréter, mais peut-être considérée de la façon suivante. Soit w_1 un point de Σ. On trace alors l'ensemble des points $2\rho w_1$, qui se place donc sur une droite. Si on a un w_2 qui est proche de l'un de ces points, alors w_1 doit être petit.

La figure-ci dessous illustre la situation. Si le point noir (ici $(1,1)$) est dans Σ, alors les zones rouges, qui sont simplement des cercles de centre ρw_1 avec ρ entier, sont interdites. On a aussi mis en jaune, la zone interdite de (i).



L'idée de la preuve apparaît alors clairement. Si on enferme w_1 dans un petit cône, les cercles rouges issues de (ii) vont interdire à d'autres points de Σ de trop grande norme d'être aussi dans le cône. De son côté, la cercle jaune de (i) va interdire les points trop proches de w_1. Finalement, on va pouvoir borner le nombre de points de cônes. Comme on sait par 8.3.4 qu'on peut obtenir un recouvrement de l'espace tout entier par un nombre fini de tels cônes, on a gagné.

Par contre, cet ne marchera que pour des points assez loin de l'origine, et ne dira rien pour ceux qui sont proches. Mais on pourra alors utiliser (iii).

Dès lors, le plan de la preuve est clair :

- La propriété 8.3.4 nous dit qu'on peut recouvrir l'espace V avec un nombre fini de cônes bien définis. On va montrer que chacun de ces cônes contient un nombre fini d'éléments de « grande » norme, c'est-à-dire en dehors d'une boule d'un rayon $c_3(\epsilon)$ bien choisi. On notera cette boule B_ϵ. Cela permettra de majorer $\Sigma \cap \overline{B_\epsilon}$
- Ensuite, on s'attaque aux points dans la boule de B_ϵ. On va alors montrer que les points de Σ peuvent être mis deux par deux dans des boules disjointes. En vertu de la proposition 8.3.3, on pourra donner une borne sur le nombre maximal de telles boules qui sont dans B_ϵ, ce qui permettra de borner $\Sigma \cap B_\epsilon$.
- On somme alors ces deux majorations pour obtenir le résultat final.

Passons à la partie technique. Soient ϵ un réel tel que $0 < \epsilon < \frac{1}{10}$.

Soit $c_3(\epsilon) = \frac{c_2}{1-10\epsilon}$. Ce sera la limite des « grandes » normes. Notons B_ϵ la boule de centre 0 et de rayon $c_3(\epsilon)$. Pour obtenir une majoration de $|\Sigma \cap \overline{B_\epsilon}|$, on travaille cône par cône. Soit

e un vecteur unitaire de V. On considère le cône

$$C_e = \Big\{ \mathbf{v} \in V \,\Big|\, \mathbf{v} = \|\mathbf{v}\| e + \mathbf{v}',\ \|\mathbf{v}'\| \leq \epsilon \|\mathbf{v}\| \Big\}.$$

On se propose de montrer que pour $w_1, w_2 \in \Sigma \cap C_e$ vérifiant $c_3(\epsilon) < \|w_1\| \leq \|w_2\|$, on a

$$\frac{5}{4}\|w_1\| \leq \|w_2\| \leq \Big(1 + \frac{4}{\epsilon}\Big)\|w_1\|.$$

C'est exactement le type de relation qui apparaît sur notre dessin. On verra que cela donnera une borne agréable pour $|\Sigma \cap \overline{B_\epsilon} \cap C_e|$.

Supposons d'abord par l'absurde qu'il existe $w_1, w_2 \in \Sigma \cap C_e$ et que $\|w_1\| \leq \|w_2\| \leq \frac{5}{4}\|w_1\|$. Il s'agit ici d'étudier un problème de proximité avec w_1, on utilise donc (i).

Écrivons, pour $i \in \{1, 2\}$, $w_i = \|w_i\| e + w_i'$ avec l'écriture du cône. D'après (i) on obtient

$$\begin{aligned}
\|w_1\| &\leq \ln(2) + 2\|w_2 - w_1\| \\
&= \ln(2) + 2\Big\|\Big(\|w_2\| - \|w_1\|\Big)e + w_2' - w_1'\Big\| \\
&\leq \ln(2) + 2\Big(\|w_2\| - \|w_1\|\Big) + 2\epsilon\Big(\|w_2\| + \|w_1\|\Big) && (\text{car } \|w_i'\| \leq \epsilon\|w_i\|) \\
&\leq \ln(2) + 2\frac{1}{4}\|w_1\| + 2\epsilon\frac{9}{4}\|w_1\|, && (\text{car } \|w_2\| \leq \tfrac{5}{4}\|w_1\|)
\end{aligned}$$

ce qui nous donne

$$\|w_1\| \leq \frac{2\ln(2)}{1 - 9\epsilon} \leq c_3(\epsilon),$$

ce qui est **absurde**.

Supposons maintenant par l'absurde que $w_1, w_2 \in \Sigma \cap C_e$ et que $\|w_2\| > (1+4/\epsilon)\|w_1\|$. Cette fois on est loin de w_1, donc on utilise (ii). Choisissons alors $\rho \in \mathbb{N}$ tel que $\|w_2\| = (2\rho + \delta)\|w_1\|$ avec $|\delta| \leq 1$. On remarque $\rho \geq \frac{2}{\epsilon} \geq 20$. En particulier, on a donc

$$\begin{aligned}
\|w_2 - \rho w_1\| &= \Big\|\|w_2\| e + w_2' - \rho\Big(\|w_1\| e + w_1'\Big)\Big\| \\
&= \Big\|(2\rho + \delta)\|w_1\| e + w_2' - 2\rho\|w_1\| e - 2\rho w_1'\Big\| \\
&= \Big\|\delta\|w_1\| e + w_2' - 2\rho w_1'\Big\|.
\end{aligned}$$

Alors, d'après (ii),

$$\begin{aligned}
\|w_1\| &\leq c_1 + \frac{1}{\rho}\Big(\ln(2) + 2\|w_2 - \rho w_1\|\Big) \\
&\leq c_1 + \frac{1}{\rho}\Big(\ln(2) + 2\big\|\delta\|w_1\|e + w_2' - 2\rho w_1'\big\|\Big) \\
&\leq c_1 + \frac{\ln(2)}{20} + \frac{2}{\rho}\Big(\|w_1\| + \epsilon(\|w_2\| + 2\rho\|w_1\|)\Big) \\
&\qquad\qquad (\text{car } \rho \geq \tfrac{2}{\epsilon} \geq 20,\ |\delta| \leq 1 \text{ et } \|w_i'\| \leq \epsilon\|w_i\|) \\
&\leq c_2 + \frac{2}{\rho}\|w_1\| + \epsilon\Big(8 + \frac{4}{\rho}\Big)\|w_1\| \\
&\qquad\qquad (\text{car } c_2 = \max\Big(2\ln(2), c_1 + \tfrac{\ln(2)}{20}\Big) \text{ et } \|w_2\| = (2\rho + \delta)\|w_1\|) \\
&\leq c_2 + \epsilon\|w_1\| + 9\epsilon\|w_1\|. \qquad (\text{car } \rho \geq \tfrac{2}{\epsilon})
\end{aligned}$$

On obtient donc $\|w_1\| \leq \frac{c_2}{1-10\epsilon} \leq c_3(\epsilon)$, ce qui est également **absurde**.

Maintenant, utilisons le résultat de ces deux inégalités. Soit $N \in \mathbb{N}$ le plus petit entier tel que $(5/4)^{N-1} > 1 + 4/\epsilon$. Montrons que chaque cône C_e contient au plus $N-1$ éléments de norme supérieure à $c_3(\epsilon)$.

Supposons par l'absurde qu'il existe $w_1, ..., w_N$ distincts appartenant à $\Sigma \cap C_e$ rangés par ordre croissant de module.

$$\begin{gathered}
(5/4)\|w_1\| \leq \|w_2\| \leq (1 + 4/\epsilon)\|w_1\| \\
(5/4)\|w_2\| \leq \|w_3\| \leq (1 + 4/\epsilon)\|w_2\| \\
\vdots \\
(5/4)\|w_{N-1}\| \leq \|w_N\| \leq (1 + 4/\epsilon)\|w_{N-1}\|
\end{gathered}$$

En multipliant ces inégalités et en simplifiant par les termes redondants on obtient

$$(5/4)^{N-1}\|w_1\| \leq \|w_N\|.$$

Or, en appliquant l'encadrement simplement pour w_1 et w_N on finit par avoir

$$(5/4)^{N-1}\|w_1\| \leq \|w_N\| \leq (1 + 4/\epsilon)\|w_1\|,$$

ce qui est **absurde** (par définition de N). Ainsi chaque cône contient au plus $N-1$ points distincts de norme supérieure à $c_3(\epsilon)$.

Regardons maintenant le nombre de tels cônes. L'avantage est qu'on a réussi à les prendre de taille uniforme. D'après le résultat de recouvrement 8.3.4, l'espace V peut-être recouverts avec $(4 + 4/\epsilon)^r$ de tels cônes. Il s'ensuit que le nombre de points de Σ qui ont une norme plus grande que $c_3(\epsilon)$ est plus petit que $(N-1)(4 + 4/\epsilon)^r$. Or, puisque $\epsilon < 0.1$, on a $N - 1 < 2/\epsilon$ (on peut obtenir ce résultat en passant au log et en étudiant les fonctions obtenues ou tout simplement en dessinant un graphe). Le nombre de points est donc majoré par $(2/\epsilon)(4 + 4/\epsilon)^r$. **La première étape est ainsi achevée**.

Il nous reste maintenant à regarder le nombre des éléments de norme plus petite que $c_3(\epsilon)$. La propriété (iii) empêche 3 points d'être très proches l'un de l'autre, mais n'empêche pas qu'il y ait seulement deux points qui le soient. On va donc prendre un système de représentants de nos points de façon à empêcher n'importe quels deux points d'être très proches.

Posons la relation d'équivalence sur les points de Σ de norme plus petite que $c_3(\epsilon)$, définie par

$$x\mathcal{R}y \iff \|x-y\| < c_0.$$

C'est une relation d'équivalence sur Σ. Le seul point à vérifier est que la relation est transitive. Soient donc x, y et $z \in \Sigma$ tels que $x\mathcal{R}y$ et $y\mathcal{R}z$. Prenons $x \neq y$ sinon il n'y a rien à faire. Alors par (iii), si z est distinct de x et y on sait que $\max(\|x-y\|, \|y-z\|) \geq c_0$. Or on a $\max(\|x-y\|, \|y-z\|) < c_0$, ce qui conclut que $x = z$ ou $y = z$. Ainsi $x\mathcal{R}z$: la transitivité est vérifiée. On en déduit par ailleurs que chaque classe d'équivalence contient au plus deux éléments.

Choisissons maintenant dans chaque classe d'équivalence un représentant unique. Cela revient à prendre, à chaque fois qu'on a deux points très proches, seulement l'un des deux. De plus, pour $x, y \in \Sigma$ deux représentants de deux classes disjointes, on a automatiquement

$$\|x-y\| \geq c_0.$$

Ainsi, l'ensemble Σ' des représentants vérifie que

(i) $|\Sigma| \leq 2|\Sigma'|$,

(ii) Les boules B_x de centre $x \in \Sigma'$ et de rayon $\frac{c_0}{2}$ sont disjointes.

Cela nous donne un ensemble de points vérifiant les conditions d'application de la propriété de recouvrement 8.3.3. L'application de cette propriété donne la majoration

$$|\Sigma'| \leq \left(1 + 2\frac{c_3(\epsilon)}{c_0}\right)^r$$

d'où on déduit

$$|\Sigma| \leq 2\left(1 + 2\frac{c_3(\epsilon)}{c_0}\right)^r.$$

On obtient ainsi

$$|\Sigma| \leq \frac{2}{\epsilon}\left(4 + \frac{4}{\epsilon}\right)^r + 2\left(1 + 2\frac{c_3(\epsilon)}{c_0}\right)^r.$$

On choisit alors ϵ tel que

$$\frac{4}{\epsilon} = 2\frac{c_3(\epsilon)}{c_0},$$

ce qui revient à dire que, en regardant la formule de $c_3(\epsilon)$,

$$\epsilon = \left(10 + 0.5\frac{c_2}{c_0}\right)^{-1}.$$

En particulier, on a bien $\epsilon < 0.1$. On peut donc écrire

$$|\Sigma| \leq \frac{1}{2}\left(44 + 2\frac{c_2}{c_0}\right)^{r+1}.$$

C'est exactement la borne qu'on voulait. □

On passe maintenant au résultat de type fini annoncé. Il s'agit simplement d'appliquer le théorème géométrique au cas d'un groupe de $\mathbb{Q}$-clôture de rang sans torsion fini.

Théorème 22 (Théorème de Beukers et Schlickewei pour le type fini)**.** *Soit H un sous-groupe de $(\overline{Q}^*)^2$ de type fini et de rang sans torsion r. Soit G la $\mathbb{Q}$-clôture de H. Alors l'équation*

$$x + y = 1, \quad (x, y) \in G,$$

a au plus 2^{8r+8} solutions.

Démonstration. On reprend les notations de 8.2.7. On note S l'ensemble des solutions dans G, et $p : G \to V_G$ la projection canonique. V_G est donc un $\mathbb{R}$-espace vectoriel de dimension r. On sait alors que $|S| \leq 2|p(S)|$, et on a noté $\mathcal{S} = p(S)$. On vérifie alors que $\mathcal{S}$ vérifie les conditions de la proposition 21.

- La proposition 8.2.8 garantit que pour w_1, w_2 deux points distincts de $\mathcal{S}$ on a $\|w_1\| \leq \ln(2) + 2\|w_2 - w_1\|$.
- La proposition 8.2.9 donne $c_1 = \ln(6\sqrt{3})$.
- La proposition 8.2.10 donne $c_0 \approx 0.022522...$

Par le théorème 21, on a la majoration (après approximation numérique) :

$$|\mathcal{S}| \leq \frac{1}{2}\left(44 + 2\frac{c_2}{c_0}\right)^{r+1} \leq \frac{1}{2}2^{8r+1}.$$

Ainsi on a bien :

$$|S| \leq 2^{8r+1}.$$

□

8.3.4 • Corollaire : borne du nombre de solutions de l'équation aux S-unités

Théorème (Théorème de Beukers et Schlickewei pour les S-unités – Théorème 3)**.** *Soit K un corps de nombres. Soit S un ensemble d'idéaux premiers non nuls de $\mathcal{O}_K$. L'équation*

$$x + y = 1, x, y \in \mathcal{O}_{K,S}^{\times} \tag{9}$$

admet au plus $2^{16(r+s)+8}$ solutions, où $r = r_1 + r_2 - 1$ avec les notations de 1.5.8.

Démonstration. On sait que $\mathcal{O}_{K,S}^{\times} \cong \mu(K) \times \mathbb{Z}^{r+s}$. On pose $H = (\mathcal{O}_{K,S}^{\times})^2 \subset \overline{(\mathbb{Q}^*)}^2$ comme dans 8.1.1.

$$\begin{aligned} H &\cong (\mathcal{O}_{K,S}^{\times})^2 \\ &\cong (\mu(K) \times \mathbb{Z}^{r+s})^2 \\ &\cong \mu(K)^2 \times \mathbb{Z}^{2(r+s)} \end{aligned}$$

Ainsi la torsion de H est exactement $\mu(K)^2$, H est de type fini et de rang sans torsion $2(r+s)$. Dès lors, on note G sa $\mathbb{Q}$-clôture. On peut donc appliquer le théorème 22.

On en déduit que le nombre de solutions de l'équation

$$x + y = 1, \quad x, y \in G$$

est inférieur à $2^{16(r+s)+8}$. Or le nombre de solutions de

$$x + y = 1, \quad x, y \in (\mathcal{O}_{K,S}^{\times})^2$$

est encore plus petit puisque $H \subset G$. Ainsi, on obtient notre théorème. □

RÉFÉRENCES

[1] K. Mahler : Zur approximation algebraischer zahlen. I. (Über den größten primteiler binärer formen). *Mathematische Annalen*, 107:691–730, 1933.

[2] F. Beukers et H.P. Schlickewei : The equation x+y=1 in finitely generated groups. *Acta Arithmetica*, 78, 01 1996.

[3] Axel Thue : Über annäherungswerte algebraischer zahlen. *Journal für die reine und angewandte Mathematik*, 1909.

[4] Carl Siegel : Über einige anwendungen diophantischer approximationen. 1:209–266, 1929.

[5] D. Lewis et Kurt Mahler : On the representation of integers by binary forms. *Acta Arithmetica*, 6(3):333–363, 1961.

[6] J.H. Evertse : On equation in s-units and the thue-mahler equation. *Inventiones mathematicae*, 75:561–584, 1984.

[7] F. Beukers et Don Zagier : Lower bounds of heights of points on hypersurfaces. *Acta Arithmetica*, 79, 01 1997.

[8] Alejandra Alvarado, Angelos Koutsianas, Beth Malmskog, Christopher Rasmussen, Christelle Vincent et Mckenzie West : A robust implementation for solving the s-unit equation and several applications, 2019.

[9] J.-H. Evertse, K. Győry, C. L. Stewart et R. Tijdeman : *S-unit equations and their applications*, page 110–174. Cambridge University Press, 1988.

[10] U. Zannier et F. Amoroso : *Lecture Notes on Diophantine Analysis*. Publications of the Scuola Normale Superiore. Scuola Normale Superiore, 2009.

[11] Kálmán Győry : S-unit equation in number fields : effective results, generalization, abc conjecture. *RIMS Kokyusoku*, 1710:71–84.

[12] Olivier Debarre : *Algèbre 2*. École Normale Supérieure, 2012-2013.

[13] Mathilde Gerbelli-Gauthier : *Le théorème des unités*. 2013.

[14] Gaëtan Chenevrier : *Théorie algébrique des nombres*. École polytechnique, 2018-2019.

[15] Lionel Duclos : *Idéaux inversibles – Anneaux de Dedekind*. Université de Poitiers, 2009.

[16] Gilles Auriol : *Groupe des classes d'idéaux d'un corps de nombres*. 2008.

[17] Michel Cretin : *Théorie de Galois et nombres algébriques*. Université Claude Bernard Lyon 1.

[18] Jean-François Dat : *Cours introductif de M2, Théorie des Nombres*. Université Pierre et Marie Curie, 2012-2013.

[19] 3Blue1Brown : What does it feel like to invent math ?

[20] Pierre Colmez : *Les nombres p-adiques, notes du cours de M2*. Université Pierre et Marie Curie.

[21] Mourad ABOUZAID : *Hauteurs et équations diophantiennes*. Institut de Mathématiques de Bordeaux.

[22] Bjorn Poonen : *Lecture on rational points on curves*. University of California, Berkeley, 2006.

[23] Keith Conrad : *Ostrowski's theorem for $F(T)$*. University of Connecticut.

[24] José Felipe Voloch : The equation $ax + by = 1$ in characteristic p. *Journal of Number Theory*, 73:195–200.

[25] G. H. Hardy et E. M. Wright : *An Introduction to the Theory of Numbers*. 1938.

[26] David Renard : *Calcul Différentiel et analyse complexe*. Département de Mathématiques Ecole Polytechnique, 2018.

[27] Krzysztof JAN NOWAK : Some elementary proofs of puiseux's theorems. 1996.

[28] Daniel Murfet : *Hensel's Lemma*, 2005.

[29] Patrick Polo : *Algèbre et théorie de Galois*. Paris VI, 2005-2006.

[30] F.Beukers et R.Tijdeman : On the multiplicities of binary complex recurrences. *Compositio Mathematica*, pages 193–213, 1984.

[31] Daniel Perrin : *Réseaux et applications*.