Cours de mathématiques

TOME II

RUDIMENTS

Mathématiques générales

France $\sim$ 2025

Écrit et réalisé par Louis Lascaud

Table des matières

Chapitre 1

Calcul littéral

Résumé

On s'intéresse aux techniques primitives de l'algèbre permettant la simplificaton des quatre opérations usuelles : l'addition, la soustraction, la multiplication et la division. Un intérêt tout particulier est voué à l'efficacité des écritures.

1.1 Fractions

Exercice 1 *(Calcul de fractions à l'égyptienne)*

Résoudre $\frac{x+1}{s+1} = \frac{x}{s}$.

▷ **Éléments de réponse.**

Les solutions sont $((x,s), s \neq 0, -1, x = s)$.

1.2 Grosses formules qui se simplifient

Formule. ***(Gamma et logarithme intégral)***

$$\int_0^\infty \sum_{n=1}^{\infty} \frac{(-1)^n}{n^s} \Gamma(\frac{3}{2}n^2) e^{-\zeta(s)} \mathrm{d}s = \lim_{z \to 0} \left(\frac{\partial^2}{\partial z^2} (\mathrm{Li}_3(z^2) + \frac{z}{\pi^z} \Gamma(z)\psi(z)) \right).$$

Chapitre 2

Théorie des graphes

2.1 Lexique des graphes

2.1.1 Graphes remarquables

2.1.1.1 Graphes réguliers

Définition. ***(Graphe bipartite)***

Soit $k \in \mathbb{N}$. Un graphe *(régulier) de degré* k est un graphe dont tous les sommets ont même degré k.

2.1.1.2 Graphes bipartites

Définition. ***(Graphe bipartite)***

Un graphe est *bipartite* si l'ensemble des sommets se partitionnent en deux ensembles A et B tels que toute arête du graphe est entre un sommet de A et un sommet de B, mais jamais entre deux sommets de A ou deux sommets de B.

2.1.1.3 Arbre

Définition. ***(Arbre enraciné)***

Un arbre est un graphe tel qu'entre deux sommets donnés, il existe un unique chemin entre ces deux sommets.

VOC Soit $n \in \mathbb{N}$. Un arbre n-aire est un arbre où le degré maximal des sommets est n, et il existe un sommet de degré n.

Définition. ***(Arbre enraciné)***

Soit $n \in \mathbb{N}$. Un arbre enraciné est la donnée d'un arbre et d'un sommet de cet arbre, appelé *racine*, de degré exactement n.

2.2 Problème du plus court chemin

Principe. ***(Principe fondamental de la complexité)***

Soit G un graphe orienté de profondeur p dont le nombre d'incidence est borné par n. Le calcul du nombre de chemins sur G est en $\mathcal{O}(\underbrace{n^{n^{\cdot^{\cdot^{\cdot^{n}}}}}}_{p \text{ occurrences}})$.

2.3 Expansion

2.3.1 Définitions

2.3.1.1 Graphes localement finis

Définition. ***(Graphe localement fini)***

Un graphe X est localement fini si $\deg(x) < \infty$ pour tout sommet x de X.

2.3.1.2 Opérateur de Markov

Remarque. On considère implicitement l'espace des fonctions numériques $\ell^2(X) = \{f : X \to \mathbb{R} \text{ ou } \mathbb{C} \mid \sum_{x \in X} f^2(x) < +\infty\}$; en particulier, si X est fini, $\ell^2(X) = \mathcal{F}(X,\mathbb{R})$.

Définition. ***(Opérateur de Markov sur un graphe)***

Soit X un graphe localement fini. L'*opérateur de Markov* sur X, noté $M_X = M$, est,l'opérateur linéaire défini sur $\ell^2(X) \to \ell^2(X)$ par $f \longmapsto Mf : x \mapsto \frac{1}{\deg(x)} \sum_{y \in X, y \sim x} f(y)$; autrement dit, Mf calcule la moyenne des valeurs sous f des sommets adjacents.

2.3.1.3 Laplacien discret sur un graphe

Définition. ***(Laplacien discret)***

Soit X un graphe localement fini. On note M l'opérateur de Markov sur X. Le *laplacien discret* sur X, noté $\Delta_X = \Delta$, est l'opérateur linéaire défini sur $\ell^2(X) \to \ell^2(X)$ et vaut $\Delta := id - M$, c'est-à-dire pour tout $x \in X$, $\Delta f(x) = f(x) - \frac{1}{\deg(x)} \sum_{y \sim x} f(y)$.

On appelle *valeurs propres du graphe* X, celles de son laplacien défini sur $\ell^2(X,\mathbb{R})$.

Exercice 1 *(Positivité du laplacien)*

On considère les fonctions sur les graphes à valeurs réelles. Montrer que sur tout graphe fini de cardinal n, $\Delta \in S_n^+(\mathbb{R})$. En particulier, les valeurs propres d'un graphe sont des réels positifs.

▷ **Éléments de réponse.**

Le laplacien est symétrique, car on considère des graphes non orientés. De plus, si f est un vecteur positif, *i.e.* $f(x) \geqslant 0$ pour les n sommets x de X, alors $\langle \Delta f,f\rangle = \sum_{x\in X}\sum_{y\sim x} \frac{1}{\deg(x)} f(x)f(y) \geqslant 0$, d'où le résultat.

2.3.1.4 Constantes isopérimétriques

Heuristique

La constante isopérimétrique dans un graphe mesure le taux de connectivité des sommets de ce graphe.

Définition. ***(Frontière d'une partie d'un graphe)***

Soit X un graphe localement fini. Soit A une partie finie des sommets de X. La *frontière* de A est l'ensemble des arêtes $\{(x,y),x \in A,y \in \complement_X A\}$.

Définition. ***(Constante isopérimétrique sur un graphe)***

Soit X un graphe localement fini. La *constante isopérimétrique* associée à X est la quantité

$$h(X) = \inf\{\frac{\mathrm{card}(\partial A)}{\mathrm{card}(A)},A \in \mathrm{Fin}(X)\}.$$

Exemples. ***(Constante isopérimétrique sur des graphes)***

1. La constante isopérimétrique d'un graphe est nulle si et seulement s'il est non connexe.
2. La constante isopérimétrique d'un graphe est égale à 1 s'il est connexe et contient une partition des sommets en A,B telles qu'il n'existe aucune arête entre A et B, sauf une (a,b) pour un certain $a \in A$ et un certain $b \in B$.

Dans le cas d'un graphe fini, c'est le taux d'expansion qui remplace la constante isopérimétrique.

2.3.1.5 Graphes expanseurs

Définition. ***(Taux d'expansion, graphe expanseur)***

① Soit X un graphe fini de cardinal n. Le *taux d'expansion* ou *nombre isopérimétrique (d'expansion)* ou *constante de Cheeger* de X est défini par

$$h(X) = \min_{A \subseteq X, \operatorname{card}(A) \leqslant \frac{n}{2}} \frac{\operatorname{card}(\partial A)}{\operatorname{card}(A)}.$$

② Une suite de graphes finis $(X_n)_{n\in\mathbb{N}}$ de degré fixé k **dont le cardinal tend vers l'infini** est une *suite d'expanseurs* s'il existe $c > 0$ une constante telle que $h(X_n) \geqslant c > 0$ pour tout $n \in \mathbb{N}$.

Fait

Il n'y a pas d'expanseurs de degré 2.

En effet, un tel graphe est un cycle, et dans un cycle de longueur n, on peut considérer un chemin de $\lfloor \frac{n}{2} \rfloor$ sommets consécutifs, où alors $\frac{\operatorname{card}(\partial A)}{\operatorname{card}(A)} = \frac{2}{\frac{n}{2}} = \frac{4}{n} \underset{n\to+\infty}{\longrightarrow} 0$, ce qui contredit la condition d'expansion.

$\longrightarrow$ *Convention.* On peut donc supposer $k \geqslant 3$ dans la définition précédente de suite d'expanseurs.

Heuristique

Pour un degré k fixé, le graphe infini de degré k à la plus grande constante isopérimétrique est l'arbre T_k, graphe sans cycle : c'est le meilleur « expanseur infini ».
Par contre, les arbres font les pires expanseurs finis.

Pour montrer l'existence d'expanseurs, on utilie la notion suivante.

2.3.1.6 Construction d'expanseurs

Définition. ***(Graphe aléatoire)***

Soient n,k deux entiers naturels. On note $X(2n,k)$ l'ensemble des (n,k)-*graphes aléatoires*, construits de la manière suivante : notre graphe est bipartite (I,O) qui sont respectivement appelés *inputs* et *outputs*, où I et O ont chacun n éléments numéroté de 1 à n. On choisit k permutations $(\pi_1,...,\pi_k)$ de $[\![1,n]\!]$ et on trace les arêtes $(i \in I, \pi_j(i) \in O)$ où i parcourt I et j parcourant $[\![1,k]\!]$. Un tel graphe a donc bien $2n$ sommets et est régulier de degré k par construction.
On distinguera au sens du cardinal card′ deux graphes de $X(2n,k)$ s'ils sont définis par deux k-uplets de $\mathfrak{S}_n$ différents, ce qui est plus fort que l'isomorphie et même que l'égalité des graphes. Autrement dit, $X(2n,k) \simeq \mathfrak{S}_n^k$.

Le résultat suivant est contraire à l'intuition, car les graphes expanseurs sont difficiles à construire, mais pourtant :

Théorème. ***(Théorème de Pinsker)***

Soient n,k deux entiers naturels. Pour $k \geqslant 5$,

$$\frac{\text{card}'(X \in X(2n,k) \mid h(X) \geqslant \frac{1}{2})}{\text{card}'(X(2n,k))} \underset{n\to+\infty}{\longrightarrow} 1.$$

▷ On définit juste pour un moment : $\overline{h}(X) = \min\{\frac{\text{card}(\partial' A)}{\text{card}(A)} \mid A \subseteq I, \text{card}(A) \leqslant \frac{\text{card}(I)}{2} = \frac{n}{2}\}$. On a en particulier $\overline{h}(X) \geqslant h(X)$. Pour un graphe tel que $\overline{h}(X) \leqslant \frac{3}{2}$, on prend $\text{card}(A) \leqslant \frac{n}{2}$ où $A \subseteq I$, et $B \subseteq O$ où $\text{card}(B) = \lfloor \frac{3}{2}\text{card}(A) \rfloor$ de sorte que $\pi_j(A) \subseteq B$ pour tout $j \in [\![1,k]\!]$. Alors le nombre de mauvais choix est majoré par $\sum_{\substack{A\subseteq I \\ \text{card}(A)\leqslant \frac{n}{2}}} \sum_{\substack{B\subseteq O \\ \text{card}(B)=\lfloor \frac{3}{2}\text{card}(A)\rfloor}} [|B|(|B|-1)...(|B|-|A|+1)(n-|A|)!]^k = \sum_{i=1}^{\frac{n}{2}} \binom{n}{i}\binom{n}{\lfloor \frac{3}{2}i \rfloor}\left(\frac{(\lfloor \frac{3}{2}i \rfloor)!}{(\lfloor \frac{i}{2} \rfloor)!}(n-i)!\right)^k$. Comme le nombre de choix favorables est de $\text{card}'(X(2n,k)) = n!^k$, le rapport tend vers 0, ce qui conclut. ■

Corollaire

Pour tout entier $k \geqslant 5$, il existe des expanseurs de degré k.

▷ Pour n arbitrairement grand, les graphes de $X(2n,k)$ sont « presque » tous expanseurs de degré k pour la constante $c = \frac{1}{2}$, « presque » pris au sens de la densité pour *card*. En particulier, il existe une suite $(n_i)_{i\in\mathbb{N}}$ d'entiers tendant vers l'infini, telle que $X_n \in X(2n,k)$ et $h(X) \geqslant \frac{1}{2}$. ■

Chapitre 3

Théorie des réseaux

Résumé

Après l'exposé des théorèmes classiques sur les sous-groupes de $\mathbb{R}$ puis les sous-groupes de $\mathbb{R}^n$ et $\mathbb{C}^n$, et notamment leurs sous-groupes fermés et discrets, on s'intéresse de près au cas particulier des réseaux et à la théorie qui en découle, qui pave la voie aux grands théorèmes de la théorie algébrique des nombres relatifs à la structure des corps de nombres.

3.1 Sous-groupes de $\mathbb{R}^n$

3.1.1 Sous-groupes additifs de $\mathbb{R}$

Théorème. ***(Sous-groupes additifs des réels)***

Les sous-groupes de $(\mathbb{R},+)$ sont monogènes, c'est-à-dire de la forme $\alpha\mathbb{Z}$ pour $\alpha \in \mathbb{Z}$, ou denses dans $\mathbb{R}$.
En particulier, les sous-groupes additifs de $\mathbb{R}$ sont discrets ou denses, ces deux conditions s'excluant mutuellement, et un sous-groupe de $\mathbb{R}$ est discret si et seulement s'il est engendré par un seul élément ou encore si et seulement s'il est fermé ou impropre.

▷ Soit H un sous-groupe non nul de $\mathbb{R}$. Soit $\alpha = \inf(H \cap \mathbb{R}_+^*)$. Distinguons deux cas. Si $\alpha > 0$, montrons que $H = \alpha\mathbb{Z}$. Vérifions que $\alpha \in H$: une partie de la preuve à ne pas négliger ! C'est un infimum du fermé H ; en effet, soit $(g_n)_{n\in\mathbb{N}} \in H^{\mathbb{N}}$ une suite convergente dans $\mathbb{R}$. Alors $g_n - g_{n-1}$ converge vers zéro. Ainsi, à partir d'un certain rang, $|g_n - g_{n-1}| < \alpha$. Absurde, car $g_n - g_{n-1} \in H$. Remarquons que $x \in H \iff -x \in H$. Réciproquement, $H \subseteq \alpha\mathbb{Z}$. En effet, si $x \in H$, on peut faire une pseudo-division euclidienne par $\alpha \neq 0$: $\frac{x}{\alpha} = \lfloor \frac{x}{\alpha} \rfloor + \{\frac{x}{\alpha}\}$, d'où $x = q\alpha + r$ où $q \in \mathbb{Z}$ et $r \in [0, \alpha[$. En appliquant le même argument que dans $\mathbb{Z}$ (principe de minimalité), on trouve $x = q\alpha$. Si maintenant $\alpha = 0$, on vérifie que H est dense dans $\mathbb{R}$. C'est la même preuve que la densité de $\mathbb{Q}$. Soient $x < y$ deux réels. Alors $\varepsilon = y - x > 0$; soit donc $h \in H$, $h \in]0,\varepsilon[$. Soit p le plus entier tel que $ph \geqslant x$. Alors $k = ph \in H$ et $x \leqslant k$ et $(p-1)h = k - h < x$ d'où $k - x < h < y - x$ puis $k < y$, ce qu'il fallait montrer. ■

On en déduit la propriété suivante :

Propriété. ***(Structure des peignes réels doubles)***

Soient $a,b \in \mathbb{R}$ non nuls. Alors $a\mathbb{Z} + b\mathbb{Z}$ est dense dans $\mathbb{R}$ si et seulement si a et b sont incommensurables.

▷ Immédiat avec la propriété précédente. ■

Corollaire

Soient $a,b \in \mathbb{R}$ non nuls. Alors $a\mathbb{N} + b\mathbb{Z}$ est dense dans $\mathbb{R}$ si et seulement si a/b est irrationnel.

▷ Là, ce n'est plus du tout évident. Le sens direct est clair puisque c'est une condition plus forte que celle de la propriété précédente. Supposons a/b irrationnel. Soit $]u,v[$ un intervalle ouvert non trivial de $\mathbb{R}$, soit $u < v$. Si $0 \in]u,v[$, on peut aller se coucher. Sinon, supposons $u > 0$; on se ramène à ce cas car, sinon, $v < 0$ et l'on invoque la propriété d'isotropie des sous-groupes des réels : $x \in H \iff -x \in H$. Comme dans toute preuve de densité (prendre par exemple la précédente), il suffit de montrer que $]0,\varepsilon[\cap (a\mathbb{N} + b\mathbb{Z}) \neq \emptyset$ où $\varepsilon = v - u$, car la suite ne fait intervenir que des dilatations $p \in \mathbb{N}$ qui préservent donc $a\mathbb{N} + b\mathbb{Z}$.

Justifions ce point crucial. Il existe une infinité de $na + bm$ avec $n,m \in \mathbb{Z}$ dans $]0,\varepsilon[$, infinité grâce aux propriétés usuelles de densité de $\mathbb{R}$ en lui-même. Or s'il n'en est aucun avec $n \in \mathbb{N}$, soit au moins un (qui n'est donc pas dur à trouver) donné par $x = an + bm$, $n < 0$. Il y a encore une infinité de $an' + bm'$ dans $]0,x[$, qui ont encore tous $n' < 0$, sinon contradiction avec l'hypothèse, car $]0,x[\subseteq]0,\varepsilon[$! Mais pourtant, pour un entier $p \in]n,0[$, il n'y a qu'un nombre fini de $ap + bm'$ dans $]0,x[$. Comme il n'y a aussi qu'un nombre fini d'entiers $p \in]n,0[$, il n'y a qu'un nombre fini d'éléments dans $]0,x[$ de la forme $an' + bm'$ avec $n' > n$. En particulier il existe au moins un (qui n'est donc pas dur à trouver) donné par $x' = an' + bm'$ avec $p,m' \in \mathbb{Z}$ et $n' \leqslant n$. Mais alors $x - x' \in]0,\varepsilon[$ s'écrit bien $a(n - n') + b(m - m')$ et $n - n' \in \mathbb{N}$, d'où le résultat. ■

Corollaire

Le sous-groupe $\{a + b\delta \mid a,b \in Z\}$ est discret si et seulement si $\delta \in \mathbb{Q}$.

Exemple fondamental

Le sous-anneau $\mathbb{Z}[\sqrt{2}]$ est dense dans $\mathbb{R}$.

Corollaire

Le complémentaire d'un sous-groupe additif strict de $\mathbb{R}$ est indénombrable.

Exercice 1

Montrer que le sous-anneau $\mathbb{Z}[\delta] = \{P(\delta) \mid P \in \mathbb{Z}[X]\}$ n'est jamais discret, sauf si $\delta \in \mathbb{Z}$, soit $\mathbb{Z}[\delta] = \mathbb{Z}$. En déduire que le groupe additif $(\mathbb{R}, +)$ contient des sous-groupes abéliens libres de tout rang, et donc, qu'il n'est pas libre de type fini.

Exercice 2 *(Amélioration)*

Montrer qu'un sous-anneau contenant strictement $\mathbb{Z}$ est dense dans $\mathbb{R}$.

▷ **Éléments de réponse.**

Si $\delta \in R \setminus \mathbb{Z}$, on écrit $\delta = \lfloor \delta \rfloor + r$ où $r \in R$ et donc contient la suite $(r^n)_n$ qui tend vers zéro, et il est facile de conclure.

3.1.2 Sous-groupes additifs de l'espace euclidien

Soit n un entier naturel.

3.1.2.1 Un mot d'abord sur les sous-groupes de (ℂ,+)

Lemme

$(\mathbb{C},+)$ est sans torsion.

Proposition. ***(Existence d'une base sur un sous-groupe additif de $\mathbb{C}$)***

Soit G un sous-groupe additif non nul de type fini de $\mathbb{C}$, c'est-à-dire qu'il existe des scalaires $x_1,...,x_p$ tels que $G \subseteq \sum_{l=1}^{p} \mathbb{Z}x_l$. Il existe alors une famille $e_1,...,e_m$ dans G, avec $1 \leqslant m \leqslant p$ telle que $G = \bigoplus_{1 \leqslant l \leqslant m} \mathbb{Z}e_l$.

La famille des e_l est une base du groupe G, c'est-à-dire que tout $g \in G$ s'écrit de façon unique sous la forme $\sum a_l e_l$ avec des a_l entiers relatifs, l'entier m ne dépendant que de G ; c'est le *rang de* G.

Proposition. ***(Théorème de la base adaptée)***

Soit G un sous-groupe de type fini de $(\mathbb{C},+)$ et plus précisément de rang m. Si H désigne un sous-groupe de G, alors ile xiste uen famille $(e_1,...,e_m)$ dans G et des entiers $d_1,...,d_m$ tels que $G = \sum \mathbb{Z}e_l$ et $H = \sum \mathbb{Z}d_l e_l$. La famille des e_l est une abse du groupe G, dite *adaptée* à H.

En outre, H est un sous-groupe de G d'indice fini si, et seulement si, les d_l sont tous non nuls ; dans ce cas, l'ordre du groupe quotient G/H est $\prod d_l$.

Tout sous-groupe H de G est aussi de type fini, de rang $\leqslant m$. Enfin, H est d'indice fini

$\iff$ il est lui-même de rang m.

3.1.2.2 Rappels de rappels sur les sous-groupes de $\mathbb{Z}^n$

Théorème. ***(Théorème de la base adaptée)***

Soit H un sous-groupe additif de $\mathbb{Z}^n$. Alors, H est abélien libre de type fini, de rang $\leqslant n$. Il exsite une base $(e_1,...,e_n)$ de $\mathbb{Z}^n$ et des entiers $d_1 \mid d_2 \mid ... \mid d_r$ tels que $(d_1e_1,...,d_re_r)$ soit une base de H. Les entiers d_i, appelés *facteurs invariants* de H, sont déterminés de manière unique au signe près. La base e est dite *adaptée au sous-module* H de $\mathbb{Z}^n$.
De plus, le quotient $\mathbb{Z}^n/H$ est isomorphe au groupe abélien de type fini $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times ... \times \mathbb{Z}/d_r\mathbb{Z} \times \mathbb{Z}^{n-r}$, et deux sous-groupes H_1,H_2 sont conjugués sous l'action de $GL_n(\mathbb{Z})$ si et seulement si $\mathbb{Z}^n/H_1 \simeq \mathbb{Z}^n/H_2$.

Corollaire. ***(Facteur direct parmi les sous-groupes de $\mathbb{Z}^n$)***

En particulier, H est facteur direct si et seulement si tous les facteurs invariants sont égaux à 1, en particulier les noyaux de morphismes $\mathbb{Z}^n \to \mathbb{Z}^m$.

Reformulation pratique

Soit M un morphisme de $\mathbb{Z}^n$ dans $\mathbb{Z}^m$. Soient $(d_1,...,d_r)$ les coefficients diagonaux de la forme normale de Smith de M. Alors les d_i s'avèrent être les facteurs invariants de l'image de M dans $\mathbb{Z}^m$, et

$$\mathrm{Coker}(M) = \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times ... \times \mathbb{Z}/d_r\mathbb{Z} \times \mathbb{Z}^{m-r}.$$

3.1.2.3 Classification des sous-groupes fermés de $\mathbb{R}^n$

Nous nous intéressons maintenant au cas général des groupes fermés. On laisse au lecteur le soin de se convaincre qu'il est illusoire de vouloir classifier tous les sous-groupes additifs de $\mathbb{R}^n$ (sans l'hypothèse de fermeture).

Théorème. ***(Sous-groupes additifs fermés de l'espace euclidien)***

Les sous-groupes fermés G de $(\mathbb{R}^n, +)$ sont discrets ou contiennent une droite, ces deux conditions s'excluant mutuellement. De plus, dans le second cas, la composante connexe de G contenant l'origine est un sous-espace vectoriel W et l'image de G dans $\mathbb{R}^n/W$ est discrète.
En d'autres termes, il existe un sous-espace vectoriel unique V et un sous-groupe discret (non unique) H tels que $G = V \oplus H$, c'est-à-dire, avec des éléments plus lointains, il existe

$d \leqslant r \leqslant n$ et $(e_1,...,e_d, \varepsilon_{d+1},..., \varepsilon_r)$ une famille $\mathbb{R}$-libre telle que :

$$G = \bigoplus_{i=1}^{d} \mathbb{R}e_i \oplus \bigoplus_{i=d+1}^{r} \mathbb{Z}e_i.$$

Ainsi, pour tout groupe fermé G de $\mathbb{R}^n$, il existe un unique couple d'entiers (d,r) tels que $G \simeq \mathbb{R}^d \oplus \mathbb{Z}^{d-r}$. De plus, G est un espace vectoriel si et seulement si $r = d$, et G est discret si et seulement si $d = 0$.

▷ Soit H un sous-groupe fermé de $\mathbb{R}^n$. Supposons qu'il n'est pas discret. Quitte à prendre une différence, soit $(t_n)_{n\in\mathbb{N}}$ qui tende vers 0. Par hypothèse, cette suite n'est pas stationnaire à zéro. Quitte à extraire une sous-suite, supposons qu'elle ne s'annule pas. Alors $(t_n/\|t_n\|)_n$ tend vers $h \in S(0,1)$. Montrons que pour tout $t \in \mathbb{R}$, $th \in H$. Pour tout $n \in \mathbb{N}$, il existe un unique entier m_n tel que $0 \leqslant m_n - \frac{t}{\|g_n\|} < 1$, c'est la partie entière de $\frac{t}{\|g_n\|}$. Alors $\left\|m_n g_n - g\frac{g_n}{\|g_n\|}\right\| \leqslant \|g_n\| \to 0$, donc $m_n g_n \to th$. Puisque $m_n \in \mathbb{Z}$, $g_n \in H$ et H est fermé, th est dans H. Ainsi, H contient la droite Vect(h).

Montrons maintenant que $c_0(G)$ est un sous-espace vectoriel. Soit x dedans. Le raisonnement précédent montre que, si x est dans $c_0(G) \subseteq G$, alors Vect(x) aussi. Ainsi, $c_0(G) = W$ est la réunion des droites vectorielles contenues dans G. Montrons que c'est un espace vectoriel ; par définition, c'est le plus grand sous-espace vectoriel inclus dans G, d'où l'unicité. Pour tous $x,y \in V$, $\lambda, \mu \in \mathbb{R}$, t réel, $t(\lambda x + \mu y) = (t\lambda)x + (t\mu)y$. Puisque par définition $\mathbb{R}x$, $\mathbb{R}y$ sont dans G, par somme dans G, $\mathbb{R}(\lambda x + \mu y)$ est dans G. Donc W est un sous-espace vectoriel. Alors G/W est discret dans $\mathbb{R}^n/W$, car c'est un sous-groupe de $\mathbb{R}^n/W$ qui est un espace euclidien mais G/W ne contient aucune droite vectorielle par maximalité de W, d'où la discrétion par contraposée du point précédent. ■

Exercice 3

Soit G un sous-groupe discret de $\mathbb{R}^n$. Montrer que $\mathbb{R}^n/G$ est compact si et seulement si $G \simeq \mathbb{Z}^n$.

Exercice 4 *(Un contre-exemple)*

Montrer que $\{(a + b\sqrt{2},a - b\sqrt{2}), a,b \in \mathbb{Z}\}$ est un sous-groupe discret de $\mathbb{R}^2$ avec $\mathbb{R}^2/G$ compact.

3.1.2.4 Sous-groupes discrets de $\mathbb{R}^n$

On s'intéresse maintenant au cas des sous-groupes discrets qui préfigure la théorie des réseaux de l'espace euclidien. Grâce à la structure de groupe, la condition de discrétion s'uniformise :

Propriété. ***(Les sous-groupes discrets de $\mathbb{R}^n$ le sont uniformément)***

Un sous-groupe additif H de $\mathbb{R}^n$ est discret, si et seulement si, il existe $\varepsilon > 0$ tel que $H \cap B(0,\varepsilon) = \{0\}$.

▷ En effet, H est discret si et seulement si pour tout $x \in H$, il existe $\varepsilon > 0$ tel que $B(x,\varepsilon) \cap H = \{x\}$. Mais en fait, $H \cap B(x,\varepsilon) = x + [(H-x) \cap B(0,\varepsilon)]$. Ainsi H est discret si et seulement s'il existe $\varepsilon > 0$ tel que $H \cap B(0,\varepsilon) = \{0\}$. ■

Exemples. ***(Sous-groupes discrets de $\mathbb{R}^n$)***

1. Soit $(e_1,...,e_n)$ une base de $\mathbb{R}^n$. Alors le *réseau* $\oplus_{i=1}^r \mathbb{Z}e_i$ est un sous-groupe discret de $\mathbb{R}^n$.
2. $\mathbb{Q}$ n'est pas un sous-groupe discret de $\mathbb{R}$.

Lemme. ***(Les sous-groupes discrets de $\mathbb{R}^n$ sont fermés)***

Un sous-groupe discret H de $\mathbb{R}^n$ est fermé.
En particulier, pour tout compact K de $\mathbb{R}^n$, $H \cap K$ est fini.

▷ Soit $\varepsilon > 0$ tel que $B(0,\varepsilon) \cap H = \{0\}$. Soit (x_n) une suitee suite de H qui converge vers $y \in \mathbb{R}^n$. Elle est de Cauchy, donc il existe $N \in \mathbb{N}$ tel que pour tous $p,q \geqslant N$, $|x_p - x_q| < \varepsilon$. Donc $x_p = x_q$. Donc (x_n) est stationnaire, donc $y \in H$.

Pour K compact, $K \cap H$ est fermé dans K donc compact, discret comme sous-espace d'un discret, donc fini. ■

Théorème. ***(Structure des sous-groupes discrets de $\mathbb{R}^n$)***

Soit H un sous-groupe discret de $\mathbb{R}^n$. Alors H est un $\mathbb{Z}$-module libre de rang $r \leqslant n$ et toute base de H est une famille $\mathbb{R}$-libre.

▷ On écarte le cas nul. Soit r maximal tel qu'il existe $(e_1,...,e_r) \in H^r$ qui soit $\mathbb{R}$-libre, en particulier $r \leqslant n$. Alors $P = \{\sum_{i=1}^r x_i e_i \mid 0 \leqslant x_i \leqslant 1\}$ est un compact. Pour $x \in H$ non nul, $x = \sum_{i=1}^r \lambda_i e_i$ où $\lambda_i \in \mathbb{R}$, car r est maximal. Ainsi $H \ni x = \sum_{i=1}^r \{\lambda_i\} e_i + \sum_{i=1}^r \lfloor \lambda_i \rfloor e_i$ où le premier terme est dans $P \cap H$, le second dans H. Ainsi, H est engendré par $P \cap H$ fini et $(e_1,...,e_r)$. Donc H est de type fini. Pour tout entier $j \geqslant 1$, $H \ni jx = \sum_{i=1}^r \{j\lambda_i\} e_i + \sum_{i=1}^r \{j\lambda_i\} e_i$ avec de même, le premier terme dans $H \cap P$, le second dans H. Ainsi, $x_j = jx - \sum_{i=1}^r \{j\lambda_i\} e_i \in H \cap P$ fini, donc il existe $j \neq l$ tel que $x_j = x_l$, donc $\{j\lambda_i\} = \{k\lambda_i\}$ pour tout i, d'où $\lambda_i \in \mathbb{Q}$. Ainsi $H \subseteq \bigoplus_{i=1}^r \mathbb{Q}e_i$. Je peux chasser les dénominateurs : il existe $d \geqslant 1$ tel que $dH \subseteq \bigoplus_{i=1}^r \mathbb{Z}e_i$, car H est de type fini. Donc $\bigoplus_{i=1}^r \mathbb{Z}e_i \subseteq H \subseteq \bigoplus_{i=1}^r \frac{\mathbb{Z}}{d} e_r$, donc H est

libre de rang r. Enfin, les $\mathbb{Z}$-bases d'un $\mathbb{Z}$-module libre de rang r se déduisent les unes des autres via l'action de $GL_r(\mathbb{Z})$, donc il existe une base de H $\mathbb{R}$-libre si et seulement si toute base de H est $\mathbb{R}$-libre. Or $(\frac{e_1}{d},...,\frac{e_r}{d})$ est une base de H qui est $\mathbb{R}$-libre. ■

3.2 Théorie des réseaux de $\mathbb{R}^n$

PARMI les sous-groupes discrets de $\mathbb{R}^n$, on peut distinguer les réseaux.

Définition. ***(Réseau de $\mathbb{R}^n$)***

Un *réseau* de $\mathbb{R}^n$ est un sous-groupe additif de $\mathbb{R}^n$ et discret et isomorphe à $\mathbb{Z}^n$. Autrement dit, c'est un sous-groupe additif discret de rang maximal.

Exercice 5

L'hypothèse de discrétion est-elle superflue ?

▷ **Éléments de réponse.**

Non ! Dans $\mathbb{R}^2$, le sous-groupe de $\mathbb{R}$, et donc de $\mathbb{R}^2$, $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ est isomorphe à $\mathbb{Z}^2$. Pourtant, il n'est pas discret.

En revanche, d'après le théorème de description des sous-groupes additifs fermés de $\mathbb{R}^n$ d'une part et le lemme précédent d'autre part, la condition *discret* peut être échangée par *fermé* sans problème.

Théorème. ***(Caractérisation des réseaux)***

Soit R un sous-groupe additif de $\mathbb{R}^n$. Alors les conditions suivantes sont équivalentes :

1. *(Caractérisation algébrique)* le sous-groupe R est engendré par les n vecteurs d'une base de l'espace vectoriel $\mathbb{R}^n$, autrement dit, les éléments de R sont exactement les combinaisons à coefficients entiers des vecteurs d'une base de $\mathbb{R}^n$;
2. *(Caractérisation topologique)* le sous-groupe R est discret (donc en particulier fermé dans $\mathbb{R}^n$) et cocompact, *i.e.* $\mathbb{R}^n/R$ est compact ;
3. *(Caractérisation mixte)* R est un réseau de $\mathbb{R}^n$.

▷ (3) $\implies$ (1) : On commence par montrer le cas de la dimension 2. Le réseau n'est alors pas limité au vecteur nul, car il engendre l'espace vectoriel $\mathbb{R}^n$, il existe au moins un vecteur de norme non nul, soit b cette norme. Le disque de centre le vecteur nul et de rayon b intersecte le réseau en un autre point que l'origine et contient un nombre fini du points du réseau. Ce qui montre qu'il existe au moins un vecteur α non nul de plus petite norme dans le réseau. On considère maintenant le réseau diminué des multiples de α. L'ensemble est non vide car sinon le réseau n'engendrerait pas l'espace vectoriel $\mathbb{R}^n$, le même raisonnement que le précédent montre l'existence d'un vecteur β de longueur

minimale, dans le réseau, à l'exception peut-être de quelques multiples de α, correspondant à la bande bleue sur la figure 3.2.1c. Le gros point bleu est l'origine. Le vecteur α est bien un vecteur non nul de plus petite norme du réseau et vient ensuite β, dont la norme n'est minorée que par celle de α, son inverse et le vecteur nul.

Il n'existe au plus qu'une manière d'écrire un vecteur du réseau comme combinaison linéaire de α et β. En effet, cette propriété est une conséquence du fait que ces deux vecteurs sont libres dans l'espace vectoriel $\mathbb{R}^n$. Il n'existe qu'une manière d'écrire un vecteur quelconque de $\mathbb{R}^n$ comme combinaison linéaire de α et β, ce qui est en particulier vrai pour les vecteurs du réseau.

Montrons maintenant que tout vecteur du réseau est combinaison linéaire de α et β, à coefficients entiers. Considérons le disque rouge, de centre α et de rayon la norme de β, un tel disque ne peut contenir comme point du réseau, en dehors de sa frontière, que quelques multiples de α dans la zone bleue sur la figure 3.2.1c, d'après la définition de la norme de β. Le disque vert est de centre β et de rayon la norme de α. Le même raisonnement montre que l'intérieur de ce disque ne peut contenir aucun point du réseau. Le segment $[0, \alpha]$ ne peut contenir que ses extrémités comme point du réseau, il en est de même pour le segment $[0, \beta]$. Il en est aussi de même pour $[\alpha, \beta]$ et $[\beta, \alpha + \beta]$ car sinon, en soustrayant α ou β, on aurait une contradiction. En résumé, le parallélogramme, en jaune, de sommets $0, \alpha, \beta$ et $\alpha + \beta$ ne contient aucun autre point du réseau que ses sommets. On remarque que ce parallélogramme est constitué des vecteurs de $\mathbb{R}^n$ ayant deux coefficients compris entre 0 et 1 dans la base (α, β).

Considérons un élément quelconque λ du réseau. Il est nécessairement combinaison linéaire de la base α,β de $\mathbb{R}^n$, et $\lambda = a\alpha + b\beta$ avec a et b réels. L'objectif est de montrer que a et b sont entiers. Soit p_a (resp. p_b) la partie entière de a (resp. b) et r_a (resp. r_b) sa partie fractionnaire. Comme α et β sont des éléments du réseau et que p_a et p_b sont des nombres entiers, $p_a\alpha + p_bbet$ est un point du réseau au même titre que λ. Leur différence, égale à $r_a\alpha + r_b\beta$, est donc dans le réseau. C'est aussi un point du parallélogramme jaune car ses deux coordonnées sont comprises entre 0 et 1. Il existe quatre points du réseau possible, comme une partie fractionnaire est toujours strictement plus petite que 1, la seule valeur possible est 0, ce qui montre que a est égal à p_a et b à p_b. Autrement dit, les coordonnées de λ dans la base sont entières, ce qui termine la démonstration dans le cas $n = 2$.

Démontrons ce résultat par récurrence sur n. Pour les dimensions 1 et 2, une démonstration est déjà présentée. Supposons la propriété démontrée à l'ordre $n - 1$ et démontrons la à l'ordre n. Le réseau forme une famille génératrice de $\mathbb{R}^n$, de toute famille génératrice, il est possible d'extraire une base, il existe donc une sous-famille du réseau de cardinal n qui engendre l'espace entier. Soit (f_i), pour i variant de 1 à n, une telle base. Elle n'est pas a priori celle recherchée car rien n'indique que les éléments du réseau s'expriment comme combinaison linéaire à coefficients entiers dans cette base. Soit S l'espace vectoriel engendré par (f_i), pour i variant de 1 à $n - 1$. L'intersection du réseau et de S est un groupe discret engendrant S, il existe une base (b_i), pour i variant de 1 à $n - 1$ de l'intersection du réseau et de S, par hypothèse de récurrence. L'hyperplan S est représenté sur la figure 3.2.1e, couleur crème, le vecteur nul est le point bleu. La famille (b_i) est un bon candidat pour la base recherchée, mais il manque encore un vecteur. Soit φ une forme linéaire nulle sur S telle que l'image du réseau par φ ne soit pas réduite à 0. Une telle forme existe, sinon le réseau n'engendrerait que l'espace S et pas l'espace entier. L'objectif est de montrer que l'image par φ du réseau est un sous-groupe discret de $\mathbb{R}$, c'est-à-dire qu'il existe un réel strictement positif ε tel que si u est un élément du réseau, l'image

du réseau par φ ne contient que la valeur $\varphi(u)$ entre $\varphi(u) - \varepsilon$ et $\varphi(u) + \varepsilon$. On remarque que l'on peut supposer u nul ; en effet, si l'image par φ du réseau n'est pas discret, quel que soit ε, il existe deux vecteurs u et v d'images distinctes par φ et dont la différence est, en valeur absolue, inférieure à ε, ce qui montre que l'image par φ de $u - v$ est, en valeur absolue, inférieure à ε. Pour montrer ce résultat, on va montrer qu'il n'existe qu'un nombre fini de valeurs atteintes par φ sur l'intervalle $[-1, 1]$. Tous les points du réseau ayant une image par φ dans cet intervalle se trouvent entre les hyperplans affines d'équation $\varphi(x) = -1$ et $\varphi(x) = 1$, représentés en bleu sur la 3.2.1e. Soit V le volume de $\mathbb{R}^n$ composé des vecteurs compris entre les deux hyperplans et dont les coordonnées, dans la base (b_i), de la projection orthogonale par p sur S, sont toutes comprises entre 0 et 1. Le volume V est représenté en vert sur la figure 3.2.1e. On remarque que V est bien borné car il représente l'ensemble des vecteurs de $\mathbb{R}^n$ ayant des coordonnées comprises entre 0 et 1 dans la base (b_i,π). Ici π désigne le vecteur orthogonal à S et d'image égale à 1 par la forme φ. Si δ est un nombre réel, compris entre -1 et 1, et image du réseau par φ, δ possède un antécédent dans V. En effet, il existe un vecteur u du réseau compris entre les deux hyperplans et tel que $\varphi(u) = \delta$. Le vecteur $p(u)$ est dans S et se décompose sur la base (b_i) ; soit (u_i) les coordonnées de $p(u)$ dans cette base. Si q_i désigne la partie entière de u_i et r_i la partie fractionnaire :

$$u = q + r \text{ avec } q = \sum_{i=1}^{n-1} q_i b_i, r = \sum_{i=1}^{n-1} r_i b_i.$$

On remarque que q est un élément du réseau car combinaison linéaire de la famille (b_i) à coefficients dans $\mathbb{Z}$. Son image par φ est nulle car il est élément de S. Le point $u - q$ est constitué de la différence de deux éléments du réseau et fait partie du réseau. L'image de q par φ est nulle et φ est linéaire. Le projeté orthogonal de $u - q$ sur l'hyperplan engendré par S est égal à r, ce qui montre que $u - q$ est bien un élément de V. Le volume V est borné, il ne contient qu'un nombre fini de points du réseau, car le réseau est discret. Il ne peut exister qu'un nombre fini de valeurs prises par l'image du réseau par la fonction φ entre -1 et 1, ce qui montre que la valeur 0 est bien isolée dans cette image.

Soit Δ une droite vectorielle de $\mathbb{R}^n$ non contenue dans S et contenant un point non nul du réseau. L'image par φ de Δ est un groupe discret d'après la démonstration précédente, il existe un point b_n de Δ et du réseau de plus petite image a strictement positive par φ ; ce point est représenté en rouge sur la figure 3.2.1e. Soit enfin un élément λ quelconque du réseau, l'élément λ s'exprime comme une combinaison linéaire de (b_i), car cette famille est une base de $\mathbb{R}^n$. Il faut alors montrer que les différents coefficients sont des entiers :

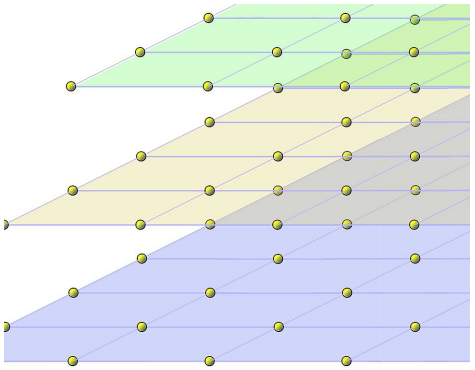
$$\lambda = \sum_{i=1}^{n-1} \lambda_i b_i + \lambda_n b_n.$$

L'image par φ de λ est égale à $\lambda_n a$, qui est un élément de $a.\mathbb{R}$, l'image de Δ par φ. On en déduit que λ_n est entier. Le vecteur $\lambda - \lambda_n b_n$ est élément du réseau et de S, ce qui montre que les coordonnées λ_i sont toutes entières. La famille (b_i), pour i variant de 1 à n de $\mathbb{R}^n$ est génératrice du réseau. Le fait qu'elle soit de cardinal n termine la démonstration.

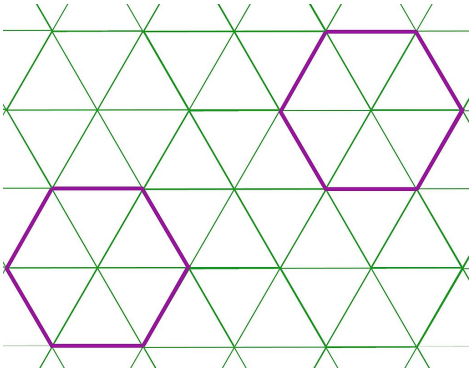
(1) $\implies$ (3) : l'isomorphie à $\mathbb{Z}^n$ est immédiate par hypothèse. Il reste à montrer que R est discret. Soit d' le minimum des normes des n vecteurs considérés ; soit $d = \frac{d'}{2}$. Alors on voit que $R \cap B(0,d) = \{0\}$.

(3) $\implies$ (2) : il suffit de montrer que $\mathbb{R}^n/R$ est compact. Or ce quotient est isomorphe au tore $\mathbb{R}^n/Z^n$ qui est homéomorphe à $(S^1)^n$, compact.

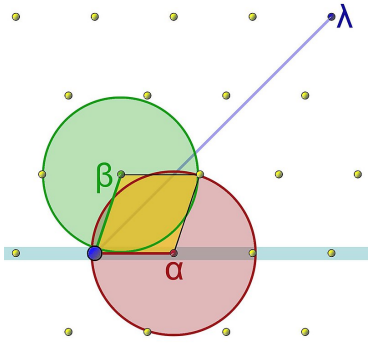
(2) $\Longrightarrow$ (1) : par hypothèse, R est discret donc fermé et même par le théorème de description, il est de la forme $\bigoplus_{i=1}^{r} \mathbb{Z}e_i$, et c'est ce qu'il fallait montrer. ■



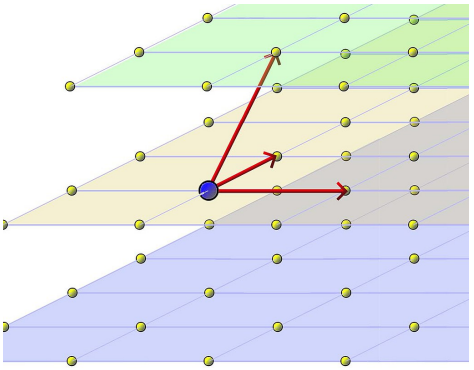
(a) *Réseau.* — Un réseau est un ensemble discret disposé dans un espace vectoriel réel de dimension finie de manière régulière, au sens où la différence de deux éléments du réseau est encore élément du réseau.



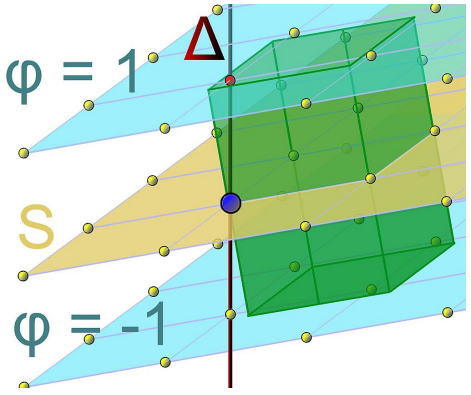
(b) *Réseau par pavage hexagonal.* — L'hexagone est une figure permettant de construire un réseau en dimension 2.



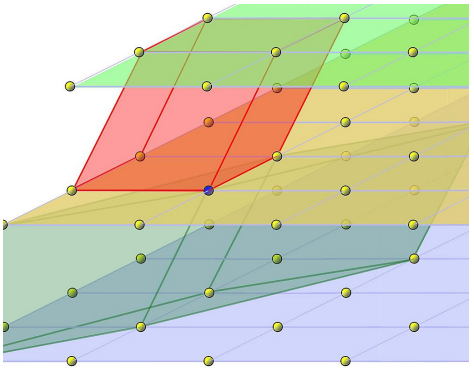
(c) *Preuve du théorème de caractérisation des réseaux, cas $n = 2$.* —



(d) *Réseau tridimensionnel.* — Dans un réseau, il existe une famille, illustrée en rouge sur la figure, telle que tout point s'exprime comme combinaison linéaire de manière unique, des points de la famille.



(e) *Preuve du théorème de caractérisation des réseaux, cas général.* —



(f) *Domaine fondamental d'un réseau.* — Deux domaines fondamentaux ont même volume.

FIGURE 3.2.1 : *Réseaux de l'espace euclidien.* —

Exemples. ***(Réseaux de $\mathbb{R}^n$)***

1. $\mathbb{Z}^n \subseteq \mathbb{R}^n$ bien sûr.
2. D'après ce qui précède, les réseaux sont exactement les $\mathbb{Z}$-modules de $\mathbb{R}^n$ engendrés par des bases de $\mathbb{R}^n$.
   Il y a une bijection naturelle de $GL_n(\mathbb{R})/GL_n(\mathbb{Z})$ sur les réseaux dans $\mathbb{R}^n$ qui à $g \longmapsto g\mathbb{Z}^n$. En effet, $GL_n(\mathbb{R})$ agit transitivement sur les bases de $\mathbb{R}^n$, il agit aussi transitivement sur les réseaux. De plus, $\mathrm{Stab}_{GL_n(\mathbb{Z})}(\mathbb{Z}^n) = \{g \mid g\mathbb{Z}^n = \mathbb{Z}^n\} = GL_n(\mathbb{Z})$.

Heuristique

Dans le cas des sous-groupes de $\mathbb{Z}^n$, on ne peut espérer produire des exemples généraux au choix comme image ou noyau d'une application linéaire, car de tels noyaux, contrairement au cas de $\mathbb{R}^n$, sont toujours purs. Néanmoins, on peut remplacer cette construction par celle d'un noyau d'un morphisme d'un $\mathbb{Z}^n$ dans $\mathbb{Z}/a_1\mathbb{Z} \times ... \mathbb{Z}/a_s\mathbb{Z} \times \mathbb{Z}^{m-s}$; autrement dit, un sous-groupe de $\mathbb{Z}^n$ est toujours ou bien paramétré sur une famille de vecteurs de $\mathbb{Z}^n$, ou bien l'ensemble des solutions d'un système de congruences, qui en est une description *cartésienne*. Ceci nous pousse à la définition suivante.

Définition. ***(Sous-groupe basique de $\mathbb{Z}^n$)***

On dit que H est un sous-groupe *basique* de $\mathbb{Z}^m$ si la base canonique lui est adaptée, *i.e.* s'il est engendré par des multiples entiers des s premiers vecteurs de la base canonique, et s'écrit donc sous la forme $a_1\mathbb{Z} \oplus ... \oplus a_s\mathbb{Z} \oplus \{0\} \oplus ... \oplus \{0\}$.
Autrement dit, une description cartésienne d'un sosu-groupe de $\mathbb{Z}^n$ est sa donnée comme image réciproque d'un sous-groupe basique de $\mathbb{Z}^m$ par un morphisme de $\mathbb{Z}^n$ dans $\mathbb{Z}^m$.

On munit $\mathbb{R}^n$ de sa mesure de Lebesgue usuelle.

Définition. ***(Région, domaine fondamental)***

Soit H un réseau de $\mathbb{R}^n$. On appelle *région fondamentale* de H toute partie de $\mathbb{R}^n$ en bijection avec $\mathbb{R}^n/H$.
Parfois, et même souvent, on se limite à une région de la forme $A + P_e$ où P_e est le parallélotope associé à une base du réseau H *(voir ci-dessous)*. Lorsque A est l'origine d'un repère fixé, on parle de *domaine fondamental*. Parfois, on confond les deux termes.

Définition. ***(Parallélotope)***

Si H est un réseau de $\mathbb{R}^n$ et $e = (e_i)_{i\in[\![1,n]\!]}$ une $\mathbb{Z}$-base de H, on définit le *parallélotope* associé à cette base par :

$$P_e = \{x = \sum_{i=1}^{n} x_i e_i \mid 0 \leqslant x_i < 1\}.$$

Proposition. ***(Action du réseau sur son parallélotope)***

- Le sous-groupe H agit sur $\mathbb{R}^n$ par translations.
- Cette action est *prudente* à partir de tout parallélotope, en un sens à préciser.
- En particulier, on a une bijection $P_e \simeq \mathbb{R}^n/H$, autrement dit, P_e est un domaine fondamental pour H (sous entendu pour son action sur $\mathbb{R}^n$.

▷ En effet, soit $x \in \mathbb{R}^n$. Alors il existe un unique $y \in P_e$ tel qu'il existe $h \in H$ tel que $x = y + h$. En effet, si $x = \sum_{i=1}^{n} x_i e_i$, alors $y = \sum_{i=1}^{n} (x_i - \lfloor x_i \rfloor) e_i$. ■

On voudrait définir un invariant de type volume associé à H, qui serait le volume du quotient $\mathbb{R}^n/H$, $\mathbb{R}^n$ muni de la mesure de Lebesgue, H muni de la mesure de comptage.

Définition. ***(Volume d'un réseau)***

On définit le *(co-)volume* de H, comme :

$$\mathrm{vol}(H) := \mathrm{vol}(P_e).$$

Autrement dit, c'est le volume d'un domaine fondamental.

Remarques.

1. Sous la première définition, le volume de H ne dépend pas du choix de la base. En effet, si $f = (f_i)$ est une autre base de H, il existe $g \in GL(n, \mathbb{R})$ telle que $ge_i = f_i$ pour tout i, et donc $\mathrm{vol}(P_f) = |\det(g)|\mathrm{vol}(P_e)$. On observe que $\mathrm{Mat}_e(g) \in GL_n(\mathbb{Z})$, car f est une base, donc $|\det(g)| = 1$.
2. Les deux définitions sont équivalentes (ce qui démontre en particulier le premier point).

Théorème

Soit H un réseau de $\mathbb{R}^n$ et $S \subseteq \mathbb{R}^n$ un ensemble mesurable de volume supérieur à $\mathrm{vol}(H)$. Alors il existe x,$y \in S$ distincts tels que $x - y \in H$.

▷ Soit e une base de H. Alors P_e est un domaine fondamental de H et $\mathbb{R}^n = \bigsqcup_{h\in H}(h+P_e)$, d'où $S = \bigsqcup_{h\in H} S\cap(h+P_e)$, réunion dénombrable. Ainsi, $\mathrm{vol}(S) = \sum_{h\in H}\mathrm{vol}(S\cap(h+P_e))$ où $S\cap(h+P_e) = h+(S-h)\cap P_e$. La mesure de Lebesgue est invariante par translations. Ainsi, $\mathrm{vol}(S\cap(h+P_e)) = \mathrm{vol}((S-h)\cap P_e)$. Ainsi, $\mathrm{vol}(S) = \sum_{h\in H}\mathrm{vol}((S-h)\cap P_e)$. On cherche à montrer qu'il existe $h\in H$ différent de 0, tel que $(S+h)\cap S \neq \emptyset$. Supposons que le contraire soit le cas. Les $(S\cdot h)_{h\in H}$ sont deux à deux disjoints, d'où $\mathrm{vol}(S) = \sum_{h\in H}\mathrm{vol}((S-h)\cap P_e) = \mathrm{vol}((\bigcup_{h\in H}(S\cdot h))\cap P_e) \leqslant \mathrm{vol}(P_e) = \mathrm{vol}(H)$, ce qui contredit l'hypothèse. ■

On peut préciser ce résultat :

Corollaire. ***(Théorème de Minkowski géométrique)***

Soit H un réseau de $\mathbb{R}^n$ et S une partie mesurable de $\mathbb{R}^n$, convexe et centralement symétrique par rapport à l'origine.

- Si $\mathrm{vol}(S) > 2^n\mathrm{vol}(H)$, alors $S\cap H$ contient un élément non nul.
- Si $\mathrm{vol}(S) \geqslant 2^n\mathrm{vol}(H)$ et S est compacte, alors $S\cap H$ contient un élément non nul.

▷ On applique le théorème à l'homothétique $S' = \frac{1}{2}S$. Ainsi $\mathrm{vol}(S') = 2^{-n}\mathrm{vol}(S)$. Par hypothèse, $\mathrm{vol}(S') > \mathrm{vol}(S)$, donc il existe $x,y\in S'$ avec $x\neq y$ et $x-y\in H$. Or $y\in S'$, donc $-y\in S'$, donc $[x_i,y]\subseteq S'$. Donc $\frac{x-y}{2}\in S'$. Ainsi, $x-y\in 2S' = S$. Or $x-y\in H$ est non nul.

On fait maintenant la deuxième hypothèse. Pour $\varepsilon>0$, on note $S_\varepsilon = (1+\varepsilon)S$, d'où $\mathrm{vol}(S_\varepsilon) > 2^n\mathrm{vol}(H)$, donc $(H\cap S_\varepsilon)\setminus\{0\}$ est non vide, où $H\cap S_\varepsilon$ est fini, car H est discret et S_ε compact. Ainsi, $\bigcap_{\varepsilon>0}(H\cap S_\varepsilon)\setminus\{0\}$ est une suite décroissante d'ensembles finis, donc non vide. ■

Il est assez visuel que la convexité et la symétrie empêchent de créer des boules de pâte à modeler se faufilant entre les mailles du réseau. L'hypothèse de compacité est légèrement plus subtile.

Contre-exemple

Dans la deuxième condition, la compacité est nécessaire.

Prenons e une base de H et $S = \{\sum_{i=1}^n x_ie_i \mid -1<x_i<1\}$. Alors $\mathrm{vol}(S) = 2^n\mathrm{vol}(H)$, S est symétrique et convexe, mais $S\cap H = \{0\}$. □

Conséquence

En particulier, la constante 2^n est optimale dans le théorème de Minkowski.

Chapitre 4

Arithmétique et théorie des nombres

Résumé

Pour ce qui est de la théorie algébrique des nombres, après un bref topo sur les valeurs absolues sur $\mathbb{Q}$, on traite de la notion d'élément entier sur un anneau, proche de celle d'élément algébrique sur un corps, puis, en tant qu'application, on étudie les anneaux d'entiers des corps de nombres. On mentionne dans cette perspective les anneaux noethériens et les anneaux de Dedekind. Enfin, nous décrivons le groupe de classe d'idéaux et démontrons le théorème des unités de Dirichlet après l'étude des réseaux de l'espace euclidien.

Pour ce qui est de la théorie analytique des nombres, le but est de préciser la répartition des nombres premiers.

Contexte. Dans le cadre ce cours, tous les anneaux sont commutatifs et unitaires (c'est l'hypothèse de l'algèbre commutative). On rappelle que cette convention ne signifie pas simplement la neutralité vis à vis de la divisibilité latérale. On note 1 l'élément neutre pour sa loi multiplicative.

Si A,B sont des anneaux, si $\varphi \in \mathrm{Hom}_{\mathrm{Ann}}(A,B)$, on impose bien $\varphi(1_A) = 1_B$.

Soit A un anneau et M un A-module. On dit que M est de type fini si M est engendré en tant que A-module, par une partie finie.

4.1 Les valeurs absolues des nombres rationnels

4.1.1 Valeurs absolues d'un corps

Définition. ***(Valeur absolue sur un corps)***

Soit K un corps (commutatif). Une *valeur absolue* sur K est une fonction $|\cdot| : K \to \mathbb{R}_+^*$ telle que pour tous $x,y \in K$,

(i) $|x| = 0 \iff x = 0$;

(ii) $|xy| = |x||y|$ *(*$|\cdot|$ *est un morphisme de* K^* *dans* $\mathbb{R}_+^*$*)* ;

(iii) $|x+y| \leqslant |x| + |y|$ *(inégalité triangulaire).*

On dit que $(K, |\cdot|)$ est un *corps valué*, autrement dit un corps muni d'une valeur absolue. Souvent, par abus, on omet l'expression de la valeur absolue.

Exemples. ***(Valeurs absolues sur un corps)***

1. *(Valeur absolue triviale)* Pour tout corps, on peut définir une valeur absolue par $|x| = 1$ si $x \neq 0$ et $|0| = 0$.
2. Si $i : K \hookrightarrow \mathbb{C}$ est un plongement, l'application $x \mapsto |i(x)|_\infty^k$ pour $0 < k \leqslant 1$ est une valeur absolue.

Définition-propriété. ***(Distance associée à une valeur absolue)***

Soit $(K, |\cdot|)$ un corps valué. Alors l'application $d : (x,y) \mapsto |x-y|$ est une distance sur l'ensemble K, dite associée à $|\cdot|$.
La topologie associée à $|\cdot|$ est la topologie issue de la distance d.

Définition. ***(Équivalence de valeurs absolues)***

Deux valeurs absolues $|\cdot|_1$ et $|\cdot|_2$ sur un même corps sont dites *équivalentes* s'il existe $\alpha \in \mathbb{R}_+$ tel que $|\cdot|_2 = |\cdot|_1^\alpha$.

Remarque. La valeur absolue triviale est seule dans sa classe d'équivalence.

Propriété

Deux valeurs absolues équivalentes définissent la même topologie.

▷ On montre qu'elles définissent les mêmes boules. ■

Remarque. Les applications $x \mapsto |x|$, $x \mapsto x+y$ pour tout $y \in K$, $x \mapsto xy$ pour tout $y \in K$, sont continues sur K. L'application $x \mapsto \frac{1}{x}$ est continue sur K^*.

Exercice 1 *(Une seule notion d'équivalence pour les valeurs absolues)*

Montrer que si deux valeurs absolues définissent la même topologie, alors elles sont équivalentes.

INDICATION Supposons le contraire. Soit $(\alpha_1, \alpha_2) \in K^2$. Montrer que pour tout nombre réel $\varepsilon > 0$, il existe $\beta \in K$ tel que pour $i = 1$ ou 2, on ait $|\beta - \alpha_i|_i < \varepsilon$.

Définition. ***(Valeur absolue non archimédienne)***

Une valeur absolue est dite *non archimédienne* si la distance associée est ultramétrique.

Reformulation pratique. *(Valeur absolue non archimédienne)*

Une valeur absolue est non archimédienne si $|x+y| \leqslant \max(|x|,|y|)$ pour tous $x,y \in K$.

Fait

Le caractère non-archimédien est préservé par équivalence.

Définition. *(Valeur absolue archimédienne)*

Une valeur absolue est dite *archimédienne* si elle n'est pas non archimédienne.

Propriété. *(Valeur absolue d'une racine de l'unité)*

Soit K un corps valué et x une racine de l'unité. Alors $|x| = 1$.

Corollaire. *(Valeurs absolues sur un corps fini)*

Si K est un corps fini, la seule valeur absolue sur K est triviale.

4.1.2 Valuations discrètes

Définition. *(Anneau de valuation discrète)*

Un *anneau de valuation discrète (avd)* A est un anneau principal (intègre) ayant un unique idéal premier non nul, noté $\mathfrak{m}_A$.

VOC On pose les conventions suivantes.

1. Un générateur de $\mathfrak{m}_A$ s'apelle une *uniformisante*.
2. $\mathfrak{m}_A$ est donc aussi l'unique idéal maximal de A.
3. Le corps $A/\mathfrak{m}_A$ s'appelle *corps résiduel*.

Lemme. *(Idéaux d'un anneau de valuation discrète)*

Dans un anneau de valuation discrète A, tout idéal $I \neq 0$ de A est de la forme $\mathfrak{m}_A^n$ avec n entier naturel.

▷ On a $I \subseteq \mathfrak{m}_A$ ou $I = A$. Supposons le premier cas. Soit π un générateur de $\mathfrak{m}$, par principalité. Posons $J = \bigcap_{k\geqslant 0} \mathfrak{m}_A^k = \bigcap_{k\geqslant 0} \pi^k A$. C'est un idéal premier, en effet : si $x,y \in A$ sont tels que $xy \in J$, supposons $x \in \pi^n A$ et $y \in \pi^m A$. On a $xy \in \pi^{n+m+1}A$ et donc $\frac{x}{\pi^n} \times \frac{y}{\pi^m} \in \pi A = \mathfrak{m}_A$. Or $\mathfrak{m}_A$ étant premier, $\frac{x}{\pi^n} \in \pi A$ ou $\frac{y}{\pi^m} \in \pi A$, soit $x \in \pi^{n+1}A$ ou $y \in \pi^{m+1}A$. Par itération, $x \in J$ ou $y \in J$, ce que l'on voulait. Comme $J \neq \mathfrak{m}_A$, on a donc $J = 0$. On sait par ailleurs qu'il existe un entier minimal n tel que $I \subseteq \mathfrak{m}_A^n$. Alors $\pi^{-n}I$ est un idéal de A avec $\pi^{-n}I \subsetneq \mathfrak{m}_A$. Donc $\pi^{-n}I = A$. Donc $I = \mathfrak{m}_A^n$. ■

Définition-propriété. ***(Valuation sur un anneau de valuation discrète)***

Soit A un anneau de valuation discrète et $x \in A$, $x \neq 0$. On définit la valuation $v(x)$ de x est l'entier n maximal tel que $x \in \mathfrak{m}_A^n$. Par convention, $v(0) = +\infty$.
On étend v à $K = Frac(A)$ par $v(x/y) = v(x) - v(y)$. On en déduit $v : K^* \to \mathbb{Z}$ un morphisme surjectif de groupes.

▷ On a $v(xy) = v(x) + v(y)$ et $v(x+y) \geqslant \min(v(x),v(y))$. ■

Exemples. ***(Anneaux de valuation discrète)***

1. Soit p un nombre premier. Alors $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$ est un anneau de valuation discrète d'idéal maximal $p\mathbb{Z}_{(p)}$ et corps des fractions $\mathbb{Q}$.
2. $\mathbb{Z}_p$ l'anneau des entiers p-adiques est un anneau de valuation discrète de corps des fractions $\mathbb{Q}_p$.
3. Pour k corps, $k[[T]]$ est un anneau de valuation discrète d'idéal maximal $Tk[[T]]$, de corps des fractions $k((T))$.

Contre-exemple. ***(Anneau qui n'est pas de valuation discrète)***

L'anneau $\mathbb{Z}_{(p)} \times_{\mathbb{Z}/p\mathbb{Z}} \mathbb{Z}_{(p)} = \{(a,b) \in \mathbb{Z}_{(p)}^2 \mid a \equiv b \ [p]\}$ n'est pas un anneau de valuation discrète. Pourtant, il admet un unique idéal maximal. □

D'un anneau de valuation discrète, on peut déduire un corps en passant aux fractions. On peut inverser l'opération.

Proposition

Soit K un corps et $v : K^* \to \mathbb{Z}$ un morphisme surjectif de groupes qui vérifie $v(x+y) \geqslant \min(v(x),v(y))$ pour tous $x,y \in K^*$. Alors $A = \{x \in K^* \mid v(x) \geqslant 0\} \cup \{0\}$ est un anneau de valuation discrète d'idéal maximal $\{x \in K^* \mid v(x) > 0\} \cup \{0\}$.

▷ On laisse au lecteur le soin de vérifier que A est un anneau grâce aux hypothèses faites sur v. De même, $\mathfrak{m}_A$ est un idéal de A. Il est de plus maximal, car $A^* = \{x \in K^* \mid v(x) = 0\}$ d'où $\mathfrak{m}_A = A \setminus A^*$.

Soit $\pi \in K$ tel que $v(\pi) = 1$. Tout élément de A s'écrit $a_0\pi^n$ avec $a_0 \in A^*$, n entier naturel. Soit I un idéal non nul de A. Soit n maximal tel que $I \subseteq \mathfrak{m}_A^n$ et $\frac{1}{\pi^n} I \not\subseteq \mathfrak{m}_A$. Donc $I = \pi^n A$ par maximalité. Il est donc principal et premier si et seulement si $n = 1$. ■

Définition-propriété. ***(Valeur absolue sur les fractions d'un avd)***

Soit A un anneau de valuation discrète et K son corps des fractions. Alors l'application

$$\begin{array}{rcl} K & \longrightarrow & \mathbb{R}_+ \\ x & \longmapsto & a^{-v(x)} \text{ pour } x \neq 0,\ 0 \text{ sinon} \end{array}$$

est une valeur absolue sur K pour tout réel $a > 1$ fixé. De plus, sa classe d'équivalence ne dépend pas de a.

Remarque. Si le corps résiduel k est fini d'ordre $|k|$, on a un choix privilégié $a = |k|$.

Exemple fondamental. *(Valeur absolue p-adique)*

Pour $K = \mathbb{Q}$ et p premier, on obtient la *valeur absolue p-adique*

$$\begin{array}{rccl} v_p\colon & \mathbb{Q} & \longrightarrow & \mathbb{R}_+ \\ & x & \longmapsto & |x|_p = x^{-v_p(x)}. \end{array}$$

On a $v_p(x_0 p^n) = n$ pour tout $x_0 \in \mathbb{Z}_{(p)}^{\times}$.
Pour $x \in \mathbb{Q}$, on pose $|x|_\infty$ la valeur absolue réelle de x.

Exercice 2 *(Comparaison de $|\cdot|_\infty$ avec les v.a. p-adiques)*

Pour tout nombre premier p, $|\cdot|_\infty$ et v_p ne sont pas équivalentes.

▷ **Éléments de réponse.**

Elle ne définissent pas les mêmes boules !

4.1.3 Valeurs absolues de $\mathbb{Q}$

Théorème. *(Ostrowski)*

Soit $|\cdot|$ une valeur absolue non triviale de $\mathbb{Q}$. Alors $|\cdot|$ est équivalente à $|\cdot|_\infty$ ou $|\cdot|_p$ pour un certain p premier.

▷ La démonstration est très particulière. On distingue deux cas.

Commençons par le cas où il existe $x_0 \in \mathbb{Z}$ tel que $|x_0| > 1$. Soit $x \in \mathbb{Z}$, $x > 1$. Soit n un entier supérieur à 1. Considérons $x_0^n = \sum_{i=0}^{k} \alpha_i x^i$ l'écriture en base x de x_0^n. On a $\alpha_i \in \{0,1,\ldots,x-1\}$. Posons également $c_x = \max\{|0|,|1|,\ldots,|x-1|\}$. On a $|x_0|^n = |x_0^n| = \left|\sum_{i=0}^{k} \alpha_i x^i\right| \leqslant \sum_{i=0}^{k} |\alpha_i||x|^i \leqslant c_x(k+1)\max(1,|x|^k)$. On a $k \leqslant \log_x(x_0^n) = n\log_x(x_0)$, d'où $|x_0|^n \leqslant c_x \log_x(x_0^n + 1)\max(1,|x|^n)^{\log_x(x_0)}$. Ainsi $|x_0| \leqslant c_x^{\frac{1}{n}}(n\log_x(x_0)+1)^{\frac{1}{n}}\max(1,|x|^{\log_x(x_0)})$. C'est vrai pour tout $n \in \mathbb{N}$; en faisant tendre n vers $+\infty$, on obtient $1 < |x_0| \leqslant \max(1,|x|)^{\log_x(x_0)} = |x|^{\log_x(x_0)}$. Donc $|x| > 1$ et l'on a $|x_0|^{\frac{1}{\log(x_0)}} < |x|^{\frac{1}{\log(x)}}$. En échangeant x et x_0, on a $|x_0|^{\frac{1}{\log(x_0)}} = |x|^{\frac{1}{\log(x)}}$. Par suite, il existe $a \in \mathbb{R}_+$ tel que $|x| = a^{\log(x)}$, x étant dans $\mathbb{N}^*$. Donc $|\cdot|$ est équivalente à $|\cdot|_\infty$.

Dans le deuxième cas, pour tout $x \in \mathbb{Z}$, $|x| \leqslant 1$. Montrons que $|\cdot|$ est non archimédienne. Soient $x,y \in \mathbb{Z}$. Soit n un entier $\geqslant 1$. On a $|x+y|^n = \left|\sum_{k=0}^{n} \binom{k}{n} x^k y^{n-k}\right| \leqslant \sum_{k=0}^{n} \left|\binom{k}{n}\right| |x|^k |y|^{n-k} \leqslant (n+1)\max(|x|^n,|y|^n)$, car pour tous k,n, $\left|\binom{k}{n}\right| \leqslant 1$. Donc $|x+y| \leqslant (n+1)^{\frac{1}{n}} \max(|x|,|y|)$, d'où $|x+y| \leqslant \max(|x|,|y|)$ quand n tend vers $+\infty$. Considérons $\{x \in \mathbb{Q} \mid |x| < 1\}$. C'est un idéal premier de $\{x \in \mathbb{Q} \mid |x| \leqslant 1\}$. De même, $\{x \in \mathbb{Z} \mid |x| < 1\}$ est un idéal premier de $\mathbb{Z}$, donc de la forme $p\mathbb{Z}$ pour p premier. Soit $a_0 p^n \in \mathbb{Q}^*$ avec $a_0 \in \mathbb{Z}_{(p)}^{\times}$. On a $|a_0 p^n| = |a_0||p|^n = |p|^n$, donc $|\cdot|$ est équivalente à $|\cdot|_p$. ■

Remarque. On verra que le théorème d'Ostrowski détermine les valeurs absolues des extensions finies de $\mathbb{Q}$ et que dans ce cas, on a plus d'une valeur absolue non archimédienne.

Heuristique

Ce théorème a des conséquences profondes dans toute la théorie des nombres. En effet, il signifie en quelque sorte qu'il y a des nombres premiers « manquants » ; les efforts de cette théorie cherchent à trouver un tel nombre manquant.

La formule suivante, pas très difficile, énonce une certaine harmonie dans le choix de définition des valeurs absolues rationnelles.

Proposition. ***(Formule du produit)***

Soit $x \in \mathbb{Q}^*$. On a $\prod_{p \text{ premier}} |x|_p \times |x|_\infty = 1$.

▷ Tout d'abord, ce produit est fini, car $|x|_p = 1$ pour presque tout p. De plus, l'application $\begin{array}{ccc} \mathbb{Q}^* & \longrightarrow & \mathbb{R}_+^* \\ x & \longmapsto & \prod_{p \text{ premier}} |x|_p \times |x|_\infty \end{array}$ est un morphisme de groupes. Or on sait que $\mathbb{Q}^*$ est engendré par les nombres premiers. Soit q premier. On a $|q|_p = 1$ si $q \neq p$, $|q|_p = p^{-1}$ si $q = p$ et $|q|_\infty^p = q$, donc la formule duu produit est vérifiée pour q. Elle est donc vérifiée en général. ■

Exercice 3 *(Valeurs absolues de $k(T)$)*

Soit k un corps. Soient P un polynôme irréductible de k, $Q = P^n \frac{u}{v}$ où u,v sont deux polynômes premiers entre eux et premiers à P et $n \in \mathbb{Z}$. Soit $\delta \in \mathbb{R}$, $0 < \delta < 1$. Posons $|Q|_P = \delta^n$.

1. Montrer que $|\cdot|_P$ est une valeur absolue de $k(T)$.
2. Montrer que l'application qui à $Q = \frac{u}{v} \in k(T)$ associe $\delta^{\mathrm{d}^0 v - \mathrm{d}^0 u}$ est une valeur absolue de $k(T)$.
3. Démontrer que les valeurs absolues de $k(T)$ triviales sur k sont de l'un des deux types précédents à équivalence près.

4. En déduire que, lorsque k est un corps fini, les valeurs absolues sont de l'un des deux types précédents tout court.

Heuristique

(Quelques commentaires sur les analogies en arithmétique) Les extensions finies des corps $\mathbb{Q}$ et $\mathbb{F}(T)$ sont respectivement les *corps de nombres* et les *corps de fonctions*. Les propriétés arithmétiques de ces corps sont très analogues, mais généralement plus difficiles à établir pour les corps de nombres. D'un point de vue technique, l'étude des corps de fonctions revient à l'étude des courbes algébriques sur les corps finis, ce qui est du ressort de la géométrie algébrique. Prenons note de quelques différences entre $\mathbb{Q}$ et $\mathbb{F}(T)$:

- ⋆ Le corps $\mathbb{Q}$ possède une valeur absolue archimédienne contrairement à $\mathbb{F}(T)$. Dans l'esprit qui prévaut en théorie des nombres, cette valeur absolue doit être prise en compte et, éventuellement, placée à égalité avec les valeurs absolues non archimédiennes.
- ⋆ Les anneaux de valuation discrète associés aux valeurs absolues de $\mathbb{F}(T)$ (respectivement $\mathbb{Q}$) ont des corps résiduels qui ont tous même caractéristique (respectivement $\mathbb{Q}$) ont des caractéristiques toutes différentes).
- ⋆ Le corps $\mathbb{F}(T)$ possède des extensions finies obtenues en considérant les extensions de $\mathbb{F}$ (on s'accorde toutefois à penser que certaines extensions de $\mathbb{Q}$ obtenues en ajoutant des racines de l'unité seraient les analogues de ces extensions).
- ⋆ On peut faire sur l'anneau $F[T]$ (qui est l'anneau des entiers de $\mathbb{F}(T)$) l'opération suivante $F[T] \otimes F[T] = F[T_1,T_2]$. On ne voit pas comment faire une telle opération pour le corps $\mathbb{Q}$ (*i.e.* on a $\mathbb{Z} \otimes \mathbb{Z} = \mathbb{Z}$, ce qui n'est pas très intéressant).
- ⋆ Le corps $\mathbb{F}(T)$ est muni d'une application $\mathbb{F}$-linéaire donnée par la dérivation. C'est parfois un outil très commode dont on aimerait bien disposer pour étudier les nombres.

4.1.4 Places

Définition. ***(Place)***

Une *place* d'un corps K dans un corps L est une application $K \cup \{\infty\} \to L \cup \{\infty\}$ qui respecte l'addition et la multiplication prolongées partiellements à $K \cup \{\infty\}$ et $L \cup \{\infty\}$ par $x + \infty = \infty$ pour tout x dans K ou L, $x\infty = \infty$ pour tout x non nul dans K ou L et $\infty + \infty = \infty$.
Une place est *finie* ou *infinie* selon que L l'est ou non.

Exemples. ***(Places)***

1. Tout homomorphisme de corps $K \hookrightarrow L$ fournit une place de K dans L.
2. Soit p un nombre premier. La réduction modulo p fournit une place finie de $\mathbb{Q}$ dans $\mathbb{F}_p$, en convenant que la réduction d'un rationnel non p-entier est infinie. Ces places coïncident avec les valeurs absolues non archimédiennes de $\mathbb{Q}$.
3. La place triviale de $\mathbb{Q}$ dans $\mathbb{Q}$ coïncide quant à elle à la valeur absolue triviale sur $\mathbb{Q}$. Signalons que toutes les places de $\mathbb{Q}$ sont obtenues en composant celles mentionnées ci-dessus avec des homomorphismes de corps.
4. Les valeurs absolues sur un corps K définies à l'aide d'un plongement définissent des places de K dans $\mathbb{C}$.

Remarque. Ainsi, à un homomorphisme de corps près, les places de $\mathbb{Q}$ correspondent donc aux valeurs absolues de $\mathbb{Q}$ à équivalence près. Cette remarque trouve son intérêt dans le fait que la notion de place est plus intrinsèque que la notion de valeur absolue : Elle ne recourt pas au corps des nombres réels.

4.2 Théorie algébrique des nombres (TAN1)

4.2.1 Éléments entiers sur un anneau

4.2.1.1 Définition et premières propriétés

Soit R un anneau. Soit A un sous-anneau de R et $x \in R$. On note $A[x]$ le sous-anneau de R engendré par x et A. On vérifie avec les définitions que $A[x] = \{P(x) \mid P \in A[X]\}$.

Théorème. ***(Caractérisation des éléments entiers sur un anneau)***

Les propriétés suivantes sont équivalentes :

1. Il existe un $n \geqslant 1$ entier et des éléments $a_0,...,a_{n-1} \in A$ tels que

$$x^n + a_{n-1}x^{n-1} + ... + a_0 = 0$$

   (on dit que x satifsait une *équation de dépendance intégrale*), autrement dit, x est est racine d'un polynôme unitaire à coefficients dans A : il existe $P \in A[X]$ de degré $\geqslant 1$, unitaire et tel que $P(x) = 0$
2. Le A-module $A[x]$ est de type fini (notons bien que la structure de A-module sur $A[x]$ vient de la loi additive de cet anneau et de la restriction à $A \times A[x]$ de sa multiplication d'anneau).
3. Il existe B un sous-anneau de R contenant A et x tel que B est un A-module de type fini.

▷ Par principe de minimalité. Supposons qu'il existe $P \in A[X]$ unitaire de degré $n \geqslant 1$ tel que $P(x) = 0$. Pour tout $y \in A[x]$, il existe par définition $Q \in A[X]$ tel que $y = Q(x)$. On effectue alors la division euclidienne de Q par P, licite, car le coefficient dominant de P est une unité : $Q = PB + R$ avec B,$R \in A[X]$ et $\deg(R) < \deg(P) = n$. En évaluant en x, $Q(x) = y = P(x)B(x) + R(x) = R(x)$. Si $R = r_0 + r_1X + ... + r_{n-1}X^{n-1}$, on obtient $y = r_0 + r_1x + ... + r_{n-1}x^{n-1}$ donc y appartient au modulé engendré par la sous-partie finie $1_A, x, x^2,...,x^{n-1}$.

Il est clair que le deuxième point implique le troisième.

Pour la dernière implication, il faut travailler un peu plus. On part de $B \ni x, \supseteq A$ un sous-anneau qui soit un A-module de type fini. Par hypothèse, il existe $(y_1,...,y_n)$ éléments de B tels que B soit engendré par $\{y_1,...,y_n\}$ comme A-module. Soit $1 \leqslant i \leqslant n$. Comme $y_i \in B, x \in B$ et B est un anneau, $xy_i \in B$. Ainsi, il existe $(a_{i,j})_{1 \leqslant i \leqslant n}$ tels que $xy_i = \sum_{j=1}^{n} a_{i,j}y_j$. Introduisons la matrice $M = xI_n - (a_{i,j})_{i,j} \in \mathfrak{M}_n(B)$. Ainsi on peut récrire $MY = 0$ où Y est le vecteur colonne $(y_1,...,y_n)$. On note $\tilde{M}$ la transposée de la comatrice de M. Alors[1] $M\tilde{M} = \tilde{M}M = \det(M).I_n$ avec $\det(M) \in B$. Ainsi $\tilde{M}MY = \det(M)Y$. Ainsi $\det(M)y_i = 0$ pour tout i. Or $1 \in B$, donc il existe $z_1,...,z_n \in A$ tel que $1 = \sum_{i=1}^{n} z_iy_i$, donc $\det(M) = \sum_{i=1}^{n} z_i(\det(M)y_i) = 0$. Or $\det(M) = \chi_{(a_{ij})_{i,j}}(x)$ qui est un polynôme en x à coefficients dans A, unitaire et de degré $n \geqslant 1$, d'où le résultat. ■

Définition. ***(Élément entier sur un anneau)***

Soit A un sous-anneau d'un anneau R. On dit que $x \in R$ est *entier sur* A s'il vérifie l'une des trois conditions équivalentes du théorème, c'est-à-dire, s'il existe une relation de dépendance intégrale $P(x) = 0$ où $P \in A[X]$ est unitaire de degré $\geqslant 1$.
On appelle *degré* de x le plus petit degré de tous les polynômes unitaires à coefficients dans A et non nuls annulant x, qui existe par propriété fondamentale de $\mathbb{R}$. Il est clair que, *si R est intègre*, tout polynôme annulateur de x dans $A[X]$ unitaire de degré $\deg(x)$ est irréductible (il y a une petite subtilité quand même).

La notion d'intégralité rappelle celle d'algébricité sur un corps ; cependant, la différence

[1] Dans un anneau commutatif quelconque, on dispose des théorèmes classiques sur le déterminant des matrices carrées défini par la formule de Leibniz : $\det(M) = \sum_{n \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} M_{i,\sigma(i)}$ (multiplicativité, formule de composition, propriétés opératoires, développement en échiquier, formule de la comatrice, caractérisation de l'inversibilité), mis à part la définition par les formes antisymétriques qui ne vaut pas en caractéristique 2. Par exemple, $M \in GL_n(\mathbb{Z})$ si et seulement si $\det(M) = \pm 1$. Toutes ces propriétés que l'on connaît sur les corps s'étendent à un anneau.

Illustrons la démarche pour démontrer la multiplicativité du déterminant dans un anneau commutatif A. Remarquons d'abord que si A est intègre, il suffit de plonger A dans son corps des fractions et le tour est joué. Dans le cas général, étant données deux matrices $M = (a_{i,j})$ et $N = (b_{i,j})$ à coefficients dans A, l'universalité des anneaux de polynômes donne qu'il existe un (unique) homomorphisme d'anneaux $\mathbb{Z}[X_{i,j},Y_{i,j}, 1 \leqslant i,j \leqslant n] \longrightarrow A$ envoyant $X_{i,j}$ sur $a_{i,j}$ et $Y_{i,j}$ sur $b_{i,j}$. Comme le résultat est déjà connu dans $\mathbb{Z}[X_{i,j}, Y_{i,j}]$ qui est intègre, on en déduit la formule voulue dans A.

Toutes les formules additivo-multiplicatives peuvent se démontrer de la même manière.

crucial est que, hors d'un corps, on ne peut supposer la relation de dépendance intégrale donnée par la notion d'algébricité fournie par un polynôme unitaire ; elle est donc plus forte que celle-ci. On compte sur ce que l'étudiant a déjà manipulé un minimum les entiers algébriques parmi les complexes, ce qui lui facilitera en esprit le début de cette étude.

Exemples. ***(Éléments entiers sur $\mathbb{Z}$)***

1. *(Classique : clôture intégrale des rationnels)* Soit $\mathbb{Z} \subseteq \mathbb{Q}$. Quels sont les $x \in \mathbb{Q}$ entiers sur $\mathbb{Z}$? D'après le test des racines rationnelles, vu que le polynôme de la relation de dépendance intégrale doit être unitaire, pour une racine $x = p/q$, on a $q \mid p^n$ où n est le degré de ce polynôme puis si la fraction est irréductible, $q = 1$. Donc x est entier au sens usuel. Réciproquement, tout élément $n \in \mathbb{Z}$ est annulé par $X - n$. Ainsi, les éléments de $\mathbb{Q}$ entiers sur $\mathbb{Z}$ sont les éléments de $\mathbb{Z}$.
2. Soit $n \geqslant 2$ un entier naturel ; alors $\sqrt{n} \in \mathbb{R}$. On considère $\mathbb{Z}$ sous-anneau de $\mathbb{R}$. Puisque $X^2 - n$ annule $\sqrt{n}$, $\sqrt{n}$ est entier sur $\mathbb{Z}$.
   Quid de $\frac{1}{\sqrt{n}}$? Supposons qu'il le soit. Soit $Q \in \mathbb{Z}[X]$ dans la relation de dépendance intégrale. Le polynôme $(-1)^{\deg(Q)}Q(X)Q(-X)$ est pair et unitaire, il s'écrit donc sous la forme $P(X^2)$ et P est donc annulateur de $\frac{1}{n}$. Donc $\frac{1}{n}$ est entier sur $\mathbb{Z}$. Puisqu'il est rationnel, il est entier donc $n = 1$. (Par contre, $\frac{1}{\sqrt{n}}$ est algébrique sur $\mathbb{Q}$.)
3. Les nombres $e, \pi \in \mathbb{R}$ sont transcendants, c'est-à-dire non algébriques sur $\mathbb{Q}$; a fortiori *(voir la remarque suivante)*, ils ne sont pas entiers.
4. *(Racines de l'unité)* $i \in \mathbb{C}$ est entier sur $\mathbb{Z}$, car $X^2 + 1$ annule i. Plus généralement, toute racine de 1 est entière sur $\mathbb{Z}$. Ainsi, non seulement les entiers sur $\mathbb{Z}$ sont en grand nombre irrationnels (mais toujours algébriques), certains sont irréels.
5. Les éléments de $\mathbb{C}$ sont entiers sur $\mathbb{R}$, car $\mathbb{C}$ est une extension finie donc algébrique des réels. Explicitement, si $z \in \mathbb{C}$, $(X - z)(x - \overline{z}) \in \mathbb{R}[X]$ annule z, est de degré $2 \geqslant 1$ et unitaire.

Remarques.

1. *(Entiers triviaux)* On remarque que tout élément de A est entier sur A, en effet, pour tout $a \in A$, $P(a) = 0$ avec $P = X - a$.
2. *(Propagation de l'intégralité)* Si $A \subseteq B \subseteq R$ sont des sous-anneaux et si $x \in R$ est entier sur A, a fortiori x est entier sur B, car un polynôme unitaire à coefficients dans A est à coefficients dans B.
3. *(Cas des corps et lien avec les nombres algébriques)* Si $A = K$ est un corps, et $K \subseteq R$ est un sous-anneau de R, alors $x \in R$ est entier sur K si et seulement si x est algébrique sur K, ou encore il existe $P \in K[X]$ tel que $P(x) = 0$, P non nul ; ici P n'est pas unitaire a priori, car si P est de coefficient directeur a_n, $a_n^{-1}P$ annule encore x. Ainsi, dans une certaine mesure, les résultats d'intégralité impliquent des résultats d'algébricité.
   On rappelle qu'un *nombre algébrique* $x \in L$ extension de K sur K est par définition

tel que le sous-corps engendré par lui $K(x)$ égal le sous-anneau $K[x]$, ou encore, si $K(x)$ est de dimension finie en tant que K-espace vectoriel.

▷ Soit $x \in L/K$. Si $P(x) = 0$ pour $P \in K[X]$ non nul, alors tout corps est un anneau donc de toute manière $K[x] \subseteq K(x)$. Réciproquement, prenons P minimal (possible, car $K[X]$ est principal). Alors en passant le terme constant (donc non nul) de P de l'autre côté de la RDI, on obtient, toujours dans K donc la division par un coefficient étant possible, que l'inverse de x est un polynôme en x. Donc $K(x) \subseteq K[x]$. L'équivalence avec le troisième énoncé est une conséquence du théorème d'isomorphisme et de la structure du quotient par un polynôme, cf ALGÈBRE GÉNÉRALE, EXTENSIONS DE CORPS. Supposons maintenant que $K(x) = K[x]$. D'après la remarque précédente, il est de dimension finie n. Ainsi $(1,...,x^n)$ qui a $n+1$ éléments est liée, ce qui fournit une RDI sur x à coefficients dans K. ■

4. *(Instabilité opératoire)* Comme le montre le deuxième exemple précédent, l'intégralité ne passe par à l'inverse (contrairement aux nombres algébriques !). Mais on a les autres propriétés de stabilité, comme on va le montrer juste après.

Propriété

Soit $A \subseteq R$ un sous-anneau et $(x_1,...,x_n)$ une famille finie d'éléments de R, tel que pour tout $i \geqslant 1$, l'élément x_i est entier sur le sous-anneau engendré par A et $x_1,...,x_{i-1}$: $A[x_1,...,x_{i-1}]$ (x_1 est entier sur A, x_2 est entier sur $A[x_1]$, etc.). Alors $A[x_1,...,x_n]$ est un A-module de type fini.

▷ On fait la récurrence sur n. L'initialisation vient de la première caractérisation des entiers sur un anneau. On admet le résultat jusqu'à $n-1$. On note $B = A[x_1,...,x_{n-1}]$ A-module de type fini. Soit $(y_1,...y_r)$ dans B tels que $B = Ay_1 + ...Ay_r$. Par le théorème, x_n est entier sur B donc $B[x_n]$ est un B-module de type fini. Il existe donc $z_1,...,z_l$ tel que $B[x_n] = Bz_1 + ... + Bz_l$. Or $A[x_1,...,x_n] = B[x_n] = \sum_{i=1}^{n} Bz_i = \sum_{i=1}^{l} \left(\sum_{j=1}^{r} Ay_j \right) z_i = \sum_{i,j} Ay_j z_i$. ■

$A[x_1,...,x_n]$ n'est pas l'ensemble des combinaisons linéaires de $x_1,...,x_n$! (Ce n'est pas le module engendré mais l'anneau !) Par contre, $A[x_1,...,x_n] = \{P(x_1,...,x_n), P \in A[X_1,...,X_n]\}$. Lorsque x est entier, $A[x] = A + Ax + ... + Ax^{n-1}$ pour n assez grand ; sinon, $A[x] = \langle x^i, i \in \mathbb{N} \rangle$ en tant que A-module.

Remarquons que, dans la propriété précédente, **chaque x_i est entier sur A est une condition suffisante**.

Corollaire. *(Opérations sur les entiers)*

Soit $A \subseteq R$ un sous-anneau, $x,y \in R$ entiers sur A. Alors $x+y$, $x-y$ et xy sont entiers sur A.

▷ D'après la propriété précédente, $A[x,y]$ est un A-module de type fini. Or $x+y \in A[x,y]$ donc d'après le théorème de caractérisation, $x+y$ est entier sur A. De même pour les autres. ■

Corollaire. ***(Conjugué d'un entier)***

Le conjugué d'un entier algébrique est algébrique.

▷ Un polynôme a coefficient dans $\mathbb{Z}$ est invariant sous l'action de la conjugaison. ■

Exercice 4

Soient $p,n \geqslant 2$ deux entiers naturels. On a $\sqrt[p]{n} \in \mathbb{R}$. Puisque $X^p - n$ annule $\sqrt[p]{n}$, $\sqrt[p]{n}$ est entier sur $\mathbb{Z}$. Son inverse est-il entier sur $\mathbb{Z}$?

▷ **Éléments de réponse.**

Non. Sinon, sa puissance p-ième $\frac{1}{n}$ le serait, absurde.

Corollaire. ***(Structure des entiers algébriques)***

Soit $A \subseteq R$ un sous-anneau. L'ensemble A' des éléments de R entiers sur A est un sous-anneau de R contenant A.

▷ En effet, on a vu que $A \subseteq A'$. Il est clair donc que $0 \in A'$ et $1_R = 1_A \in A'$. De plus, pour $x,y \in A$, $x-y \in A'$ donc $(A',+)$ est un sous-groupe de R. Puisque $xy \in A'$, c'est bien un sous-anneau. ■

4.2.1.2 Anneaux entiers, anneaux intégralement clos

Définition. ***(Fermeture intégrale, clôture intégrale)***

Soient $A \subseteq R$ un sous-anneau. Le sous-anneau A' des éléments qui sont entiers sur A s'appelle la *fermeture (ou parfois clôture) intégrale* de A dans R.
Si A est un anneau intègre, le sous-anneau des éléments de $K = Frac(A)$ qui sont entiers sur A s'appelle la *clôture intégrale* de A. Cette deuxième notion est extrinsèque.

Définition. ***(Sur-anneau entier, anneau intégralement clos)***

Si $A \subseteq R$ est un sous-anneau. On dit que l'anneau R est *entier sur* A si tout élément de R est entier sur A. Autrement dit, la fermeture intégrale de A dans R est R.
On dit qu'un anneau intègre A est *intégralement clos* s'il est égal à sa clôture intégrale, autrement dit : si toute racine d'un polynôme unitaire de $A[X]$ est dans A.

Exemples. ***(Anneaux entiers sur un autre, clôtures intégrales)***

1. Le corps $\mathbb{C}$ est entier sur $\mathbb{R}$.
2. Toute extension d'anneaux B/A où B est un A-module de type fini définit, par la troisième caractérisation des éléments entiers, un anneau entier sur A.
3. Trivialement, tout corps est intégralement clos car il est égal à son corps des fractions.
4. La clôture intégrale de $\mathbb{Z}$ est $\mathbb{Z}$ lui-même : en effet, son corps des fractions est $\mathbb{Q}$ et l'on a vu que $\mathbb{Z}'_{\mathbb{Q}} = \mathbb{Z}$. Ainsi, $\mathbb{Z}$ est intégralement clos.
5. On rappelle que $(1 + i\sqrt{3})(1 - i\sqrt{3}) = 2 \times 2$ et que $(1 + i\sqrt{5})(1 - i\sqrt{5}) = 2 \times 3$. On peut démontrer que l'anneau $\mathbb{Z}[i\sqrt{5}]$, quoique non factoriel (voir le théorème suivant) est bien intégralement clos. En revanche, on observe que $\mathbb{Z}[i\sqrt{3}]$ n'est ni intégralement clos, ni factoriel a fortiori.

La condition donnée au deuxième point n'est pas nécessaire. En effet, on connaît ne seraient-ce que des extensions algébriques de degré infini, telles que $\overline{\mathbb{Q}}$.

Contre-exemple. ***(Un anneau non intégralement clos)***

Considérons k un corps, par exemple $\mathbb{R}$, et l'anneau $A = \frac{k[x,y]}{(y^2-x^3)}$ où x,y sont des variables formelles. Il n'est pas intégrablement clos.

Les familiers du cours d'arithmétique des anneaux savent par ailleurs que cet anneau est noethérien, non factoriel. En effet, c'est un quotient d'un anneau noethérien mais il n'est pas intégralement clos donc non factoriel d'après la suite. Déterminons la clôture intégrale de A.

On préfère étudier la réalisation de l'anneau $A = k[x^2,y^3]$. L'idée pour la voir est de paramétrer la courbe $y^2 = x^3$. On introduit le morphisme de k-algèbres défini par :

$$\begin{array}{rccc} \phi\colon & k[x,y] & \longrightarrow & k[t] \\ & P(x,y) & \longmapsto & P(t^2,t^3). \end{array}$$

Il est clair que son image est la réalisation précédente. De plus, le noyau de ϕ contient clairement $y^2 - x^3$, donc l'idéal qu'il engendre. Réciproquement, soit $P \in \mathrm{Ker}(\phi)$. On effectue la division euclidienne dans $(k[x])[y]$: $P = Q(y^2 - x^3) + R_1(x)y + R_0(x)$. En évaluant en t (c'est-à-dire, en prenant l'image par ϕ), on obtient que $R_1(t^2)t^3 = R_0(t^2)$. Le degré de l'un n'a pas la même parité que le degré de l'autre, donc $R_1 = R_0 = 0$.

On peut également voir sans peine que l'image de ce morphisme est $\{a_0 + a_2t^2 + ... + a_3t^3 + ...\}$, autrement dit, $\{P \in k[t], P'(0) = 0\}$. On prétend que $Frac(A) = k(t)$. En effet, $k[t] \subseteq Frac(A)$, car $t = \frac{t^3}{t^2}$. Ainsi $k(t) \subseteq Frac(A)$ d'où le résultat par minimalité du corps des fractions.

La clôture intégrale de A dans $k(t)$ est $k[t]$. En effet, $k[t]/A$ est entier, car $X^2 - t^2$ (ou, mieux, $Xt^2 - t^3$) $\in A[X]$ annule t, donc t est entier sur A, donc $A[t] = k[t]$ est un A-module de type fini. D'autre part, les éléments entiers sur A de $k(t)$ sont dans $k[t]$. Soit $F(t) \in k(t)$ entier sur A. Alors $F(t)$ est entier sur $k[t]$ qui est intégralement clos, car principal, donc $F(t) \in k[t]$. Le résultat s'ensuit.

On peut garder en tête ce procédé de *désingularisation.* □

On ré-énonce donc la propriété immédiate suivante :

Propriété. ***(Type fini $\Longrightarrow$ entier)***

Soient $A \subseteq B$ un sous-anneau. Si B est un A-module de type fini, alors B est entier sur A.

Propriété. ***(Tour de sur-anneaux entiers)***

Soient $A \subseteq B \subseteq C$ des sous-anneaux successifs. Si B est entier sur A et C est entier sur B, alors C est entier sur A. La réciproque est vraie.

▷ Pour la réciproque : on a déjà dit qu'alors C est entier sur B ; de plus, B est clairement entier sur A, car $B \subseteq C$. Soit $x \in C$. Il s'agit de voir que x est entier sur A. Comme x est entier sur B, il existe $n \geqslant 1, b_i \in B$ et $x^n + b_{n-1}x^{n-1} + ... + b_0 = 0$ où x est entier sur $A[b_0,...,b_{n-1}]$. Or chaque b_i est entier sur A. D'après la propriété précédente, $A[b_0,...,b_{n-1}]$ est un A-module de type fini. Ainsi, $A[b_0,...,b_{n-1},x]$ est un A-module de type fini, qui contient x et A, qui est donc entier sur A. ■

Ainsi, de même que pour les extensions algébriques de corps, l'intégralité ne permet pas de « sauter trop haut ».

Théorème. ***(Factoriel $\Longrightarrow$ intégralement clos)***

Tout anneau factoriel est intégralement clos.

▷ C'est exactement la même démonstration que pour $\mathbb{Z}$: le test des racines rationnelles conclut que les racines dans le corps de fractions sont à dénominateur divisant une puissance du numérateur. Or, dans un anneau factoriel, on dispose du lemme de Gauss ; donc ce dénominateur est une unité. ■

On énonce enfin une propriété utile pour la suite que l'on gardera en mémoire :

Propriété. ***(Corps et anneau entier)***

Soient $A \subseteq B$ sous-anneau où B est un anneau intègre. On suppose que B est entier sur A. Alors A est un corps, si et seulement si, B est un corps. De plus, l'inverse d'un élément $x \in B$ est un polynôme en x.

▷ Supposons que A soit un corps. Il faut voir que pour tout $x \in B$, x non nul, x est inversible. Puisque B/A est entier, x est entier sur A donc $A[x]$ est un A-module de type fini ; autrement dit, $A[x]$ est un A-espace vectoriel de dimension finie. On introduit l'application :

$$\begin{array}{rccc} m_x : & A[x] & \longrightarrow & A[x] \\ & y & \longmapsto & xy \end{array}$$

avec $m_x \in \mathrm{End}_{A\text{-ev}}(A[x])$. L'application m_x est injective, car B, donc $A[x]$, est intègre. Par égalité des dimensions finies, c'est un automorphisme de $A[x]$. L'image réciproque de 1 donne un inverse de x. Donc $x \in B^\times$. On a même $x \in A[x]^\times$, c'est-à-dire que $x^{-1} \in A[x]$.

Supposons que B est un corps. Soit $x \in A \setminus \{0\}$. Alors il existe $y \in B$ tel que $xy \in B$, car B est un corps. Or y est dans B donc entier sur A, donc $y^n + a_{n-1}y^{n-1} + ... + a_1 y + a_0 = 0$ pour une certaine relation de dépendance intégrale. En multipliant par x^{n-1}, on obtient $(xy)^{n-1}y + a_{n-1}(xy)^{n-1} + ... + a_1 x^{n-1}y + a_0 x^{n-1} = 0$ avec $y + a_{n-1} + a_{n-2}x(xy)^{n-2} + ... + a_1 x^{n-2}(xy) + a_0 x^{n-1} = 0$. Comme $xy = 1$, $y \in A[x] \subseteq A$. Donc il existe $y \in A$ tel que $xy = 1$, donc $x \in A^\times$. On remarque que c'est la même idée de preuve que dans le cas algébrique pour montrer que l'inverse d'un élément est un polynôme en cet élément, mais on n'inverse plus directement. ■

Notons que cette proposition intervient dans une preuve du Nullstellensatz de Hilbert.

4.2.1.3 Corps de nombres, entiers algébriques

On note $\overline{\mathbb{Q}} = \{x \in \mathbb{C} \mid x \text{ algébrique sur } \mathbb{Q}\}$ dont on vérifie (cf Algèbre générale, Théorie de Galois) que c'est la clôture algébrique de $\mathbb{Q}$.

Définition. ***(Corps de nombres algébriques)***

Un *corps de nombres (algébriques)* est une extension finie de $\mathbb{Q}$.

Ce n'est pas « une extension finie d'un corps infini ».

Rappels.

1. En particulier, c'est une extension algébrique.
2. Dans ce cas, en notant K ce corps de nombres, on peut introduire $n = [K : \mathbb{Q}] := \dim_{\mathbb{Q}}(K)$. Pour $n = 2$, on parle de corps quadratique. Pour $n = 3$, on parle de *corps cubique*, etc.
3. On a $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$. On a même $K \subseteq \overline{\mathbb{Q}}$.
4. Le théorème de l'élément primitif s'applique : il existe $x \in K$ tel que $K = \mathbb{Q}(x) = \mathbb{Q}[x]$ (par algébricité). Plus précisément : tout sous-corps de $\mathbb{C}$ engendré par un nombre fini de nombres $\mathbb{Q}$-algébriques est un corps de nombres. Réciproquement, tout corps de nombres est de cette forme, et peut même donc être engendré par un seul nombre algébrique.
5. Pour tout élément, en particulier pour x, le polynôme minimal μ_x de x existe ; c'est un polynôme irréductible de degré n.
6. L'extension est galoisienne, donc $\mathrm{Hom}_{\mathrm{Krp}}(K, \mathbb{C}) = \mathrm{Aut}(K/\mathbb{C})$ est de cardinal n. Un de ses éléments σ est déterminé par $\sigma(x)$. On remarque : $\sigma(\mu_x(x)) = \mu_x(\sigma(x)) = 0$. Ainsi, $\sigma(x)$ est une racine de μ_x. Or μ_x est séparable (*i.e.* à racines 2 à 2 distinctes dans $\mathbb{C}$), donc pour toute racine α de μ_x, il existe un unique σ tel que $\sigma(x) = \alpha$.

Autrement dit, l'action du groupe de Galois d'un polynôme irréductible à coefficients dans $\mathbb{Q}$ sur l'ensemble de ses racines est simplement transitive.

7. De plus, l'anneau A_K *(voir ci-dessous)* est stable par tout automorphisme de K.
8. Le corps des nombres algébriques n'est pas un corps de nombres algébriques !

Définition. ***(Anneau des entiers algébriques)***

L'anneau $A = A_K = \mathcal{O}_K$ *des entiers algébriques* de K est la fermeture intégrale de $\mathbb{Z}$ dans K, autrement dit, l'ensemble des $x \in K$ entiers sur $\mathbb{Z}$.

Si le lecteur pense que $A_K = K$, c'est qu'il faut retourner à la case départ.

Heuristique

Un entier algébrique est un élément d'un corps de nombres qui y joue un rôle analogue à celui d'entier relatif dans le corps des nombres rationnels (en arithmétique : dans une théorie purement algébrique, ce sont les éléments de la copie canonique de $\mathbb{Z}$ dans K, contenant $\mathbb{Q}$ comme sous-corps premier, qui joueraient ce rôle).

Fait

Pour tout $x \in K$, il existe $b \geqslant 1$ un entier naturel tel que $bx \in A_K$. Ainsi, tout élément de K est une fraction d'un entier algébrique divisé par un entier naturel :

$$\forall x \in K \ \exists a \in A_K, n \in \mathbb{N}^\times \quad x = \frac{a}{b},$$

à retenir.

En effet, il existe $m \geqslant 1$, a_0,...,$a_{m-1} \in \mathbb{Q}$ tels que $x^m + a_{m-1}x^{m-1} + ... + a_0 = 0$, car x est algébrique sur $\mathbb{Q}$. On chasse les dénominateurs en prenant leur ppcm b. En multipliant par b^m, on obtient $(bx)^m + a_{m-1}b(bx)^{m-1} + ... + (a_1b)b^{m-2}(bx) + a_0b.b^{m-1} = 0$. Puisque ces coefficients sont dans $\mathbb{Z}$, bx est entier sur $\mathbb{Z}$, c'est-à-dire $bx \in A_K$.

Fait

On a donc $\mathbb{Z} \subseteq A_K$ et $Frac(A_K) = K$.

L'inclusion réciproque vient de la remarque précédente, l'inclusion directe est évidente.

De plus, A_K est intégralement clos.

Car si $x \in K$ est entier sur A_K, comme A_K est entier sur $\mathbb{Z}$, $A_K[x]$ est entier sur A_K donc $A_K[x]$ est entier sur $\mathbb{Z}$, donc x est entier sur $\mathbb{Z}$, donc $x \in A_K$. (Sinon, par définition et la remarque précédente.)

On a donc montré :

Propriété. ***(Intégralité des anneaux d'entiers algébriques)***

L'anneau des entiers algébriques d'un corps de nombres est intégralement clos.

On démontrera plus tard

Propriété. ***(Noethérianité des anneaux d'entiers algébriques)***

L'anneau des entiers algébriques d'un corps de nombres est noethérien.

Ceci ne contredit certainement pas l'exercice précédent (pourquoi ?).

On retiendra l'identité suivante :

Propriété. ***(Quotient d'un anneau d'entiers algébriques par un idéal premier)***

Soit K un corps de nombres et $A = \mathcal{O}_K$. Soit p un nombre premier. Soit α tel que $K = \mathbb{Q}(\alpha)$ et $m = (\mathcal{O}_K : \mathbb{Z}[\alpha])$. Soit Q le polynôme minimal de α, dans $\mathbb{Z}[X]$ et $\tilde{Q}$ sa réduction modulo p. Alors m est fini et si p ne divise pas m,

$$\mathcal{O}_K/p\mathcal{O}_K \simeq {}^{\mathbb{F}_p[X]}\!/_{(\tilde{Q})}.$$

▷ On le montre d'abord dans le cas où $\mathcal{O}_K = \mathbb{Z}[\alpha]$, ce qui n'est alors qu'un jeu d'écriture. Pour passer au cas général, on utilise une relation de Bézout entre m et p pour montrer que $\mathcal{O}_K = \mathbb{Z}[\alpha] + p\mathcal{O}_K$ et l'on peut conclure semblablement. ■

4.2.1.4 Cas des corps quadratiques

Définition. ***(Corps quadratique)***

On appelle *corps quadratique* une extension de degré 2 de $\mathbb{Q}$.

Théorème. ***(Description des corps quadratiques)***

Les corps quadratiques sont exactement de la forme $\mathbb{Q}(\sqrt{d})$ où $d \in \mathbb{Z}$, $d \neq 0, 1$ et d est un entier relatif sans facteur carré.
Dans le cas $d \geqslant 0$, on parle de *corps quadratiques réels*. Dans le cas $d < 0$, on parle de *corps quadratiques imaginaires*.

▷ Puisque $K/\mathbb{Q}$ est quadratique, il existe $x \in K$ tel que $\mathbb{Q}[x] = K$. Alors $\mu_x = X^2 + bX + c$, et b,$c \in \mathbb{Q}$. Le discriminant de ce trinôme s'écrit $\Delta = b^2 - 4c = \frac{u}{v} = \frac{uv}{v^2} = \left(\frac{f}{v}\right)^2 d$ avec $(u,v) = 1$, u,$v \in \mathbb{Z}$, $v \neq 0$ et $uv = f^2.d$ où d est sans facteur carré, avec $f.d \in \mathbb{Z}$. On a alors $x = \dfrac{-b \pm \frac{f}{v}\sqrt{d}}{2}$ d'où $Q(x) \subseteq \mathbb{Q}(\sqrt{d})$ d'où par égalité des degrés, $\mathbb{Q}[x] = \mathbb{Q}[\sqrt{d}]$. Puisque $x \notin \mathbb{Q}$, $d \neq 0$,1. ■

Exemples. ***(Corps quadratiques)***

1. $\mathbb{Q}[\sqrt{3}]$ est un corps quadratique, où ici $d = 3$.
2. $\mathbb{Q}[i]$ est un corps quadratique, où ici $d = -1$.

Ainsi, tout corps quadratique est monogène. Pas de surprise (merci le TEP). Par contre, nous allons voir plus fortement que tout anneau d'entiers algébriques d'un corps quadratique est également monogène, ce qui n'est plus nécessairement le cas pour le degré $n \geqslant 3$.
Nous voyons en même temps que $\mathcal{O}_{\mathbb{Q}(\omega)} \neq \mathbb{Z}[\omega]$ a priori (mais c'est vrai pour $d \equiv 2{,}3$ [4], et pour les corps cyclotomiques ; en quelque sorte, $\mathcal{O}_K$ n'en est jamais bien loin).

Le théorème suivant vérifie que la description précédente est univoque.

Théorème. ***(Sous-corps des corps quadratiques)***

Les sous-corps $\mathbb{Q}[\sqrt{d}]$ où $d \in \mathbb{Z}$, $d \neq 0, 1$, d est sans facteur carré sont deux à deux distincts et deux à deux non isomorphes.

▷ Prenons d,d' comme dans l'énoncé. Supposons que $\mathbb{Q}[\sqrt{d}] \simeq \mathbb{Q}[\sqrt{d'}]$. Dans ce dernier corps, $X^2 - d'$ a une racine, donc $X^2 - d'$ a une racine dans $\mathbb{Q}(\sqrt{d})$, disons $a + b\sqrt{d}$, a,$b \in \mathbb{Q}$. Alors $d' = (a + b\sqrt{d})^2 = a^2 + db^2 + 2ab\sqrt{d}$. Or $(1, \sqrt{d})$ est une famille $\mathbb{Q}$-libre, donc $d' = a^2 + db^2$ et $2ab = 0$. Soit $a = 0$, donc $d' = db^2$ donc $b = 1$, car d' est non nul et sans facteur carré, soit $b = 0$, d'où $d' = a^2$, interdit également. ■

On décrit maintenant A_K dans le cas où $[K : \mathbb{Q}] = 2$.

Théorème. ***(Anneau des entiers algébriques d'un corps quadratique)***

Je fixe $d \in \mathbb{Z}$ non nul, non égal à 1, et sans facteur carré. On note $K = \mathbb{Q}(\sqrt{d})$. Alors $(1, \sqrt{d})$ est une $\mathbb{Q}$-base de K. Pour $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(K)$, il est donné par $\sigma(a + b\sqrt{d}) = a \pm b\sqrt{d}$ avec a,$b \in \mathbb{Q}$. **Nous notons alors σ la conjugaison dans cet anneau.**

Remarques.

1. $\sigma(A_K) \subseteq A_K$, car si $P \in \mathbb{Z}[X]$ est unitaire et annule $x \in K$, alors $\sigma(P(x)) = P(\sigma(x))$, donc puisque alors $P(\sigma(x)) = 0$, $\sigma(x) \in A_K$.
2. d est sans facteur carré donc 4 ne divise pas d. Par suite, $d \equiv 1{,}2{,}3$ [4]. Ceci justifie la discussion suivante.

On a :

1. Si $d \equiv 2{,}3 \bmod 4$,
$$A_K = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a,b \in \mathbb{Z}\}.$$

2. Si $d \equiv 1 \bmod 4$, alors

$$A_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} = \left\{\frac{u+v\sqrt{d}}{2} \mid u,v \in \mathbb{Z}, u \equiv v \ [2]\right\}.$$

▷ On suppose que $x = a + b\sqrt{d}$ pour $a,b \in \mathbb{Q}$ est dans A_K. Alors $\sigma(x) = a - b\sqrt{d} \in A_K$. Ainsi $x + \sigma(x) = 2a \in A_K$, et $x\sigma(x) = a^2 - b^2 d \in A_K$. Ces deux rationnels sont entiers donc entiers (lol), car $\mathbb{Z}$ est intégralement clos. C'est une condition nécessaire pour que $x \in A_K$. Remarquons que c'est une condition suffisante, car $(X - x)(X - \sigma(x)) = X^2 - 2aX + a^2 - b^2 d$, dans ce cas, annule x.

La condition nécessaire implique que $4(a^2 - b^2 d) \in \mathbb{Z}$. Or $4a^2 \in \mathbb{Z}$, donc $4b^2 d \in \mathbb{Z}$. D'autre part, si $2b \in \frac{p}{q}$ avec $(p,q) = 1$, alors $q^2 \mid p^2 d$ donc $q = 1$ puis $2b \in \mathbb{Z}$ car d est sans facteur carré. De plus, si $a = \frac{u}{2}, b = \frac{v}{2}, u,v \in \mathbb{Z}$, la CNS équivaut à ce que $u^2 - dv^2 \in 4\mathbb{Z}$.

Si v est pair, alors $v^2 \equiv 0 \ [4]$, donc $u^2 \equiv 0 \ [4]$, donc u est pair. Si maintenant v est impair, $v^2 \equiv 1 \ [4]$ donc $u^2 \equiv d \ [4]$. Donc $d \equiv 1 \ [4]$ et u est impair. Réciproquement, ces conditions impliquent la CNS. ■

On retiendra bien la preuve précédente, assez instructive.

Exemples. ***(Anneaux d'entiers des corps quadratiques)***

1. $A_{\mathbb{Q}(i)} = \mathbb{Z}[i]$.
2. $A_{\mathbb{Q}(\sqrt{3})} = \mathbb{Z}[\sqrt{3}]$.
3. $A_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

La principale application est le fait suivant, qui rentre parfaitement dans le cadre de notre étude.

Exercice 5 *(Application : anneau d'entiers quadratiques intégralement clos)*

Soit $d \in \mathbb{Z}$, $d \neq 0,1$, d sans facteur carré. Pour quelles valeurs de d, l'anneau $\mathbb{Z}[\sqrt{d}]$ est-il intégralement clos ?

▷ **Éléments de réponse.**

D'après le théorème, pour $d \equiv 2,3 \ [4]$, $\mathbb{Z}[\sqrt{d}] = A_K$ où $K = \mathbb{Q}(\sqrt{d}) = Frac(\mathbb{Z}[\sqrt{d}]$. D'après un fait précédent, l'anneau $\mathbb{Z}[\sqrt{d}]$ est intégralement clos. De plus, en toute généralité, les éléments de K qui sont entiers sur $\mathbb{Z}[\sqrt{d}]$ (a fortiori ils sont entiers sur $\mathbb{Z}$, car $\mathbb{Z}[\sqrt{d}]$ est $\mathbb{Z}$-entier) sont exactement les éléments de $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ si $d \equiv 1 \ [4]$, qui n'est pas $\mathbb{Z}[\sqrt{d}]$. Ainsi, on retiendra que $\mathbb{Z}[\sqrt{d}]$ est intégralement clos ssi $d \equiv 2,3 \ [4]$.

Exemples

1. $\mathbb{Z}[i\sqrt{3}]$ n'est pas intégralement clos, car $-3 \equiv 1 \ [4]$. Explicitement, $\zeta = -\frac{1}{3} + \frac{\sqrt{3}}{2}i$ vérifie $\zeta^2 + \zeta + 1$ entier sur $\mathbb{Z}$ et $\zeta \notin \mathbb{Z}[i\sqrt{3}]$.

2. $2\cos(\frac{2\pi}{n})$ est entier sur $\mathbb{Z}$.

En effet, $\zeta = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$ vérifie $\zeta^n = 1$. Ainsi, ζ est entier, donc $\overline{\zeta}$ est entier. Donc $2\cos(\frac{2\pi}{n}) = \zeta + \overline{\zeta}$ est entier. (Il est moins facile d'exhiber son polynôme caractéristique... Il s'agit d'une variante célèbre autour du polynôme cyclotomique d'ordre n.)

4.2.1.5 L'anneau des entiers algébriques

Définition. ***(Entier algébrique)***

On appelle *entier algébrique* un élément de $\mathbb{C}$ qui est entier sur $\mathbb{Z}$. On note $\overline{\mathbb{Z}}$ l'ensemble des $x \in \mathbb{C}$ tels que x soit entier sur $\mathbb{Z}$. Remarquons que c'est un sous-anneau de $\mathbb{C}$, que clairement $\overline{\mathbb{Z}} \subseteq \overline{\mathbb{Q}}$ et que par définition, pour tout corps de nombres K, $A_K = \overline{\mathbb{Z}} \cap K$.

Exercice 6

Montrer que $Frac(\overline{\mathbb{Z}}) = \overline{\mathbb{Q}}$ et que $\overline{\mathbb{Z}}$ est intégralement clos, mais ni factoriel, ni noethérien.

▷ **Éléments de réponse.**

$\overline{\mathbb{Q}}$ est un corps, donc $Frac(\overline{\mathbb{Z}}) \subseteq \overline{\mathbb{Q}}$. Soit maintenant $x \in \overline{\mathbb{Q}}$. Alors $\overline{\mathbb{Q}}(x)$ est un corps de nombres, donc il s'écrit comme fraction d'un entier algébrique avec un entier naturel (en particulier algébrique), d'où le résultat.

Montrons maintenant que $\overline{\mathbb{Z}}$ est intégralement clos. Soit $x \in \overline{\mathbb{Q}} = Frac(\overline{\mathbb{Z}})$ entier sur $\overline{\mathbb{Z}}$ et montrons que $x \in \overline{\mathbb{Z}}$. On a $\overline{\mathbb{Q}}(x)$ entier sur $\mathbb{Z}$ et par définition $\mathbb{Z}$ est entier sur $\mathbb{Z}$, donc $\overline{\mathbb{Q}}(x)$ est entier sur $\mathbb{Z}$, donc x l'est, $x \in \overline{\mathbb{Z}}$. Donc $\overline{\mathbb{Z}}$ est intégralement clos.

Montrons qu'il n'est pas factoriel. Pour chaque entier n, $2 = \sqrt[n]{2}^n$ où $\sqrt[n]{2}$ est un entier algébrique. Vérifions que $\sqrt[n]{2}$ n'est pas inversible dans $\overline{\mathbb{Z}}$. Il suffit de vérifier que $1/2$ ne l'est pas par produit. Cela vient du fait qu'un polynôme annulateur de $1/2$ à coefficients entiers, a son coefficient dominant pair. De même, $\overline{\mathbb{Z}}$ n'est pas noethérien. On introduit $I_n = \sqrt[n!]{2}$, de sorte que $I_n \subseteq I_{n+1}$. Seulement, si $I_n = I_{n+1}$ pour un certain n, alors $x_0 = 2^{\frac{1}{(n+1)!} - \frac{1}{n!}} \in \overline{\mathbb{Z}}$, puis $2^{n-1}x_0^{(n+1)!} = 1/2 \in \overline{\mathbb{Z}}$. Remarquons là que ce n'aurait pas marché avec n seulement et pas $n!$.

Exemples. ***(Entiers algébriques)***

1. Soit d un entier relatif congru à 1 modulo 4. Alors $\frac{1+\sqrt{d}}{4}$ est un entier algébrique.
2. Soit d,d' deux entiers relatifs congrus modulo 4. Alors $\frac{\sqrt{d}+\sqrt{d'}}{2} := \omega$ est un entier algébrique.

   En effet, en exploitant la congruence et en calculant $(2\omega)^2$, on obtient un polynôme de $\mathbb{Z}[\omega] = \sqrt{dd'}$. Il s'agit d'élever encore au carré (méthode générale) pour obtenir une dépendant intégrale.

Propriété. ***(Caractérisation des entiers algébriques)***

Soit $z \in \mathbb{C}$. Alors z est un entier algébrique, si et seulement si, il existe un sous-groupe additif G de $\mathbb{C}$ de type fini non nul tel que $zG \subseteq G$.

▷ Soit G un tel groupe, nécessairement abélien. C'est un $\mathbb{Z}$-module de type fini, donc libre. Soit x_1,...,x_m une base de G avec $m = \mathrm{rg}(G)$. Soit $V = \mathrm{Vect}_{\mathbb{Q}}(x_1,...,x_m)$. Alors m_z la multiplication par z stabilise V par hypothèse. On note encore m_z l'endomorphisme induit. Alors χ_{m_z} est unitaire à coefficients dans $\mathbb{Z}$. En effet, (x_i) étant $\mathbb{Q}$-libre, c'est une base B du $\mathbb{Q}$-espace vectoriel V ; puisque $zx_i \in G$ pour chaque i, la matrice de m_x relativement à B est dans $\mathfrak{M}_m(\mathbb{Z})$. Il suffit de voir que, par Cayley-Hamilton, $\chi_{m_z}(m_z) = 0$ d'où $\chi_{m_z}(z) = \chi_{m_z}(m_z)(1) = 0$.

Réciproquement, si z est un entier algébrique annulé par un polynôme unitaire de degré k, il est immédiat que le sous-groupe $G = \mathbb{Z} + \mathbb{Z}z + ... + \mathbb{Z}^{z^{k-1}}$ est non nul, de type fini et que $zG \subseteq G$. ■

Propriété

Soit $z \in \overline{\mathbb{Q}}$. Alors $D_z = \{d \in \mathbb{Z}, dz \in \overline{\mathbb{Z}}\}$ est un idéal non nul de $\mathbb{Z}$.

▷ Encore une fois, il s'agit grosso modo de chasser des dénominateurs. ■

Exercice 7 *(Anticipation sur la partie suivante)*

Montrer que $z \in \mathbb{C}$ est un entier algébrique, si et seulement si, son polynôme minimal (unitaire) sur $\mathbb{Q}$ en tant qu'élément algébrique est à coefficients dans $\mathbb{Z}$. En déduire que $\mathbb{Z}$ est intégralement clos.

▷ **Éléments de réponse.**

On peut, pour varier avec la section suivante, donner un argument arithmétique plutôt que d'algèbre linéaire. Il s'agit alors de faire intervenir le lemme de Gauss sur le contenu pour les polynômes à coefficients dans $\mathbb{Q}$.

En effet, $\mu_x = X - x$ pour $x \in \mathbb{Q}$. Il est dans $\mathbb{Z}[X]$, si et seulement si, $x \in \mathbb{Z}$.

Ainsi, le polynôme minimal de l'entier algébrique nombre complexe z vu comme nombre algébrique fait figure également de polynôme minimal de z vu comme entier algébrique.

4.2.1.6 Normes et traces

Le cadre est le suivant : on prend deux anneaux $A \subseteq B$, où A est un sous-anneau de B. On suppose que B est un A-module libre de type fini. Pour tout $b \in B$, la multiplication $m_b : B \longrightarrow B$ qui à $x \mapsto bx$ est dans $\mathrm{End}_{A\text{-Mod}}(B) \ni m_x$, ce qui justifie les définitions suivantes.

Définition. ***(Norme d'un élément d'un anneau)***

Soit $b \in B$. La *norme* de b sur A, notée $N_{B/A}(b)$, est définie comme $\det(m_b)$. Si le contexte est clair, j'omets B/A dans la notation.
Notons que $N_{B/A}(b) \in A$.

Définition. ***(Trace d'un élément d'un anneau)***

Soit $b \in B$. La *trace* de b sur A, notée $\mathrm{Tr}_{B/A}(b)$, est définie comme $\mathrm{tr}(m_b)$. Si le contexte est clair, j'omets B/A dans la notation.
Notons que $\mathrm{Tr}_{B/A}(b) \in A$.

Définition. ***(Polynôme caractéristique d'un élément d'un anneau)***

Soit $b \in B$. Le *polynôme caractéristique* de b sur A, notée $\chi_{b,B/A}$, est défini comme χ_{m_b}. Si le contexte est clair, j'omets B/A dans la notation.
Notons que $\chi_{b,B/A} \in A[X]$ est un polynôme unitaire de degré $\mathrm{rg}_A(B) := n$.

Remarque. L'application norme est polynomiale ; l'application trace est une forme linéaire.

Propriétés. ***(Opérations sur les normes et les traces)***

Soient b,$b' \in B$ et $a \in A$.

1. *(Multiplicativité de la norme, additivité de la trace)* $N(bb') = N(b)N(b')$, $\mathrm{Tr}(b+b') = \mathrm{Tr}(b) + \mathrm{Tr}(b')$.
2. *(Norme et trace d'un élément de l'anneau de base)* $N(a) = a^n$, $\mathrm{Tr}(a) = na$.
3. *(Homogénéités de la norme et de la trace)* $N(ab) = a^n N(b)$ et $\mathrm{Tr}(ab) = a\mathrm{Tr}(b)$.

▷ Remarquons que si b,$b' \in B$, $m_b + m_{b'} = m_{b+b'}$ et $m_b \circ m_{b'} = m_{bb'}$. De plus, si $a \in A$, $\mathrm{Mat}(m_a) = aI_n$ dans une base de B puisqu'il en est. ■

Remarque. On peut bien sûr appliquer ces constructions au cas où L/K est simplement une extension finie de corps. Si A,B sont des anneaux **intègres** et B un A-module libre de type fini, en notant $K = Frac(A)$, on peut étendre les scalaires grâce à $B \otimes_A K$ qui est un K-espace vectoriel de dimension finie : ici, puisque $B \simeq A^n$, le produit tensoriel $B \otimes_A K \simeq K^n$. Pour tout $b \in B$, on a alors $N_{B/A}(b) = N_{B\otimes K/K}(b)$ *(invariance de la norme par extension des scalaires).*

Propriété. ***(Expression de la norme, de la trace et du χ par les racines)***

Soit K un corps de caractéristique nulle. Soit L/K un extension de corps de degré fini n. Soit $x \in L$ (x est automatiquement algébrique sur K). Soit μ_x le polynôme minimal de x sur K. Notons bien que $\deg(\mu_x) = [K(x) : K]$.
Soient x_1,...,x_n les racines de μ_x dans une extension de L assez grande, par exemple la

clôture algébrique, chacune répétée $d = [L : K(x)]$ fois (notons bien : $n = [L : K] = [L : K(x)] \deg(\mu_x)$). Puisque μ_x est irréductible dans une extension séparable, μ_x a exactement $[K(x) : K] = \deg(\mu_x)$ racines simples dans une extension assez grande ; de plus, $\deg(\mu_x) \mid n$. Alors :

$$\mathrm{Tr}_{L/K}(x) = x_1 + ... + x_n,$$
$$N_{L/K}(x) = x_1...x_n,$$
$$\chi_{x,L/K}(X) = \prod_{i=1}^{n}(X - x_i).$$

Autrement dit, si $\alpha_1,...,\alpha_m$ sont les racines de μ_x avec $m = [K(x) : K]$,

$$tr_{L/K}(x) = d(\alpha_1 + ... + \alpha_m),$$
$$N_{L/K}(x) = (x_1...x_n)^d,$$
$$chi_{x,L/K}(X) = \prod_{j=1}^{m}(X - \alpha_j)^d.$$

Si $L = K(x)$, on répète donc chaque terme seulement $d = 1$ fois.
En particulier, $\chi_{x,L/K}(X) = \mu_x^{[L:K(x)]}$ et si $x \in K$, $\mathrm{Tr}(x) = [L : K]x$, $N(x) = x^{[L:K]}$ (car $[L : K(x)] = [L : K]$).

▷ Commençons par le cas où $L = K(x)$. On peut écrire $\mu_x = X^n + a_{n-1}X^{n-1} + ... + a_0$ puisque $\deg(\mu_x) = n$, avec $\mu_x(x) = 0$. De plus $1,...,x^{n-1}$ est une base de L/K. Dans ce cas, $\mathrm{Mat}_{(1,...,x^{n-1})}(\mu_x) = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & \vdots \\ \vdots & 0 & & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$ est la matrice compagnon associée à $\mu(x)$, donc $\mu_x = \prod_{i=1}^{n}(X - x_i)$ où μ_x n'a que des racines simples, car irréductible dans une extension séparable. Ainsi $\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(m_x) = -a_{m-1} = \sum x_i$ et $N_{L/K}(x) = \det(m_x) = (-1)^n\mu_x(0) = (-1)^n a_0 = \prod_{i=1}^{n} x_i$. Alors $\chi_{x,L/K} = \chi_{m_x} = \mu_x = \prod(X - x_i)$.

En général, on prend une base $y_1,...,y_d$ de L sur $K(x)$. Alors $d = [L/K(x)]$ où $d|n$ avec $md = n$ où $m = [K(x) : K]$. D'après le théorème de la base télescopique, $(y_i x^j)_{1\leqslant i\leqslant d, 0\leqslant j\leqslant m-1}$ est une base de L sur K. Dans ce cas, la matrice de m_x dans cette base est diagonale par blocs $Diag(c_x,....,c_x)$ où c_x est la matrice compagnon associée à μ_x, d'où $\mathrm{Tr}_{L/K}(x) = d\mathrm{Tr}(c_x)$ et $N_{L/K}(x) = \det(c_x)^d$ et $\chi_{x,L/K} = (\chi_{c_x})^d$. Or $\chi_{c_x} = \prod_{i=1}^{m}(X - s_i)$ où $\{s_1,...,s_m\}$ sont les racines de μ_x. ■

Remarque. On peut énoncer la proposition précédente de la façon suivante :

$$\mathrm{Tr}_{L/K}(x) = \sum_{\sigma\in\mathrm{Hom}_K(L,\overline{L})} \sigma(x),$$
$$N_{L/K}(x) = \prod_{\sigma\in\mathrm{Hom}_K(L,\overline{L})} \sigma(x),$$
$$\chi_{x,L/K}(X) = \prod_{\sigma\in\mathrm{Hom}_K(L,\overline{L})} (X-\sigma(x)).$$

En effet, le résultat est clair si $L = K(x)$ puisqu'alors $\deg(\mu_x) = n$ et si $\{x_1,...,x_n\}$ est l'ensemble des racines (simples) de μ_x, on a une bijection $\mathrm{Hom}_K(K(x),\overline{L}) \simeq \{x_1,...,x_n\}$ qui à $\sigma \mapsto \sigma(x)$. En général, l'application de $\mathrm{Hom}_K(L,\overline{L}) \longrightarrow \mathrm{Hom}_K(K(x),\overline{L})$ qui à $\sigma \mapsto \sigma_{|K(x)}$ est surjective à fibres de cardinal $[L : K(x)]$ (en effet, il revient à composer par un automorphisme de $K(x)/L$ et l'on applique de lemme d'Artin) d'où bien $[L : K(x)] \sum_{\sigma\in\mathrm{Hom}_K(K(x),\overline{L})} \sigma(x) = \sum x_i$ par le lemme des bergers, ce qu'il fallait montrer.

Corollaire. ***(Transitivité de la norme et de la trace)***

Pour $K \subseteq L' \subseteq L$ une suite d'extensions, on a :

$$\mathrm{Tr}_{L/K} = \mathrm{Tr}_{L'/K} \circ \mathrm{Tr}_{L/L'} \qquad \text{et} \qquad N_{L/K} = N_{L'/K} \circ N_{L/L'}.$$

▷ Soit $\sigma \in \mathrm{Hom}_K(L',\overline{L})$ et $\tilde{\sigma} \in \mathrm{Hom}_K(\overline{L},\overline{L})$ tel que $\tilde{\sigma}_{|L'} = \sigma$. L'application de restriction $\mathrm{Hom}_K(L,\overline{L}) \longrightarrow \mathrm{Hom}_K(L',\overline{L})$ est surjective, les fibres ont exactement $[L,L']$ éléments. Plus exactement, la fibre de $\sigma \in \mathrm{Hom}(L',\overline{L})$ est $\{\tilde{\sigma}\circ\tau \mid \tau \in \mathrm{Hom}_{L'}(L,\overline{L})\}$. Ainsi, d'après la remarque, $\mathrm{Tr}_{L/K}(x) = \sum_{\delta\in\mathrm{Hom}_K(L,\overline{L})} \delta(x) = \sum_{\sigma\in\mathrm{Hom}_K(L',\overline{L})} \sum_{\delta,\delta_{|L'}=\sigma} \delta(x)$ où $\sum_{\delta,\delta_{|L'}=\sigma} \delta(x) = \sum_{\tau\in\mathrm{Hom}_{L'}(L,\overline{L})} \tilde{\sigma}\circ\tau$ donc égale $\sum_{\sigma\in\mathrm{Hom}_K(L',\overline{L})} \tilde{\sigma}\left(\sum_{\tau\in\mathrm{Hom}_{L'}(L,\overline{L})} \tau(x)\right)$ où cet argument est $\mathrm{Tr}_{L/L'}(x) \in L'$. Or $\tilde{\sigma}_{L'} = \sigma$, conséquemment cette quantité égale $\sum_{\sigma\in\mathrm{Hom}_K(L',\overline{L})} \sigma(\mathrm{Tr}_{L/L'}(x)) = \mathrm{Tr}_{L'/K}(\mathrm{Tr}_{L/L'}(x))$. ■

Remarque. L'hypothèse essentielle de la propriété est que L/K est séparable.

Exercice 8

Retrouver les formules de transitivité avec la méthode de la preuve de la propriété.

▷ **Éléments de réponse.**

En exercice.

Corollaire. ***(« Théorème de Cayley-Hamilton »)***

Soit K un corps de caractéristique nulle et L/K une extension finie. Soit $x \in L$. Alors $\chi_{x,L/K}(x) = 0$.

▷ Au moins trois façons de le voir. D'abord, μ_x divise χ_x de façon triviale avec nos définitions, car $\chi_x = \mu_x^m$ où m est le co-degré de $K(x)/K$ dans L. Sinon, on voit dans l'expression factorisée du χ que l'une des racines est x, donnée par $\sigma = id$. Enfin, on peut utiliser le théorème de Cayley-Hamilton (le vrai !) dans un module de type fini sur un anneau commutatif. On l'applique à μ_x, de sorte que χ_{m_x} annule m_x ; or $\chi_{m_x}(\mu_x)(1) = \chi_x x$ qui est donc nul. Dans les trois cas, on voit que la démonstration est particulièrement grossière. ■

Revenons à nos entiers.

Propriété. ***(Expression de la norme, de la trace et du χ par les racines)***

Soit A un anneau intègre, $K = Frac(A)$, $\mathrm{car}(K) = 0$ et L/K une extension finie. Soit $x \in L$, x entier sur A. Alors les coefficients de $\chi_{x,L/K}$ sont entiers sur A. Ainsi, $N_{L/K}(x)$ et $\mathrm{Tr}_{L/K}(x)$ sont entiers sur A.
En particulier, si A est intégralement clos, $\chi_{x,L/K} \in A[X]$, et donc $N_{L/K}(x), \mathrm{Tr}_{L/K}(x) \in A$.

▷ Puisque x est entier sur A, il existe $P \in A[X]$ unitaire, de degré $\geqslant 1$ tel que $P(x) = 0$. Pour tout $\sigma \in \mathrm{Hom}_K(L, \overline{K})$, $\sigma(P(x)) = P(\sigma(x)) = 0$ donc $\sigma(x)$ est entier sur A. Donc, $\chi_{x,L/K} = \prod_{\sigma \in \mathrm{Hom}_K(L,\overline{L})} (X - \sigma(x))$. Les coefficients de $\chi_{x,L/K}$ sont des éléments de K, ce sont des polynômes en les $\sigma(x)$, entiers. Ainsi les coefficients de $\chi_{x,L/K}$ sont entiers.

Pour le deuxième point, les coefficients de χ sont des entiers de K, or si A est intégralement clos, un entier de K est dans A. ■

Exercice 9

Montrer que, sous les conditions du corollaire, les coefficients de μ_x sont dans A.

▷ **Éléments de réponse.**

On remarque que l'expression du χ par les racines donne explicitement (cf la preuve) que $\mu_x \mid \chi_x$ dans tous les cas. Ainsi, il suffit d'appliquer l'exact même raisonnement que dans la propriété au polynôme minimal.

Exercice 10

Soit K un corps de nombres.

1. Montrer que $x \in K$ est entier algébrique si et seulement si $\chi_{x,K/\mathbb{Q}} \in \mathbb{Z}[X]$.
2. Montrer que $x \in K$ est entier algébrique si et seulement si son polynôme minimal $\mu_{x,K/\mathbb{Q}} \in \mathbb{Z}[X]$.

▷ **Éléments de réponse.**

Conséquence de la propriété pour le premier point et de l'exercice précédent pour le second (et, dans les deux cas, des tours d'extensions entières).

Méthode. ***(Calculer une norme ou une trace)***

On dispose de quatre méthodes d'astuciosité croissante :

- Si l'élément est dans la base, il suffit d'en prendre un itéré ou une puissance selon le degré de l'extension.
- On peut lire la norme et la trace sur les coefficients du polynôme minimal annulateur.
- Moins généralement, on peut calculer ces valeurs si l'on connaît ses racines.
- Si l'on sait décrire $\mathrm{Aut}(L/K)$, il suffit d'écrire une somme ou un produit sur ses éléments.

4.2.1.7 Discriminants et application à la structure de module de la fermeture intégrale

On suppose toujours que A est un sous-anneau de l'anneau B et que B est un A-module libre de type fini, et l'on note $\mathrm{rg}_A(B) := n$.

Définition. ***(Discriminant d'une famille d'éléments)***

Soit $(x_1,...,x_n)$ une famille d'éléments de B. Le *discriminant* de $(x_1,...,x_n)$ est :

$$D_{B/A}(x_1,...,x_n) = \mathrm{Disc}(B/A) := \det((\mathrm{Tr}_{B/A}(x_ix_j))_{1\leqslant i,j\leqslant n}) = \begin{vmatrix} \mathrm{Tr}(x_1^2) & \dots & \mathrm{Tr}(x_1x_n) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}(x_nx_1) & \dots & \mathrm{Tr}(x_n^2) \end{vmatrix}.$$

En particulier, $D_{B/A}(x_1,...,x_n) \in A$ toujours par définition.

Propriété. ***(Formule de changement de base)***

Soient $x = (x_i)$ et $y = (y_j)$ deux familles d'éléments de B à n termes. Soit $M = (a_{ij}) \in \mathfrak{M}_n(A)$ telle que $X = MY$, *i.e.* $x_i = \sum_{j=1}^{n} a_{ij}y_j$. Alors

$$D(x_1,...,x_n) = (\det(M))^2 D(y_1,...,y_n).$$

▷ En effet, $\mathrm{Tr}(x_ix_j) = \sum_{k=1}^{n} a_{i,k}\mathrm{Tr}(y_k,x_j) = \sum_{k=1}^{n} a_{i,k}\sum_{l=1}^{n} a_{j,l}\mathrm{Tr}(y_ky_l)$ d'où $(\mathrm{Tr}(x_ix_j))_{i,j} = M(\mathrm{Tr}(y_ly_k))_{l,k}\,{}^tM$. On conclut en prenant les déterminants. ■

Comme pressenti, on applique cette formule à des bases (x_i) et (y_i) de B libre, avec $\det(M) \in A^\times$ (par théorème du déterminant).

Corollaire

Le discriminant d'une base ne dépend pas du choix de la base à multiplication près par un carré d'un élément de $A^\times$.

Ceci permet d'introduction la définition suivante :

Définition. ***(Discriminant d'un sur-anneau)***

Le *discriminant* de B/A noté $\mathcal{D}_{B/A}$ est l'idéal de A engendré par $D(x_1,...,x_n)$ où $(x_1,...,x_n)$ est une base de B sur A.

Exemple fondamental. ***(Discriminant d'une extension simple)***

Si $B = A[x]$ et que $1,...,x^{n-1}$ est une base de B sur A, alors $\mathcal{D}_{B/A}$ est engendré par

$$\det(\mathrm{Tr}(x^{i+j})_{i,j}).$$

Proposition. ***(Caractérisation des bases par le discriminant)***

Supposons que $\mathcal{D}_{B/A}$ contienne un élément qui n'est pas un diviseur de 0 et $\mathcal{D}_{B/A} \neq (0)$. Alors $(x_1,...,x_n)$ est une base de B si et seulement si $D(x_1,...,x_n)$ engendre $\mathcal{D}_{B/A}$.

▷ Le sens direct découle du corollaire précédent. Réciproquement, soit $(e_1,...,e_n)$ une base de B sur A. Posons $d = D(e_1,...,e_n)$ qui est par définition un générateur de $\mathcal{D}_{B/A}$. Par hypothèse, d n'est pas un diviseur de zéro et d est non nul. Ainsi, si $d' = D(x_1,...,x_n)$, $d'A = \mathcal{D}_{B/A}$. Il existe $M \in \mathfrak{M}_n(A)$ tel que $(x_1,...,x_n)^T = M(e_1,...,e_n)^T$. Or $d \in \mathcal{D}_{B/A}$ donc il existe $\alpha \in A$ tel que $d = \alpha d'$. Or $d' = (\det(M))^2 d$. Ceci implique $d = \alpha(\det(M))^2 d$ d'où $d(1 - \alpha\det(M)^2) = 0$ d'où par hypothèse $\alpha\det(M)^2 = 1$. Ainsi, $\det(M) \in A^\times$ et donc (par formule de la comatrice), il existe $N \in M(n,A)$ tel que $MN = NM = I_n$, c'est-à-dire que M est inversible. Donc $(x_1,...,x_n)$ est une base de B. ■

De la formule de changement de base, on tire :

Corollaire. ***(Discriminant d'un réseau)***

Soit K un corps de nombres. Soit $M \subseteq \mathcal{O}_K$ un réseau d'indice m dans $\mathcal{O}_K$. Alors le discriminant (absolu) de M sur $\mathbb{Z}$ vaut $m^2\mathrm{Disc}(\mathcal{O}_K/\mathbb{Z})$.

▷ Notons que ce fait n'a de sens que l'une fois que l'on a prouvé (ce sera pour plus tard) que $\mathcal{O}_K$ est libre de degré $n = [K/\mathbb{Q}]$. Soit donc M un sous-groupe de $\mathcal{O}_K$ de rang n, *i.e.* isomorphe à $\mathbb{Z}^n$ et d'indice $m = \mathrm{card}(\mathcal{O}_K/M)$. Alors par théorème de la base adaptée, il existe $(e_1,...,e_n)$ une base de $\mathcal{O}_K$ sur $\mathbb{Z}$ tels que pour certains facteurs invariants $a_1,...,a_n$, $(a_1e_1,..., a_ne_n)$ soit une $\mathbb{Z}$-base de M et $a_1...a_n = m$ par théorème fondamental de structure des modules sur $\mathbb{Z}$, ce produit étant le déterminant d'un changement de base clairement diagonal. D'où la formule. ■

Soit K un corps de caractérisation nulle et L/K une extension finie, ou plus généralement un corps quelconque et L/K une extension finie séparable.

On a une application φ K-bilinéaire symétrique :

$$\begin{aligned} L \times L &\longrightarrow K \\ (x,y) &\longmapsto \mathrm{Tr}_{L/K}(xy) \end{aligned}$$

qui est non dégénérée, c'est-à-dire que pour tout $x \in L$, $(\forall y \in L \quad \mathrm{Tr}_{L/K}(xy) = 0) \implies x = 0$.

▷ En effet, si $z \neq 0 \in L$, alors $\varphi(z,z^{-1}) = \mathrm{Tr}_L(1) = [L : \mathbb{Q}] \neq 0$, et l'on conclut ainsi. ■

Dans ce cas, l'application linéaire :

$$\begin{aligned} L &\longrightarrow L^\star = \mathrm{Hom}_{K\text{-Vect}}(L/K) \\ x &\longmapsto y \mapsto \mathrm{Tr}_{L/K}(xy) \end{aligned}$$

est injective.

En particulier, pour tout K-base (x_i) de L,

$$D_{L/K}(x_1,...,x_n) = \det(\mathrm{Tr}_{L/K}(x_i x_j)) \neq 0$$

où $n = [L : K]$.

Proposition. ***(Expression du discriminant)***

Si $\{\sigma_1,...,\sigma_n\} = \mathrm{Hom}_K(L, \overline{L})$,

$$D(x_1,...,x_n) = \det(\sigma_i(x_j))^2$$

et pour toute base $(x_1,...,x_n)$, on a $\det(\sigma_i(x_j)) \neq 0$, et donc $D(x_1,...,x_n) \neq 0$.

▷ $\mathrm{Tr}_{L/K}(x_i x_j) = \sum_{\sigma \in \mathrm{Hom}_K(L,\overline{L})} \sigma(x_i x_j) = \sum_{\sigma \in \mathrm{Hom}_K(L,\overline{L})} \sigma(x_i)\sigma(x_j) = \sum_{k=1}^{n} \sigma_k(x_i)\sigma_k(x_j)$ d'où $(\mathrm{Tr}(x_i x_j)) = (\sigma_k(x_i))_{i,k} \times (\sigma_k(x_j))_{k,j}$, d'où $D(x_1,...,x_n) = \det(\sigma_k(x_j))\det(\sigma_k(x_j)) = \det(\sigma_k(x_j))^2$ par transposition.

On a $\det(\sigma_i(x_j)) \neq 0$ comme conséquence du lemme de Dedekind (ou Artin), appliqué aux restrictions à $L^\times$, énoncé comme suit : si G est un groupe et F un corps, $\chi_1,...,\chi_n \in \mathrm{Hom}(G, F^\times$ deux à deux distincts, alors $\chi_1,...,\chi_n \in F^G$ est F-libre, qui donne qu'ils sont linéairement indépendants : si ce déterminant était nul, on aurait $(\lambda_i) \in \overline{L}^n$ telle que $\sum \lambda_i \sigma_i(x_i) = 0$ pour tout j et donc $\sum \lambda_i \sigma_i(x) = 0$ pour tout $x \in L$.

La fin s'ensuit. ■

Application. ***(Discriminants fondamentaux)***

Soit K un corps quadratique : $K = \mathbb{Q}(\sqrt{d})$ avec $d \neq 0,1$ sans facteur carré. On peut calculer (laissé en exercice) D_K le discriminant de K.
Pour résumer, on a :

- si $d \equiv 2,3\ [4]$, $D_K = 4d$.
- si $d \equiv 1\ [4]$, $D_K = d$.

Tout entier de cette forme est appelé *discriminant fondamental*, *i.e.* les $N = 4q + 1$, $8 + 16q'$ ou $12 + 16q''$ pour q,q',q'' parcourant $\mathbb{Z}$.

En dimension finie, l'application linéaire :

$$\begin{aligned} L &\longrightarrow L^\star = \mathrm{Hom}_{K\text{-Vect}}(L/K) \\ x &\longmapsto y \mapsto \mathrm{Tr}_{L/K}(xy) \end{aligned}$$

est donc bijective, et si (x_i) est une K-base de L, alors il existe une base duale = base du dual (y_i) de L telle que $\mathrm{Tr}_{L/K}(y_i x_j) = \delta_{ij}$.

Nous pouvons maintenant démontrer le théorème suivant :

Théorème. ***(Structure de la fermeture intégrale)***

Soit A un anneau intégralement clos et $K = Frac(A)$ de caractéristique nulle ; soit L/K une extension finie de degré n. Soit A' la fermeture intégrale de A dans L. Alors A' est un sous-A-module d'un A-module libre de rang n.

On aura besoin du lemme suivant :

Lemme. ***(Construction d'une base d'entiers algébriques)***

Il existe une base de L/K formée d'éléments de A'. De plus, cette base a le même cardinal (ouf !) et chaque vecteur est un à un proportionnel aux précédents, en préservant même leur ordre.

▷ En effet, soit (x_i) une base quelconque de L/K. Alors les x_i sont algébriques sur K, donc il existe $m \leqslant n$ et $a'_0,...,a'_{m-1} \in K$ tels que $x_i^m + a'_{m-1}x_i^{m-1} + ... + a'_1 x_i + a'_0 = 0$. Je peux chasser les dénominateurs, comme d'habitude et l'on obtient que $a_m x_i \in A'$ et je peux remplacer x_i par $a_m x_i$. ■

On peut donc démontrer le théorème :

Preuve.

▷ Soit donc (x_i) une K-base de L formée d'éléments de A'. Soit (y_i) la base duale telle que $\mathrm{Tr}_{L/K}(x_i y_j) = \delta_{i,j}$. Soit $\alpha \in A'$ avec α entier sur A. Alors par une propriété du cours, $K \ni \mathrm{Tr}_{L/K}(x_i\alpha)$ est dans A, car A est intégralement clos. Ainsi $\alpha = \sum \beta_i y_i$ où $\beta_i = \mathrm{Tr}_{L/K}(x_i\alpha) \in A$ par un simple

calcul d'algèbre linéaire. Par suite, $A' \subseteq \bigoplus_{i=1}^{n} Ay_i$, d'où le théorème. ■

Corollaire. ***(Structure de la fermeture intégrale dans le cas principal)***

Supposons de plus A principal. Alors A' est un A-module libre de rang n.

▷ Avec les notations de la preuve du théorème,

$$\sum_{i=1}^{n} Ax_i \subseteq A' \subseteq \sum_{i=1}^{n} Ay_i$$

Par la théorie des modules sur un anneau principal, A' est un A-module libre de rang $\leqslant n$ et $\geqslant n$, donc de rang n. ■

Attention, sur un anneau principal, la théorie de la dimension ne stipule PAS que si M' est un sous-module de M de même rang fini, $M = M'$.

Exemple. ***(Structure des anneaux d'entiers de corps de nombres)***

Si $A = \mathbb{Z}$ et $K/\mathbb{Q}$ est un corps de nombre, A_K est un $\mathbb{Z}$-module libre de rang $n = \dim_{\mathbb{Q}}(K)$, donc $A_K \simeq \mathbb{Z}^n$ par un isomorphisme de $\mathbb{Z}$-modules. *(Rappel : on l'a vérifié explicitement dans le cas* $[K : \mathbb{Q}] = 2$*.)*

Remarque. Le fait que $\mathbb{Z}$ est principal ne se généralise pas aux anneaux d'entiers, en témoigne la proposition suivante : si d est sans facteur carré, $d \equiv 1{,}2 \ [4]$, $d > 2$, il résulte de la proposition que $\mathbb{Z}[i\sqrt{d}]$ est un anneau d'entiers non factoriel et donc non principal.

Proposition. ***(Factorialité des anneaux*** $\mathbb{Z}[i\sqrt{d}]$***)***

Soit $d > 0$. L'anneau $\mathbb{Z}[i\sqrt{d}]$ est factoriel si et seulement si $d = 1$ ou $d = 2$.

▷ Il est bien connu que si $d = 1$ ou $d = 2$, l'anneau est euclidien donc factoriel.

Soit $d > 2$. $K = \mathbb{Q}(i\sqrt{d})$ est une extension quadratique de $\mathbb{Q}$ donc si $A = \mathbb{Z}[i\sqrt{d}]$, $A/\mathbb{Z}$ est entier. Soit $x \in A$. On observe que $x \in A^\times$ si et seulement si $N_{K/\mathbb{Q}}(x) = \pm 1$. En effet, si c'est le cas, il existe $y \in A$ tel que $xy = 1$ d'où $N(xy) = N(x)N(y) = 1$ où $N(x), N(y) \in \mathbb{Z}$ d'où le résultat ; réciproquement, si $N(x) = \pm 1 = x\sigma(x)$, alors $\sigma(a + bi\sqrt{d}) = a - bi\sqrt{d}$ où $a,b \in \mathbb{Q}$ et $\sigma(A) \subseteq A$, d'où $\pm\sigma(x) \in A$ racine de x. On remarque que si $u = a + bi\sqrt{d})$, $N(u) = a^2 + b^2 d \geqslant 0$.

Vérifions que 2 est irréductible dans A. Si $2 = uv$ avec $u,v \in A$, alors $4 = N(2) = N(u)N(v)$, d'où $N(u) = 1{,}2$ ou 4. Or si $N(u) = 1$ ou 4, $u \in A^\times$ ou $v \in A^\times$. Donc $N(u) = 2 = a^2 + db^2$ où $d > 2$ d'où $b = 0$ et $2 = a^2$, impossible.

2 divise $d(d+1) = (d+i\sqrt{d})(d-i\sqrt{d}))$ dans $\mathbb{Z}$ et donc dans A. Donc si A est factoriel, $2 \mid_A (d+i\sqrt{d})$ ou $2 \mid_A (d - i\sqrt{d})$ donc il existe $a,b \in \mathbb{Z}$ tels que $2a + 2bi\sqrt{d} = d \pm i\sqrt{d}$, impossible ; donc 2 est

irréductible non premier, donc A n'est pas factoriel. ■

Remarque. Si d est sans facteur carré et $d \equiv 3\ [4]$, alors on a vu que $\mathbb{Z}[i\sqrt{d}]$ n'est pas factoriel, car il n'est pas intégralement clos : $i\sqrt{d} = \sqrt{-d}$ et $-d \equiv 1\ [4]$.

On raffine le théorème de structure précédent en donnant explicitement un module de rang n dans lequel la fermeture est inclus. On l'appelle le *module dual* de $A[x]$ pour x primitif, défini dans la proposition suivante.

Proposition. ***(Structure de la fermeture intégrale, bis repetita)***

Soit A un anneau intégralement clos et $K = Frac(A)$, avec $\text{car}(A) = 0$. On suppose qu'une extension L/K est finie, de degré n. Soit B la fermeture intégrale de A dans L. En pratique, $L = K(x)$ pour un $x \in B$ *(voir la remarque ci-dessous sur le polynôme caractéristique)* et il existe un sous-anneau $C = A[x]$ de B contenant A et qui est un A-module libre de rang n de base $1,x,...,x^{n-1}$ par le TEP. Soit f le polynôme caractéristique de x pour L/K, $f \in A[X]$ car A est intégralement clos.
On note le *module dual de* C, $\check{C} = \{y \in L \mid \text{Tr}_{L/K}(yz) \in A \qquad \forall z \in C\}$ et on lit : « C tchèque », l'ensemble des éléments de l'extension dont toutes les traces des dilatations par des élément de $A[x]$ retombent dans $A \subseteq K$.
Alors $B \subseteq \check{C}$ et $\check{C}$ est le A-module libre de rang n de base $\left(\frac{x^i}{f'(x)}\right)_{0 \leqslant i \leqslant n-1}$ en notant f' le polynôme dérivé de f.

Remarque. Vu que $(1,...,x^{n-1})$ est A-libre, elle est K-libre en chassant les dénominateurs, donc f est le polynôme minimal de x sur K. Il est irréductible, donc à racines simples, car $K = 0$. Ainsi $f(x) = 0$ donc $f'(x) \neq 0$, et donc l'écriture précédente est licite.

Preuve.

▷ Le premier point est clair. Sinon, $f(T) = \prod_{i=1}^{n}(T - x_i)$ où x_i a ses racines dans $\overline{L}$. On peut décomposer en éléments simples : $\frac{1}{f(T)} = \sum_{i=1}^{n} \frac{1}{f'(x_j)} \frac{1}{T - x_i}$. On peut alors développer en séries de Laurent formelles : $\frac{1}{T - x_i} = \frac{1}{T} \cdot \frac{1}{1 - \frac{x_i}{T}} = \frac{1}{T} \sum_{k=0}^{\infty} \left(\frac{x_i}{T}\right)^k$. Ainsi, $\frac{1}{f(T)} = \sum_{i=1}^{n} \frac{1}{f'(x_i)} \sum_{k=0}^{\infty} \frac{x_i^k}{T^{k+1}} = \sum_{k=0}^{\infty} \left[\sum_{i=1}^{n} \frac{x_i^k}{f'(x_i)}\right] \frac{1}{T^{k+1}}$ et $\sum_{i=1}^{n} \frac{x_i^k}{f'(x_i)} = \sum_{i=1}^{n} \sigma_i \left(\frac{x_i^k}{f'(x_i)}\right) = \text{Tr}_{L/K}\left(\frac{x^k}{f'(x)}\right)$ où $L = K(x)$, $\text{Hom}_K(L,\overline{L}) = \{\sigma_1,...,\sigma_n\} \simeq \{x_1,...,x_n\}$ et $\sigma_i(x) = x_i$.

Ainsi $f(T) = T^n + a_{n-1}T^{n-1} + ... + a_0 = T^n(1 + \frac{a_{n-1}}{T} + \frac{a_{n-2}}{T^2} + ... + \frac{a_0}{T^n})$ où $1 + \frac{a_{n-1}}{T} + \frac{a_{n-2}}{T^2} + ... + \frac{a_0}{T^n} \in K[\frac{1}{T}] \subseteq K[[\frac{1}{T}]]$ l'anneau des séries formelles. Ainsi $\frac{1}{f(T)} \in \frac{1}{T^n}K[[\frac{1}{T}]]$. Plus précisément, $\frac{1}{f(T)} = \frac{1}{T^n} + \frac{b_0}{T^{n+1}} + ...$ une série formelle $b_0 + \frac{b_1}{T} + \frac{b_2}{T^2} + ...$ avec $b_0 \neq 0$ donc dans $K[[\frac{1}{T}]]^\times$, d'inverse $c_0 + \frac{c_1}{T} + ...$ et $c_0 b_0 = 1$. De cela, on extrait $\text{Tr}_{L/K}(\frac{x^k}{f'(x)}) = 0$ si $k + 1 < n, 0 \leqslant k \leqslant n - 2$ et 1 si $k = n - 1$.

On pose $M = (\mathrm{Tr}_{L/K}(\frac{x^i x^j}{f'(x)}))_{0\leqslant i,j\leqslant n-1}$. Ses coefficients sont nuls si $i+j < n-2$, et les coefficients sur l'antidiagonale sont 1. De plus, $M \in \mathfrak{M}_n(A)$. En effet, on a $x^m = \sum_{i=0}^{n-1} \alpha_i x^i$, les $\alpha_i \in A$, donc $x^m \in C = \bigoplus_{i=0}^{n-1} Ax^i$ d'où $\mathrm{Tr}_{L/K}\left(\frac{x^m}{f'(x)}\right) = \sum_{i=0}^{n-1} \alpha_i \mathrm{Tr}_{L/K}\left(\frac{x^i}{f'(x)}\right)$ où $\alpha_i \in A$ et $\mathrm{Tr}_{L/K}(\frac{x^i}{f'(x)}) = 0$ ou 1. La matrice M de taille n (numérotée de 0 à $n-1$) s'écrit sous la forme $\begin{pmatrix} 0 & \cdots & 1 \\ \vdots & 1 & \\ 1 & & * \end{pmatrix}$. On peut donc calculer le déterminant antidiagonal : $\det(M) = (-1)^{n-1} \times (-1)^n \times \ldots \times (-1) = (-1)^{\frac{n(n-1)}{2}}$. Donc $M \in GL_n(A)$. Ainsi, il existe $N \in \mathfrak{M}_n(A)$ telle que $MN = I_n$. En notant $N = (n_{i,j})$, $\delta_{i,k} = \sum_{j=1}^{n} \mathrm{Tr}_{L/K}\left(\frac{x^i x^j}{f'(x)}\right) n_{j,k} = \mathrm{Tr}_{L,K}\left(x^i \sum_{j=1}^{n} \frac{x^j}{n_{j,k}}\right)$ donc $\left(\sum_{j=1}^{n} \frac{n_{j,k} x^j}{f'(x)}\right)_k$ base duale de (x^i) forme une A-base de $\check{C}$, donc comme $N \in GL_n(A)$, $(\frac{x^d}{f'(x)})_j$ forment une A-base de $\check{C}$. ■

Corollaire. ***(Cardinal du module co-dual)***

Soit $A = \mathbb{Z}$, $K = \mathbb{Q}$. Le $\mathbb{Z}$-module $\check{C}/C$ est fini, de cardinal $|N_{L/\mathbb{Q}}(f'(x))|$.

▷ On note toujours m_a la multiplication par a. On a : $\check{C} = \bigoplus_{i=0}^{n-1} \mathbb{Z}\frac{x^i}{f'(x)}$ et $C = \bigoplus_{i=0}^{n-1} \mathbb{Z}x^i$. On considère l'application $\check{C} \xrightarrow[m_{f'(x)}]{} \check{C}$. Alors $\check{C}/C = \check{C}/\mathrm{Im}(m_{f'(x)})$. Alors comme $m_{f'(x)}$ est injective, car L est un corps, $\check{C}/\mathrm{Im}(m_{f'(x)})$ est fini de cardinal $|\det(m_{f'(x)})| = |N_{L/\mathbb{Q}}(f'(x))|$ (cette dernière égalité étant définitionnelle). ■

On a utilisé le lemme calculant le cardinal d'un conoyau qui constitue un exercice classique de théorie des modules principaux et que l'on rappellera plus tard dans ce cours, sous-section Norme d'un idéal.

Méthode. ***(Algorithme de calcul de la fermeture intégrale)***

Ce théorème donne un moyen algorithmique de trouver l'anneau B pour un corps de nombres $L/\mathbb{Q}$: on trouve x entier tel que $L = \mathbb{Q}(x)$ (comme on peut). Alors $C = \bigoplus_{i=0}^{n-1} \mathbb{Z}x^i \subseteq B \subseteq \bigoplus_{i=0}^{n-1} \mathbb{Z}\frac{x^i}{f'(x)} = \check{C}$. On considère alors un ensemble fini de représentants $\{y\}$ de $\check{C}/C$. Pour chaque y, on calcule le polynôme caractéristique $\chi_{y,\mathbb{Q}}$ et on regarde si $\chi_{y,\mathbb{Q}} \in \mathbb{Z}[X]$, c'est-à-dire si $y \in B$. On obtient donc $y_1,\ldots,y_r$ par ce procédé avec $r \leqslant |N_{L/\mathbb{Q}}(f'(x))|$. Une fois ceci fait, soit disons $t \in B$. Alors $t \in \check{C}$, donc $t = y_i + c$ où $c \in C$ et $i \in [\![1,r]\!]$. Ainsi, B est le module engendré par $\{x^i, y_j, i \in [\![0,n-1]\!], j \in [\![1,r]\!]\}$.

Corollaire. ***(Calcul pratique du discriminant monogène)***

Sous les hypothèses de la proposition,

$$D_{L/K}(1,x,...,x^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(x))$$

En particulier, si K est un corps de nombres, α un entier algébrique et f le polynôme minimal de α, alors le discriminant (absolu) de $\mathbb{Z}[\alpha]/\mathbb{Z}$ est égal à $(-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(x))$.

▷ $(\mathrm{Tr}_{L/K}(x^i x^j))_{0\leqslant i,j\leqslant n-1}$ est la matrice de présentation des (x^j) dans la base duale des (x^j), soit par changement de base de déterminant $(-1)^{\frac{n(n-1)}{2}}$, la base de $(\frac{x^i}{f'(x)})$. Ainsi par le calcul de la preuve précédente, $D_{L/K}(1,...,x^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \det(\mathrm{Mat}(1,...,x^{n-1})) = \det(\frac{x^i}{f'(x)})$. Or cette matrice est $\mathrm{Mat}(m_{f'(x)})$ dont le déterminant vaut $N_{L/K}(f'(x))$. ■

Notons :

Preuve.

▷ *(Une technique directe)* En utilisant $\mathrm{Tr}_{L/K}(x) = \sum_{\sigma\in \mathrm{Hom}_K(L,\overline{L}) \simeq \{\text{ racines de } f\ \}} \sigma(x)$ et un déterminant de Vandermonde, on peut retrouver directement ce résultat : $f(X) = \prod_{i=1}^{n}(X - x_i)$ (f est ici irréductible sur K donc les x_i sont deux à deux distincts, car $\mathrm{car}(K) = 0$), où $x_1 = x$ qui donne comme on sait $f'(x) = \prod_{i=2}^{n}(x - x_i)$ et $f'(x_i) = \prod_{j\neq i}(x_i - x_j)$ plus généralement. D'où $N_{L/K}(f'(x)) = \prod_{\sigma_i\in \mathrm{Hom}_K(L,\overline{L})} \sigma_i(f'(x)) = \prod_{i\neq j}(x_i - x_j)$, car $\sigma_i(f'(x)) = f'(x_i)$ avec $x_i = \sigma_i(x)$. ■

Définition. ***(Discriminant absolu d'un corps de nombres)***

Soit K un corps de nombres de degré n. Soit A l'anneau des entiers de K qui est un $\mathbb{Z}$-module libre de rang n. Les discriminants des $\mathbb{Z}$-bases de A diffèrent par le carré d'un inversible de $\mathbb{Z}$, autrement dit, elles sont toutes égales. La quantité $D_{L/\mathbb{Q}}(e_1,...,e_n)$ est donc indépendante du choix de la $\mathbb{Z}$-base (e_i) de A ; on l'appelle le *discriminant absolu*.

Remarque. (Lien avec le discriminant polynomial) Sous les conditions de la proposition, on a vu que $N_{L/K}(f'(x)) = \prod_{i\neq j}(x_i - x_j)$ est le discriminant du polynôme f (résultant du polynôme f et du polynôme dérivé) où $f = \prod_{i=1}^{n}(X - x_i)$ avec f irréductible sur K de degré n.

Exemple. ***(Calcul du discriminant d'un polynôme réduit)***

Calculons le discriminant pour f irréductible sur K, a,$b \in K$, $b \neq 0$, $f(X) = X^n + aX + b$ (ce que nous appelons *polynôme réduit*), $L = K(x)$ et $f(x) = 0$. On veut calculer le discriminant de f, donc calculer $N_{L/K}(f'(x))$. C'est le terme constant du polynôme minimal de $y = f'(x)$. On a les équations

$$x^n + ax + b = 0 \qquad (I)$$
$$\text{et } y = f'(x) = nx^{n-1} + a \qquad (II)$$

d'où l'on déduit en tapant bien dessus : $x = -\frac{nb}{y+(n-1)a}$. Or f est le polynôme minimal de x, donc f est le polynôme minimal de $-\frac{nb}{y+(n-1)a}$. Ainsi $(-\frac{nb}{y+(n-1)a})^n - -\frac{anb}{y+(n-1)a} + b = 0$. En réduisant au même dénominateur, le numérateur est le polynôme minimal de y, à savoir $(Y + (n-1)a)^n - na(Y + (n-1)a)^{n-1} + (-1)^n n^n b^{n-1}$. Le terme constant s'écrit donc $\underbrace{((n-1)a)^n - na((n-1)a)^{n-1}}_{-a((n-1)a)^{n-1}} + (-1)^n n^n b^{n-1}$. Ainsi,

$$\boxed{N_{L/K}(f'(x)) = N_{L/K}(y) = n^n b^{n-1} - (-1)^n((n-1)a)^{n-1}a}.$$

En application, on obtient :

- dans le cas $n = 2$, $4b - a^2$ (ouf !) ;
- dans le cas $n = 3$, $27b^2 + 4a^3$ (que de choses connues) ;
- etc. (et oui !)

C'est bien égal au discriminant de f au sens de $\mathrm{Res}(f,f')$. On a aussi une formule en passant pour $D(1,...,x^{n-1})$ en passant.

Proposition. ***(Discriminant d'une tour de corps de nombres)***

Soient $\mathbb{Q} \subseteq K \subseteq L$ des corps de nombres. Alors on a la formule :

$$\mathrm{Disc}(\mathcal{O}_L/\mathbb{Z}) = N_{K/\mathbb{Q}}(\mathrm{Disc}(\mathcal{O}_L/\mathcal{O}_K))\mathrm{Disc}(\mathcal{O}_K/\mathbb{Z})^{[L:K]}.$$

▷ Démonstration difficile. Elle repose sur la relation de transitivité des différentes et leur lien avec le discriminant. ■

Proposition. ***(Discriminant d'un compositum de corps de nombres)***

Soient deux corps de nombres K_1,K_2 **linéairement disjoints**, *i.e.* $[K_1K_2 : \mathbb{Q}] = [K_2 : \mathbb{Q}]$, et dont les discriminants absolus $\mathrm{Disc}(\mathcal{O}_{K_1}/\mathbb{Z})$, $\mathrm{Disc}(\mathcal{O}_{K_1}/\mathbb{Z})$ sont premiers entre eux. Alors $\mathcal{O}_{K_1K_2} = \mathcal{O}_{K_1}\mathcal{O}_{K_2}$ et :

$$\mathrm{Disc}(\mathcal{O}_{K_1K_2}/\mathbb{Z}) = \mathrm{Disc}(\mathcal{O}_{K_1}/\mathbb{Z})^{[K_2:\mathbb{Q}]}\mathrm{Disc}(\mathcal{O}_{K_1}/\mathbb{Z})^{[K_1:\mathbb{Q}]}.$$

4.2.1.8 Cas des corps cyclotomiques

Soit $n \in \mathbb{N}^*$, et ζ une racine primitive n-ième de 1. Soit ϕ_n le polynôme minimal annulateur de ζ ; alors $\mathbb{Q}(\zeta)/\mathbb{Q}$ est une extension de degré $\varphi(n)$. On admet donc l'irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$; notons qu'elle est plus simple à établir dans le cas où $n = p^r$ avec p premier, avec le critère d'Eisenstein.

Proposition. ***(Anneau des entiers des corps cyclotomiques)***

L'anneau des entiers de $\mathbb{Q}(\zeta)$ est $\mathbb{Z}[\zeta]$.
C'est le $\mathbb{Z}$-module libre engendré par 1,...,$z^{\varphi(n)-1}$, qui est de rang $\varphi(n)$.

▷ On commmence la preuve par le cas $n = p^r$, p premier. On sait que cet anneau A est un $\mathbb{Z}$-module de rang $\varphi(n)$. ζ est annulé par $\phi_n \in \mathbb{Z}[X]$ (ou encore $X^n - 1$) donc $\zeta \in A$, d'où $\mathbb{Z}[\zeta] \subseteq A$. Posons $x = 1 - \zeta$. Alors $\phi_n(1 + X)$ est le polynôme minimal de $-x$ sur $\mathbb{Q}$. On voit que $\phi_n(1) = p$. Donc $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(-x) = (-1)^{\varphi(n)}p$, donc $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(x) = p$. De même, si on regarde ζ^i avec $\zeta^i \neq 1$, *i.e.* p^r ne divise pas i : $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta^i) = N_{\mathbb{Q}(\zeta^i)/\mathbb{Q}}(N_{\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta^i)}(1-\zeta^i)) = [N_{\mathbb{Q}(\zeta^i)/\mathbb{Q}}(1-\zeta^i)]^{[\mathbb{Q}(\zeta):\mathbb{Q}(z^i)]} = p^{[\mathbb{Q}(\zeta):\mathbb{Q}(\zeta^i)]}$. En raisonnant sur $\mathbb{Q}(\zeta^i)$,

$$|D_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1,\zeta,...,\zeta^{\varphi(n)-1}| = |N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\phi_n'(\zeta))| = \prod_{\zeta'\neq\zeta,\zeta'\in\mu_n} |N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta-\zeta')|)$$
$$= \prod_{\zeta'\neq\zeta} |N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta')| \prod_{\zeta'\neq\zeta} N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta\zeta'^{-1}-1)$$

qui est une puissance de p, car $\zeta\zeta'^{-1} \neq 1$. Or $\zeta' \in A^\times$ donc $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta') \in \mathbb{Z}^\times = \{\pm 1\}$, donc ce discriminant égale $p^\star$ avec $\star \geqslant 1$. J'en déduis d'après un corollaire pour $C = \mathbb{Z}[\zeta]$, $A/C \hookrightarrow \check{C}/C$ avec $C \subseteq A \subseteq \check{C}$. On a vu que $|\check{C}/C| = |D(1,...,\zeta^{\varphi(n)-1}| = p^\star$, donc $A/\mathbb{Z}[\zeta]$ est fini d'ordre p^N et $p^N A \subseteq \mathbb{Z}[\zeta] \subseteq A$. Or $x = 1 - \zeta \in A$. Le morphisme $\psi : \mathbb{Z} \longrightarrow A/Ax$ qui à $1 \mapsto \overline{1}$ est d'anneaux ; son noyau est un idéal de $\mathbb{Z}$, propre, car sinon $\overline{1} \in Ax$ d'où $x \in A^\times$, d'où $p = N(x) = \pm 1$, impossible. Or $p = N(x) \in xA$, donc $p \in \mathrm{Ker}(\psi)$, d'où $p\mathbb{Z} \subseteq \mathrm{Ker}(\psi)$, donc $\mathrm{Ker}(\psi) = p\mathbb{Z}$, donc $\mathbb{Z}/p\mathbb{Z} \hookrightarrow A/Ax$. Or $|A/Ax| = |\det(m_x)|$ et A est un $\mathbb{Z}$-module libre de rang $\varphi(n)$, donc A/Ax est de cardinal $p = |N(x)|$. En fait donc $\mathbb{Z}/p\mathbb{Z} \simeq A/Ax$, d'où $A = \mathbb{Z} + Ax = \mathbb{Z}[\zeta] + Ax$. Par récurrence, $A = \mathbb{Z}[\zeta] + Ax^i$ pour tout $i \geqslant 1$. On rappelle que $Ap^N \subseteq \mathbb{Z}[\zeta]$ et $p = N(x) = N(1-\zeta) = \prod_{\zeta'\in\mu_n} 1 - \zeta' = x^{\varphi(n)} \prod_{\zeta'\in\mu_n} \frac{1-\zeta'}{1-\zeta}$. Or $N\left(\frac{1-\zeta'}{1-\zeta}\right) = \frac{N(1-\zeta)'}{N(1-\zeta)} = \frac{p}{p} = 1 \in \mathbb{Z}^\times$. Or $\zeta' = \zeta^i$, donc $\frac{1-\zeta'}{1-\zeta} \in \mathbb{Z}[\zeta]$ et $N(...) \in \mathbb{Z}^\times$ d'où $\frac{1-\zeta'}{1-\zeta} \in A^\times$, donc $x^{\varphi(n)} \in pA$ d'où $(x^{\varphi(n)})^N \in p^N A$ puis $A = \mathbb{Z}[\zeta] + Ax^{\varphi(n)N} \subseteq \mathbb{Z}[\zeta] + p^N A \subseteq \mathbb{Z}[\zeta]$, d'où $A = \mathbb{Z}[\zeta]$.

Pour le cas général, on écrit $n = p_1^{r_1}...p_s^{r_s}$, et l'on note $K_n = \mathbb{Q}(e^{\frac{2\pi i}{m}})$. Alors K_n s'écrit comme compositum des corps $K_{p_i^{r_i}}$ et l'on peut conclure avec la formule donnée plus haut. ■

Exercice 11

Calculer de même la trace de x : $\mathrm{Tr}(x) = \varphi(n) = p^r - p^{r-1}$.

4.2.2 Anneaux noethériens en arithmétique et anneaux de Dedekind

4.2.2.1 Rappels sur les modules et anneaux noethériens

On renvoie au cours d'Algèbre linéaire sur les Modules. Mentionnons en particulier :

Propriété. ***(Anneau noethérien, intégralement clos sans spectre premier)***

Soit A un anneau noethérien, intégralement clos et possédant un unique idéal premier non nul $\mathfrak{m}$. Alors A est principal.

4.2.2.2 Application de la noethérianité aux anneaux d'entiers

Proposition. ***(Noethérianité des anneaux d'entiers)***

Soit A un anneau noethérien intégralement clos et $K = Frac(A)$, $\text{car}(K) = 0$. Soit une extension L/K de degré $n \geqslant 1$ fini. Soit A' la clôture intégrale de A dans L. Alors A' est un A-module de type fini et un anneau noethérien.

▷ On a vu que A' est un sous-A-module d'un A-module libre M de type fini, donc M est noethérien, car A est noethérien. Donc A' est de type fini. Montrons que A' est un anneau noethérien. Soit $I \subseteq A'$ un idéal. A fortiori, c'est un sous-A-module de A' donc de type fini, car A' est un A-module de type fini sur A noethérien, donc noethérien comme A-module. Ainsi I est un A-module de type fini, donc A' est un module de type fini. Donc A' est noethérien. ■

Exemple

L'anneau des entiers d'un corps de nombres est noethérien (pour $A = \mathbb{Z}, \mathbb{Q}$), comme on l'avait annoncé.

4.2.2.3 Préliminaires sur les idéaux premiers

On renvoie également au cours d'Algèbre générale sur les Idéaux premiers, maximaux.

Propriété. ***(Idéaux premiers de $\mathbb{Z}$)***

Dans $\mathbb{Z}$, les idéaux premiers sont les (0) et (p) pour p un nombre premier.

▷ Simple. ■

Propriété. ***(Idéaux premiers de $\mathbb{Z}[X]$)***

Dans $\mathbb{Z}[X]$, les idéaux premiers sont (0), (p) pour p un nombre premier, (f) pour $f \in \mathbb{Z}[X]$ irréductible, et les (p,f).

▷ Beaucoup plus compliqué. ■

4.2.2.4 Idéaux fractionnaires

On suppose A intègre. Soit K son corps des fractions.

Définition. ***(Idéal fractionnaire)***

Un *idéal fractionnaire* de A est un sous-A-module M de K tel qu'il existe $d \in A, d \neq 0$ tel que $dM \subseteq A$ (ou encore $M \subseteq \frac{1}{d}A$).
Intuitivement, les éléments de M sont certes des fractions, mais on un dénominateur commun.

Remarques.

1. Immédiatement, tout idéal de A est un idéal fractionnaire, pour $d = 1$. On parle parfois d'*idéaux entiers* pour les distinguer des « vrais » idéaux fractionnaires. Inversement, si l'on peut prendre $d \in A^\times$ dans la définition ci-haut, alors l'idéal fractionnaire M est un idéal de A.
2. Tout sous-A-module de type fini de K est un idéal fractionnaire. En effet, il suffit de prendre le produit, par exemple, des dénominateurs d'un système de générateurs. (Attention, le ppcm n'existe pas toujours.)
   En particulier, si K est un A-module noethérien, tout sous-module de K est un idéal fractionnaire de A. On voit une réciproque juste après.
3. On définit sans problème les opérations usuelles sur les idéaux (intersection, somme, produit) dans le cas fractionnaire. On vérifie alors que le résultat reste fractionnaire, ce qui est facile à voir.

Propriété. ***(Idéaux fractionnaires d'un anneau noethérien)***

Si A est noethérien, tout idéal fractionnaire de A est de type fini.

▷ Sous entendu, en tant que A-module (mais c'est la même chose de toute manière). Soit M un idéal fractionnaire de A. Soit d non nul tel que $dM \subseteq A$. Comme A est noethérien, dM idéal de A est de type fini, donc $dM = \sum Ax_i$ puis $M = \sum Ad^{-1}x_i$ qui est donc de type fini. ■

4.2.2.5 Lien avec les anneaux de valuation discrète

On a facilement :

Propriété. ***(Localiser en un anneau de valuation discrète)***

Soit A un anneau noethérien et intégralement clos. Soit $\mathfrak{p}$ un idéal premier minimal et maximal non nul. Alors $A_{(p)}$ est un anneau de valuation discrète, d'idéal maximal $\mathfrak{p}A_{(\mathfrak{p})}$.

VOC On note toujours $v_{\mathfrak{p}}$ la valuation sur ce nouvel anneau.

Fait

Tout idéal fractionnaire de $A_{(p)}$ est de la forme $p^n A_{(p)}$ avec $n \in \mathbb{Z}$.

On utilisera ce qui suit :

Lemme

Si A est intégralement clos, $A_{(p)}$ est intégralement clos.

▷ Soit $x \in K$ tel que $x^n + \frac{a_{n-1}}{b}x^{n-1} + ... + \frac{a_n}{b} = 0$ avec $a_0,...,a_{k-1} \in A$, $b \ni A \setminus \mathfrak{p}$. Alors bx est entier sur A car $(bx)^n + a_{n-1}(bx)^{n-1} + ... + b^{n-1}a_0 = 0$. Donc $bx \in A$. Donc $x \in A_{(p)}$. ■

4.2.2.6 Anneaux de Dedekind

Définition. ***(Anneau de Dedekind)***

Un *anneau de Dedekind* est un anneau intègre, intégralement clos, noethérien et tel que tout idéal premier non nul est maximal.

Dans un anneau intègre, tout élément premier est irréductible. Ceci ne suffit pas à montrer que tout idéal premier est maximal, car tous les idéaux premiers, maximaux ne sont pas principaux, bien qu'en toute généralité, un élément est premier si et seulement s'il engendre un idéal premier (en outre, un élément est irréductible si et seulement s'il engendre un idéal maximal *parmi les idéaux principaux propres*).

Exemples. ***(Anneaux de Dedekind)***

1. Tout corps est un anneau de Dedekind.
2. $\mathbb{Z}$ est principal, donc intégralement clos et noethérien. Les idéaux premiers de $\mathbb{Z}$ sont les $p\mathbb{Z}$ pour p premier ou nul. Si $p \neq 0$, $p\mathbb{Z}$ est maximal.
   Plus généralement, tout anneau principal est de Dedekind.
3. *(Dedekind-ité des anneaux d'entiers de corps de nombres)* Nous allons voir que les anneaux d'entiers des corps de nombres sont des anneaux de Dedekind. Il suffit en effet de prendre $A = \mathbb{Z}$, $K = \mathbb{Q}$, $L/\mathbb{Q}$ un corps de nombres dans le théorème qui suit ; dans ce cas, A_L la fermeture intégrale de $\mathbb{Z}$ dans L est de Dedekind.
   En particulier, il existe des anneaux factoriels qui ne sont pas des anneaux de

Dedekind.

4. $\mathbb{R}[X,Y]$ n'est pas de Dedekind.

Théorème. ***(Fermeture intégrale des anneaux de Dedekind)***

Soit A un anneau de Dedekind et K son corps des factions que l'on suppose de caractéristique nulle. Soit L/K une extension finie. Soit A' la fermeture intégrale de A dans L. Alors A' est un anneau de Dedekind.
En particulier (c'est le cas K/K), la clôture intégrale d'un anneau de Dedekind est de Dedekind.

▷ Clairement, $A' \subseteq L$ est intègre et intégralement clos, car tout élément de L entier sur A' est aussi entier sur $\mathbb{Z}$ par typage fini, donc est dans A'. Il est noethérien, on l'a vu précédemment. Soit donc β' un idéal de A' premier non nul. Soit $x \in \beta'$ non nul. Comme $x \in A'$, il existe $n \geqslant 1$ et $a_{n-1},...,a_0 \in A$ tels que $x^n + a_{n-1}x^{n-1} + ... + a_0 = 0$. Je peux et je vais supposer que n est minimal. En particulier, $a_0 \neq 0$. Alors $a_0 = -x^n - a_{n-1}x^{n-1} - ... - a_1 x \in Ax \subseteq A'x \subseteq \beta'$. Ainsi $0 \neq a_0 \in \beta' \cap A$ est un idéal premier de A, non nul, donc maximal, car A est de Dedekind. Ainsi le corps $A/(\beta' \cap A) \hookrightarrow A'/\beta'$ en tant qu'anneaux. Or A'/β' est clairement entier sur $A/(\beta' \cap A)$, donc par propriété, A'/β' est un corps, donc β' est maximal. ■

Remarque. Les anneaux d'entiers des corps de nombre ne sont pas principaux ni factoriels en général. Au niveau des idéaux fractionnaires, dans un anneau de Dedekind, on récupère des énoncés de factorisation en idéaux premiers.

Exercice 12

Placer les anneaux de Dedekind sur la carte heuristique des propriétés arithmétiques des anneaux.

▷ **Éléments de réponse.**

Il suffit de colorier la case des anneaux principaux unie à la partie des anneaux noethériens qui ne sont pas factoriels.

On peut fournir les caractérisations suivantes des anneaux de Dedekind.

Théorème. ***(Caractérisation des anneaux de Dedekind)***

Soit A un anneau intègre et noethérien, K son corps des fractions. Alors les conditions :

(i) A est de Dedekind ;

(ii) pour tout idéal premier non nul $\mathfrak{p}$, $A_{(\mathfrak{p})}$ est de valuation discrète ;

(iii) tout idéal fractionnaire de K est inversible *(voir la section suivante pour la définition)* ;

sont équivalentes.

▷ $(i) \implies (ii)$: par hypothèse, $A_{(\mathfrak{p})}$ est noethérien et intégralement clos. Si $\mathscr{N}$ est un idéal premier non nul de $A_{(p)}$, $\mathscr{N} \cap A$ est un idéal premier non ul de A. Donc $\mathscr{N} \cap A \subseteq \mathfrak{m} \cap A$? idéal maximal de $A_{(p)}$. On a $\mathscr{N} = (\mathscr{N} \cap A)A_{(\mathfrak{p})} = (\mathfrak{m} \cap A)A_{(\mathfrak{p})} = \mathfrak{m}$. Par la proposition, A est un anneau de valuation discrète.

$(ii) \implies (iii)$: soit I fractionnaire. Quitte à remplcaer I par aI, on peut supposer $I \subseteq A$. Considérons $II^{-1} \subseteq A$. C'est un idéal. Si $II^{-1} \neq A$, $II^{-1} \subseteq \mathfrak{p}$ idéal premier de A. Soit $x \in II^{-1}$ tel que $v_{\mathfrak{p}}(x)$ soit minimal. Alors on a $IA_{(\mathfrak{p})} = xA_{(\mathfrak{p})}$. Soient $(a_1,...,a_n)$ des générateurs de I. On écrit $a_i = x\frac{u_i}{v_i}$ avec $u_i \in A$, $v_i \in A \setminus \mathfrak{p}$. Posons $v = \prod_i v_i \in A \setminus \mathfrak{p}$, $\mathfrak{p}$ premier. On a $v\frac{a_i}{x} \in A$, donc $\frac{v}{x} \in I^{-1}$, car $(a_1,...,a_n)$ engendre I. Donc $v \in xI^{-1} \subseteq II^{-1} \subseteq \mathfrak{p}$, absurde ; donc $\mathfrak{p}$ n'existe pas. Donc $II^{-1} = A$, donc I est inversible.

$(iii) \implies (i)$: soit $x \in K$ entier sur A. Alors $A[x]$ est de type fini sur A. On a $A[x].A[x] = A[x] = A[x](A[x].A[x]^{-1})$, car $A[x]$ est inversible, d'où $A[x].A[x] = A[x]A[x]^{-1} = A$. Donc $x \in A$. Donc A est intégralement clos. Soit $\mathfrak{p} \subseteq A$ premier non nul. Soit $\mathfrak{m}$ un idéal maximal de A, $\mathfrak{p}$ dans $\mathfrak{m}$. On a $\mathfrak{m}^{-1}\mathfrak{p} \subseteq \mathfrak{m}^{-1}\mathfrak{m} = A$. On a $(\mathfrak{m}^{-1}\mathfrak{p}\mathfrak{m}) = \mathfrak{p}$ donc $\mathfrak{p} = \mathfrak{m}$ ou $\mathfrak{p}\mathfrak{m}^{-1} \subseteq \mathfrak{p}$. Si $\mathfrak{p}\mathfrak{m}^{-1} \subseteq \mathfrak{p}$, on a $\mathfrak{m}^{-1} = \mathfrak{p}\mathfrak{p}^{-1}\mathfrak{m}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = A$, absurde ; donc $\mathfrak{p} = \mathfrak{m}$. ■

Corollaire. ***(Valuation sur un anneau de Dedekind)***

Soit A de Dedekind et $\mathfrak{p}$ premier non nul. On dispose d'une valuation $v_{\mathfrak{p}} : A_{(\mathfrak{p})} \to \mathbb{Z}$ et pour I fractionnaire, on pose $v_{\mathfrak{p}}(I) = \min\{v_{\mathfrak{p}}(x), x \in I, x \neq 0\}$.

On démontrera plus tard que :

Propriété. ***(Anneaux de Dedekind factoriels)***

Un anneau de Dedekind est factoriel si et seulement s'il est principal.

Il nous faut voir d'abord que, muni du produit d'idéaux, l'ensemble des idéaux fractionnaires non nuls d'un anneau de Dedekind est un groupe abélien.

4.2.2.7 Le groupe de classes d'idéaux

Théorème. ***(Inversion d'un idéal fractionnaire)***

Soit A un anneau de Dedekind qui n'est pas un corps. Pour tout idéal maximal m de A, il existe un idéal fractionnaire non nul m' de A tel que $m.m' = A$.

Avant de démontrer cela, on démontre la propriété suivante.

Propriété. ***(Un idéal fractionnaire particulier)***

Sous les mêmes hypothèses que le théorème, $m' = \{x \in K, xm \subseteq A\}$. Alors m' est un idéal fractionnaire de A et $A \subsetneq m'$.

▷ $m \neq (0)$, car A n'est pas un corps. Il existe $d \neq 0 \subseteq m$ et donc par définition de m', $dm' \subseteq A$. De plus $A \subseteq m'$ évidemment, car m est un idéal. Soit $a \neq 0$ dans m, alors $Aa \subseteq m$. Vu que A est un anneau noethérien intègre, il existe un produit d'idéaux premiers $\neq (0)$ inclus dans Aa, explicitement : $p_1...p_n \subseteq Aa$. Je suppose que n est minimal. On a $p_1...p_n \subseteq m$, donc m contient l'un des facteurs. Quitte à réindexer, $p_1 \subseteq m$ où p_1 est un idéal premier non nul de A anneau de Dedekind, donc maximal, donc $p_1 = m$. Posons $\beta = p_2...p_n$. Par minimalité de n, β n'est pas inclus dans aA. Il existe donc $b \in \beta$ tel que $b \notin aA$, c'est-à-dire $a^\times \notin A$. Or $\beta m \subseteq aA$, donc $bm \subseteq aA$, d'où $a^{-1}bm \subseteq A$. Donc $a^{-1}b \in m'$ et $a^{-1}b \notin A$, donc $A \subsetneq m'$. ■

On a encore besoin du lemme suivant :

Lemme. ***(Intégralité close sur les idéaux)***

Soit A un anneau noethérien intégralement clos et I un idéal de A non nul. Alors pour tout $x \in K = Frac(A)$ tel que $xI \subseteq I$, on a $x \in A$.

▷ $AI \subseteq I$ et $AxI \subseteq AI \subseteq I$, puis $Ax^2I \subseteq (Ax)(xI) \subseteq AxI \subseteq I$, puis, de fil en aiguille, $A[X].I \subseteq I$. Soit $d \in I$ non nul, alors $dA[x] \subseteq I \subseteq A$, donc $A[x]$ est un idéal fractionnaire de A, donc de type fini, car A est noethérien. Ainsi x est entier sur A, donc par hypothèse, dans A. ■

On peut revenir au théorème.

Preuve.

▷ Soit donc A un anneau de Dedekind qui n'est pas un corps. Soit $m \subseteq A$ un idéal maximal. Alors $m' = \{x \in K, xm \subseteq A\}$ est un idéal fractionnaire de A contenant A. Donc $m = Am \subseteq m'.m \subseteq A$ par définition de A. Donc $m'm$ est un sous-A-module de A, c'est-à-dire un idéal, compris en m maximal et A. On a soit $mm' = m$, soit $mm' = A$. Si $mm' = m$, pour tout $x \in m'$, $xm \in mm' = m$, donc par le lemme $x \in A$. On aurait $m' \subseteq A$, ce qui n'est pas. Donc $mm' = A$, ce qui prouve le théorème. ■

Remarques pratiques.

1. Il existe un *unique* idéal fractionnaire m' de A tel que sous les hypothèses du théorème, $mm' = A$. En effet, si $mm' = mm'' = A$, $m''mm' = m''A = m''$ mais $Am' = m''m = m'$, d'où $m' = m''$.
2. L'inversion des idéaux est croissante pour l'inclusion.

⟶ *Notation.* Dans la suite, on note donc m^{-1} l'idéal m'.

Théorème. ***(Théorème de factorisation des idéaux premiers)***

Soit A un anneau de Dedekind et $\mathcal{P}$ l'ensemble de ses idéaux premiers non nuls $\iff$ maximaux.

1. *(Théorème de décomposition des idéaux fractionnaires)* Tout idéal fractionnaire non nul de A s'écrit de façon unique sous la forme $I = \prod_{p\in\mathcal{P}} p^{v_p(I)}$ où $(v_p(I))_{p\in\mathcal{P}} \in \mathbb{Z}^{(\mathcal{P})}$. Ici, l'exponentiation note le produit itéré d'idéaux et les exposants négatifs les inverses au sens des idéaux fractionnaires. De plus, $p^0 = A$ par convention.
2. *(Structure du groupe d'idéaux)* L'ensemble des idéaux fractionnaires non nuls de A (ou encore des sous-modules de type fini de $Frac(A)$) est un groupe abélien pour le produit d'idéaux, d'élément neutre A. Ce groupe est donc de plus abélien libre, de base $\mathcal{P}$.

▷ On considère d'abord le cas des idéaux entiers. Dans ce cas, on a de plus $v_p(I) \geqslant 0$. Par hypothèse, A n'est pas un corps. Notons ϕ l'ensemble des idéaux non nuls de A qui ne sont pas produit d'idéaux maximaux. Montrons que ϕ est vide. Si ce n'était pas le cas, comme A est noethérien, il existe un idéal I non nul élément maximal de ϕ. Alors $I \neq A$ qui est le produit vide d'idéaux maximaux. Donc I est un idéal propre. Donc il est contenu dans un idéal maximal propre m, strictement, car $m \notin \phi$. Je peux considère m^{-1} l'idéal fractionnaire inverse de m. On rappelle que $A \subseteq m^{-1}$. Alors $I = IA \subseteq Im^{-1} \subseteq mm^{-1} = A$. Si $I = Im^{-1}$, pour tout $x \in m^{-1}$, $xI \subseteq I$, donc par le lemme, $x \in A$, impossible par la propriété. Donc $I \subsetneq Im^{-1}$. Donc $(0) \neq I^{m-1} \notin \phi$. Donc il existe p_1,...,p_n des idéaux maximaux tels que $Im^{-1} = p_1...p_n$. Mais alors $I = (Im^{-1})m = p_1...p_nm$ et donc $I \notin \phi$, contradiction.

Montrons l'existence en général. Soit I un idéal fractionnaire non nul. Il existe d non nul tel que $dI \subseteq A$. dI est un idéal entier donc se décompose en $dI = \prod_{p\in\mathcal{P}} p^{v_p(dI)}$. De plus, $dA = \prod_{p\in\mathcal{P}} p^{v_p(dA)}$ avec $v_p(dI), v_p(dA) \geqslant 0$. Ainsi, $\prod_{p\in\mathcal{P}} p^{v_p(dI)-v_p(dA)} = (dI)\prod_{p\in\mathcal{P}} p^{-v_p(dA)} = I(dA)\prod_{p\in\mathcal{P}} p^{-v_p(dA)} = I.\prod_{p\in\mathcal{P}} p^{v_p(dA)-v_p(dA)} = I.A = I$.

Montrons l'unicité de la décomposition. La preuve est la même que dans $\mathbb{Z}$. Supposons $\prod p^{v_p} = \prod p^{w_p}$, avec $(v_p), (w_p) \in \mathbb{Z}^{(\mathcal{P})}$. On a donc $\prod p^{v_p - w_p} = A$, montrons que $v_p = w_p$ pour tout p. On est ramené à prouvé que si $\prod p^{v_p} = A$ alors $v_p = 0$. En séparant les exposants selon leur signe, cela revient à montrer que pour tous r,$s \geq 1$, si pour tout $1 \leqslant i \leqslant r, 1 \leqslant j \leqslant s$, $n_i \geqslant 0, m_j \geqslant 0$, si p_i, q_j sont des idéaux maximaux deux à deux distincts, si $p_1^{n_1}...p_r^{n_r} = q_1^{m_1}...q_s^{m_s}$. Le membre de gauche est inclus dans q_1 si $m_1 > 0$. Si $n_1 = ... = n_r = 0$, $A \subseteq q_1$, ce qui est absurde. Mais alors il existe $1 \leqslant i \leqslant r$ tel que $p_i \subseteq q_i$, d'où par maximalité des deux, $p_i = q_i$, contradiction, donc $m_i = 0$ et pour tout j, $m_j = 0$. Ainsi $p_1^{n_1}...p_r^{n_r} = A$, puis $A \subseteq p_1$ si $n_1 > 0$. Donc $n_1 = ... = n_r = 0$.

C'est un groupe abélien, car le produit définit une loi de composition interne, est associatif, de neutre A. L'inverse est donné pour $I = \prod p^{v_p(I)}$ par $I^{-1} = \prod p^{-v_p(I)}$, car $I^{-1}I = A$ dans ce cas. ■

Méthode. ***(Déterminer l'inverse d'un idéal)***

Déterminer la puissance d'un idéal n'est qu'une écriture de définition, ce qui n'est pas la cas des exposants négatifs. On en revient toujours à calculer l'inverse d'un idéal $\mathfrak{p}$. Deux cas se présentent (pour l'instant, seul le premier apparemment) :

1. $\mathfrak{p}$ est entier, *i.e.* $p \subseteq A$. Alors d'après la preuve du théorème surprécédent, $p^{-1} = \{x \in Frac(A) \mid x\mathfrak{p} \subseteq A\}$.
2. $\mathfrak{p}$ est fractionnaire. Par définition, il existe $d \in A$ tel que $d\mathfrak{p}$ soit un idéal de A. D'après le point précédent, on sait calculer $(d\mathfrak{p})^{-1}$ et alors $d(d\mathfrak{p})^{-1}$ est l'inverse de $\mathfrak{p}$.

Remarques.

1. Parfois, si $I \subseteq K$ un A-module, on note $I^{-1} = \{x \in K \mid xI \subseteq A\}$ en toute généralité. On dit alors, si I est un idéal fractionnaire, que I est inversible si de plus $II^{-1} = A$.
2. On note parfois $K(I) = \{x \in K \mid xI \subseteq I\}$.

Exercice 13 *(Quelques propriétés des idéaux fractionnaires)*

Montrer, ou redémontrer :

1. soient I_1,I_2 des idéaux fractionnaires contenus dans $a_1^{-1}A$ et $a_2^{-1}A$ respectivement, avec a_1,$a_2 \in A$. Alors I_1I_2 est un idéal fractionnaire ;
2. sous les mêmes hypothèses, $I_1 + I_2$ est un idéal fractionnaire ;
3. sous les mêmes hypothèses, $I_1 \cap I_2$ est un idéal fractionnaire.

En application, on peut maintenant démontrer :

Propriété. ***(Anneaux de Dedekind factoriels)***

Un anneau de Dedekind est factoriel si et seulement s'il est principal.

▷ Soit A un anneau de Dedekind factoriel. Comme A est factoriel, tout élément irréductible engendre un idéal premier. Soit m un idéal maximal. Il existe $x \neq 0$ dans m, x non inversible, tel que $x = \varepsilon \prod_{i=1}^{r} p_i^{n_i}$ une décomposition de x en produit d'irréductibles, avec $\varepsilon \in A^\times$. Ainsi $(x) = \prod_{i=1}^{r} (p_i)^{n_1} \subseteq m$. Il existe i tel que $(p_i) \subseteq m$ avec (p_i) premier non nul, donc maximal par Dedekinditude. Ainsi $m = (p_i)$. Donc m est principal. Tous les idéaux sont alors principaux par factorisation des idéaux. ■

Le théorème de décomposition donne une application v_p, unique, presque nulle, de l'ensemble des idéaux premiers non nuls de A, noté $\mathcal{P}$, dans $\mathbb{Z}$.

Propriété. ***(Formulaire sur la valuation p-adique dans les Dedekind)***

Soient A un anneau de Dedekind et I,J deux idéaux fractionnaires non nuls de A. Alors, pour tout $p \in \mathcal{P}$,

1. $v_p(I.J) = v_p(I) + v_p(J)$,
2. $v_p(I^{-1}) = -v_p(I)$,
3. $I \subseteq J \iff v_p(I) \geqslant v_p(J)$; en particulier, $I \subseteq A \iff v_p(I) \geqslant 0$,
4. $v_p(I + J) = \min(v_p(I), v_p(J))$,
5. $v_p(I \cap J) = \max(v_p(I), v_p(J))$.

▷ Successivement :

1. C'est évident à cause de l'unicité de la décomposition.
2. Cela vient de ce qui suit : $v_p(II^{-1}) = v_p(A) = 0$.
3. Si $I \subseteq A$, $v_p(I) \geqslant 0$ pour tout $p \in \mathcal{P}$, et l'implication réciproque est évidente car $p \subseteq A$ pour tout $p \in \mathcal{P}$. Pour la première équivalence, si $I \subseteq J$, en multipliant par J^{-1}, $IJ^{-1} \subseteq JJ^{-1} = A$ qui équivaut à $v_p(IJ^{-1}) = v_p(I) - v_p(J) \geqslant 0$. Réciproquement, on multiplie par J.
4. Pour tout idéal a, $I \subseteq a$ et $J \subseteq a$ si et seulement si $I + J \subseteq a$. Soit $p \in \mathcal{P}$. Pour tout $n \in \mathbb{Z}$, $\min(v_p(I), v_p(J)) \geqslant n = v_p(p^n) \iff I \subseteq p^n$ et $J \subseteq p^n$, lui-même équivalent à $I + J \subseteq p^n$, lui-même équivalent à $v_p(I + J) \geqslant n = v_p(p^n)$ en utilisant libre le deuxième point. Donc $\min(v_p(I), v_p(J)) = v_p(I + J)$.
5. Même chose dans l'autre sens. ■

Définition. ***(Groupe de classes)***

Soit $I(A)$ l'ensemble des idéaux fractionnaires non nuls d'un anneau de Dedekind A. On note $P(A)$ le sous-groupe des idéaux fractionnaires non nuls principaux, soit $\{xA \mid x \in K^\times\}$ où $K = Frac(A)$.
Sa loi est donnée d'après le théorème précédent, par $(xA)^{-1} = x^{-1}A$ et $(xA)(yA) = xyA$.
On note $\mathcal{C}\ell(A) := I(A)/P(A)$, et l'on appelle *groupe des classes* ce quotient.

Heuristique

Le groupe de classes mesure le défaut de principalité de l'anneau A.
En effet, A est principal (et donc factoriel), si et seulement si, $\mathcal{C}\ell(A) = \{0\}$.

▷ Si A est principal, tous les idéaux maximaux/premiers sont principaux. Soit $\beta = (p)$. Alors $I = \prod \beta^{v_\beta(I)} = (\prod p^{v_\beta(I)})$ est principal. Réciproquement, si I est un idéal non nul, $I = xA$ avec $x \in K$ et si $I \subseteq A$, $x \in A$ (si vous n'avez pas compris l'intérêt de cette dernière phrase, veuillez revenir à la définition précédente). ■

4.2.2.8 Norme d'un idéal

Soit K un corps de nombres et A son anneau des entiers. Alors A est un anneau de Dedekind et un $\mathbb{Z}$-module libre de rang $[K : \mathbb{Q}]$.

Ces deux propriétés ne se déduisent pas l'une de l'autre : $A \simeq \mathbb{Z}^k$ en tant que modules, dont on ne peut déduire la Dedekinditude (d'ailleurs, $\mathbb{Z}^k$ n'est même pas intègre) !

Dans toute la suite, pour $x \in K$, on note $N(x) = N_{K/\mathbb{Q}}(x)$. On rappelle que si $x \in A$, sa norme $N(x) \in \mathbb{Z}$.

Lemme. ***(Cardinal du conoyau et déterminant)***

Soit M un $\mathbb{Z}$-module libre de rang fini n et $\phi \in \mathrm{End}_{\mathbb{Z}}(M)$ injectif. Alors $M/\mathrm{Im}(\phi)$ est fini de cardinal $|\det(\phi)| \in \mathbb{Z} \setminus \{0\}$.

▷ Soit $M = \oplus \mathbb{Z} e_i$, soit (e_i) une $\mathbb{Z}$-base de M. ϕ est injective donc $\mathrm{Im}(\phi) = \oplus \mathbb{Z}\phi(e_i)$ est libre de rang n, sous-module de M. Par principalité de $\mathbb{Z}$, je peux choisir la base (e_i) de M et $c_1 \mid c_2 \mid ... \mid c_n \in \mathbb{Z} \setminus \{0\}$ tel que $(c_1 e_1, ..., c_n e_n)$ une $\mathbb{Z}$-base de $\mathrm{Im}(\phi)$. Alors $M/\mathrm{Im}(\phi) \simeq \prod \mathbb{Z}/e_i\mathbb{Z}$, d'où $|M/\mathrm{Im}(\phi)| = |\prod_{i=1}^{n} c_i|$. Ainsi $\mathrm{Im}(\phi)$ possède deux bases : $(c_i e_i)$ et $(\phi(e_i))$. On passe de l'un à l'autre par une matrice dans $GL_n(\mathbb{Z})$ donc de déterminant ± 1. Ainsi $\det_{(e_i)}(e_i e_i) = \prod c_i = \pm \det_{(e_i)}(\phi(e_i)) = \pm \det(\phi)$. ■

On en déduit le résultat plus précis suivant, avec les notations de la section :

Propriété. ***(Introduction de la norme d'un idéal)***

Soit $x \in A \setminus \{0\}$. Alors A/Ax est fini de cardinal $|N(x)|$.

▷ Il suffit de considérer l'application m_x dans le lemme précédent. ■

Définition. ***(Norme d'un idéal)***

Soit $I \subseteq A$ un idéal non nul. On pose $N(I) = \mathrm{card}(A/I)$.

Propriété

$1 \leqslant N(I) < \infty$.

▷ Il existe $x \neq 0$, $x \in I$ avec donc $xA \subseteq I$ d'où la suite exacte $0 \xrightarrow{I} /xA \xrightarrow{A} /xA \xrightarrow{A} /I \xrightarrow{0}$, où A/xA est fini, donc A/I est fini. Ceci vient donc du fait que A est un module de rang fini, car c'est l'entier d'un corps de nombres qui par hypothèse est une extension finie. ■

Donc. ***(Norme d'un idéal principal)***

$N(xA) = |N(x)|$.

Remarque. Le générateur choisi varie à unité près, mais la norme est multiplicative et la norme d'une unité est une unité de $\mathbb{Z}$, et $|\pm 1| = 1$.

Propriété. ***(Multiplicativité de la norme des idéaux)***

Soient I,J deux idéaux non nuls de A. Alors $N(IJ) = N(I)N(J)$.

▷ On utilise la factorisation. Il suffit, par récurrence, de prouver $N(I.p) = N(I)N(p)$ pour tout $p \in \mathcal{P}$. Or $N(I.p) = |A/I.p|$, $N(I) = |A/I|$ et $N(p) = |A/p|$. Le troisième théorème d'isomorphisme donne, après renversement, $|A/I.p|/|A/I| = |I/I.p|$. Il nous reste à voir que $|I/I.p| = |A/p|$. Or $I/I.p$ est un A-module, en tant qu'idéal de $A/I.p$, et même, c'est un A/p-module, car la loi externe passe au quotient. Or p est premier, donc maximal, car A est de Dedekind, donc A/p est un corps. Donc $I/I.p$ est un A/p-espace vectoriel de dimension finie. Montrons qu'il est de dimension 1. Or $I/I.p$ est non nul, et les sous-A/p-espaces vectoriels de $I/I.p$ sont les $J/I.p$ où $I.p \subseteq J \subseteq I$. En inversant par I, on trouve $p \subseteq JI^{-1} \subseteq A$, donc par maximalité, $JI^{-1} = p$ ou A, soit $J = I.p$ ou I. D'où le résultat. ■

Corollaire. ***(Primalité des idéaux de norme première)***

Dans un anneau de Dedekind, tout idéal de norme un entier naturel premier est un idéal premier.

▷ Immédiat par décomposition. ■

4.2.2.9 Différentes

Le cadre est le suivant : A est un anneau de Dedekind, K son corps des fractions que l'on suppose de caractéristique nulle. Soit B la fermeture de A dans L/K une extension finie. On a vu que c'était un anneau de Dedekind. On fixe une base de L incluse dans B. Soit C le A-module engendré par cette base (par exemple, $1,...,x^{n-1}$ pour $x \in B$ primitif, soit $K(x) = L$, d'où $C = A[x]$), et $\check{C} = \{x \in L \mid \mathrm{Tr}_{L/K}(xC) \subseteq A\}$ comme défini précédemment ; de même, on définit le module dual $\check{B}$ de B.

On a vu que C et $\check{C}$ sont des A-modules libres, on en a même exhibé des bases. Puisque $C \subseteq B \subseteq \check{B} \subseteq \check{C}$ (étant clair que $\vee$ inverse l'inclusion), $\check{B}$ est un A-module de type fini et $\check{B}$ est un B-module, donc $\check{B}$ est un idéal fractionnaire de B.

Définition. ***(Différente, co-différente)***

La *différente inverse* ou *codifférente* est l'idéal $\check{B}$. La *différente* est l'idéal $\mathfrak{d}_{L/K} := (\check{B})^{-1}$ de B.

Remarques.

1. La trace étant à valeurs entières, la différente inverse contient l'anneau.
2. On en déduit que la différente est un idéal entier de l'anneau.

Définition. ***(Conducteur)***

Si $C = A[x]$ avec $x \in B$ primitif, C est un sous-anneau. Le *conducteur* de B dans C, est par définition $R = \{y \in C \mid yB \subseteq C\}$.

Remarques.

1. Alors R est un idéal de C.
2. C'est aussi un idéal de B, car si $y \in R, b \in B$, $ybB \subseteq yB \subseteq C$.

Propriété. ***(Lien entre le conducteur et la différente inverse)***

Soit f le polynôme caractéristique de x sur K, qui, ici, égale le polynôme minimal. On a $R_{B,C} = f'(x)\check{B}$.

▷ On a vu que $\check{C} = f'(x)^{-1}C$. Alors $y \in R \iff yB \subseteq C \iff yf'(x)^{-1}B \subseteq f'(x)^{-1}C = \check{C} \iff \mathrm{Tr}_{L/K}(yf'(x)^{-1}BC) \subseteq A \iff yf'(x)^{-1} \in \check{B} \iff y \in f'(x)\check{B}$, car $BC = B$. ■

Propriété. ***(Transitivité des différentes)***

Pour une tour $F/L/K$ avec les hypothèses précédentes,

$$\mathfrak{d}_{F/K} = \mathfrak{d}_{F/L}\mathfrak{d}_{L/K}.$$

Dans le cas des corps de nombres, on dispose d'une identité cruciale.

Lemme

Soient $I \subseteq J$ deux idéaux fractionnaires non nuls de B. Alors $\mathrm{card}(J/I) = N(IJ^{-1})$.

▷ En effet, on a $IJ^{-1} = p_1 ... p_n$ en tant qu'idéal entier. Donc $J \supsetneq J_1 = Jp_1 \supsetneq J_2 = J_1p_2 \supsetneq ...$ et en général $J_{n-1} \supsetneq J_n = J_{n-1}p_n = I$. Donc $\mathrm{card}(J/I) = \mathrm{card}(J/J_1)\mathrm{card}(J_1/I) = \mathrm{card}(J/J_1)\mathrm{card}(J_1/J_2)...\mathrm{card}(J_{n-1}/I)$. On a déjà prouvé que $\mathrm{card}(J_k/J_{k+1}) = \mathrm{card}(J_k/p_kJ_k) = \mathrm{card}(A/p_k) = N(p_k)$, d'où en somme $\mathrm{card}(J/I) = \prod_{k=1}^{n} N(p_k) = N\left(\prod_{k=1}^{n} p_k\right) = N(IJ^{-1})$. ■

Propriété. ***(Lien fondamental entre la différente et le discriminant)***

Si $A = \mathbb{Z}$, $K = \mathbb{Q}$, L extension finie de $\mathbb{Q}$, la norme de la différente est égale à la valeur absolue du discriminant (absolu) de L. Explicitement :

$$|\mathrm{Disc}(\mathcal{O}_L/\mathbb{Z})| = N_{L/\mathbb{Q}}(\mathfrak{d}_{L/\mathbb{Q}}).$$

▷ Dans ce cas, on sait que B est un $\mathbb{Z}$-module libre de rang $[L : \mathbb{Q}]$ et $\check{B}$ est un $\mathbb{Z}$-module libre de rang $[L : \mathbb{Q}]$ contenant B. Ainsi, $\mathrm{card}(\check{B}/B)$ est la valeur absolue du déterminant de la matrice

de présentation d'une $\mathbb{Z}$-base (e_i) de B dans la base duale de $\check{B}$, c'est-à-dire $|\det(\mathrm{Tr}_{L/\mathbb{Q}}(e_i,e_j)_{i,j})|$ la valeur absolue du discriminant. D'après le lemme, $\mathrm{card}(\check{B}/B) = N(\check{B}^{-1})$ qui est, par définition, la norme de la différente. ■

4.2.3 Groupe de classes et théorème des unités de Dirichlet

4.2.3.1 Rappels sur les sous-groupes de $\mathbb{R}^n$

On conseille simplement de relire le cours de Théorie des réseaux.

4.2.3.2 Plongement canonique d'un corps de nombres

Soit K un corps de nombres de degré n et x un élément primitif, μ_x son $\mathbb{Q}$-polynôme minimal, de sorte de $K \simeq \mathbb{Q}[X]/(\mu_x)$. Le polynôme μ_x est irréductible dans $\mathbb{Q}[X]$, mais il ne l'est pas forcément dans $\mathbb{R}[X]$. Plus précisément, grâce à la séparabilité de μ_x, on peut l'écrire : $\mu_x = P_1...P_{r_1}Q_1...Q_{r_2}$ avec les $P_i, Q_i \in \mathbb{R}[X]$ unitaire, les P_i de degré 1, les Q_j de degré 2 de discriminant < 0, et les P_i,Q_j deux à deux distincts. On identifie le degré $r_1 + 2r_2 = \deg(\mu_x) = n$. Ainsi, $K \simeq \mathbb{Q}[X]/(\mu_x) \hookrightarrow \mathbb{R}[X]/(\mu_x) = \mathbb{R}[X]/(P_1...P_{r_1}Q_1...Q_{r_2})$. Par théorème chinois, cet anneau s'identifie à $\mathbb{R}[X]/(P_1) \times ... \times \mathbb{R}[X]/(Q_{r_2}) \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, d'où un plongement de K dans $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Ce plongement n'est pas canonique, car il dépend du choix des racines de Q_i.

On peut interpréter ce plongement en termes de $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, qui a n éléments. On note x_1,...,x_n les racines de μ_x dans $\mathbb{C}$ (les éléments de $\mathrm{Hom}_{\mathbb{Q}}(K,C)$ soient en bijection avec $\{x_1,...,x_n\}$). À une racine y, on associe $\sigma : K[X]/(\mu_x) \to \mathbb{C}$ qui à $\overline{P} \mapsto P(y)$.) de sorte que x_i soit racine réelle de P_i, x_{r_1+j} racine complexe de Q_j et $x_{r_1+r_2+j} = \overline{x_{r_1+j}}$. On note σ_i le plongement associé à x_i. Je peux donc interpréter K comme l'image de

$$\boxed{\sigma : x \mapsto ((\sigma_i(x))_{1 \leqslant i \leqslant r\text{ç}1}, (\gamma_i(x))_{r_1+1 \leqslant i \leqslant r_1+r_2})},$$

ceci n'étant pas canonique, puisqu'on aurait pu remplacer $\sigma_i(x)$ par $\overline{\sigma_i(x)} = \sigma_{i+r_1}(x)$ pour $r_1+1 \leqslant i \leqslant r_1+r_2$. On le choisit une fois pour toute ainsi, pour résumer : $\{\sigma_1,...,\sigma_{r_1}, \sigma_{r_1+1}, \overline{\sigma_{r_1+1}} = \sigma_{r_1+r_2+1}, \sigma_{r_2+2}, \overline{\sigma_{r_1+2}}, ..., \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}\}$ avec $n = r_1 + 2r_2$ éléments, r_1 plongements réels et r_2 paires de plongements complexes, paires de conjugués ; on en déduit $\sigma : K \to \mathbb{R}^n$ en choisissant seulement un plongement complexe dans chaque paire, et tous les plongements réels.

VOC Dans la suite, on note $\mathbb{R}^n = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

On va regarder la structure de $\mathbb{R}$-espace vectoriel de K.

Proposition. ***(Image d'un réseau par le plongement canonique)***

Soit $M \subseteq K$ un sous-$\mathbb{Z}$-module libre de rang n et $(x_i)_{1 \leqslant i \leqslant n}$ une base de M. Alors $\sigma(M)$ est un réseau de $\mathbb{R}^n$, et $\mathrm{vol}(\sigma(M)) = 2^{-r_2}|\det((\sigma_i(x_j))_{1 \leqslant i,j \leqslant n})|$.

▷ On a $\sigma : K \longrightarrow \mathbb{R}^n$ qui à

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

Ainsi, dans la base canonique de $\mathbb{R}^n$, $\det(\sigma(x_i)) = \det\begin{pmatrix} \sigma_1(x_i) \\ \vdots \\ \sigma_{r_1}(x_i) \\ \mathfrak{Re}(\sigma_{r_1+1}(x_i)) \\ \mathfrak{Im}(\sigma_{r_1+1}(x_)) \\ \vdots \end{pmatrix} =$

$(-2)^{-r_2}\det\begin{pmatrix} \sigma_1(x_i) \\ \vdots \\ \sigma_{r_1}(x_i) \\ \sigma_{r_1+1}(x_i) \\ (-2).\mathfrak{Im}(\sigma_{r_1+1}(x_i)) \\ \vdots \end{pmatrix} = (-2)^{-r_2}\det\begin{pmatrix} \sigma_1(x_i) \\ \vdots \\ \sigma_{r_1}(x_i) \\ \sigma_{r_1+1}(x_i) \\ \overline{\sigma_{r_1+1}(x_i)} \\ \sigma_{r_1+2}(x_i) \\ \overline{\sigma_{r_1+2}(x_i)} \\ \vdots \end{pmatrix} = \pm 2^{-r_2}\det(\sigma_i(x_j))$. Par hypothèse, (x_i) forme une $\mathbb{Z}$-base de M. Elle est donc $\mathbb{Q}$-libre, donc c'est une $\mathbb{Q}$-base de K. On sait que $\det(\sigma_i(x_j)) \neq 0$. Ainsi, $(\sigma(x_1),...,\sigma(x_n))$ est une famille $\mathbb{R}$-libre de $\mathbb{R}^n$. Par suite, $\sigma(M)$ est un sous-$\mathbb{Z}$-module de $\mathbb{R}^n$ engendré par la base $(\sigma(x_1),...,\sigma(x_n))$, donc un réseau. De plus, $\mathrm{vol}(\sigma(M)) = |\det_{\text{b.c.}}(\sigma(x_1) - \sigma(x_n)) = 2^{r-2}|\det(\sigma_i(x_j))|$. ■

On applique cela bien naturellement à la théorie algébrique des nombres.

Proposition. ***(Volume d'un anneau d'entiers de corps de nombres)***

Soit d le discriminant absolu de K et A son anneau des entiers. Alors :

1. $\sigma(A)$ est un réseau de $\mathbb{R}^n$ de volume $\mathrm{vol}(\sigma(A)) = 2^{-r_2}d^{1/2}$.
2. Soit I un idéal non nul de A. Alors $\sigma(I)$ est un réseau de $\mathbb{R}^n$ de volume $\mathrm{vol}(\sigma(I)) = 2^{-r_2}d^{1/2}N(I)$.

▷ Le discriminant $D(x_1,...,x_n) = \det(\sigma_i(x_j))^2$ par une propriété connue et dans le cas où (x_i) est une $\mathbb{Z}$-base de A, par définition $d = D(x_1,...,x_n)$. On sait que A est un $\mathbb{Z}$-module de rang $n = [K : \mathbb{Q}]$, et $I \subseteq A$ est un sous-$\mathbb{Z}$-module de A d'indice fini, donc libre de même rang. Ainsi, $\sigma(I), \sigma(A)$ sont des réseaux par la proposition précédente, d'où le résultat. Pour le deuxième volume, $\sigma(I) \subseteq \sigma(A)$ avec σ injective donc c'est un sous-groupe d'indice $N(I)$, d'où le résultat. ■

4.2.3.3 Finitude du groupe de classes d'idéaux

On énonce plusieurs résultats notables.

Théorème. ***(Théorème de la borne de Minkowski)***

Soit $K/\mathbb{Q}$ de degré $n < \infty$ et $A \subseteq K$ l'anneau de ses entiers. Soit d son discriminant absolu, dans $\mathbb{Z} \setminus \{0\}$. On extrait r_1,r_2 de son plongement canonique dans $\mathbb{R}^n$.
Soit I un idéal non nul de A. Alors, il existe $x \in I$ non nul tel que

$$|N_{K/\mathbb{Q}}(x)| \leqslant \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2} N(I).$$

On appelle $M_K = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2}$ la *constante de Minkowski* du corps K. Elle ne dépend que de K.

▷ Soit $t > 0$ et $B_t = \{(y_1,...,y_r,z_1,...,z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid \sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| \leqslant t\}$. Alors B_t est convexe, symétrique par rapport à l'origine et compact. On peut calculer que $\mathrm{vol}(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}$, ce que nous faisons en annexe. On prend t tel que $\mathrm{vol}(B_t) = 2^n \mathrm{vol}(\sigma(I)) = 2^{n-r_2}|d|^{1/2}N(I)$, de sorte que $t^n = n! 2^{n-r_1}\pi^{-r_2}|d|^{1/2}N(I)$. Par le théorème, il existe $x \in I$ non nul tel que $\sigma(x) \in B_t$ c'est-à-dire $\sum_{i=1}^{r_1} |\sigma_i(x)| + 2\sum_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)| \leqslant t$. On veut majorer $|N_{K/\mathbb{Q}}(x)| = \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|^2$. Pour conclure, on utilise la convexité de l'exponentielle. On pose $x_i = \log|\sigma_i(x)|$, d'où $|N_{K/\mathbb{Q}}(x)|^{1/n} = (\prod |\sigma_i(x)|)^{1/n} = \exp(\frac{\sum \log|\sigma_i(x)|}{n} \leqslant \frac{1}{n}\sum \exp\log|\sigma_i(x)|) = |\frac{1}{n}\sum_{i=1}^{n} -\sigma_i(x)| \leqslant \frac{t}{n}$. Ainsi, $|N_{K/\mathbb{Q}}(x)| \leqslant \frac{t^n}{n^n} = \frac{n!}{n^n} 2^{n-r_1}\pi_{-r_2}|d|^{1/2}N(I)$ où $n - r_1 = 2r_2$ d'où $2^{n-r_1}\pi_{-r_2} = \left(\frac{4}{\pi}\right)^{r_2}$. ■

Corollaire. ***(Borne de Minkowski des idéaux entiers)***

Toute classe d'idéaux fractionnaires non nuls de K contient un idéal entier $I \subseteq A$ tel que $N(I) \leqslant M_K$.

▷ Soit I' un représentant de la classe considérée. Alors $(I')^{-1}$ est un idéal fractionnaire, donc il existe $a \in A$ non nul tel que $a(I')^{-1} \subseteq A$, où $a(I')^{-1} = (a^{-1}I')^{-1}$. Quitte à remplacer I' par $a^{-1}I'$, je peux supposer que $I = (I')^{-1}$ est entier. D'après la proposition précédente, il existe $x \in I \neq 0$ tel que $|N(x)| \leqslant M_K N(I)$. Or xI' est dans la classe de I'. Ainsi, $N(xI') = N(xI^{-1}) = |N(x)||N(I)|^{-1} \leqslant \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}|d|^{1/2}$. Ainsi $|N(x)| = N(xA) = N(xI^{-1}I) = N(xI^{-1})N(I)$. ■

Corollaire. ***(Minoration du discriminant d'un corps de nombres)***

Pour tout corps de nombres K de degré $n \geqslant 2$, on a

$$|d| \geqslant \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}.$$

En particulier, $[K : \mathbb{Q}] = n$ est majoré en fonction de $|d|$, par $n \leqslant \frac{\log(\frac{9|d|}{4})}{\log(\frac{3\pi}{4})}$.

▷ Dans la classe de A, il existe un idéal entier I tel que $1 \leqslant N(I) \leqslant M_K$, d'où $|d| \geqslant (\frac{\pi}{4})^{2r_2}\frac{n^{2n}}{(n!)^2} \geqslant (\frac{\pi}{4})^{n}\frac{n^{2n}}{(n!)^2} = a_n$ où $0 < \frac{\pi}{4} < 1$ et $n \geqslant 2r_2$. Or $\frac{a_{n+1}}{a_n} = \frac{\pi}{4}\frac{(\frac{n+1}{n})^{2n}(n+1)^2}{(n+1)^2} = \frac{\pi}{4}(1+\frac{1}{n})^{2n} \geqslant \frac{3\pi}{4}$ où $(1 + 2n\frac{1}{n} + ...) \geqslant 3$. Par suite, $|d| \geqslant a_n = \frac{a_n}{a_{n-1}}...\frac{a_3}{a_2}a_2 \geqslant (\frac{3\pi}{4})^{n-2}\frac{\pi^2}{4} = (\frac{3\pi}{4})^{n-1}\frac{\pi}{3}$. ■

Parmi les corollaires non triviaux, citons également :

Théorème. ***(Théorème d'Hermite-Minkowski)***

Soit K un corps de nombres de degré $\geqslant 2$. Alors son discriminant $d \neq \pm 1$.
Autrement dit, le discriminant de tout corps de nombres non trivial admet des facteurs premiers. On dit que ceux-ci se *ramifient* dans K. Un facteur premier non ramifié dans le discriminant considéré est dit *inerte*.

▷ On a en effet une minoration de l'entier $|d| \geqslant (\frac{\pi}{3})(\frac{3\pi}{4})^{n-1} \geqslant (\frac{3\pi}{4})^{2-1} = \frac{3\pi}{4} > 1$ si $n \geqslant 2$, car $\frac{\pi}{3} > 1$. ■

On en vient au théorème suivant :

Théorème. ***(Finitude du groupe de classes, Dirichlet)***

Le groupe de classes d'un anneau d'entiers algébriques de corps de nombres est fini.

▷ Il suffit de montrer que $\mathcal{C}\ell(A)$ a un nombre fini de représentants. Or $\{I \subseteq A \mid N(I) \leqslant (\frac{4}{\pi})^{r_1}\frac{n!}{n^n}|d|^{1/2}\}$ contient un système de représentants par un des corollaires précédents. Cet ensemble est fini. En fait, $\{I \subseteq A \mid N(I) = a\}$ où a est un entier est fini. En effet, il est inclus dans $\{I \mid aA \subseteq I \subseteq A\}$ qui est en bijection avec l'ensemble des idéaux du quotient A/aA, fini. ■

Méthode. ***(Décrire le groupe d'idéaux d'un anneau d'entiers)***

Soit $\mathcal{C}$ la classe d'idéaux de $\mathcal{O}_K$. D'après le théorème de Minkowski, il existe $a \in \mathcal{C}$ avec $N(a) \leqslant \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\mathrm{Disc}(\mathcal{O}_K)|}$ où $n = r_1 + 2r_2 = [K : \mathbb{Q}]$.
On fait la liste des idéaux premiers/maximaux de norme $N(\mathfrak{p}_i) \leqslant M_K$, en notant les idéaux (en nombres finis) : $\mathfrak{p}_1$,...,$\mathfrak{p}_r$ et leurs classes respectives a_1,...,a_s. Alors $\mathcal{C}\ell_K = \{[a_1],..., [a_s]\}$.
Ensuite, on cherche les relations entre idéaux *(voir en exercice)*.

4.2.3.4 Applications des théorèmes de finitude aux corps quadratiques

Les théorèmes précédents fournissent des arguments puissants pour l'étude des anneaux d'entiers de corps de nombres. Dans le cas des corps quadratiques imaginaires, ce sont même des marteaux-pilons ! Voyons plutôt.

Exemple. ***(Application : $\mathcal{O}_{\mathbb{Q}(\sqrt{-7})}$ est principal)***

On sait que $-7 \equiv 1[4]$, donc le discriminant de $K = \mathbb{Q}(\sqrt{-7})$ est $-7 = d_K$. Dans ce cas, $r_1 = 0$ et $r_2 = 1$ (il est plus que clair que $r_1 = 0$, car K ne peut se plonger dans $\mathbb{R}$) !.
On reprend la preuve du théorème de finitude du groupe de classes. Toute classe a un représentant $I \subseteq A$ tel que $1 \leqslant n(I) \leqslant (\frac{4}{\pi})^{r_2} \frac{n!}{n^n} |d_K|^{1/2} < 2$, soit $N(I) = 1$, soit $I = A$. Donc il n'y a qu'une seule classe ! Donc A_K est principal.

Exemple. ***(Application : $\mathcal{O}_{\mathbb{Q}(\sqrt{13})}$ est principal)***

Dans ce cas, le discriminant de K est $d_K = 13$. On a $r_1 = 2$ et $r_2 = 0$, donc la manipulation précédente donne $N(I) \leqslant \frac{\sqrt{13}}{2} < 2$, donc $\mathcal{O}_K$ est principal.

Remarque. On peut montrer de la même manière que pour $d = 2,3,5,13, -1, -2, -3, -7$, $\mathcal{O}_K$ est principal.

Méthode. ***(Montrer que l'anneau d'entiers A d'un corps de nombres K est principal)***

On rappelle que, puisqu'il est de Dedekind, c'est vraiment ce qui nous intéresse (l'euclidianité étant un problème tout autre, assez peu algébrique).
On rappelle que toute classe d'ideaux de $\mathcal{C}\ell(A)$ contient un idéal entier de norme $\leqslant M_K$.
La première chose à faire est de calculer cette constante intrinsèque : on trouve le degré n de K, puis le nombre de plongements complexes (ou le nombre de plongements réels).
Enfin, on calcule le discriminant absolu de K, qui est celui de $A/\mathbb{Z}$.
Il s'agit de montrer que M_K est strictement inférieur à 2. Alors toute classe contient un idéal de norme 1, c'est-à-dire un idéal égal à A, donc toute classe contient l'élément neutre, donc il n'y a qu'une seule classe, donc par caractérisation, A est principal.

4.2.3.5 Un autre théorème d'Hermite

Théorème. ***(Théorème d'Hermite)***

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

▷ On rappelle que tout corps de nombres est dans $\mathbb{C}$. On a vu que dis d est fixé, $[K : \mathbb{Q}]$ est majoré. Donc, on peut supposer $[K : \mathbb{Q}] = n$ fixé, ainsi que r_1,r_2 et même d_K.

Je suppose $r_1 > 0$. On reprend $B_t = \{(y_1,...,y_{r_1}, z_1, ..., z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid |y_1| \leqslant t, |y_i| \leqslant 1/2 \text{ pour } i > 1, |z_j| \leqslant 1/2 \ 1 \leqslant j \leqslant r_2\}$. Soit $t \geqslant 0$ tel que $\text{vol}(B_t) > 2^n \text{vol}(\sigma(A))$. Comme d'habitude, il existe $x \neq 0 \in A$ tel que $\sigma(x) \in B_t$. Avec les notations usuelles, $|\sigma_1(x)| \leqslant t$, $|\sigma_i(x)| \leqslant 1/2$, $i > 1$. Ainsi, $1 \leqslant |N_{K/\mathbb{Q}}(x)| = \prod |\sigma_i(x)| \prod |\sigma_j(x)|^2 < |\sigma_1(x)|$, $|N_{K/\mathbb{Q}}(x)|$ entier, d'où pour tout $i > 1$, $\sigma_1(x) \neq \sigma_i(x)$, donc $K = \mathbb{Q}(x)$. Or x est annulé par $\prod_{i=1}^{n} (X - \sigma_i(x)) \in \mathbb{Z}[X]$, unitaire de degré n. Les coefficients sont bornés en terme de d_K. Prenons $t = \frac{2^{n-r_2}|d|^{1/2}}{v_0}$. Il y a un nombre fini de tels polynômes, donc de tels

$x \in \mathbb{C}$ tels que $[\mathbb{Q}(x) : \mathbb{Q}] = n$, soit $d_{\mathbb{Q}(x)} = d$.

Si $r_1 = 0$, soit B l'ensemble des éléments $(z_1,...,z_{r_2}) \in \mathbb{R}^{r_2}$ tels que $|z_1 - \overline{z_1}| \leqslant 2^n \left(\frac{\pi}{2}\right)^{1-r_2} |d|^{1/2}$, $|z_1 + \overline{z_1}| \leqslant \frac{1}{2}$ et $|z_j| \leqslant \frac{1}{2}$ pour $j = 2,...,r_2$. Clairement, B est un compact convexe symétrique par rapport à l'origine de volume $2^{n-r_2}|d|^{1/2}$, ce que l'on peut calculer en observant que B est produit d'intervalles, de disques et d'un rectangle. On conclut comme précédemment. ■

4.2.3.6 Théorème des unités de Dirichlet

Théorème. ***(Théorème des unités de Dirichlet)***

Soit K un corps de nombres contenant A l'anneau de ses entiers. Son groupe des unités $A^\times$ est un groupe abélien. Soit $n = [K : \mathbb{Q}] = r_1 + 2r_2$. Le groupe $A^\times$ est isomorphe à $G \times \mathbb{Z}^r$ où G est un groupe cyclique et $r = r_1 + r_2 - 1$.
En fait, G est le groupe des racines de l'unité dans K, et donc dans A (par une propriété sur le polynôme caractéristique). On a donc : $G = A \cap \mathbb{U}_\infty$ où $\mathbb{U}_\infty$ est le groupe de toutes les racines de l'unité de $\mathbb{C}$ en identifiant K à son plongé canonique.
Explicitement, il existe des unités $\varepsilon_1,...,\varepsilon_r \in A^\times$, dites *unités fondamentales*, telles que pour tout $x \in A^\times$, x s'écrit de manière unique sous la forme :

$$x = \mu\varepsilon_1^{n_1}...\varepsilon_r^{n_r}$$

où $\mu \in A^\times$ est une racine de 1 et $n_i \in \mathbb{Z}$.

▷ Soit $L : \begin{array}{ccc} K^\times & \longrightarrow & \mathbb{R}^{r+1} \\ x & \longmapsto & \log|\sigma_i(x)|,...,\log|\sigma_{r_1}(x)|,\log|\sigma_{r_1+1}(x)|,...,\log|\sigma_{r_1+r_2}(x)| \end{array}$ où $\{\sigma_1,...,\sigma_{r_1+1},\overline{\sigma_{r_1+1}},...,\sigma_{r_1+r_2},\overline{\sigma_{r_1+r_2}}\} = \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})$. L'application L est un morphisme de groupes. Soit $B \subseteq \mathbb{R}^{r+1}$ une partie compacte de l'espace. Alors $A^\times \cap L^{-1}(B) = \{x \in A^\times \mid L(x) \in B\}$ est fini : en effet, $B \subseteq [-m,m]^{r+1}$ et il existe $0 < \alpha < 1$ tel que $x \in A^\times$ et $L(x) \in B$ et $\alpha \leqslant |\sigma_i(x)| \leqslant \alpha^{-1}$ pour tout $1 \leqslant i \leqslant r_1 + r_2$, et ainsi, le polynôme caractéristique de x est de degré n, dans $\mathbb{Z}[X]$, donc ses coefficients, expressions symétriques en les $\sigma_i(x)$, sont bornés en fonction de α et donc de B, d'où la finitude de cet ensemble.

Par conséquence, $A^\times \cap \mathrm{Ker}(L) = A^\times \cap L^{-1}(\{0\})$ où $\{0\}$ est compact est un sous-groupe fini de $A^\times$. Un sous-groupe fini de $A^\times$ est toujours inclus dans μ_K le groupe des racines de 1. Inversement, si $x \in \mu_K$, x est un élément de torsion dans $A^\times$, donc $L(x)$ est un élément de torsion dans $\mathbb{R}^{r=1}$, donc $L(x) = 0$. On a $\mu_K = A^\times \cap \mathrm{Ker}(L)$ et ce groupe est fini, donc cyclique, car tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.

Reste à comprendre $A^\times/\mu_k \simeq L(A^\times)$. Or $L(A)^\times$ est un sous-groupe de $\mathbb{R}^{r+1}$ discret, car $B \subseteq \mathbb{R}^{r+1}$ une partie compacte. Donc $L(A^\times) \cap B = L(A^\times \cap L^{-1}(B))$ est fini. Donc $L(A^\times)$ est un $\mathbb{Z}$-module libre de rang $\leqslant r+1$, et même en fait de rang $< r+1$. Si $x \in A^\times$, $N(x) \in \mathbb{Z}^\times = \{\pm 1\}$, d'où $|N(x)| = 1$, c'est-à-dire $\prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{i=1}^{r_2} |\sigma_{r_1+i}(x)|^2 = 1$. Soit $W \subseteq \mathbb{R}^{r+1}$ l'hyperplan défini par $y_1 + ... + y_{r_1} + 2(y_{r_1+1} + ... + y_{r_1+r_2}) = 0$. Alors $L(A^\times) \subseteq W$ d'où $\mathrm{rg}(L(A^\times)) \leqslant r$. Il nous reste à montrer que $L(A^\times) = r$. On va montrer que $L(A^\times)$ n'est jamais inclus dans un sous-espace vectoriel propre de

W, ou encore, que $L(A^\times)$ n'est inclus dans aucun hyperplan de W. Soit f une forme linéaire non nulle sur W. On va montrer qu'il existe $x \in A^\times$ telle que $f(L(x)) \neq 0$. Au vu de la définition de W, pour $(y_i) \in W$, $f((y_i)) = \sum_{i=1}^{r} c_i y_i$ où $(c_i) \neq (0)$. Cela devient un peu technique. Je fixe $\alpha > 0$ assez grand. Pour tous $(\lambda_1,...,\lambda_r) \in (\mathbb{R}_+^*)^r$, soit $\lambda_{r+1} > 0$ tel que $\lambda_1...\lambda_{r_1}(\lambda_{r_1+1}...\lambda_{r_1+r_2})^2 = \alpha$. Soit maintenant $B = \{(y_1,...,y_{r_1}, z_{r_1+1},..., z_{r_1+r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \ ||y_i| \leqslant \lambda_i, 1 \leqslant i \leqslant r_1, |z_i| \leqslant \lambda_i, r_1+1 \leqslant i \leqslant r_1+r_2\}$. Dans ce cas, $\mathrm{vol}(B) = \star \cdot \alpha$. On suppose α assez grand pour que $\mathrm{vol}(B) \geqslant 2^n \mathrm{vol}(\sigma(A)) = 2^{n-r_2}|d_K|^{1/2}$. Il existe $x \in A$, $x \neq 0$ tel que $|\sigma_i(x)| \leqslant \lambda_i$ pour tout $i \in [\![1, r_1+r_2]\!]$, et alors $1 \leqslant \underbrace{|N(x)|}_{\in \mathbb{Z}} = \prod_{1 \leqslant r_1} |\sigma_i(x)| \prod_{i \geqslant r_1+1} |\sigma_i(x)|^2 \leqslant \prod_{i \leqslant r_1} \lambda_i \prod_{i \geqslant r_1+1} \lambda_i^2 = \alpha$. Or $|\sigma_i(x)| = \dfrac{|N(x)|}{\prod_{j \neq i, j \leqslant r_1} |\sigma_j(x)| \prod_{j \neq i, j > r_1} |\sigma_j(x)|^2} \geqslant \dfrac{\lambda_i}{\alpha}$. On trouve donc : $\frac{\lambda_i}{\alpha} \leqslant |\sigma_i(x)| \leqslant \lambda_i$, d'où en passant au logarithme : $\log(\lambda_i) - \log(\alpha) \leqslant \log|\sigma_i(x)| \leqslant \log(\lambda_i)$. Ainsi, $|f(\log(\lambda_i)) - f(L(x))| = |\sum c_i(\log(\lambda_i) - \log(|\sigma_i(x)|)| \leqslant (\sum |c_i|)\log(\alpha)$. Soit $\beta > (\sum |c_i|)\log(\alpha)$. Pour tout $k \in \mathbb{Z}$, soit (λ_i^k) tels que $f(\log \lambda_i^k) = 2\beta k$, car f est une forme linéaire non nulle donc surjective. Soient les $x_k \in A \setminus \{0\}$ associé tel que $|f(L(x_k)) - 2\beta k| < \beta$. Alors $\beta(2k-1) < f(L(x_k)) < \beta(2k+1)$. Ainsi, les $f(L(x_k))$ sont deux à deux distincts ; or, les $N(x_k)$ restent bornées par α, donc $N(x_k A)$ est borné, donc $\{x_k A, k \in \mathbb{Z}\}$ est fini. Donc il existe $k \neq k'$ tels que $Ax_k = Ax_k'$, soit $x_k(x_{k'})^{-1} \in A^\times$. Ainsi, $f(L(x_k x_k'^{-1})) = f(L(x_k) - L(x_k')) = f(L(x_k)) - f(L(x_k')) \neq 0$. On conclut que $L(A^\times) \simeq \mathbb{Z}^r$, d'où la suite exacte

$$1 \to \mu_k \to A^\times \to L(A^\times) \simeq \mathbb{Z}^r \to 0.$$

Il est facile de scinder la suite : on peut prendre $s(e_i) = a_i$ où e est la base canonique et a_i est tel que $L(a_i) = e_i$, d'où une application de $A^\times \to \mu_K \times \mathbb{Z}^r$, $a \mapsto (as(L(a))^{-1}, L(a))$. ■

4.2.3.7 Unités des corps quadratiques

Avec le théorème des unités, $r_1 = 0$ et $2r_2 = 2$ d'où $r_2 = 1$ et $r_1 + r_2 - 1 = 0$. Ainsi $A^\times$ est le groupe des racines de l'unité dans K.

On peut faire plus précis avec un exercice de théorie des nombres élémentaires que l'on suppose connu.

Proposition. ***(Unités des corps quadratiques imaginaires)***

Si K est un corps quadratique imaginaire, $\mathcal{O}_K^\times$ est égal à $\{\pm 1\}$, excepté dans l'un des deux cas suivants :

- si $K = \mathbb{Q}(i)$, $\mathcal{O}_K^\times = \{\pm 1, \pm i\}$;
- si $K = \mathbb{Q}(\sqrt{-3})$, $\mathcal{O}_K^\times = \{\pm 1, \frac{\pm 1 \pm i\sqrt{3}}{2}\}$ qui est $\mathbb{U}_6$.

Le théorème est beaucoup plus intéressant dans le cas des unités des corps quadratiques réels.

Dans ce cas, $r_1 = 1$ et $r_2 = 0$, d'où $r = 1$. Ainsi, $A^\times \simeq \mu_K \times \mathbb{Z}$. Or $\mu_k = \{\pm 1\}$, puisque $K \subseteq \mathbb{R}$. Il existe ε une unité fondamentale telle que pour tout $x \in A^\times$, il existe un unique $n \in \mathbb{Z}$

tel que $x = \pm\varepsilon^n$. On peut supposer $\varepsilon > 0$, et $\varepsilon \neq 1$, donc on peut supposer $\varepsilon > 1$. Si $\varepsilon < 1$, $\varepsilon^{-1} > 1$.

Proposition. ***(Unités des corps quadratiques réels)***

Il existe $\varepsilon > 0$ dans $A^\times$ tel que pour toute $x \in A^\times$, $x > 0$, $\exists! n \in \mathbb{Z}, x = \varepsilon^n$. Il existe donc un unique générateur > 1 du groupe $A^\times \cap \mathbb{R}_+^*$. On l'appelle l'*unité fondamentale* de K.

Variante. Soit $x \in K$, $x = a + b\sqrt{d}$, $a,b \in \mathbb{Q}$. Si x est une unité, il en est de même de $x^{-1}, -x, -x^{-1}$. Sur ces quatre nombres, il y en a un seul > 1 si $x \neq 1$. C'est le plus grand des quatre ; si $a > 0, b > 0$, c'est $a+b\sqrt{d}$, car $N(x) = \pm 1$, $x \neq \pm 1$ et $\{x, x^{-1}, -x, -x^{-1}\} = \{\pm a \pm \sqrt{d}\}$. Les unités > 1 sont de la forme $a + b\sqrt{d}$, $a,b \in \mathbb{Q}$, $a > 0, b > 0$.

Supposons $d \equiv 2,3\ [4]$. Soit $A = \{a + b\sqrt{d}, ab \in \mathbb{Z}\}$. Pour $a,b \in \mathbb{Z}$, $a + b\sqrt{d} \in A^\times \iff N(a + b\sqrt{d}) = a^2 - db^2 = \pm 1$. On cherche à résoudre pour $a,b \geqslant 1$ l'équation de Pell-Fermat : $a^2 - db^2 = \pm 1$. On sait qu'il existe une solution (a_1,b_1), dite *fondamentale*, telle que $\varepsilon = a_1 + b_1\sqrt{d}$ est le générateur > 1 de $A^\times \cap \mathbb{R}_+^\times$. En posant $a_n + b_n\sqrt{d} = (a_1 + b_1\sqrt{d})^n$, les autres solutions sont les (a_n,b_n), $n \geqslant 1$.

Méthode. ***(Trouver la solution fondamentale d'une équation de Pell-Fermat)***

En pratique, on observe que la suite $(b_n)_{n\in\mathbb{N}}$ est strictement croissante. En effet, $b_{n+1} = a_1 + a_n b_1 \geqslant b_n$.

On dresse le tableau :

b	1	2	3
db^2	d	4d	9d
$db^2 + 1$			

à continuer.

Pour $d = 7$, $d \equiv 3\ [4]$, on cherche l'unité fondamentale de $\mathbb{Q}(\sqrt{7})$. On écrit :

b	1	2	3
$7b^2$	7	28	63
$7b^2 - 1$	6	27	62
$7b^2 + 1$	8	29	$64 = 8^2$

Ainsi, (8,3) est la solution fondamentale de $a^2 - 7b^2 = 1$, donc $8 + 3\sqrt{7}$ est l'unité fondamentale, de norme 1.

Remarque. L'équation $a^2 - 7b^2 = -2$ n'a pas de solutions entières, car l'unité fondamentale est de norme 1. Généralement :

Fait

Si l'unité fondamentale est de norme 1, l'équation $a^2 - db^2 = -1$ n'a pas de solutions ; si elle est de norme -1, les solutions de $a^2 - db^2 = 1$ sont les (a_{2n},b_{2n}) et celles de $a^2 - db^2 = -1$ sont les (a_{2n+1}, b_{2n+1}).

Traitons maintenant le cas $d \equiv 1\ [4]$. On a $A = \left\{\dfrac{a + b\sqrt{d}}{2}, a,b \in \mathbb{Z} \text{ de même parité}\right\}$.

$\varepsilon = \frac{a+b\sqrt{d}}{2}$ est une unité $\iff$ $a^2 - db^4 = \pm 4$. De même que précédemment, on cherche les solutions en entiers $\geqslant 1$ de cette équation. Les solutions sont de la forme (a_n,b_n) avec $\frac{a_n+b_n\sqrt{d}}{2} = (\frac{a_1+b_1\sqrt{d}}{2})^n$ et $\varepsilon = \frac{a_1+b_1\sqrt{d}}{2}$ est une unité fondamentale.

Méthode. ***(Déterminer*** $B^\times$ ***où*** $B = \mathbb{Z}\sqrt{d} \subseteq A$***)***

On traite le cas $d \equiv 1$ [4]. Alors $B^\times \cap \mathbb{R}_+^\times$ est un sous-groupe de $A^\times \cap \mathbb{R}_+^\times$. Soit $\frac{a_1+b_1\sqrt{d}}{2} = \varepsilon$ l'unité fondamentale de $A^\times$.
On sait que $a_1 \equiv b_1$ [2]. Si de plus $a_1,b_1 \equiv 0$ [2], alors $\varepsilon \in B^\times$. Alors $B^\times \cap \mathbb{R}_+^\times = A^\times \cap \mathbb{R}_+^\times$. Si $a_1,b_1 \equiv 1$ [2], je dis que $\varepsilon \notin B$ et $\varepsilon^3 \in B^\times$. En effet, $\left(\frac{a_1+b_1\sqrt{d}}{2}\right)^3 = \frac{a_1^3+3a_1b_1^2d}{8} + \sqrt{d}\frac{3a_1^2b_1+b_1^3d}{8}$ et $a_1^2 - db_1^2 = \pm 4 \equiv 0$ [4] puis $a_1^3 + 3a_1b_1^2d = a_1(a_1^2+3b_1^2d) = a_1(4b_1^2d \pm 4) = 4a_1(b_1^2d \pm 1) \equiv 0$ [2], et $3a_1^2b_1 + b_1^3d = b_1(3a_1^2+b_1^2d) = b_1(4a_1^2 \pm 4) = 4b_1(a_1^2 \pm 1) \equiv 0$ [2]. De plus, $\varepsilon^2 \notin B^\times$, car sinon ε le serait ce qui n'est pas. On en déduit : $B^\times \cap \mathbb{R}_+^\times = \varepsilon^{3\mathbb{Z}}$.

4.2.3.8 Annexe : le calcul d'un volume

On termine la preuve du théorème de la borne de Minkowski dont on avait laissé un calcul en suspens.

Lemme

Soient $r_1,r_2 \in \mathbb{N}$ et $n = r_1 + 2r_2$. Soit $t \geqslant 0$ et B_t l'ensemble des $(y_1,...,y_{r_1},z_1,...,z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ tels que $\sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| \leqslant t$. Soit μ la mesure de Lebesgue sur $\mathbb{R}^n$. Alors :

$$\mu(B_t) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!}.$$

▷ ■

Ce qu'il faut retenir

→ Le cas le plus commun (et déjà très riche) étant celui des corps de nombres, dont on a largement étudié le cas $n = 2$, assez représentatif (mis à part la monogénéité qui tombe en défaut pour $n \geqslant 3$, mais pas pour les corps cyclotomiques par exemple), on se concentre là-dessus. On rappelle que l'on a affaire à une extension finie K de $\mathbb{Q}$, de degré n. Son groupe de Galois a donc n éléments $\sigma_1,...,\sigma_n$ et on plonge naturellement $K \simeq \mathbb{Q}^n$ dans $\mathbb{R}^n \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ où $n = r_1 + 2r_2$, r_1 le nombre de plongements associés aux facteurs irréductibles de degré 1, dits réels, du polynôme minimal d'un élément primitif de $K/\mathbb{Q}$, r_2 le nombre de plongements associés aux facteurs irréductibles de degré 2, dits complexes.

→ L'ensemble $A_K = \mathcal{O}_K$ des éléments entiers sur $\mathbb{Z} \subseteq \mathbb{Q}$ inclus dans K, c'est-à-dire les entiers algébriques dans K (c'est-à-dire qu'ils engendrent un module de type fini (mais attention, pas forcément engendré par les puissances d'un élément)), forme un sous-anneau de K. Cet

anneau est intègre, intégralement clos, son corps des fractions est K, il est noethérien et de Dedekind, *i.e.* les idéaux premiers non nuls et maximaux sont les mêmes. En particulier, il est principal si et seulement s'il est factoriel.

→ En outre, on sait que A_K est un $\mathbb{Z}$-module libre de rang $n = \dim_{\mathbb{Q}}(K)$ et l'on peut donc choisir e_1,...,e_n une $\mathbb{Z}$-base de A_K. Pour déterminer A_K, si $C = A[x]$ où x est K-primitif, $\check{C}$ le module dual des éléments y de K tels que $\mathrm{Tr}(yC) \subseteq A$, dont a montré qu'une base était $\left(\frac{x^i}{f'(x)}\right)$, on trouve un système de représentants (fini, par théorème !) $y_j\}$ de $\check{C}/C$ et $A_K = \langle x^i, y_j \in A_K \rangle$.

→ La norme et la trace d'un élément $x \in A_K$ retombe dans $\mathbb{Z}$. Il en est de même donc du discriminant absolu de $K/\mathbb{Q}$ ou de $A_K/\mathbb{Z}$. Celui-ci vaut $d = \det(\mathrm{Tr}_{K/\mathbb{Q}}(e_i e_j))$. Il vaut également $d = (\det(\sigma_i(e_j)))^2$. Si $K = \mathbb{Z}[\alpha]$, on a aussi $d = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(\mu'_{K,\alpha}(\alpha))$. On sait aussi que dans le cas où A_K est un réseau d'un certain $B \subseteq K$ d'indice m dans B, on a $d = m^2 \mathrm{Disc}(B/\mathbb{Z})$.

→ Si $\mathcal{P}$ est l'ensemble des idéaux premiers non nuls/maximaux de A_K, tout idéal fractionnaire I non nul/sous-module non nul de K de type fini se décompose sous la forme $I = \prod_{p \in \mathcal{P}} p^{v_p(I)}$. L'inverse d'un idéal entier m est l'idéal fractionnaire $m' = \{x \in K \mid xm \subseteq A_K\}$. On dispose de toutes les propriétés voulues sur la valuation. Ainsi, cet ensemble est un groupe abélien libre d'élément neutre A_K. Quotienté par le sous-groupe des idéaux fractionnaires principaux non nuls, on obtient encore un groupe abélien libre dit groupe de classes qui est trivial si et seulement si A_K est principal/factoriel.

→ Puisque K (et donc A_K) se plonge par σ dans $\mathbb{R}^n$, en l'identifiant à son image par σ, c'est un réseau de $\mathbb{R}^n$, *i.e.* un sous-groupe discret (donc fermé et cocompact) de rang maximal, *i.e.* engendré par une base de $\mathbb{R}^n$. Son volume, qui est celui de tout parallélotope, est $2^{-r_2}\sqrt{d}$. Si I est un idéal de A_K, le volume de $\sigma(I)$ est $\mathrm{vol}(\sigma(A_K))N(I)$. En particulier, si S une partie mesurable, convexe et symétrique de volume $> 2^{r_1+r_2}\sqrt{d}$, ou largement si S est de plus compact, alors S contient un élément non nul de A_K. On aurait aussi pu dire, si S est simple mesurable de volume $> 2^{-r_2}\sqrt{d}$, alors il existe deux éléments dans S dont la différence est dans le réseau.

→ Pour tout idéal I non nul de A_K, il existe $x \in I$ non nul de norme (qui est aussi la norme de $N(xA_K)$) inférieure à $M_K = N(I)$ où $M_K = c_K = \left(\frac{4}{\pi}\right) \frac{n!}{n^n} \sqrt{|d|}$. De plus, toute classe du groupe de classes contient un idéal entier de norme $N(I) \leqslant M_K$.

→ On en déduit que le discriminant d'un corps de nombres est majoré, ramifié et ne correspond toujours qu'à un nombre fini de corps de nombres une fois fixé.

→ Le groupe de classes est toujours fini, et de plus, ses idéaux sont souvent soumis à des relations (voir le cas important $n = 2$).

→ Le groupe des unités $A_K^\times$ est de la forme $G \times \mathbb{Z}^r$ où $r = r_1 + r_2 - 1$ et G est le groupe cyclique des racines de l'unité qui sont dans K, et l'on appelle unités fondamentales ε_1,...,ε_r des générateurs de chaque membre en $\mathbb{Z}$. Pour les trouver, il s'agit de résoudre une équation de Pell-Fermat dans le cas $n = 2$ car l'on en revient à un calcul de normes.

4.2.4 La décomposition des idéaux premiers dans une extension de corps

4.2.4.1 Décomposition des premiers dans les corps quadratiques

Soit d un entier sans facteur carré et K le corps quadratique associé. Soit A l'anneau de ses entiers. On rappelle que $A = \mathbb{Z}[\sqrt{d}]$ pour $d \equiv 2{,}3$ [4] et $A = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}$ pour $d \equiv 1$ [4]. Dans ce cas, pour tout p, $\frac{1+\sqrt{d}}{2} = \frac{1+p+(1+p)\sqrt{d}}{2} - p\frac{1+\sqrt{d}}{2} \in \mathbb{Z}[\sqrt{d}] + pA$.

Pour p un nombre premier impair, on cherche la décomposition en idéaux premiers de A de l'idéal pA, c'est-à-dire la décomposition de p. D'après le laïus précédent, on a toujours $A/pA \simeq \mathbb{Z}[\sqrt{d}]/p\mathbb{Z}[\sqrt{d}]$ où $\mathbb{Z}[\sqrt{d}] = \mathbb{Z}[X]/(X^2 - d)$, d'où $A/pA \simeq \mathbb{Z}[X]/(p, X^2 - d) \simeq (\mathbb{Z}/p\mathbb{Z})[X]((X^2 - \overline{d})$, chose déjà vue.

L'espace $(\mathbb{Z}/p\mathbb{Z})[X]/X^2 - \overline{d}$ est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension 2. Observons trois cas.

1. C'est un corps. Ceci arrive si et seulement si $X^2 - \overline{d}$ est irréductible, c'est-à-dire ssi $\overline{d}$ n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.
2. $\overline{d}$ est un carré non nul. Cela revient à dire que $X^2 - \overline{d}$ est le produit de deux polynômes de degré 1 unitaires distincts, soit, par le théorème dit chinois, si et seulement si $A/pA \simeq (\mathbb{Z}/p\mathbb{Z})^2$. C'est le produit de deux corps : il est réduit (c'est-à-dire sans nilpotents) mais pas intègre.
3. $\overline{d} = 0$. Alors $\mathbb{Z}/p\mathbb{Z}[X]/(X^2)$ est un anneau non réduit, car $\overline{X}$ est nilpotent.

Il est remarquable que ces trois conditions s'excluent mutuellement.

A priori, $pA = \mathfrak{p}_1^{r_1} ... \mathfrak{p}_k^{r_k}$ puis $A/pA = \prod_{i=1}^{k} A/p_i^{r_i}$ où $p_i \neq p_j$ pour $i \neq j$. Alors $|A/p_i^{r_i}| = N(p_i)^{r_i}$. D'où $\dim_{\mathbb{Z}/p\mathbb{Z}}(A/p_i^{r_i}) = r_i \dim_{\mathbb{Z}/p\mathbb{Z}}(A/p_i) \geqslant r_i$. De plus, $pA \subseteq p_i^{r_i}$ donc $A/p_i^{r_i}$ est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel et $2 = \dim_{\mathbb{Z}/p\mathbb{Z}}(A/pA) = \sum_{i=1}^{k} r_i \dim(A/p_i)$ implique $k = 1$ ou 2, car $2 \geqslant r_i \geqslant 1$ et $\dim(A/p_i) \geqslant 1$. Pour $k = 2$, cela donne $r_i = 1$ et $k = 1$ donne $r_i = 1$ ou 2. Ainsi, pour résumer :

1. *(p est inerte)* $pA = p_1$ donne $A/pA = A/p_1$ est un corps.
2. *(p est (totalement) décomposé)* $pA = p_1 p_2$ donne $A/pA \simeq A/p_1 \times A/p_2$ qui est un anneau non intègre mais réduit, *i.e.* sans nilpotents.
3. *(p est ramifié à proprement parler)* $pA = p_1^2$ donne $A/p_1 = A/p_1^2$ anneau non réduit par $cl(x)$ pour $x \in p_1 \setminus p^2$ qui est nilpotent.

Ces trois conditions s'excluent mutuellement et permettent de classifier p.

Exemple

Traitons le cas $p = 2$. Pour $d \equiv 2,3\ [4]$, comme avant, $A/2A \simeq \frac{\mathbb{Z}/2\mathbb{Z}[X]}{X^2-\overline{d}}$. Pour $d \equiv 2$, $\overline{d} = 0$ donc 2 est ramifié : $2A = p^2$. Pour $d \equiv 3$, $\overline{d} = 1$, on obtient $\mathbb{Z}/2\mathbb{Z}[X]/(X^2+1)$ où comme $X^2 + 1 = (X+1)^2$, 2 est ramifié soit encore $2A = p^2$. Maintenant, pour $d \equiv 1\ [4]$, $A = \mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \mathbb{Z}[X]/(X^2 - X + \frac{1-d}{4})$ d'où $A/2A = \frac{\mathbb{Z}/2\mathbb{Z}[X]}{X^2+X+\overline{\frac{1-d}{4}}}$. Si $\overline{\frac{1-d}{4}} = 0$, $X(X+1)$ donne le cas totalement décomposable et $2A = p_1p_2$ où $p_1 \neq p_2$. Si $\overline{\frac{1-d}{4}} = 1$, $X^2 + X + 1$ est irréductible et donne le cas inerte, et donc $2A$ est premier.

On cite un fait utile :

Fait

Soit A un anneau de Dedekind. Supposons que $N(I) = |A/I| = k$ un entier premier apparaissant dans une copie de $\mathbb{Z}$ dans I. Alors $kA \subseteq I$.

En effet, on a alors $k\,(A/I) = \{0\}$, ce qui équivaut à I divise kA, soit $kA \subseteq I$. Autrement dit, si I est premier, il est dans la décomposition de k.

4.2.4.2 Conséquence : une preuve du théorème des deux carrés

On se place ici dans le cas $K = \mathbb{Q}(i)$, $A = \mathbb{Z}[i]$ ses entiers.

Donnons la nature de pA pour p premier. Si $p = 2$, $2\mathbb{Z}[i] = p^2$ est ramifié. Si p est impaire, on sait que -1 est un carré modulo p si et seulement si $p \equiv 1\ [4]$. Ainsi, si $p = 1 + 4k$ pour un $k \in \mathbb{Z}$, on tombe sur le cas décomposé et $pA = p_1p_2$ pour $p_1 \neq p_2$. Si $p = 3 + 4k$ pour un $k \in \mathbb{Z}$, on tombe sur le cas inerte et pA est premier.

Proposition. ***(Fermat)***

Si $p \equiv 1\ [4]$, alors p est somme de deux carrés.

▷ $pA = p_1p_2$ avec $p_1 \neq p_2$ premiers non nuls d'après ce qui précède. Par suite, $p^2 = N(pA) = N(p_1)N(p_2)$. Or $N(p_i) > 1$, car $p_i \subsetneq A$, d'où $N(p_i) = p$. Or $A = \mathbb{Z}[i]$ est principal, donc il existe $a,b \in \mathbb{Z}$ tels que $p_i = (a+ib)$, d'où $N(p_i) = N(a+ib) = a^2 + b^2$ pour $i = 1,2$. Par produit, p est somme de deux carrés. ■

On peut conclure.

Théorème. ***(Deux carrés, Fermat)***

Soit $n \geqslant 1$ un entier. Il se décompose en $n = \prod_{p\in\mathcal{P}} p^{v_p(n)}$. Alors :

$$n \text{ est une somme de 2 carrés} \iff v_p(n) \text{ est paire pour tout premier } p \equiv 3\ [4].$$

▷ Notons S cet ensemble. C'est l'ensemble des normes d'éléments de $\mathbb{Z}[i]$. On sait également que S est multiplicative. Pour montrer la condition suffisante, il suffit donc de traiter le cas où n a un seul facteur premier. Successivement :

1. Pour $p = 2$, $p = 1^2 + 1^2$. C'est vrai pour toute puissance de deux également.
2. Pour $p \equiv 1$ [4], on applique la proposition précédente. C'est vrai pour toute puissance de p également, toujours par multiplicativité de S.
3. Pour $p \equiv 3$ [4], par hypothèse, p apparaît sous une valuation paire, et $p^{2k} = (p^k)^2 \in S$.

Montrons que la condition donnée est suffisante. Si $n = a^2 + b^2 = N(a + ib) = (a + ib)\overline{(a + ib)}$, $nA = \prod (pA)^{v_p(n)} = (a+ib)A.(a-ib)A$. Pour p congru à 3 modulo 4, pA est un idéal premier de A. Pour q premier différent de p, pA n'apparaît pas dans la décomposition primaire de qA, car sinon $qA \subseteq pA$ d'où $qA \cap \mathbb{Z} = q\mathbb{Z} \subseteq pA \cap \mathbb{Z} = p\mathbb{Z}$. Or $p \neq q$. Ainsi, $v_{pA}(nA) = v_p(n)$, pA étant un idéal premier ; or $(a + ib) = \prod p_i^{v_{p_i}(a+ib)}$ et $(a - ib) = \prod p_i^{v_{p_i}(a-ib)}$. Je dis que $v_{pA}((a + ib)) = v_{pA}((a - ib))$, car si $(pA)^k \mid (a+ib)$, $(pA)^k \mid \overline{a + ib} = (a_ib)$. Ainsi, $v_{pA}(n) = v_p(n) = v_{pA}(a+ib) + v_{pA}(a-ib) = 2v_{pA}(a+ib)$, qui est paire. ■

À propos. ***(Déclinaison du théorème des deux carrés)***

⋆ Cette façon de faire se décline profitablement pour montrer des variantes, et il y en a, du théorème des deux carrés. Le lecteur pourra, par exemple, s'entraîner à donner une condition pour qu'un nombre entier s'écrive sous la forme $a^2 + 3b^2$, a,$b \in \mathbb{Z}$.

4.3 Théorie analytique des nombres (TAN2)

4.3.1 Théorie multiplicative des nombres

4.3.1.1 Retour sur les nombres premiers

4.3.1.1.1 Carrés dans $\mathbb{Z}/p\mathbb{Z}$

Propriété. ***(Théorème de Fermat moitié)***

Soit p un nombre premier. Soit $a \in \mathbb{Z}/p\mathbb{Z}$ non nul. Alors

$$a^{\frac{p-1}{2}} = \begin{cases} 1 \text{ si } a \text{ est un carré modulo } p \\ -1 \text{ sinon.} \end{cases}$$

▷ Si a est un carré, on l'écrit $a = b^2$ avec $b \in a \in \mathbb{Z}/p\mathbb{Z}$ non nul, car $a \neq 0$. Alors $a^{\frac{p-1}{2}} = b^{p-1} = 1$ par le petit théorème de Fermat. Étudions le cas où a n'est pas un carré modulo p. Pour cela, adaptons la preuve du théorème de Wilson. On sait que le produit des éléments de $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ est égal à -1. De plus, pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, il existe un unique $y \in \mathbb{Z}/p\mathbb{Z}$ tel que $xy = a$, car $\mathbb{Z}/p\mathbb{Z}$ est un corps. Par hypothèse, on a toujours $x \neq y$. Ainsi, le produit $-1 = 1 \times 2 \times ... \times (p-1)$ se récrit sous la forme $(x_1y_1)...(x_{\frac{p-1}{2}}y_{\frac{p-1}{2}})$ avec donc $(p-1)/2$ couples et pour tout i, $x_iy_i = a$, d'où

$-1 = a^{\frac{p-1}{2}}$. ■

L'élégance de cette preuve arithmétique connaît une simplification notable en passant par les outils de l'algèbre.

Preuve.

▷ *(Autre méthode)* L'ensemble des carrés modulo p noté $(\mathbb{F}_p^\times)^2$ est un sous-groupe de $\mathbb{F}_p^\times$, car c'est l'image de l'endomorphisme $x \mapsto x^2$. Puisque son noyau est $\{\pm 1\}$, $\mathbb{F}_p$ étant intègre, on a de plus $(\mathbb{F}_p^\times)^2 \simeq {}^{\mathbb{F}_p^\times}\!/_{\{\pm 1\}}$, donc $(\mathbb{F}_p^\times)^2$ est d'indice 2. ■

Astuce !

On dispose donc d'une condition nécessaire et suffisante pour qu'un entier soit un carré dans un corps premier fini de caractéristique p : il est nul ou sa puissance $(p-1)/2$-ième égale 1.

Cette dichotomie « s'inverse » aisément pour obtenir le résultat suivant.

Propriété. ***(-1 est-il carré dans $\mathbb{Z}/p\mathbb{Z}$?)***

Soit p un nombre premier. Alors -1 est un carré modulo p si et seulement si

$$p \text{ est pair ou } p \equiv 1 \ [3].$$

▷ Le cas $p = 2$ se fait immédiatement. On a donc $p \equiv 1$ ou 3 $[3]$. Dans le premier cas, $\frac{p-1}{2} = 2q$ avec $q \in \mathbb{Z}$ et $(-1)^{2q} = 1$. Dans le second cas, $\frac{p-1}{2} = 1 + 2q'$ avec $q' \in \mathbb{Z}$ et $(-1)^{2q'+1} = 1$, d'où le résultat. ■

4.3.1.2 Critères de primalité

4.3.1.3 Fonction de zêta de Riemann et lien avec l'arithmétique

4.3.1.4 Théorème des nombres premiers

4.3.1.5 Le théorème de la progression arithmétique

4.3.2 Corps finis et arithmétique

4.3.2.1 Retours sur la théorie élémentaire des corps finis

4.3.2.2 Loi de réciprocité quadratique

4.3.2.3 Irréductibilité des polynômes à coefficients dans un corps fini

4.3.2.3.1 Algorithme de Cantor-Zassenhass

4.3.2.3.2 Algorithme de Berlekamp

4.3.3 Équations diophantiennes

4.3.3.1 Équation de Brahmagupta-Pell-Fermat

4.3.3.2 Grande équation de Fermat

4.3.3.3 Écriture d'un entier en sommes de carrés

Appendice