Cours introductif de M2
Théorie des Nombres

Jean-François Dat

2012-2013

Résumé

Ce cours est une introduction aux concepts et outils de base de la théorie algébrique des nombres : théorie des entiers, théorie des valuations, etc.

Table des matières

1 Introduction et survol

Les objets principaux que nous voulons étudier ici sont les *corps de nombres*, *i.e.* les extensions finies du corps des rationnels $\mathbb{Q}$. Ces corps peuvent être "plongés" (dans $\mathbb{C}$ ou dans une clôture algébrique $\overline{\mathbb{Q}}$ préalablement fixée), ou "abstraits".

Exemples.
- corps plongés : $\mathbb{Q}(i)$ "sous-corps de $\mathbb{C}$ engendré par i", ou plus généralement $\mathbb{Q}(e^{2i\pi/n})$.
- corps abstraits : $\mathbb{Q}[X]/(X^2+1)$ ou $\mathbb{Q}[X]/(X^3+X+1)$.

En fait, par la théorie générale des corps, on sait que :

i) tout corps de nombres abstrait peut être plongé dans $\mathbb{C}$ (théorème de d'Alembert : $\mathbb{C}$ est algébriquement clos.)

ii) tout corps de nombres plongé dans $\mathbb{C}$ est de la forme $\mathbb{Q}(\alpha)$ (théorème de l'élément primitif).

Notation. Pour un nombre algébrique $\alpha \in \mathbb{C}$, on note f_α son polynôme minimal, *ie* le générateur monique de l'idéal $\{f \in \mathbb{Q}[X],\ f(\alpha)=0\}$. On a alors un isomorphisme de corps $\mathbb{Q}[X]/(f_\alpha) \xrightarrow{\sim} \mathbb{Q}(\alpha)$ qui envoie X sur α.

Les outils principaux pour notre étude seront :
- la théorie de Galois (théorie des corps générale)
- la théorie des entiers (algèbre commutative)
- la théorie des valuations (analyse sur les corps).

1.1 Théorie de Galois (rappels et compléments)

Choisissons une clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$, par exemple la clôture de $\mathbb{Q}$ dans $\mathbb{C}$. Comme pour une extension finie, on note $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ le groupe des automorphismes du corps $\overline{\mathbb{Q}}$.

1.1.1 *Topologie de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. [1]

Si $K \subset \overline{\mathbb{Q}}$ est une extension *normale* de $\mathbb{Q}$ (*i.e.* pour tout $\alpha \in K$, P_α est scindé dans $K[X]$), alors tout automorphisme de $\overline{\mathbb{Q}}$ stabilise K, d'où une application de restriction

$$(*): \quad \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K/\mathbb{Q}),$$

dont on sait qu'elle est surjective.

1. Pour plus de détail on peut consulter les notes de cours de J. Milne "Fields and Galois theory" sur `www.jmilne.org/math/`

L'ensemble des extensions normales (=Galoisiennes puisqu'on est en caractéristique 0) est ordonné par inclusion, et filtrant pour cet ordre (car le composé de deux extensions normales est une extension normale).

Les applications $(*)$ sont compatible aux restrictions et définissent donc un morphisme :

$$\begin{aligned}\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow & \varprojlim_{K\subset\overline{\mathbb{Q}}} \mathrm{Gal}(K/\mathbb{Q}) \\ & := \{(\alpha_K)_K \in \prod_{K\subset\overline{\mathbb{Q}}} \mathrm{Gal}(K/\mathbb{Q}),\ \forall K'\subset K,\ (\alpha_K)_{|K'} = \alpha_{K'}\}\end{aligned}$$

Ce morphisme est bijectif. En effet cela découle du fait que $\overline{\mathbb{Q}}$ est réunion d'extensions finies Galoisiennes (tout élément de $\overline{\mathbb{Q}}$ appartient à une telle extension, par exemple le corps engendré par toutes les racines de son polynôme minimal).

La limite projective ci-dessus est un sous-espace fermé du produit $\prod_{K\subset\overline{\mathbb{Q}}} \mathrm{Gal}(K/\mathbb{Q})$, donc un espace profini (compact et totalement discontinu). De plus, le produit et l'inverse sont clairement continus pour cette topologie. *Nous avons donc muni* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *d'une structure de groupe topologique profini.*

Remarque. – Plus généralement, si L est une extension algébrique, séparable, et normale d'un corps F, alors $\mathrm{Gal}(L/F) = \varprojlim_{L'} \mathrm{Gal}(L'/F)$ où L' décrit les sous-extensions finies Galoisiennes, ce qui munit $\mathrm{Gal}(L/F)$ d'une topologie profinie. Si $(L_n)_{n\in\mathbb{N}}$ est une suite croissante de sous-corps, de réunion L, on a aussi $\mathrm{Gal}(L/F) = \varprojlim_n \mathrm{Gal}(L_n/F)$.

Exemple. $F = \mathbb{F}_p$ et $L = \overline{\mathbb{F}}_p$. On a ici $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \varprojlim_n \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$ (complétion profinie de $\mathbb{Z}$). Ici $\mathbb{N}$ est ordonné par divisibilité et les morphismes de transition sont les projections $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ pour $m|n$.

Le théorème fondamental de la théorie de Galois usuelle s'étend alors de la manière suivante (voir les notes de Milne "Fields and Galois Theory" chap. 7) :

1.1.2 Théorème.– *i) Si* $K \subset \overline{\mathbb{Q}}$ *est un sous-corps, alors* $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ *est un sous-groupe fermé de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *et* $\overline{\mathbb{Q}}^{\mathrm{Gal}(\overline{\mathbb{Q}}/K)} = K$.

ii) Si U *est un sous-groupe fermé de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *alors* $\overline{\mathbb{Q}}^U$ *est un corps et* $U = \mathrm{Gal}(\overline{\mathbb{Q}}/\overline{\mathbb{Q}}^U)$.

iii) Les deux procédés ci-dessus induisent une bijection décroissante entre sous-groupes fermés de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *et sous-corps de* $\overline{\mathbb{Q}}$, *qui envoie sous-groupes* distingués *sur extensions* normales *de* $\mathbb{Q}$ *et sous-groupes* ouverts *sur extensions* finies *de* $\mathbb{Q}$.

Moralité : l'études des corps de nombres est liée à l'étude du groupe topologique $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Voici quelques exemples de problèmes liés directement à ce groupe :

i) Problèmes inverses : étant donné un goupe fini simple, est-ce le groupe de Galois d'un corps de nombres ? Formulation équivalente : est-ce un quotient continu de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$? C'est un problème encore ouvert.

ii) Décrire l'abélianisé (topologique) de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$: c'est ce que fait le théorème de Kronecker-Weber, *cf* plus bas. Plus généralement, décrire l'abélianisé d'un sous-groupe ouvert $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$: c'est l'objet de la *théorie du corps de classes*.

iii) Etudier $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ via ses représentations linéaires continues. Par exemple, on sait associer à tout système d'équations algébriques (homogènes) à coefficients rationnels des représentations de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur des espaces vectoriels sur un corps fini ou ℓ-adique (cohomologie étale en géométrie algébrique). Le *programme de Langlands* est un vaste programme qui devrait permettre (grossièrement) de classifier les représentations de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ en termes d'autres objets plus analytiques ("représentations automorphes")

Attention. La nature profinie de la topologie de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ implique que tout sous-groupe ouvert est d'indice fini. Mais la réciproque est fausse. Par exemple, choisissons une suite infinie $p_1, p_2, \cdots$ de nombres premiers distincts et posons $K_n = \mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n})$ et $K = \bigcup_n K_n$. Alors $\mathrm{Gal}(K_n/\mathbb{Q}) \simeq \{\pm 1\}^n$ et $\mathrm{Gal}(K/\mathbb{Q}) = \varprojlim_n \mathrm{Gal}(K_n/\mathbb{Q}) \simeq \{\pm 1\}^{\mathbb{N}}$. Ce dernier groupe est un quotient continu de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. On sait par l'axiome du choix qu'il existe une application $\mathbb{F}_2$-linéaire *non continue* $\mathbb{F}_2^{\mathbb{N}} \longrightarrow \mathbb{F}_2$. Celle-ci fournit un quotient fini $\{\pm 1\}$ non topologique de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

1.1.3 *Extensions cyclotomiques.* Soit K un corps de caractéristique nulle et $\overline{K}$ une clôture algébrique. Notons $\mu_n \subset \overline{K}$ le groupe des racines n-èmes de l'unité. Le corps engendré $K(\mu_n)$ est Galoisien. Si ζ_n est une racine n-ème primitive de l'unité, on a un morphisme de groupe

$$\chi_{n,K} : \mathrm{Gal}(K(\mu_n)/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

qui envoie σ sur l'unique élément $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que $\sigma(\zeta_n) = \zeta_n^a$ (ne dépend pas du choix de ζ_n). Si $m|n$, la restriction $\mathrm{Gal}(K(\mu_n)/K) \longrightarrow \mathrm{Gal}(K(\mu_m)/K)$ correspond à l'application évidente $(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$.

Soit alors $K(\mu_\infty) := \bigcup_n K(\mu_n)$ l'extension de K engendrée par toutes les racines de l'unité. Les morphismes ci-dessus induisent un morphisme continu de groupes topologiques :

$$\chi_K : \mathrm{Gal}(K(\mu_\infty)/K) \longrightarrow \hat{\mathbb{Z}}^\times.$$

1.1.4 Théorème.– *Pour $K = \mathbb{Q}$, on a :*

i) $\chi_{\mathbb{Q}}$ *est un isomorphisme* $\mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) \xrightarrow{\sim} \hat{\mathbb{Z}}^\times$.

ii) (Kronecker-Weber) L'application de restriction $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q})$ *induit un isomorphisme* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})_{\mathrm{ab}} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q})$.

Le point i) revient à prouver que les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}$, ce que nous ferons plus bas.

Dans le point ii), l'abélianisé est au sens topologique : c'est le quotient par *l'adhérence* du sous-groupe engendré par les commutateurs. Le point ii) équivaut à dire que toute extension Galoisienne abélienne de $\mathbb{Q}$ se plonge dans une extension cyclotomique de $\mathbb{Q}$. Ceci n'est pas vrai en général pour les autres corps de nombres.

1.2 Entiers algébriques

Soit K un corps de nombres. On dit que $\alpha \in K$ est *entier* s'il existe $f \in \mathbb{Z}[X]$ tel que $f(\alpha) = 0$. Ceci équivaut en fait à ce que $f_\alpha \in \mathbb{Z}[X]$ en vertu de l'exercice suivant.

Exercice. – Soit $f \in \mathbb{Z}[X]$ ayant une factorisation $f = gh$ dans $\mathbb{Q}[X]$. Alors $g, h \in \mathbb{Z}[X]$.

La théorie générale des *extensions entières* nous montrera :

1.2.1 Proposition.– *Soit $\mathcal{O}_K$ l'ensemble des éléments entiers de K. Alors*

i) *$\mathcal{O}_K$ est un sous-anneau de K.*

ii) $\mathrm{Frac}(\mathcal{O}_K) = K$

iii) *$\mathcal{O}_K$ est de type fini en tant que $\mathbb{Z}$-module.*

Remarque. – La preuve usuelle de i) est non-constructive. On peut se demander s'il existe un moyen de trouver des polynômes annulant $\alpha + \beta$ ou $\alpha\beta$, connaissant f_α et f_β. La réponse est oui si on utilise le résultat intéressant suivant :

$$(*) : \mathbb{Z}[X_1, \cdots, X_n]^{\mathfrak{S}_n} \simeq \mathbb{Z}[\Sigma_1, \cdots, \Sigma_n]$$

où $\Sigma_1, \cdots, \Sigma_n$ sont les polynômes symétriques élémentaires en $X_1, \cdots, X_n$ donnés par l'égalité $\prod_{i=1}^n (T - X_i) = T^n - \Sigma_1 T^{n-1} + \cdots + (-1)^n \Sigma_n$.

En effet $(*)$ implique que si $f \in \mathbb{Z}[X]$ a pour racines $\alpha_1, \cdots, \alpha_n \in \overline{\mathbb{Q}}$, alors pour tout $g \in \mathbb{Z}[X_1, \cdots, X_n]$, le polynôme $\widetilde{g}(X) := \prod_{\sigma \in \mathfrak{S}_n} (X - g(\alpha_1, \cdots, \alpha_n))$ est dans $\mathbb{Z}[X]$. En choisissant $f = f_\alpha f_\beta$ et $g = X_1 + X_2$, resp. $g = X_1 X_2$, on obtient $\widetilde{g}(\alpha + \beta) = 0$, resp. $\widetilde{g}(\alpha\beta) = 0$ (mais bien-sûr on reste loin du polynôme minimal en général).

Puisque $\mathbb{Z}$ est principal, les points ii) et iii) de la proposition montrent que $\mathcal{O}_K$ est libre de rang $[K : \mathbb{Q}]$ sur $\mathbb{Z}$. Ceci nous amène au premier problème naturel qui se pose.

1.2.2 *Problème 1 : trouver une base de $\mathcal{O}_K$.* L'outil principal sera la théorie du discriminant. En attendant voici un exemple illustrant la complexité du problème :

Exemple. – (cas quadratique) On suppose $[K : \mathbb{Q}] = 2$. On voit alors facilement qu'il existe un unique entier d sans facteur carré tel que $K = \mathbb{Q}(\sqrt{d})$. Il est clair que $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ mais en général $\mathbb{Z}[\sqrt{d}] \neq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Par exemple :

- $d = -1$. Dans ce cas $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$. En effet $\alpha = a + ib$ est entier si et seulement si $\alpha + \bar{\alpha} = 2a$ et $\alpha\bar{\alpha} = a^2 + b^2$ sont dans $\mathbb{Z}$, et il est élémentaire d'en conclure que a et b sont alors aussi dans $\mathbb{Z}$ (exercice).
- $d = -3$. Dans ce cas l'élément $j = \frac{-1+i\sqrt{3}}{2}$ est entier ($j^3 = 1$) mais pas dans $\mathbb{Z}[\sqrt{-3}]$.

Nous montrerons plus généralement que $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}] = \mathbb{Z} \oplus \sqrt{d}\mathbb{Z}$ si $d \equiv 2, 3[4]$ et $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z} \oplus \frac{1+\sqrt{d}}{2}\mathbb{Z}$ si $d \equiv 1[4]$.

Exemple. – (Cas cyclotomique) Nous verrons que $\mathcal{O}_{\mathbb{Q}(\mu_n)} = \mathbb{Z}[\mu_n] = \mathbb{Z} \oplus \zeta_n\mathbb{Z} \oplus \cdots \oplus \zeta_n^{\varphi(n)-1}\mathbb{Z}$ où $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

Remarque. – Dans les exemples ci-dessus, $\mathcal{O}_K$ était monogène (de la forme $\mathbb{Z}[\alpha]$), mais il existe des K pour lesquels $\mathcal{O}_K$ n'est pas monogène.

1.2.3 *Problème 2 : contrairement à $\mathbb{Z}$, $\mathcal{O}_K$ n'est pas toujours principal.* Ni même factoriel (unique factorisation). Illustrons ce qui peut se passer par l'exemple des corps quadratiques.

Exemple. – Supposons $K = \mathbb{Q}(\sqrt{d})$.

i) Si $d = -1$, un argument de type division euclidienne montre que $\mathcal{O}_K = \mathbb{Z}[i]$ est principal (et donc factoriel). En effet, si $I \subset \mathbb{Z}[i]$ est un idéal et $\beta \in I \setminus \{0\}$ est choisi de norme complexe minimale, alors pour tout $\alpha \in \mathbb{Z}[i]$, on peut choisir $\gamma \in \mathbb{Z}[i]$ tel que $|\gamma - \frac{\alpha}{\beta}|^2 \leqslant 1/2$ (dessin !). Si $\alpha \in I$, alors $\alpha - \beta\gamma$ est un élément de I de norme $< |\beta|$, donc nul. D'où $I = (\beta)$.

ii) Si $d = -5$, on constate que $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Or, chacun des nombres 2, 3, $1 + \sqrt{-5}$ et $1 - \sqrt{-5}$ est *irréductible*[2]. En effet, soit $N(\alpha) \in \mathbb{Z}$ la norme de α (*ie* $N(a + \sqrt{-5}b) = a^2 + 5b^2$). On voit que $N(\alpha) = \pm 1 \Leftrightarrow \alpha \in \mathcal{O}_K^\times$ (auquel cas $\alpha^{-1} = N(\alpha)/\bar{\alpha}$). Comme $N(1 + \sqrt{-5}) = 6$, si $1 + \sqrt{-5} = \alpha\beta$ avec α, β non-inversibles, on doit avoir $N(\alpha) = 2$ ou $N(\beta) = 2$, ce qui est impossible. Ceci montre l'irréductibilité de $1 + \sqrt{-5}$ et de même on vérifie celle des 3 autres éléments ci-dessus. Finalement, les deux factorisations de 6 du début montrent bien que $\mathcal{O}_K$ *n'est pas factoriel* dans ce cas.

Il n'est *pas principal* non plus ; considérons l'idéal $\mathcal{I} = (2, 1 + \sqrt{-5})$. Ce n'est pas l'idéal unité car $\mathcal{O}_K/\mathcal{I} = \mathbb{Z}[X]/(X^2+5, 1+X, 2) = \mathbb{F}_2[X]/(X+1, (X+1)^2) = \mathbb{F}_2 \neq 0$. Il n'est pas principal, puisque 2 et $1+\sqrt{-5}$ sont irréductibles et non-équivalents, donc n'ont pas de facteur commun.

Pour étudier les anneaux d'entiers, l'idée fondamentale, qui remonte à Dedekind, est de s'intéresser aux *idéaux* plutôt qu'aux nombres eux-mêmes, et aux *idéaux premiers* plutôt qu'aux éléments irréductibles. En effet, on montrera :

THÉORÈME. – *Tout idéal non nul $\mathcal{I}$ de $\mathcal{O}_K$ se factorise de manière "unique" en un produit $\mathcal{I} = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\cdots\mathcal{P}_r^{e_r}$ où les $\mathcal{P}_i$ sont des idéaux premiers deux à deux distincts.*

Exemple. – Dans l'exemple ii) ci-dessus, l'idéal (2) n'est pas premier, bien que 2 soit un élément irréductible. Il se décompose $(2) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})$. (En effet $2 = (1 + \sqrt{-5})(1 - \sqrt{-5}) - 2 \times 2$.)

Le défaut de principalité de $\mathcal{O}_K$ est mesuré par son *groupe de classes* $\mathcal{C}\ell(\mathcal{O}_K)$. Celui-ci est le quotient du groupe multiplicatif formé par les idéaux non nuls par le sous-groupe engendré par les idéaux principaux. Par exemple on peut montrer que $\mathcal{C}\ell(\mathbb{Z}[\sqrt{-5}]) = \mathbb{Z}/2\mathbb{Z}$. C'est un problème généralement difficile que de calculer ce groupe. Un des résultats les plus profonds de ce cours sera :

2. Un élément a d'un anneau est "irréductible" si $a = bc \Rightarrow (b \in A^\times$ ou $c \in A^\times)$ pour tous b, c. Deux éléments irréductibles a, a' sont "équivalents" s'il existe $b \in A^\times$ tel que $a' = ab$.

THÉORÈME. (Dirichlet, Dedekind, Minlowski) – *$\mathcal{C}\ell(\mathcal{O}_K)$ est un groupe fini.*

1.2.4 *Problème 3 : décomposer (p) en un produit d'idéaux premiers.* Ici p est un nombre premier. C'est l'un des problèmes fondamentaux du sujet, qui n'a pas de solution générale. Ecrivons $(p) = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\cdots\mathcal{P}_r^{e_r}$ la décomposition cherchée. On montrera les faits généraux suivants :

- Si $f_i := [\mathcal{O}_K/\mathcal{P}_i : \mathbb{F}_p]$, alors $[K:\mathbb{Q}] = \sum_{i=1}^r e_i f_i$.
- Si K est Galoisienne, alors $e_1 = e_2 = \cdots = e_r$ et $f_1 = f_2 = \cdots = f_r$.

On introduira aussi la terminologie suivante :

- p est dit "ramifié" s'il existe i tel que $e_i \neq 1$. Ces p là sont "détectés" par le discriminant et sont en nombre fini.
- p est dit "totalement décomposé" si $r = [K:\mathbb{Q}]$
- p est dit "inerte" s'il est non ramifié et $r = 1$, *i.e.* si (p) est un idéal premier de $\mathcal{O}_K$.

Une question beaucoup moins ambitieuse serait de caractériser les premiers qui sont totalement décomposés dans $\mathcal{O}_K$. Une règle précise sera donnée pour les extensions cyclotomiques et quadratiques (ou, plus généralement, abéliennes), mais en général seule une estimée (Thm de densité de Chebotarev) est disponible.

Exemples. – Considérons le cas K quadratique. Dans ce cas on a trois possibilités : (p) est premier, $(p) = \mathcal{P}_1\mathcal{P}_2$, ou $(p) = \mathcal{P}^2$. Supposons pour simplifier que $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Alors $\mathcal{O}_K/(p) = \mathbb{F}_p[X]/(X^2+d)$. On a alors trois cas :

- Si $p|d$ ou $p = 2$, alors $\mathcal{O}_K/(p)$ est non-réduit donc p est ramifié.
- Si $d \in (\mathbb{F}_p^\times)^2$ alors p est décomposé. Concrètement, si a est tel que $p|a^2 - d$, alors $(p) = (p, \sqrt{d} - a)(p, \sqrt{d} + a)$.
- Si d n'est pas un carré modulo p, alors p est inerte.

On voit que la dichotomie inerte-décomposé fait intervenir la *loi de réciprocité quadratique.*

$$p \text{ décomposé } \Leftrightarrow \left(\frac{d}{p}\right) = 1 \Leftrightarrow p \text{ satisfait certaines congruences.}$$

Par exemple, on trouve que p est décomposé dans $\mathbb{Z}[i]$ si $p \equiv 1[4]$ et inerte si $p \equiv 3[4]$. Pour $d = -5$, on trouve que p est décomposé si $p \equiv 1, 3, 7, 9[20]$ et inerte si $p \equiv 11, 13, 17[20]$.

Le symbole au milieu de l'équivalence ci-dessus est le *symbole de Legendre* qui vit dans $\{\pm 1\}$. Pendant des décennies, les mathématiciens ont essayé de généraliser cette caractérisation des premiers décomposés par des conditions de congruences. En fait, ce n'est pas possible en général, mais la *théorie du corps de classes* le fait pour toute extension *abélienne* K d'un corps de nombres L. De manière très grossière, si $\mathcal{P}$ est un idéal premier de $\mathcal{O}_L$, on lui associe son *symbole d'Artin* $\left(\frac{K/L}{\mathcal{P}}\right) \in \mathrm{Gal}(L/K)$ et on a des équivalences

$$\mathcal{P} \text{ totalement décomposé } \Leftrightarrow \left(\frac{K/L}{\mathcal{P}}\right) = 1 \Leftrightarrow \mathcal{P} \text{ satisfait certaines "congruences".}$$

La seconde équivalence fait partie de la "loi de réciprocité d'Artin", vaste généralisation de la loi de réciprocité quadratique.

Dans ce cours nous nous contenterons du cas $L = \mathbb{Q}$ et nous prouverons en particulier la loi de réciprocité quadratique.

1.2.5 *Problème 4 : déterminer $\mathcal{O}_K^\times$.* C'est encore un problème difficile et toujours étudié de nos jours. La torsion $(\mathcal{O}_K^\times)_{\text{tors}}$ est un groupe de racines de l'unité, donc cyclique. Si K admet un plongement réel, on a simplement $(\mathcal{O}_K^\times)_{\text{tors}} = \mathbb{Z}/2\mathbb{Z}$.

Nous démontrerons le fameux théorème des unités de Dirichlet :

THÉORÈME. – *$\mathcal{O}_K^\times$ est un groupe abélien de type fini de rang $r-1$ où r est le nombre de plongements $K \longrightarrow \mathbb{C}$ modulo conjugaison.*

Par exemple, on voit que $\mathcal{O}_K^\times$ est fini si et seulement si K est quadratique imaginaire.

Le problème qui reste difficile est de trouver un *système d'unités fondamentales*, *ie* $r-1$ unités qui engendrent le quotient $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)_{\text{tors}}$.

Exemple. – $\mathbb{Z}[\sqrt{3}]^\times = \{\pm 1\} \times (2+\sqrt{3})^{\mathbb{Z}}$.

1.3 Théorie des valuations (normes)

Une norme (ou valuation multiplicative) sur un corps K est une application $|.| : K \longrightarrow \mathbb{R}_+$ telle que pour tout x, y on a

- $|xy| = |x||y|$
- $|x+y| \leqslant |x| + |y|$
- $|x| = 0 \Leftrightarrow x = 0$.

A une telle norme on associe la topologie engendrée par les boules ouvertes. Deux normes sont équivalentes si elles définissent la même topologie, les classes d'équivalences sont appelées *places de K.*

Exemple. – Sur $\mathbb{Q}$, on a la valeur absolue usuelle, que l'on note $|.|_\infty$, et pour chaque premier p, on a la norme p-adique définie par $|x|_p = p^{-r}$ si $x = p^r \frac{a}{b}$ avec $(a,p) = (b,p) = 1$.

Les normes p-adiques vérifient une version plus forte du deuxième axiome : pour tous x, y, on a $|x+y|_p \leqslant \max(|x|_p, |y|_p)$. De telles normes sont dites "non-archimédiennes". On montrera le théorème classique :

1.3.1 THÉORÈME. (Ostrowski)– *Sur $\mathbb{Q}$, toutes les normes sont équivalentes à $|.|_\infty$ ou une norme $|.|_p$.*

Autrement dit {places de $\mathbb{Q}$} = {nbres premiers} $\cup$ $\{\infty\}$. Plus généralement, pour un corps de nombres K on verra que

$$\{\text{places de } K\} = \{\text{idéaux premiers de } \mathcal{O}_K\} \cup \{\text{plongements } K \hookrightarrow \mathbb{C}\}_{/\text{conj}}.$$

Il y a une analogie intéressante avec les corps de fonctions : en effet on montre aussi que :

$$\begin{aligned}\{\text{places de } \mathbb{C}(X)\} &= \{\text{idéaux premiers de } \mathbb{C}[X]\} \cup \{f \mapsto \deg(f)\} \\ &= \{\text{points de la droite affine complexe}\} \cup \{\text{point à l'infini}\} \\ &= \mathbb{P}^1(\mathbb{C})\end{aligned}$$

et plus généralement pour le corps des fonctions méromorphes $\mathcal{M}(S)$ d'une surface de Riemann S, on a

$$\{\text{places de } \mathcal{M}(S)\} = S.$$

Ainsi on peut penser à l'ensemble des places d'un corps de nombre comme à une "complétion" ou "compactification" de l'ensemble des idéaux premiers de son anneau d'entiers.

1.3.2 *Complétion.* On sait bien que $\mathbb{Q}$ n'est pas complet pour $|.|_\infty$ et que le complété est (par définition) $\mathbb{R}$. De même, $\mathbb{Q}$ n'est pas complet pour $|.|_p$ et le complété se note $\mathbb{Q}_p$ et est appelé "corps des nombres p-adiques". C'est un corps localement compact, sur lequel on peut faire de l'analyse comme sur $\mathbb{R}$.

Applications :
- La décomposition de (p) dans $\mathcal{O}_K$ se "lit" sur $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$. Par exemple, p est totalement décomposé si et seulement si $K \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \mathbb{Q}_p^{[K:\mathbb{Q}]}$.
- Pour montrer qu'une équation algébrique sur $\mathbb{Q}$ n'a pas de solution, il suffit de trouver p tel que cette équation n'a pas de solution dans $\mathbb{Q}_p$. L'avantage est que l'on peut utiliser des outils analytiques dans $\mathbb{Q}_p$.

1.3.3 *Adèles.* On peut maintenant mettre tous les complétés ensemble en définissant

$$\mathbb{A} := \mathbb{R} \times \prod_p{}' \mathbb{Q}_p$$

où le $\prod'$ (produit restreint) désigne les éléments du produit dont presque toutes les composantes sont entières (dans $\mathbb{Z}_p$). On obtient un anneau localement compact. Si S est un ensemble fini de places, on définit aussi $\mathbb{A}_S$ comme le produit restreint ci-dessus auquel on enlève les facteurs indexés par S. Si le temps le permet nous montrerons :

PROPOSITION. – *i) L'image du plongement $\mathbb{Q} \hookrightarrow \mathbb{A}$ est discrète et cocompacte.*
ii) (approximation forte) l'image du plongement $\mathbb{Q} \hookrightarrow \mathbb{A}^S$ est dense pour tout $S \neq \emptyset$.

Pour un corps de nombre, on définit $\mathbb{A}_K := \mathbb{A} \otimes_{\mathbb{Q}} K$ qui est aussi le produit restreint des complétés de K en toutes ses places. Le symbole d'Artin fournit un morphisme

$$K^\times \backslash \mathbb{A}_K^\times \longrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/K)_{\mathrm{ab}}$$

qui dans le cas $K = \mathbb{Q}$ redonne l'isomorphisme $\hat{\mathbb{Z}}^\times \simeq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})_{\mathrm{ab}}$ mentionné plus haut (théorème de Kronecker-Weber).

2 Algèbre commutative

Pour plus de détails sur l'algèbre commutative, on pourra consulter le livre de D. Eisenbud "Commutative Algebra, with a view towards Algebraic Geometry".

2.1 Rappels et compléments

Sauf mention contraire, tous les anneaux considérés ici seront *unitaires* et *commutatifs*. On rappelle qu'un tel anneau est dit *intègre* si $\forall x, y \in A, (xy = 0) \Rightarrow (x = 0 \text{ ou } y = 0)$.

2.1.1 *Idéaux.* Soit A un anneau, I et J deux idéaux de A.

Opérations sur les idéaux : on définit la *somme* et le *produit* de I et J par

$$I + J = \{i + j,\ i \in I, j \in J\} \text{ et } IJ = \left\{ \sum_{k=1}^{n} i_k j_k,\ i_1, \cdots, i_n \in I, j_1, \cdots, j_n \in J \right\}$$

Ce sont aussi des idéaux. Noter que IJ est l'idéal engendré par l'ensemble $\{ij, i \in I, j \in J\}$, et que $IJ \subset I \cap J$. Le *lemme Chinois* nous dit que si $I + J = A$ (on dit que I et J sont *premiers entre eux*), alors $IJ = I \cap J$ et l'application canonique

$$A/IJ \longrightarrow A/I \times A/J$$

est bijective. Par ailleurs, on définit le *radical* de I

$$\sqrt{I} : \{x \in A, \exists n, x^n \in I\},$$

qui est encore un idéal de A, contenant I. On rappelle que A est dit *réduit* si $\sqrt{(0)} = (0)$.

Propriétés de finitude : I est *principal* (ou encore *monogène*) s'il est de la forme $I = (a) := Aa$ pour un élément a. L'anneau A est dit *principal* si tous ses idéaux le sont. Par ailleurs, I est *de type fini* s'il est engendré par un nombre fini d'éléments, *i.e.* somme d'un nombre fini d'idéaux principaux : $I = (a_1) + \cdots + (a_n)$. L'anneau A est dit *noethérien* si tous ses idéaux sont de type fini. Ceci équivaut à ce que *toute suite croissante d'idéaux soit stationnaire.*

Primalité, maximalité : l'idéal $I = A$ est appelé *idéal unité.* Les autre idéaux sont dits *propres.* Un idéal I est dit *maximal* si c'est un idéal maximal pour l'inclusion parmi les idéaux propres. Ceci équivaut à ce que A/I *soit un corps.* On note $\mathrm{Max}(A)$ l'ensemble des idéaux maximaux de A. Un idéal I est dit *premier* si $\forall x, y \in A$, $xy \in I \Rightarrow x \in I$ ou $y \in I$, ce qui équivaut à : A/I *est intègre.* On note $\mathrm{Spec}(A)$ l'ensemble des idéaux premiers de A.

2.1.2 *Divisibilité et factorisations.* Soit A un anneau *intègre*, $a, b \in A$.

Divisibilité : On dit que a divise b (notation $a|b$) si $(b) \subseteq (a)$, et divise *strictement* b si $(b) \subsetneq (a)$. On dit que a est *irréductible* s'il est non-inversible, non-nul, et n'a pas de diviseur strict non-inversible. Il est clair que

$$((a) \text{ idéal premier}) \Rightarrow (a \text{ irréductible}),$$

mais la réciproque est fausse (*cf* $a = 2$ dans $A = \mathbb{Z}[\sqrt{-5}]$).

PROPOSITION. – *Si A est noethérien, tout élément non-inversible et non-nul est produit d'éléments irréductibles ("factorisable").*

Démonstration. Puisque A est noethérien, l'ensemble E de tous les idéaux de la forme (a) avec a non factorisable admet un élément maximal, disons $I = (a)$, *s'il est non-vide*. Par hypothése, a n'est pas irréductible donc possède un diviseur strict b non inversible. Si c est tel que $a = bc$, alors c est aussi un diviseur non-inversible de a. Par choix de a, les éléments b et c sont factorisables. Donc a aussi : contradiction. □

Remarque : l'hypothèse noethérienne est nécessaire. Par exemple dans $\overline{\mathbb{Z}} = \{\alpha \in \overline{\mathbb{Q}}, \alpha \text{ entier}\}$, il n'y a *aucun* élément irréductible, puisque tout α non-inversible est strictement divisible par $\sqrt{\alpha}$.

Un anneau A noethérien est dit *factoriel* si la factorisation de tout élément a de A est *unique*, à l'ordre près. (En anglais A est un *Unique Factorization Domain* (UFD)).

2.1.3 *Localisation.* Soit A un anneau.

Définition : Un sous-ensemble $S \subset A$ est une *partie multiplicative* de A si $1 \in S$ et $\forall s, t \in S$, $st \in S$. Le *localisé de A en S* est l'anneau

$$S^{-1}A := \left\{\frac{a}{s}, a \in A, s \in S\right\}_{/\sim} \text{ où } \frac{a}{s} \sim \frac{a'}{s'} \text{ si } \exists t \in S,\ t(sa' - s'a) = 0$$

dans lequel le produit est donné par $\frac{a}{s}\frac{a'}{s'} = \frac{aa'}{ss'}$ et l'addition par $\frac{a}{s} + \frac{a'}{s'} = \frac{as'+a's}{ss'}$. On a un morphisme canonique $A \xrightarrow{can} S^{-1}A$, $a \mapsto \frac{a}{1}$.

Exemples :

- Si A est intègre, $S := A \setminus \{0\}$ est une partie multiplicative et $S^{-1}A$ est un corps noté $\mathrm{Frac}(A)$ (corps des fractions de A). Dans ce cas, tout localisé $S'^{-1}A$ est naturellement un sous anneau de $\mathrm{Frac}(A)$. (Si A n'est pas intègre, l'ensemble S des éléments *non-diviseurs de* 0 forme une partie multiplicative dont le localisé $S^{-1}A$ est un anneau Artinien contenant A, mais pas tous ses localisés.)
- Si $\mathcal{P}$ est un idéal premier, $S := A \setminus \mathcal{P}$ est multiplicative et $S^{-1}A$ se note $A_{\mathcal{P}}$. Par exemple
$$\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbb{Q},\ (b, p) = 1\right\}.$$
- Si $f \in A$, l'ensemble $S := \{f^n, n \in \mathbb{N}\}$ est une partie multiplicative et $S^{-1}A$ se note $A[f^{-1}]$. Par exemple
$$\mathbb{Z}[p^{-1}] = \left\{\frac{a}{b} \in \mathbb{Q},\ b \in p^{\mathbb{N}}\right\}.$$

  En général, on a $A[f^{-1}] = 0$ si f est nilpotent.

Propriétés :
- Les idéaux de $S^{-1}A$ sont tous de la forme $S^{-1}I$ pour I idéal de A.
- L'application $\mathcal{P} \mapsto can^{-1}(\mathcal{P})$ est une bijection de $\mathrm{Spec}(S^{-1}A)$ sur $\{\mathcal{Q} \in \mathrm{Spec}(A), S \cap \mathcal{Q} = \emptyset\}$. La bijection réciproque est $\mathcal{Q} \mapsto S^{-1}\mathcal{Q}$.
- cas particulier : les idéaux premiers de $A_{\mathcal{P}}$ correspondent aux idéaux premiers de A contenus dans $\mathcal{P}$. En conséquence, $A_{\mathcal{P}}$ est *local* (1 seul idéal maximal) et son idéal maximal est $\mathcal{P}A_{\mathcal{P}}$ (notation abusive pour $can(\mathcal{P})A_{\mathcal{P}}$).

2.1.4 *Anneaux locaux.* Soit A un anneau local, $\mathfrak{m}$ son idéal maximal. On a clairement $\mathfrak{m} = A \setminus A^\times$.

LEMME. (Nakayama) – *Soit M un A-module de type fini. Si $\mathfrak{m}M = M$ alors $M = 0$.*

Ici $\mathfrak{m}M$ est le A-sous-module engendré par $\{am, a \in \mathfrak{m}, m \in M\}$, donc explicitement $\mathfrak{m}M = \{\sum_{k=1}^n a_k m_k,\ a_1, \cdots, a_n \in \mathfrak{m}, m_1, \cdots, m_n \in M\}$.

Démonstration. Supposons $M \neq 0$. Soit $e_1, \cdots, e_r$ une famille génératrice minimale de M. Puisque $e_1 \in \mathfrak{m}M$, on peut écrire $e_1 = a_1 e_1 + \cdots + a_r e_r$ avec $a_1, \cdots, a_r \in \mathfrak{m}$. On a donc $(1 - a_1)e_1 \in Ae_2 + \cdots + Ae_r$. Or, $1 - a_1$ est inversible, donc $e_1 \in Ae_2 + \cdots + Ae_r$ ce qui contredit la minimalité de la famille génératrice. □

2.1.5 *Produits tensoriels.* Soit A un anneau et M, N deux A-modules.

Définition : le *produit tensoriel de M et N au-dessus de A* est un A-module noté $M \otimes_A N$ muni d'une application A-bilinéaire notée

$$\begin{array}{ccc} M \times N & \to & M \otimes_A N \\ (m, n) & \mapsto & m \otimes n \end{array}$$

qui est *universelle* au sens où pour tout A-module E, l'application

$$\mathrm{Hom}_A(M \otimes_A N, E) \longrightarrow \mathrm{Bil}_A(M \times N, E)$$

donnée par $\varphi \mapsto ((m, n) \mapsto \varphi(m \otimes n))$ est bijective. En d'autres termes, le couple $(M \otimes_A N, (m, n) \mapsto m \otimes n)$ (admettant qu'il existe) représente un foncteur sur la catégorie des A-modules et, à ce titre, est unique à isomorphisme unique près. Reste à le construire.

Construction : on quotiente le A-module libre de base l'ensemble des symboles $m \otimes n$ pour $m \in M, n \in N$ par le sous-module engendré par les éléments de la forme $am \otimes n - a(m \otimes n)$ ou $m \otimes an - a(m \otimes n)$ ou $(m_1 + m_2) \otimes n - m_1 \otimes n - m_2 \otimes n$ ou $m \otimes (n_1 + n_2) - m \otimes n_1 - m \otimes n_2$.

Propriétés :

i) Si M et N sont libres de rang fini sur A, de base $m_1, \cdots, m_r$ et $n_1, \cdots, n_s$, alors $M \otimes_A N$ est libre de base $(m_i \otimes m_j)_{i=1,\cdots,r\ j=1,\cdots,s}$. En particulier $\dim_A(M \otimes_A N) = \dim_A(M) \dim_A(N)$.

ii) Si B est une A-algèbre, $B \otimes_A M$ est naturellement un B module appelé *extension des scalaires* de M à B. L'action est donnée par $b'(b \otimes m) = (b'b) \otimes m$. Le foncteur $M \mapsto B \otimes_A M$

est adjoint à gauche du foncteur de restriction des scalaires, ce qui signifie en particulier que

$$\mathrm{Hom}_B(B \otimes_A M, N) \simeq \mathrm{Hom}_A(M, N)$$

pour tout B-module N et tout A-module M.

Cas particulier :

- Si $B = A/I$ est un quotient de A, alors $B \otimes_A M \simeq M/IM$.
- Si $B = S^{-1}A$ est un localisé de A, alors $B \otimes_A M \simeq S^{-1}M$ où $S^{-1}M$ est défini de manière analogue à $S^{-1}A$.
- Si $B = A_{\mathcal{P}}$ pour $\mathcal{P} \in \mathrm{Spec}(A)$, on note aussi $M_{\mathcal{P}} := A_{\mathcal{P}} \otimes_A M$.

iii) Si B et C sont deux A-algèbres, alors $B \otimes_A C$ est naturellement une A-algèbre. Le produit est donné par $(b \otimes c)(b' \otimes c') = (bb') \otimes (cc')$.

Cas particulier : $B \otimes_A A[X] \simeq B[X]$.

2.1.6 *Produits tensoriels de corps.* Soit K un corps de nombres et L un corps de caractéristique nulle. Le produit tensoriel $K \otimes_{\mathbb{Q}} L$ est une L-algèbre séparable de dimension finie donc se décompose en un produit de corps. C'est aussi une décomposition en un produit de $K \otimes L$-algèbres. Nous allons expliciter un peu cette décomposition.

Écrivons K sous la forme $K = \mathbb{Q}[X]/(f)$, pour un polynôme irréductible $f \in \mathbb{Q}[X]$. Notons $f = f_1 f_2 \cdots f_r$ la décomposition de f en produit de polynôme irréductibles sur L. Alors, par ce qui précède et le lemme Chinois, on a

$$K \otimes_{\mathbb{Q}} L \simeq L[X]/(f) \simeq \prod_{i=1}^{r} L[X]/(f_i).$$

Voici un point de vue plus intrinsèque, sans choix d'élément primitif α. Soit $\overline{L}$ une clôture algébrique de L. À chaque plongement $\sigma : K \hookrightarrow \overline{L}$, on associe le corps composé $L_\sigma = \sigma(K)L$ dans $\overline{L}$. C'est l'image du morphisme $K \otimes_{\mathbb{Q}} L \longrightarrow \overline{L}$, $\alpha \otimes l \mapsto \sigma(\alpha)l$ donc c'est aussi une $K \otimes L$-algèbre. Le groupe de Galois absolu $G_L := \mathrm{Gal}(\overline{L}/L)$ agit par composition sur l'ensemble $\{\sigma : K \hookrightarrow \overline{L}\}$ des plongements de K dans $\overline{L}$. Remarquons que si $G_{L,\sigma}$ désigne le fixateur de σ pour cette action, alors $L_\sigma = \overline{L}^{G_{L,\sigma}}$.

Proposition. – *Soit $\sigma_1, \cdots, \sigma_r$ des représentants des G_L-orbites dans l'ensemble des plongements. Alors le morphisme produit est un isomorphisme de $K \otimes L$-algèbres :*

$$K \otimes_{\mathbb{Q}} L \xrightarrow{\sim} \prod_{i=1}^{r} L_{\sigma_i}$$

Démonstration. Soient $\alpha_1, \cdots, \alpha_n$ les racines de f dans $\overline{L}$. Les plongements $K \hookrightarrow \overline{L}$ sont de la forme $\sigma_t : X \mapsto \alpha_t$. Deux plongements σ_t, σ_s sont conjugués sous G_L si et seulement si les racines associées α_t, α_s sont racines d'un même polynôme f_i comme ci-dessus. Dans ce cas $L_{\sigma_t} \simeq L_{\sigma_s} \simeq L[X]/(f_i)$. La proposition découle donc de la décomposition précédente. □

Cas particuliers.

i) $L = \mathbb{C}$. On a une décomposition de $K \otimes \mathbb{C}$-algèbres

$$K \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\sim} \prod_{\sigma : K \hookrightarrow \mathbb{C}} \mathbb{C}_\sigma$$

où $\mathbb{C}_\sigma$ désigne l'anneau $\mathbb{C}$ muni de la structure de $K \otimes \mathbb{C}$-algèbre donnée par $\alpha \otimes z \mapsto \sigma(\alpha) z$.

ii) $L = \mathbb{R}$. On a une décomposition de $K \otimes \mathbb{R}$-algèbres

$$K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \prod_{\sigma : K \hookrightarrow \mathbb{R}} \mathbb{R}_\sigma \times \prod_{\sigma \in \mathrm{Hom}(K, \mathbb{C})/\mathrm{conj}} \mathbb{C}_\sigma = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2},$$

où r_1 désigne le nombre de plongements réels de K, et r_2 la moitié du nombre de plongements imaginaires (de sorte que $r_1 + 2r_2 = [K : \mathbb{Q}]$).

2.2 Extensions entières

Soit A un anneau (commutatif unitaire). Commençons par rappeler le théorème classique suivant.

2.2.1 Théorème. (Cayley-Hamilton)– *Soit M un A-module libre de rang fini et $u \in \mathrm{End}_A(M)$ un endomorphisme de M. Notons $\chi_u(T) = \det(T\,\mathrm{id}_M - u) \in A[T]$ le polynôme caractéristique de u. Alors dans l'anneau $\mathrm{End}_A(M)$ on a l'égalité $\chi_u(u) = 0$.*

On rappelle que (comme dans le cas des espaces vectoriels sur un corps), le déterminant d'un endomorphisme u d'un module libre de type fini sur A est le déterminant de la matrice représentant cet endomorphisme dans n'importe quelle base de M sur A.

Démonstration. Considérons le cas particulier où $A = A_n := \mathbb{Z}[X_{ij}]_{1 \leqslant i,j \leqslant n}$, $M = A^n$ et u_n est donné dans la base canonique par la matrice $(X_{ij})_{1 \leqslant i,j \leqslant n}$. Puisque A_n est intègre, considérons son corps des fractions K_n et une clôture algébrique $\overline{K}_n$ de celui-ci. Le polynôme χ_{u_n} est aussi le polynôme caractéristique de la matrice u_n vue dans $M_n(K_n)$ ou dans $M_n(\overline{K}_n)$. En mettant u_n sous forme de Jordan dans $M_n(\overline{K}_n)$, on constate que $\chi_{u_n}(u_n) = 0$ dans $M_n(\overline{K}_n)$ et puisque $M_n(A_n) \longrightarrow M_n(\overline{K}_n)$ est injective, la même égalité vaut dans $M_n(A_n)$.

Revenons à l'énoncé général du théorème. Choisissons une base de M et identifions M à A^n. Notons $(a_{ij})_{i,j}$ la matrice de u dans cette base, et considérons le morphisme d'anneaux "de spécialisation"

$$\varepsilon : \ A_n = \mathbb{Z}[X_{ij}]_{1 \leqslant i,j \leqslant n} \longrightarrow A, \ \ X_{ij} \mapsto a_{ij}.$$

Ce morphisme induit aussi des morphismes d'anneaux $A_n[T] \longrightarrow A[T]$ et $M_n(A_n) \longrightarrow M_n(A)$ encore notés ε. Il est clair que $\varepsilon(\chi_{u_n}(T)) = \chi_u(T)$ et par là que $\varepsilon(\chi_{u_n}(u_n)) = \chi_u(u)$. On en déduit $\chi_u(u) = 0$. □

2.2.2 Corollaire.– *Soit M un A-module de type fini et $u \in \mathrm{End}_A(M)$ un endomorphisme. Alors il existe un polynôme monique $f \in A[T]$ tel que $f(u) = 0$ dans $\mathrm{End}_A(M)$.*

Démonstration. Choisissons un épimorphisme $\pi : A^n \twoheadrightarrow M$ pour n convenable. Soit $(e_1, \cdots, e_n)$ la base canonique de A^n. Pour chaque $i = 1, \cdots, n$, choisissons un élément $f_i \in A^n$ tel que $\pi(f_i) = u(\pi(e_i))$. Cela définit un endomorphisme $\widetilde{u}$ de A^n donné par $\widetilde{u}(e_i) = f_i$. On a donc par construction $\pi \circ \widetilde{u} = u \circ \pi$, et par itération $\pi \circ \widetilde{u}^k = u^k \circ \pi$, et finalement $\pi \circ \chi_{\widetilde{u}}(\widetilde{u}) = \chi_{\widetilde{u}}(u) \circ \pi$. D'après le théorème précédent on a donc $\chi_{\widetilde{u}}(u) \circ \pi = 0$. Or π est surjective, donc $\chi_{\widetilde{u}}(u) = 0$. □

2.2.3 Proposition.– *Soit B une A-algèbre. Pour $b \in B$, les propriétés suivantes sont équivalentes :*

*i) b est entier sur A (*ie $\exists f \in A[X]$ *monique t.q. $f(b) = 0$)*

ii) l'anneau $A[b]$ engendré par b est un module de type fini sur A.

iii) Il existe un $A[b]$-module fidèle qui est de type fini sur A.

Rappelons qu'un A-module M est "fidèle" si l'application $A \longrightarrow \mathrm{End}_{\mathbb{Z}}(M)$ est injective.

Démonstration. i) $\Rightarrow$ ii). Soit $f = X^n + a_1X^{n-1} + \cdots + a_n$ comme dans i). On a donc $b^n \in A + Ab + \cdots + Ab^{n-1}$ et par récurrence $b^m \in A + Ab + \cdots + Ab^{n-1}$ pour tout $m \geqslant n$. Donc $A[b]$ est engendré par $1, b, \cdots, b^{n-1}$ comme A-module.

ii) $\Rightarrow$ iii). Il suffit de prendre le $A[b]$-module $A[b]$!

iii) $\Rightarrow$ i) découle du corollaire précédent. □

2.2.4 Corollaire.– *Soit B une A-algèbre. L'ensemble $\{b \in B,\ b$ entier sur $A\}$ est une sous-A-algèbre de B. On l'appelle* clôture intégrale de A dans B.

Démonstration. Supposons b et b' entiers sur A. Alors b' est *a fortiori* entier sur $A[b]$ donc $A[b][b']$ est un $A[b]$-module de type fini, et donc aussi un A-module de type fini. C'est aussi un $A[b+b']$-module fidèle (puisqu'il contient $A[b+b']$) donc $b+b'$ est entier par la caractérisation iii) de la proposition précédente. De même, bb' est entier. □

Exemple. – Si K est un corps de nombres, $\mathcal{O}_K$ est la clôture intégrale de $\mathbb{Z}$ dans K.

2.2.5 Définition.– *Si A est* intègre*, la clôture intégrale de A dans* Frac(A) *est appelée* normalisation *de A. On dit alors que A est* normal *(ou encore* intégralement clos*) s'il est égal à sa propre normalisation.*

Exemples. – i) $\mathcal{O}_K$ est normal car $K = \mathrm{Frac}(\mathcal{O}_K)$. En effet, si $x \in K$, soit $a_i \in \mathbb{Q}$ tels que $x^n + a_1x^{n-1} + \cdots + a_n = 0$. Choisissons $b \in \mathbb{Z}$ tel que $ba_i \in \mathbb{Z}$ pour tout i. Alors $(xb)^n + (a_1b)(xb)^{n-1} + \cdots + (a_nb^n) = 0$, ce qui montre que $xb \in \mathcal{O}_K$ et donc que $x \in \mathrm{Frac}(\mathcal{O}_K)$

ii) $\mathbb{Z}[\sqrt{-3}]$ n'est pas intégralement clos. Sa normalisation est $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

Exemple. – A factoriel $\Rightarrow A$ normal. En effet, soit $x \in \mathrm{Frac}A$ vérifiant l'équation entière $x^n + a_1x^{n-1} + \cdots + a_n = 0$. Puisque A est factoriel on peut écrire $x = a/b$ avec a et b sans facteur commun, de sorte que $(a, b) = A$. Alors $a^n + a_1a^{n-1}b + \cdots a_nb^n = 0$, donc $a^n \in (b)$ ce qui implique $(b) = A$.

Remarque. – Une extension $A \subset B$ d'anneaux est dite *entière* si tout élément de B est entier sur A. La proposition montre aussi que si C est entier sur B et B entier sur A, alors C est entier sur A.

Exercice. – Montrer que $\mathbb{Q}[X_1, \cdots, X_n]$ est la clôture intégrale de $\mathbb{Q}[\Sigma_1, \cdots, \Sigma_n]$ dans $\mathbb{Q}(X_1, \cdots, X_n)$.

2.2.6 PROPOSITION.– *Si A est normal et L est une extension finie de $K := \mathrm{Frac}(A)$, alors $x \in L$ est entier si et seulement si son polynôme minimal $f_x \in K[X]$ est dans $A[X]$.*

Démonstration. Seul le sens $\Rightarrow$ demande preuve. Supposons donc x entier et soit $f \in A[X]$ tq $f(x) = 0$. Alors $f_x | f$ dans $K[X]$ donc toute racine α de f_x dans une clôture algébrique $\overline{K}$ de K est une racine de f donc est entière sur A. Les coefficients de f_x sont donc aussi entiers sur A, et puisqu'ils sont dans K et que A est normal, ils sont dans A. □

Exercice. – Montrer que $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \{a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d}),\ 2a \in \mathbb{Z},\ \text{et } a^2 - db^2 \in \mathbb{Z}\}$.

Exercice. – Calculer la normalisation de l'anneau $\mathbb{C}[X, Y]/(X^2 - Y^3)$.

2.3 Traces et Normes

Soit A un anneau et B une A-algèbre, *libre de type fini en tant que A-module*. Pour $b \in B$, on note $m(b)$ le A-endomorphisme de B donné par la multiplication par b. D'où un morphisme d'anneaux *injectif*

$$\begin{array}{rccl} m : & B & \to & \mathrm{End}_A(B) \\ & b & \mapsto & m(b) : b' \mapsto bb' \end{array}$$

Puisque B est libre sur A, on peut considérer le polynôme caractéristique

$$\chi_b(T) = \chi_{B/A,b}(T) := \det(T\,\mathrm{id}_B - m(b)) \in A[T].$$

2.3.1 DÉFINITION.– *Dans le contexte ci-dessus,*
– *on définit la "trace de b" par* $\mathrm{Tr}_{B/A}(b) := \mathrm{trace}(m(b))$.
– *on définit la "norme de b" par* $N_{B/A}(b) := \det(m(b))$.

Exemple. – Soit $B = A[X]/(f)$ avec $f(X) = x^n + a_1 x^{n-1} + \cdots + a_n$, et soit b l'image de X. Alors la matrice de $m(b)$ dans la base $\{1, b, \cdots, b^{n-1}\}$ est la "matrice compagnon" de f, et $\chi_b(T) = f(T)$. En particulier, on a $\mathrm{Tr}_{B/A}(b) = -a_1$ et $N_{B/A}(b) = (-1)^n a_n$.

Exercice. – Si M est un B-module libre de type fini et $u \in \mathrm{End}_B(M)$, alors
– $\mathrm{tr}_A(u|M) = \mathrm{Tr}_{B/A}(\mathrm{tr}_B(u|M))$, et
– $\det_A(u|M) = N_{B/A}(\det_B(u|M))$ (difficile, voir Bourbaki Algèbre, ch. III, Lemme 4.1, p.112. Voir aussi feuille d'exercices à la fin du poly)

En particulier, si C est une B-algèbre libre de type fini, alors

$$\mathrm{Tr}_{C/A} = \mathrm{Tr}_{B/A} \circ \mathrm{Tr}_{C/B} \text{ et } N_{C/A} = N_{B/A} \circ N_{C/B}.$$

2.3.2 PROPOSITION.– *Soit $K \subset L$ une extension finie de corps et $n := [L : K]$. Pour $\alpha \in L$, de polynôme minimal $f_\alpha(X) = X^m + a_1 X^{m-1} + \cdots + a_m \in K[X]$, on a $m|n$ et :*
- $\mathrm{Tr}_{L/K}(\alpha) = -\frac{n}{m} a_1$
- $N_{L/K}(\alpha) = ((-1)^m a_m)^{n/m}$.

Démonstration. Le degré de $K[\alpha]$ sur $\mathbb{Q}$ divise celui de L, donc $m|n$ et $\frac{n}{m} = [L : K[\alpha]]$. On a donc $\mathrm{Tr}_{L/K[\alpha]}(\alpha) = \frac{n}{m}\alpha$ et $N_{L/K[\alpha]}(\alpha) = \alpha^{\frac{n}{m}}$. L'exemple plus haut montre que $\mathrm{Tr}_{K[\alpha]/K}(\alpha) = -a_1$ et $N_{K[\alpha]/K}(\alpha) = (-1)^m a_m$. On conclut par l'exercice ci-dessus. □

2.3.3 COROLLAIRE.– *Si L est séparable finie sur K et $\overline{K}$ désigne une clôture algébrique de K, alors pour tout $\alpha \in L$*

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma : L \hookrightarrow \overline{K}} \sigma(\alpha) \quad et \quad N_{L/K}(\alpha) = \prod_{\sigma : L \hookrightarrow \overline{K}} \sigma(\alpha)$$

Démonstration. L'application de restriction $\{\sigma : L \hookrightarrow \overline{K}\} \longrightarrow \{\sigma : K[\alpha] \hookrightarrow \overline{K}\}$ est surjective et ses fibres sont de cardinal n/m (notation de la proposition). Donc

$$\sum_{\sigma : L \hookrightarrow \overline{K}} \sigma(\alpha) = \frac{n}{m} \sum_{\sigma : K[\alpha] \hookrightarrow \overline{K}} \sigma(\alpha) = \frac{n}{m} (\sum \{\text{racines de } f_\alpha \text{ dans } \overline{L}\}) = -\frac{n}{m} a_1.$$

Idem pour la norme. □

2.3.4 COROLLAIRE.– *Soit A anneau normal (intègre), L une extension séparable finie de $K := \mathrm{Frac}(A)$, et $\alpha \in L$ entier sur A. Alors $\mathrm{Tr}_{L/K}(\alpha) \in A$ et $N_{L/K}(\alpha) \in A$.*

2.4 Discriminants

Soit A un anneau et B une A-algèbre libre de type fini en tant que A-module. On considère la forme A-bilinéaire sur B donnée par

$$\theta_{B/A} : (b, b') \mapsto \mathrm{Tr}_{B/A}(bb').$$

Si $b_1, \cdots, b_n$ sont des éléments de A, on note

$$D_{B/A}(b_1, \cdots, b_n) := \det \left(\mathrm{Tr}_{B/A}(b_i b_j) \right)_{i,j}.$$

Si $b_1, \cdots, b_n$ est une base de B sur A, c'est le *discriminant* de la forme bilinéaire $\theta_{B/A}$ dans cette base. Si $b'_1, \cdots, b'_n$ est une autre base de B sur A, et P la matrice de passage $(b'_i)_i = P.(b_i)_i$, alors

$$D_{B/A}(b'_1, \cdots, b'_n) = \det(P)^2 D(b_1, \cdots, b_n).$$

2.4.1 DÉFINITION.– *On notera* $\mathrm{disc}(B/A) \in A/(A^\times)^2$ *l'image du discriminant de $\theta_{B/A}$ dans n'importe quelle base, et* $(\mathrm{disc}(B/A))$ *l'idéal de A qu'il engendre.*

Remarque. – Dans le cas $A = \mathbb{Z}$, l'élément $\mathrm{disc}(B/A)$ vit dans $\mathbb{Z}$.

2.4.2 Proposition.– *Supposons A intègre et $\mathrm{disc}(B/A) \neq 0$, alors une famille $b_1, \cdots, b_n$ de B est une base de B sur A si et seulement si $(D_{B/A}(b_1, \cdots, b_n)) = (\mathrm{disc}(B/A))$.*

Démonstration. Exercice. □

2.4.3 Proposition.– *Soit $L \supset K$ une extension séparable finie, $\omega_1, \cdots, \omega_n$ une base de L sur K, et $\sigma_1, \cdots, \sigma_n$ les plongements $L \hookrightarrow \overline{K}$. Alors*

$$D_{L/K}(\omega_1, \cdots, \omega_n) = \Big(\det\left(\sigma_i(\omega_j)\right)_{i,j}\Big)^2.$$

Démonstration. On a $\mathrm{Tr}_{L/K}(\omega_i\omega_j) = \sum_{k=1}^n \sigma_k(\omega_i)\sigma_k(\omega_j)$. On a donc une égalité de matrices $n \times n$

$$\left(\mathrm{Tr}_{L/K}(\omega_i\omega_j)\right)_{i,j} = {}^tUU \text{ avec } U = \left(\sigma_i(\omega_j)\right)_{i,j}.$$

□

2.4.4 *Lien avec le discriminant d'un polynôme.* Rappelons que le discriminant d'un polynôme $f = X^n + a_1X^{n-1} + \cdots + a_n \in A[X]$ est défini par

$$\mathrm{disc}(f) = \Delta_n(-a_1, \cdots, (-1)^n a_n)$$

où $\Delta_n \in \mathbb{Z}[\Sigma_1, \cdots, \Sigma_n]$ vérifie $\Delta_n(\Sigma_1, \cdots, \Sigma_n) = \prod_{i<j}(X_i - X_j)^2$. Posons maintenant $B := A[X]/(f)$ et notons b l'image de X dans B.

Proposition. – *Dans ce contexte, on a*

$$\mathrm{disc}(f) = D_{B/A}(1, b, \cdots, b^{n-1}) = (-1)^{n(n-1)/2} N_{B/A}(f'(b)).$$

Démonstration. Traitons d'abord le cas particulier, mais "universel", suivant : $A = A_{univ} := \mathbb{Z}[A_1, \cdots, A_n]$ et $f = f_{univ} = X^n + A_1X^{n-1} + \cdots + A_n \in A_{univ}[X]$. Il est clair que f ne possède pas de factorisation $f = f_1f_2$ avec f_1, $f_2 \in A_{univ}[X]$ de degrés non nuls. Sinon, en spécialisant $A_1 = \cdots = A_{n-1} = 0$ et $A_n = -2$, on en déduirait une factorisation de $X^n - 2$ dans $\mathbb{Z}[X]$ contredisant l'irréductibilité de ce polynôme (cf critère d'Eisenstein plus loin). Comme A est normal, il s'ensuit que f_{univ} est irréductible dans $K[X]$, où $K = A_{univ}[X]$ (comme dans la preuve de la proposition 2.2.6). Posons alors $L := K[X]/(f_{univ})$, une extension séparable finie de K et fixons une clôture algébrique de $\overline{K}$ de K. Les plongements $L \hookrightarrow \overline{K}$ sont en bijection $\sigma \mapsto \sigma(b_{univ})$ (avec b_{univ} l'image de X) avec les racines $\alpha_1, \cdots \alpha_n$ de f_{univ} dans $\overline{K}$. Alors la matrice U de la proposition précédente (avec $\omega_j = b_{univ}^{j-1}$) est la matrice de Vandermonde $\left(\alpha_i^{j-1}\right)_{i,j}$, et par conséquent

$$D_{B_{univ}/A_{univ}}(1, b_{univ}, \cdots, b_{univ}^{n-1}) = \prod_{i<j}(\alpha_i - \alpha_j)^2 = \mathrm{disc}(f_{univ}).$$

Par ailleurs, on voit que puisque $f'_{univ}(\alpha_i) = \prod_{j\neq i}(\alpha_i - \alpha_j)$, on a

$$N_{B_{univ}/A_{univ}}(f'_{univ}(b_{univ})) = \prod_{j=1}^{n} f'_{univ}(\alpha_j) = \prod_{k\neq j}(\alpha_j - \alpha_k) = (-1)^{n(n-1)/2}\mathrm{disc}(f_{univ}).$$

Maintenant on traite le cas général par spécialisation du cas "universel" ci-dessus. On considère donc le morphisme d'anneaux $\varepsilon : A_{univ} \longrightarrow A$, $A_i \mapsto a_i$. On a donc $f = \varepsilon(f_{univ})$ et $\mathrm{disc}(f) = \varepsilon\mathrm{disc}(f_{univ})$. De plus ε se prolonge en $B_{univ} \longrightarrow B$ en envoyant b_{univ} sur b. On a alors $\varepsilon(f'_{univ}(b_{univ})) = f'(b)$, $\varepsilon \circ N_{B_{univ}/A_{univ}} = N_{B/A} \circ \varepsilon$ et enfin $\varepsilon(D_{B_{univ}/A_{univ}}(1, b_{univ}, \cdots, b_{univ}^{n-1})) = D_{B/A}(1, b, \cdots, b^{n-1})$. L'énoncé de la proposition s'ensuit. □

Cette proposition fournit une méthode de calcul de $\mathrm{disc}(f)$.

Exemple. – Soit $f(X) = X^2 + aX + b$ et α l'image de X dans B. Dans la base $1, \alpha$, la matrice de $P'(\alpha) = 2\alpha + a$ est $\begin{pmatrix} a & 2 \\ -2b & -a \end{pmatrix}$, donc $\mathrm{disc}(f) = -\begin{vmatrix} a & 2 \\ -2b & -a \end{vmatrix} = a^2 - 4b$.

Exercice. – Calculer $\mathrm{disc}(f)$ pour $f(X) = X^n + aX + b$.

2.4.5 Corollaire.– *Soit L/K une extension finie de corps, on a équivalence entre*

i) $\mathrm{disc}(L/K) \neq 0$

ii) la forme bilinéaire $\theta_{L/K}$ est non-dégénérée.

iii) L est séparable sur K

Démonstration. L'équivalence entre i) et ii) est claire. L'implication *iii)* $\Rightarrow$ *i)* découle du théorème de l'élément primitif qui nous dit que $L = K[X]/(f)$ avec f séparable, donc $f'(b) \neq 0$ si b est l'image de X, et de la proposition précédente qui nous dit que $\mathrm{disc}(f) = \pm N_{L/K}(f'(b)) \neq 0$. Enfin, si L n'est pas séparable sur K, il existe un élément $\alpha \in L$ dont le polynôme minimal est inséparable sur K, de sorte que $\mathrm{disc}(K[\alpha]/K) = 0$... □

2.4.6 Théorème.– *Soit A normal et B la clôture intégrale de A dans une extension séparable finie L de $K = \mathrm{Frac}(A)$. Alors il existe deux sous-A-modules M, M' de L, libres de rang $[L : K]$ et tels que $M \subset B \subset M'$. En particulier :*

– Si A est noethérien, alors B est un A-module de type fini.

– Si A est principal, alors B est libre de rang $[L : K]$.

Démonstration. Notons $n = [L : K]$. Soit $b_1, \cdots, b_n$ une base de L sur K contenue dans B (existe car $L = \mathrm{Frac}(B)$). On a donc $M := \bigoplus_i Ab_i \subset B$. Soit $b_1^*, \cdots, b_n^*$ la base duale pour la forme non dégénérée $\theta_{L/K}$ (séparabilité). Pour tout $b \in B$, on a

$$b = \sum_{i=1}^{n} \mathrm{Tr}_{L/K}(bb_i)b_i^*$$

et $\mathrm{Tr}_{L/K}(bb_i) \in A$ d'après le corollaire 2.3.4. Donc $B \subset M' := \bigoplus_i Ab_i^*$.

□

2.5 Application au calcul de $\mathcal{O}_K$

Nous appliquons ici les outils précédents au problème du calcul de l'anneau des entiers $\mathcal{O}_K$ d'un corps de nombres K.

2.5.1 *Finitude des anneaux d'entiers.* Le théorème ci-dessus montre que $\mathcal{O}_K$ est libre de rang $[K : \mathbb{Q}]$ sur $\mathbb{Z}$, ce qui montre d'ailleurs que $\mathcal{O}_K$ est noethérien. Par contre, si $L \subset K$ est un autre corps de nombres, $\mathcal{O}_K$ est bien de type fini sur $\mathcal{O}_L$, mais n'est pas nécessairement libre sur $\mathcal{O}_L$. Nous verrons qu'il est tout de même *projectif*, *i.e.* facteur direct d'un libre.

2.5.2 Proposition.– *Soit $K = \mathbb{Q}[\alpha]$ un corps de nombres de degré n, avec $f_\alpha \in \mathbb{Z}[X]$ (donc α entier). Si $\mathrm{disc}(f_\alpha) \in \mathbb{Z}$ est sans facteur carré, alors $\{1, \alpha, \cdots, \alpha^{n-1}\}$ est une base de $\mathcal{O}_K$ sur $\mathbb{Z}$ (et donc $\mathcal{O}_K = \mathbb{Z}[\alpha]$).*

Démonstration. Soit P la matrice de passage d'une base (quelconque) de $\mathcal{O}_K$ sur $\mathbb{Z}$ vers la famille $(1, \alpha, \cdots, \alpha^{n-1})$. On a donc $P \in \mathrm{M}_n(\mathbb{Z}) \cap \mathrm{GL}_n(\mathbb{Q})$, et $\det(P) \in \mathbb{Z}$, et aussi

$$\mathrm{disc}(f_\alpha) = D_{\mathcal{O}_K/\mathbb{Z}}(1, \alpha, \cdots, \alpha^{n-1}) = \mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) \det(P)^2.$$

D'après le rappel ci-dessous, $|\det(P)|$ est l'indice $(\mathcal{O}_K : \mathbb{Z}[\alpha])$ de $\mathbb{Z}[\alpha]$ dans $\mathcal{O}_K$. On en déduit la proposition.

Rappel : Soit M un $\mathbb{Z}$-module libre de rang m et N un sous-module de rang m. Alors il existe une base $e_1, e_2, \cdots, e_m$ de M et des entiers $a_1 | a_2 | \cdots | a_m$ tels que $a_1 e_1, a_2 e_1, \cdots, a_m e_m$ soit une base de N sur $\mathbb{Z}$. Cela se déduit du théorème "des diviseurs élémentaires" donnant la structure des groupes abéliens finis ou s'obtient aussi par échelonnage (lignes et colonnes) de n'importe quelle matrice de passage d'une base de M à une base de N. Il s'ensuit que pour toute matrice de passage d'une base de M à une base de N, on a $|\det(P)| = a_1 a_2 \cdots a_n = (M : N)$. □

Exemples. – Mêmes notations que la proposition.

i) Si $f_\alpha(X) = X^3 - X - 1$, on calcule $\mathrm{disc}(f_\alpha) = -23$, donc $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

ii) Si $f_\alpha(X) = X^3 + X^2 - 2X + 8$, alors $\mathrm{disc}(f_\alpha) = -2012 = -4 \times 503$. Dans ce cas, on peut montrer que $\mathbb{Z}[\alpha] \neq \mathcal{O}_K$.

Exercice. – Montrer la variante suivante de la proposition : *si $f \in \mathbb{Z}[X]$ est un polynôme monique irréductible dont le discriminant $\mathrm{disc}(f)$ est sans facteur carré, alors $\mathbb{Z}[X]/(f)$ est un anneau normal.*

Exemple. Soit $f(X) = X^5 - X - 1$. Montrer que f est irréducible dans $\mathbb{F}_3[X]$, donc dans $\mathbb{Q}[X]$, puis montrer que $\mathbb{Z}[X]/(f)$ est normal.

2.5.3 Proposition.– *Soit K un corps de nombres. On a*

i) $\mathrm{sgn}(\mathrm{disc}(K/\mathbb{Q})) = (-1)^{r_2}$ *où r_2 est la moitié du nombre de plongements imaginaires $K \hookrightarrow \mathbb{C}$.*

ii) $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) \equiv 0$ *ou* 1 *modulo* 4 *(Stickelberger).*

Démonstration. i) Soit $\omega_1, \cdots, \omega_n$ une base de $K/\mathbb{Q}$ et $\sigma_1, \cdots, \sigma_n$ les plongements $K \hookrightarrow \mathbb{C}$. Soit $M = (\sigma_i(\omega_j))_{i,j} \in M_n(\mathbb{C})$. On sait que $D_{K/\mathbb{Q}}(\omega_1, \cdots, \omega_n) = (\det(M))^2$ et le signe que l'on cherche est donc celui de $(\det(M))^2$. Or la matrice conjuguée $\overline{M} = (\overline{\sigma}_i(\omega_j))_{i,j}$ s'obtient à partir de M par r_2 échanges de lignes, de sorte que $\det(\overline{M}) = (-1)^{r_2}\det(M)$. On en déduit que $(\det(M)) = (-1)^{r_2}|\det(M)|^2$, d'où le signe annoncé.

ii) Soit $\alpha_1, \cdots, \alpha_n$ une base de $\mathcal{O}_K$ sur $\mathbb{Z}$ et $\sigma_1, \cdots, \sigma_n$ les plongements $K \hookrightarrow \mathbb{C}$. Alors

$$\begin{aligned}\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) = \left(\det\left(\sigma_i(\alpha_j)\right)_{i,j}\right)^2 &= \left(\sum_{\tau\in\mathfrak{S}_n,\varepsilon(\tau)=1}\prod_{i=1}^{n}\sigma_i(\alpha_{\tau(i)}) - \sum_{\tau\in\mathfrak{S}_n,\varepsilon(\tau)=-1}\prod_{i=1}^{n}\sigma_i(\alpha_{\tau(i)})\right)^2 \\ &= (P-I)^2 \\ &= (P+I)^2 - 4PI\end{aligned}$$

Nous allons montrer que $P+I$ et PI sont des entiers (dans $\mathbb{Z}$), ce qui impliquera que $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) \equiv (P+I)^2[4] \equiv 0, 1[4]$ puisque le carré d'un entier est toujours congru à 0 ou 1 modulo 4.

Puisque les $\sigma_i(\alpha_j)$ sont des entiers algébriques, $P+I$ et PI ont aussi des entiers algébriques, et il nous suffira donc de prouver qu'ils sont rationnels (dans $\mathbb{Q}$), *i.e.* invariants par $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Soit donc $\gamma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Il induit une permutation $\tau_\gamma : \sigma \mapsto \gamma\circ\sigma$ des plongements $\sigma_1, \cdots, \sigma_n$. Si τ_γ est paire, on a $\gamma(P) = P$ et $\gamma(I) = I$. Si τ_γ est impaire, on a $\gamma(P) = I$ et $\gamma(I) = P$. Il s'ensuit que $\gamma(P+I) = P+I$ et $\gamma(PI) = PI$, comme voulu. □

2.5.4 *Corps quadratiques.* Supposons $K = \mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{Z}$ sans facteur carré. On a alors

$$\mathrm{disc}(X^2 - d) = 4d = \mathrm{disc}(\mathcal{O}_K/\mathbb{Z})(\mathcal{O}_K : \mathbb{Z}[\sqrt{d}])^2,$$

ce qui laisse a priori deux possibilités pour $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z})$: soit il vaut $4d$, soit il vaut d. Dans ce dernier cas on doit avoir $d \equiv 1[4]$ d'après le théorème de Stickelberger. On en déduit la dichotomie suivante :

i) Si $d \equiv 2$ ou 3 modulo 4, alors $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) = 4d$ et $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.

ii) Si $d \equiv 1$ modulo 4, alors $\frac{1+\sqrt{d}}{2}$ est entier donc $\mathbb{Z}[\sqrt{d}] \neq \mathcal{O}_K$ et $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) = d$. Dans ce cas on a $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

2.5.5 *Un critère plus fin.* On a vu que pour un sous-anneau $B \subset \mathcal{O}_K$ d'indice fini, on a

$$\mathrm{disc}(B/\mathbb{Z}) = \mathrm{disc}(\mathcal{O}_K/\mathbb{Z})(\mathcal{O}_K : B)^2,$$

ce qui montre que lorsque $\mathrm{disc}(B/\mathbb{Z})$ est sans facteur carré, on a $B = \mathcal{O}_K$.

Problème : que faire si pour un premier p, on a $p^2|\mathrm{disc}(B/\mathbb{Z})$? Comment déterminer si $p|(\mathcal{O}_K : B)$ et si oui, comment trouver $b \in B$ tel que $\frac{b}{p} \in \mathcal{O}_K$?

THÉORÈME. – *Soit $N = \sqrt{pB}$ le radical de $(p) = pB$ dans B, et soit*

$$\begin{array}{rccc} m : & B/pB & \to & \mathrm{End}_B(N/pN) \\ & b & \mapsto & (\bar{n} \mapsto \bar{b}\bar{n}) \end{array}$$

l'action de B/pB sur N/pN.

i) Si $\mathrm{Ker}(m) = 0$, alors $\mathcal{O}_K \cap p^{-1}B = B$ et par conséquent p ne divise pas $(\mathcal{O}_K : B)$.

ii) Si $b \in B$ est tel que $0 \neq \bar{b} \in \mathrm{Ker}(m)$, alors $\frac{b}{p} \in \mathcal{O}_K$ et $\frac{b}{p} \notin B$.

Démonstration. i) Supposons $\mathrm{Ker}(m) = 0$. On a l'inclusion $B \subset \mathcal{O}_K \cap p^{-1}B$, et on veut montrer l'égalité. Introduisons l'anneau $B' = \{x \in \mathcal{O}_K, xN \subset N\}$. On a $B \subset B' \subset \mathcal{O}_K \cap p^{-1}B$.

Première étape : $B = B'$.

En effet, si $x \in B'$ on a $xpN \subset pN$ et, puisque $xp \in B$ (penser que $p \in N$), on voit que $\overline{xp} \in \mathrm{Ker}(m)$. Donc $xp \in pB$, par hypothèse, et finalement $x \in B$.

Deuxième étape : soit $x \in \mathcal{O}_K \cap p^{-1}B$ de degré n et soit m tel que $N^m \subset pB$. Alors pour tout $y \in N$ on a $(xy)^{nm} \in pB$.

En effet, $xy^m \in pxB$ et $xy^m \in B$ puisque $px \in B$. Il s'ensuit que pour tout $k \in \mathbb{N}$ on a $y^m(xy^m)^k \in pB$ et en particulier pour $1 \leqslant k \leqslant n-1$ on a $x^k y^{mn} \in pB$. Utilisant une équation entière monique de degré n pour x, on obtient $x^k y^{mn} \in pB$ pour *tout* $k \in \mathbb{N}$, et en particulier pour $k = mn$. On a donc $(xy)^{mn} \in pB$.

Troisième étape : $B' = \mathcal{O}_K \cap p^{-1}B$.

Soit $x \in \mathcal{O}_K \cap p^{-1}B$. Nous allons prouver par récurrence descendante sur $k \geqslant 1$ que $xN^k \subset N$. On commence la récurrence à $k = 2m$ puisque $xN^{2m} \subset xp^2B \subset pB \subset N$. Supposons donc $xN^{k+1} \subset N$ et prouvons $xN^k \subset N$. Soit $y \in N^k$. On a $xyN \subset N$, donc par la première étape on a $xy \in B$. Par la deuxième étape, on a $(xy)^{nm} \in pB$, donc $xy \in N$. D'où $xN^k \subset N$. Pour $k = 1$, on obtient $x \in B'$.

ii) Soit b comme dans l'énoncé. Alors $\frac{b}{p} \notin B$ et $\frac{b}{p}N \subset N$. Cette deuxième propriété implique que $\mathbb{Z}[\frac{b}{p}]$ se plonge dans $\mathrm{End}_{\mathbb{Z}}(N)$, donc est un $\mathbb{Z}$-module de type. Il s'ensuit que $\frac{b}{p}$ est entier sur $\mathbb{Z}$, *i.e.* $\frac{b}{p} \in \mathcal{O}_K$. □

Nous donnons maintenant un exemple d'application de ce théorème.

2.5.6 *Le cas Eisenstein.* Soit p un nombre premier. Rappelons qu'un polynôme $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ est dit *d'Eisenstein en p*, si $p|a_i$ pour tout i et p^2 ne divise pas a_0. L'intérêt de cette notion réside dans le critère d'irréductibilité suivant.

LEMME. (Critère d'Eisenstein) – *Si f est d'Eisenstein, alors f est irréductible.*

Démonstration. Supposons qu'il existe une factorisation $f = gh$ avec $g(X) = X^m + b_{m-1}X^{m-1} + \cdots + b_0$ et $h(X) = X^l + c_{l-1}X^{l-1} + \cdots + c_0$. Par hypothèse, p divise un seul élément parmi b_0 et c_0 ; supposons que $p|c_0$. Alors soit i le plus petit indice tel que p ne divise pas c_i. On a $a_i = c_ib_0 + c_{i-1}b_1 + \cdots c_0b_i \equiv c_ib_0[p]$, donc p ne divise pas a_i : contradiction. □

On veut appliquer le théorème ci-dessus au cas de $K = \mathbb{Q}(\alpha)$ avec f_α Eisenstein en p, et $B = \mathbb{Z}[\alpha] \simeq \mathbb{Z}[X]/(f_\alpha)$. Dans ce cas, on a $B/pB \simeq \mathbb{F}_p[X]/(X^n)$ et $N = pB + \alpha B$ (puisque N est par définition l'image réciproque dans B du nilradical de B/pB, qui est visiblement (X)).

LEMME. – *Avec les notations du théorème, on a* $\mathrm{Ker}(m) = 0$.

Démonstration. Puisque $\mathrm{Ker}(m)$ est un idéal de B/pB, il est de la forme (X^i). S'il est non-nul, il contient donc X^{n-1}, ce qui équivaut à $\alpha^{n-1}N \subset pN$. Or ceci est impossible car $\alpha \in N$ et $\alpha^n = \alpha^{n-1}\alpha \notin pN$. En effet, on a $\alpha^n = -a_0 - a_1\alpha - \cdots - a_{n-1}\alpha^{n-1} \in -a_0 + pN$, et $a_0 \notin pN$ puisque p^2 ne divise pas a_0. □

D'après ce lemme et le théorème précédent, si p est le seul premier qui apparait avec multiplicité dans $\mathrm{disc}(\mathbb{Z}[\alpha]/\mathbb{Z})$, alors on peut conclure que $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Voici un cas important où cela s'applique.

2.5.7 *Corps p-cyclotomiques.* Fixons un entier $r \geqslant 1$ et posons $\zeta_r := \exp(\frac{2i\pi}{p^r}) \in \mathbb{C}$, qui est une racine p^r-ème *primitive* de 1. On s'intéresse au corps $K = \mathbb{Q}(\zeta_r)$, qui est une extension Galoisienne de $\mathbb{Q}$ puisque tous les conjugués de ζ_r en sont des puissances. Le "polynôme p^r-cyclotomique" est un polynôme de degré $\varphi(p^r) = p^r - p^{r-1}$ défini par

$$\Phi_{p^r}(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1}.$$

Il annule clairement ζ_r. On remarque que $\Phi_{p^r}(1 + T) \equiv \frac{T^{p^r}}{T^{p^{r-1}}} = T^{p^r - p^{r-1}}$ modulo p, et puisque $\Phi_{p^r}(1) = p$, on en déduit que Φ_{p^r} est d'Eisenstein en p et en particulier est irréductible. C'est donc le polynôme minimal de ζ_r sur $\mathbb{Q}$, et on a

$$\mathbb{Q}(\zeta_r) \simeq \mathbb{Q}[X]/(\Phi_{p^r}).$$

Par comparaison des cardinaux, le morphisme injectif

$$\chi_{p^r,\mathbb{Q}} : \mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/p^r\mathbb{Z})^\times$$

défini en 1.1.3 est donc un isomorphisme.

On veut maintenant calculer le discriminant de Φ_{p^r} par la formule

$$\mathrm{disc}(\Phi_{p^r}) = (-1)^{\frac{\varphi(p^r)(\varphi(p^r)-1)}{2}} N_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\Phi'_{p^r}(\zeta_r)).$$

On a $\Phi'_{p^r}(\zeta_r) = p^r \frac{\zeta_r^{p^r-1}}{\zeta_r^{p^{r-1}}-1} = p^r \frac{\zeta_r^{-1}}{\zeta_1 - 1}$. Remarquons que $N_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\zeta_r)$ est une racine p^r-ème de l'unité dans $\mathbb{Q}$, donc vaut 1 si $p \neq 2$. Si $p = 2$, alors la formule $N_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\zeta_r) = \prod_{a \in (\mathbb{Z}/p^r\mathbb{Z})^\times} \zeta_r^a$ montre que $N_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\zeta_r) = 1$ sauf dans le cas $r = 1$ où $N_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\zeta_r) = -1$. Par ailleurs, on a

$$N_{\mathbb{Q}(\zeta_r)/\mathbb{Q}}(\zeta_1 - 1) = N_{\mathbb{Q}(\zeta_1)/\mathbb{Q}}(\zeta_1 - 1)^{[\mathbb{Q}(\zeta_r):\mathbb{Q}(\zeta_1)]} = \left(\prod_{i=1}^{p-1}(\zeta_1^i - 1)\right)^{p^{r-1}}.$$

Le produit $\prod_{i=1}^{p-1}(\zeta_1^i - 1)$ est le produit des racines du polynôme $\Phi_p(1+T) = (1+T)^{p-1} + \cdots + (1+T) + 1$, donc est égal à $(-1)^{p-1}p$. Finalement on obtient

$$\mathrm{disc}(\Phi_{p^r}) = \pm p^{r\varphi(p^r)} \frac{1}{p^{p^{r-1}}} = \pm p^{rp^r-(r+1)p^{r-1}}.$$

COROLLAIRE. – *La famille* $(1, \zeta_r, \cdots, \zeta_r^{\varphi(p^r)-1})$ *est une base de* $\mathcal{O}_{\mathbb{Q}(\zeta_r)}$. *En d'autres termes, on a* $\mathcal{O}_{\mathbb{Q}(\zeta_r)} = \mathbb{Z}[\zeta_r]$.

Démonstration. Partons de la formule

$$\mathrm{disc}(\mathbb{Z}[\zeta_r]/\mathbb{Z}) = \mathrm{disc}(\mathcal{O}_{\mathbb{Q}(\zeta_r)}/\mathbb{Z})(\mathcal{O}_{\mathbb{Q}(\zeta_r)} : \mathbb{Z}[\zeta_r])^2.$$

Elle montre que le seul premier qui peut diviser l'indice $(\mathcal{O}_{\mathbb{Q}(\zeta_r)} : \mathbb{Z}[\zeta_r])$ est p. Or, $\Phi_{p^r}(1+X)$ est d'Eisenstein en p, donc le second lemme 2.5.6 et le théorème 2.5.5 nous disent que p ne divise pas $(\mathcal{O}_{\mathbb{Q}(\zeta_r)} : \mathbb{Z}[\zeta_r])$. □

Exercice. – On considère $K = \mathbb{Q}(\sqrt[3]{17})$, et on pose $B = \mathbb{Z}[\sqrt[3]{17}]$.

i) Montrer que $\mathrm{disc}(B/\mathbb{Z}) = -3^3 17^2$.

ii) Montrer que 17 ne divise pas $(\mathcal{O}_K : B)$ et donc que $(\mathcal{O}_K : B) = 1$ ou 3.

iii) Soit $\alpha := 1 + \sqrt[3]{17}$. Montrer que $\frac{\alpha^2}{3}$ est entier.

iv) Conclure que $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\frac{\alpha^2}{3}$.

3 Anneaux de Dedekind

3.1 Anneaux de valuation discrète

3.1.1 DÉFINITION.– *Un anneau est dit "de valuation discréte" s'il est intègre, principal, et possède un unique idéal premier non nul.*

Propriétés. – Soit A de valuation discrète et $\mathfrak{m}$ son idéal premier.

i) A est *local*. On a $\mathrm{Max}(A) = \{\mathfrak{m}\}$ et $\mathrm{Spec}(A) = \{(0), \mathfrak{m}\}$.

ii) Soit ϖ un générateur de l'idéal $\mathfrak{m}$. Alors $\mathfrak{m}^i \setminus \mathfrak{m}^{i+1} = A^\times \varpi^i$ et on a une partition

$$A \setminus \{0\} = \bigsqcup_{i \in \mathbb{N}} A^\times \varpi^i.$$

En effet, A est factoriel (puisque principal) et ϖ est l'unique élément irréductible à équivalence près (puisque dans un anneau factoriel, tout élément irréductible engendre un idéal premier). Un tel élément ϖ est appelé *uniformisante de* A.

Exemples. – – $A = \mathbb{Z}_{(p)}$ et $\pi = p$
– $A = \mathbb{C}[X]_{(X-c)}$ et $\pi = X - c$
– $A = \mathbb{C}[[X]]$, et $\pi = X$.

iii) Les idéaux de A sont les $\mathfrak{m}^i = \varpi^i A$ et l'idéal nul.

iv) On a $\mathrm{Frac}(A) = A[\varpi^{-1}]$ et $\mathrm{Frac}(A) \setminus \{0\} = \bigsqcup_{i\in\mathbb{Z}} A^\times \varpi^i$.

v) Définissons une fonction $v : \mathrm{Frac}(A) \longrightarrow \mathbb{Z} \cup \{\infty\}$ en envoyant 0 sur ∞ et $x \neq 0$ sur l'unique entier $v(x)$ tel que $x \in A^\times \varpi^{v(x)}$. On a alors les propriétés suivantes :
- $v(x) = \infty \Leftrightarrow x = 0$
- $v(xy) = v(x) + v(y)$
- $v(x + y) \geqslant \min(v(x), v(y))$.

De plus on retrouve A par l'égalité $A = \{x \in \mathrm{Frac}(A), v(x) \geqslant 0\}$. Ceci permet un autre point de vue qui explique aussi la terminologie :

3.1.2 Définition.– *Soit K un corps. Une valuation (additive) est une fonction $v : K \longrightarrow \mathbb{R} \cup \{\infty\}$ qui vérifie les trois propriétés ci-dessus. Elle est dite "discrète" si $v(K^\times)$ est un sous-groupe discret de $\mathbb{R}$, et "discrète normalisée" si $v(K^\times) = \mathbb{Z}$.*

Propriétés. – Soit (K, v) un corps muni d'une valuation discrète normalisée.

i) $A := \{x \in K,\ v(x) \geqslant 0\}$ est un anneau de valuation discrète (appelé "l'anneau de la valuation v"), d'idéal maximal $\mathfrak{m} := \{x \in K, v(x) > 0\}$.

ii) $A^\times = \{x \in K, v(x) = 0\}$ et $\varpi \in K$ est uniformisante de A si et seulement si $v(\varpi) = 1$,

iii) K est le corps des fractions de A.

Exemple. – Soit p un nombre premier. On lui associe une valuation discrète normalisée v_p sur $\mathbb{Q}$ (aussi notée ord_p) en posant $v_p(x) = m$ pour $x \in \mathbb{Q} \setminus \{0\}$ de la forme $p^m \frac{a}{b}$ avec $(p, a) = (p, b) = 1$. L'anneau de cette valuation n'est autre que $\mathbb{Z}_{(p)}$.

Exemple. – Soit $\mathcal{M}$ le corps de fonctions méromorphes d'une surface de Riemann X (ou le corps de fonctions d'une courbe algébrique). On associe à tout point $x \in X$ la valuation ord_x qui envoie $f \in \mathcal{M}$ sur son ordre (pôle ou zéro) en x.

Exercice. – Soit v une valuation sur un corps K. Montrer que :

i) Si $v(x) \neq v(y)$ alors $v(x + y) = \min(v(x), v(y))$.

ii) Si $x_1 + \cdots + x_n = 0$, alors il existe $i \neq j$ t.q. $v(x_i) = v(x_j) = \min\{v(x_1), \cdots, v(x_n)\}$.

3.2 Idéaux fractionnaires inversibles

Ici A désigne toujours un anneau intègre (mais tout peut se généraliser aux anneaux non-intègres).

3.2.1 Définition.– *Un idéal fractionnaire de A est un sous-A-module $I \subset K = \mathrm{Frac}(A)$ pour lequel il existe $a \in A$ tel que $aI \subset A$.*

Il est dit principal s'il est monogène, ie *de la forme $A\alpha$ avec $\alpha \in K$.*

Exercice. – Montrer que si I et J sont des idéaux fractionnaires alors $I + J$, IJ, et $I^{-1} := \{x \in K, xI \subset A\}$ sont des idéaux fractionnaires.

3.2.2 DÉFINITION.– *L'idéal fractionnaire I est dit* inversible *si $I.I^{-1} = A$.*

Exemple. – L'idéal $I = (X, Y)$ de $\mathbb{C}[X, Y]$ n'est pas inversible. En fait $I^{-1} = \mathbb{C}[X, Y]$.

Propriétés. – *I principal $\Rightarrow$ I inversible.* Clair.
- *I inversible $\Rightarrow$ I de type fini.* En effet, écrivons $1 = x_1y_1 + \cdots + x_my_m$ avec $x_i \in I$ et $y_i \in I^{-1}$. Alors tout $a \in I$ s'écrit $a = \sum_i x_i(ay_i)$ où $ay_i \in A$. Donc $x_1, \cdots, x_n$ engendrent I.
- *Si A est local, alors I inversible $\Rightarrow$ I principal.* Comme ci-dessus, écrivons $1 = x_1y_1 + \cdots + x_my_m$ avec $x_i \in I$ et $y_i \in I^{-1}$. Alors il existe i tel que $x_iy_i \notin \mathfrak{m}$, et donc $x_iy_i \in A^\times$. On peut donc écrire $1 = x_iy_i'$ avec $y_i' \in I^{-1}$ et on en déduit comme ci-dessus que x_i engendre I.
- Si A n'est plus local, il reste que pour tout $\mathfrak{p} \in \mathrm{Spec}(A)$, l'idéal $IA_\mathfrak{p}$ de $A_\mathfrak{p}$ est inversible donc principal. On dit que *I est localement principal.*

Remarque. – Pour $\mathfrak{p} \in \mathrm{Spec}(A)$, le foncteur de localisation $M \mapsto A_\mathfrak{p} \otimes_A M = M_\mathfrak{p}$ est exact, *i.e.* $A_\mathfrak{p}$ est plat sur A. Il s'ensuit que l'application produit

$$A_\mathfrak{p} \otimes_A I \longrightarrow A_\mathfrak{p}I = IA_\mathfrak{p}$$

est un isomorphisme, et par là que le $A_\mathfrak{p}$-module $A_\mathfrak{p} \otimes_A I$ est libre de rang 1. On dit que *le A-module I est localement libre de rang* 1. Une vertu des A-modules localement libres est qu'ils sont *plats* sur A. Il en découle que pour deux idéaux inversibles I, J, l'application produit

$$I \otimes_A J \longrightarrow IJ$$

est un isomorphisme.

Si I, J sont des idéaux fractionnaires inversibles, il est clair que IJ en est un aussi. Ainsi l'ensemble de tous les idéaux fractionnaires inversibles de A est un *groupe abélien* pour la multiplication.

3.2.3 DÉFINITION.– *Pour A comme ci-dessus, on note*
- $\mathrm{Div}(A)$ *le groupe des idéaux fractionnaires inversibles.*
- $\mathrm{Div.Pr}(A)$ *le sous-groupe des idéaux fractionnaires principaux.*
- $\mathrm{Pic}(A) := \mathrm{Div}(A)/\mathrm{Div.Pr}(A)$.

3.2.4 DÉFINITION.– *La dimension de Krull d'un anneau A (pas nécessairement intègre) est la longueur maximale d'une chaîne $\mathcal{P}_0 \subsetneq \mathcal{P}_1 \subsetneq \cdots \subsetneq \mathcal{P}_l$ d'idéaux premiers.*

Exemples. – Pour A intègre, on a :
- $\dim(A) = 0 \Leftrightarrow A$ est un corps.
- $\dim(A) \leqslant 1 \Leftrightarrow$ tout idéal premier non nul est maximal.
- Si A est un AVD, alors $\dim(A) = 1$.

Par ailleurs, on peut montrer que $\dim(A[X]) = \dim(A) + 1$.

3.2.5 PROPOSITION.– *Soit A un anneau local intègre et $\mathfrak{m}$ son idéal maximal, supposé non nul. Alors on a équivalence entre :*

i) A est un AVD

ii) A est principal

iii) A est noethérien et $\mathfrak{m}$ est principal

iv) A est noethérien et $\mathfrak{m}$ est inversible

v) Tout idéal fractionnaire non nul est inversible

vi) A est noethérien, normal et $\dim(A) = 1$.

Démonstration. *i)* $\Rightarrow$ *ii)* $\Rightarrow$ *iii)* par définition. Montrons *iii)* $\Rightarrow$ *i)*. Supposons donc $\mathfrak{m}$ principal et choisissons un générateur ϖ de $\mathfrak{m}$. Soit $N := \bigcap_{n\in\mathbb{N}} \varpi^n A$. Comme A est supposé noethérien, N est de type fini. Mais comme $\mathfrak{m}N = \varpi N = N$, le lemme de Nakayama nous dit que $N = 0$. Ainsi pour tout $a \in A$ non nul il existe un unique entier n tel que $a \in \varpi^n A \setminus \varpi^{n+1}A$. On en déduit que $A \setminus \{0\} = \bigsqcup_{n\in\mathbb{N}} \varpi^n A^\times$, puis que les idéaux non nuls sont tous de la forme $\varpi^n A$ et finalement que ϖA est le seul idéal premier non nul.

iii) $\Leftrightarrow$ *iv)* puisque "inversible"="principal" dans un anneau local (cf propriétés 3.2.2). *ii)* $\Leftrightarrow$ *v)* pour la même raison.

i) $\Rightarrow$ *vi)* : on a vu que la dimension d'un AVD est 1, et tout anneau factoriel est normal.

Pour conclure, nous allons montrer *vi)* $\Rightarrow$ *iv)*. On doit donc montrer que $\mathfrak{m}\mathfrak{m}^{-1} = A$ sous les hypothèses de *vi)*, ce que nous ferons en 4 étapes.

a) posons $E(\mathfrak{m}) := \{x \in \mathrm{Frac}(A), x\mathfrak{m} \subset \mathfrak{m}\}$. Comme A est noethérien, $\mathfrak{m}$ est de type fini sur A et $E(\mathfrak{m}) \subset \mathrm{End}_A(\mathfrak{m})$ aussi. Donc $E(\mathfrak{m})$ est un anneau entier sur A donc, puisque A est normal, $E(\mathfrak{m}) = A$.

b) On a $A \subset \mathfrak{m}^{-1}$ donc $\mathfrak{m} \subset \mathfrak{m}\mathfrak{m}^{-1} \subset A$. D'où la dichotomie : soit $\mathfrak{m}\mathfrak{m}^{-1} = A$, soit $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$. Dans le dernier cas, on obtiendrait $\mathfrak{m}^{-1} \subset E(\mathfrak{m})$ donc par a) $\mathfrak{m}^{-1} \subset A$ et finalement $\mathfrak{m}^{-1} = A$. Nous allons montrer que c'est impossible en prouvant que $A \subsetneq \mathfrak{m}^{-1}$.

c) L'ensemble des idéaux I tels que $A \subsetneq I^{-1}$ est non-vide (car il contient les idéaux principaux) donc, puisque A est noethérien, admet un élément maximal, disons $\mathfrak{a}$. Si l'on prouve que $\mathfrak{a}$ est premier, alors l'hypothèse $\dim(A) = 1$ impliquera $\mathfrak{a} = \mathfrak{m}$, comme voulu.

d)Montrons que $\mathfrak{a}$ est premier. Soient $x, y \in A$ t.q. $xy \in \mathfrak{a}$ et $x \notin \mathfrak{a}$. On doit prouver que $y \in \mathfrak{a}$. Or, on a $(x) + \mathfrak{a} \supsetneq \mathfrak{a}$ et donc, par définition de $\mathfrak{a}$, il s'ensuit $((x) + \mathfrak{a})^{-1} = A$. Soit alors $z \in \mathfrak{a}^{-1} \setminus A$. On a $zy((x) + \mathfrak{a}) \subset \mathfrak{a}\mathfrak{a}^{-1} + y\mathfrak{a}\mathfrak{a}^{-1} \subset A$ donc $zy \in ((x) + \mathfrak{a})^{-1} = A$. Il s'ensuit que $z \in ((y) + \mathfrak{a})^{-1}$ et donc que $((y) + \mathfrak{a}^{-1}) \supsetneq A$. Par définition de $\mathfrak{a}$ on a donc $(y) + \mathfrak{a} = \mathfrak{a}$ et $y \in \mathfrak{a}$. □

3.3 Anneaux de Dedekind

3.3.1 THÉORÈME.– *Soit A un anneau intègre. Les propriétés suivantes sont équivalentes.*

i) A est noethérien, normal et $\dim(A) \leqslant 1$.

ii) A est noethérien et $A_\mathfrak{p}$ est un AVD pour tout idéal premier $\mathfrak{p}$ non nul.

iii) Tous les idéaux fractionnaires non nuls de A sont inversibles.

Sous ces conditions, on dit que A est un anneau de Dedekind.

Démonstration. Supposons *i*) et montrons *ii*). Soit S une partie multiplicative de A. La forme des idéaux de $S^{-1}A$ montre que $S^{-1}A$ est noethérien puisque A l'est, et $\dim(S^{-1}A) \leqslant \dim(A) \leqslant 1$. Montrons que $S^{-1}A$ est normal. Supposons que $x \in \mathrm{Frac}(S^{-1}A) = \mathrm{Frac}(A)$ satisfait l'équation $x^n + a_1x^{n-1} + \cdots + a_n = 0$ avec $a_i \in S^{-1}A$. Choisissons alors $s \in S$ tel que $sa_i \in A$ pour tout i. On a $(sx)^n + sa_1(sx)^{n-1} + \cdots + s^n a_n = 0$, donc $sx \in A$ puisque A est normal, et finalement $x \in S^{-1}A$.

Supposons maintenant *ii*) et montrons *iii*). Soit I un idéal fractionnaire de A. Pour tout idéal premier $\mathfrak{p}$, le sous-$A_\mathfrak{p}$-module $IA_\mathfrak{p}$ de $\mathrm{Frac}(A)$ est un idéal fractionnaire de $A_\mathfrak{p}$, et il est clair que $(IA_\mathfrak{p})^{-1} = I^{-1}A_\mathfrak{p}$. On a donc $(II^{-1})A_\mathfrak{p} = (IA_\mathfrak{p})(IA_\mathfrak{p})^{-1}$ et, par notre hypothèse, $(II^{-1})A_\mathfrak{p} = A_\mathfrak{p}$. Ceci signifie que l'idéal II^{-1} de A n'est contenu dans aucun idéal premier $\mathfrak{p}$. Il s'ensuit que $II^{-1} = A$.

Supposons enfin *iii*) et montrons *i*). Sous l'hypothèse *iii*), tous les idéaux sont inversibles donc, par une propriété vue plus haut, de type fini. A est donc noethérien. Montrons qu'il est normal. Soit $x \in \mathrm{Frac}(A)$ entier sur A. Alors l'anneau $B := A[x]$ est de type fini sur A, donc est un idéal fractionnaire, donc est inversible par hypothèse. Il s'ensuit que $B = BA = BBB^{-1} = BB^{-1} = A$, et en particulier que $x \in A$. Reste à montrer que $\dim(A) \leqslant 1$, ce qui équivaut à montrer que tout idéal premier *non nul* $\mathfrak{p}$ de A est maximal. Choisissons un idéal maximal $\mathfrak{m} \supset \mathfrak{p}$, de sorte que $\mathfrak{p}\mathfrak{m}^{-1} \subset A$ est un idéal (ordinaire) de A. Puisque $\mathfrak{p}$ est premier, l'égalité $\mathfrak{p} = (\mathfrak{p}\mathfrak{m}^{-1})\mathfrak{m}$ implique que $\mathfrak{p} \supset \mathfrak{m}$ ou $\mathfrak{p} \supset \mathfrak{p}\mathfrak{m}^{-1}$. Le deuxième cas est impossible car il implique $\mathfrak{m}^{-1} \subset A$ donc $A \subset \mathfrak{m}$. Le premier cas nous dit $\mathfrak{p} = \mathfrak{m}$ est maximal, comme voulu. □

Tout anneau intègre principal est donc un anneau de Dedekind. Le premier intérêt de la notion d'anneau de Dedekind est que, contrairement à celle d'anneau principal, elle est stable par clôture intégrale dans une extension séparable.

3.3.2 Proposition.– *Soit A un anneau de Dedekind et L une extension séparable finie de $K = \mathrm{Frac}(A)$. Alors la clôture intégrale B de A dans L est un anneau de Dedekind.*

Démonstration. Par construction, B est intègre et normal. D'après le théorème 2.4.6, on sait que B est un A-module de type fini. Il s'ensuit que tout idéal de B est un A-module de type fini, donc *a fortiori* un B-module de type fini : B est noethérien. Soit $\mathfrak{p}$ un idéal premier de B. Alors $A \cap \mathfrak{p}$ est un idéal premier de A. Montrons qu'il est non nul. Soit $b \in \mathfrak{p} \setminus \{0\}$ et $b^n + a_1b^{n-1} + \cdots + a_n = 0$ l'équation minimale de b sur A. Alors $a_n \in A \cap \mathfrak{p}$ est non nul, donc $A \cap \mathfrak{p} \neq (0)$. Il sensuit que $A/(A \cap \mathfrak{p})$ est un corps et $B/\mathfrak{p}$ est une $A/(A \cap \mathfrak{p})$-algèbre intègre de dimension finie, donc est aussi un corps. L'idéal $\mathfrak{p}$ est donc maximal, et $\dim(B) \leqslant 1$. □

Exemple. – Si K est un corps de nombres, $\mathcal{O}_K$ est un anneau de Dedekind.

Venons-en maintenant à la vertu essentielle des anneaux de Dedekind annoncée dans l'introduction, à savoir la propriété d'unique factorisation des idéaux.

3.3.3 *Valuations associées aux idéaux maximaux.* Soit A un anneau de Dedekind et $K = \mathrm{Frac}(A)$. On a $\mathrm{Spec}(A) = \mathrm{Max}(A) \cup \{0\}$. On pourra donc dire "idéal maximal" pour "idéal premier non nul". Soit $\mathfrak{p} \in \mathrm{Max}(A)$. Puisque $A_\mathfrak{p}$ est un anneau de valuation discrète et $\mathrm{Frac}(A_\mathfrak{p}) = K$, on a une valuation discrète normalisée

$$v_\mathfrak{p} : K \longrightarrow \mathbb{Z} \cup \{\infty\}$$

qui envoie $\alpha \in K^\times$ sur l'unique entier $v_\mathfrak{p}(\alpha)$ tel que $\alpha A_\mathfrak{p} = (\mathfrak{p}A_\mathfrak{p})^{v_\mathfrak{p}(\alpha)} = \mathfrak{p}^{v_\mathfrak{p}(\alpha)}A_\mathfrak{p}$. Réciproquement, si v est une valuation discrète normalisée sur K et *non-négative sur* A, alors $\mathfrak{p} := \{\alpha \in K, v(\alpha) > 0\}$ est un idéal maximal de A et $v = v_\mathfrak{p}$.

Plus généralement, si I est un idéal fractionnaire non nul de A, on pose

$$v_\mathfrak{p}(I) := \text{ unique entier } i \text{ tel que } IA_\mathfrak{p} = \mathfrak{p}^i A_\mathfrak{p}.$$

On a alors les propriétés faciles suivantes.

Propriétés. (Exercice) – Soient I, J deux idéaux fractionnaires de A.

i) $v_\mathfrak{p}(IJ) = v_\mathfrak{p}(I) + v_\mathfrak{p}(J)$,

ii) $v_\mathfrak{p}(I + J) = \min(v_\mathfrak{p}(I), v_\mathfrak{p}(J))$,

iii) $v_\mathfrak{p}(I \cap J) = \max(v_\mathfrak{p}(I), v_\mathfrak{p}(J))$,

iv) $I \subset J \Rightarrow (\forall \mathfrak{p} \in \mathrm{Max}(A), v_\mathfrak{p}(I) \geqslant v_\mathfrak{p}(J))$.

3.3.4 Théorème.– *Soit A un anneau de Dedekind. Pour tout idéal fractionnaire non nul I de A, l'ensemble $\{\mathfrak{p} \in \mathrm{Max}(A),\ v_\mathfrak{p}(I) \neq 0\}$ est fini et*

$$I = \prod_{\mathfrak{p} \in \mathrm{Max}(A)} \mathfrak{p}^{v_\mathfrak{p}(I)}.$$

De plus, cette factorisation est unique au sens où, pour toute factorisation $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ où les $\mathfrak{p}_i$ sont des idéaux maximaux, on a $e_i = v_{\mathfrak{p}_i}(I)$ et $v_\mathfrak{p}(I) = 0$ si $\mathfrak{p} \notin \{\mathfrak{p}_1, \cdots, \mathfrak{p}_r\}$.

Démonstration. 1) Nous montrons d'abord l'existence d'une factorisation $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Pour cela on peut supposer que I est un idéal ordinaire de A et le noter I_0. On construit alors par récurrence une suite croissante d'idéaux comme suit. Si $I_{n-1} = A$, on pose $I_n = A$. Sinon, on choisit un idéal maximal $\mathfrak{p}_n$ contenant I_{n-1} et on pose $I_n := \mathfrak{p}_n^{-1} I_{n-1}$. C'est encore un idéal, puisque $\mathfrak{p}_n^{-1} \subset I^{-1}$, et il contient *strictement* I_{n-1} puisque $A \subsetneq \mathfrak{p}_n^{-1}$. Puisque A est noethérien, la suite $(I_n)_{n \in \mathbb{N}}$ devient stationnaire à partir d'un rang n_0. Par construction, cela signifie que $I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_{n_0-1} \subsetneq I_{n_0} = A$, et que $I_0 = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k I_k$ pour tout $k \leqslant n_0$ et en particulier pour $k = n_0$ on obtient une factorisation $I_0 = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{n_0}$, que l'on peut réécrire, après changement de notation, sous la forme $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ avec les $\mathfrak{p}_i$ deux à deux distincts.

2) Nous montrons que dans toute factorisation comme ci-dessus on a $e_i = v_{\mathfrak{p}_i}(I)$ et $v_\mathfrak{p}(I) = 0$ pour $\mathfrak{p} \neq \mathfrak{p}_1, \cdots, \mathfrak{p}_r$. Pour cela, il faut remarquer que si $\mathfrak{q}$ est maximal et distinct de $\mathfrak{q}_1, \cdots, \mathfrak{q}_s$ maximaux, alors pour tout i on a $\mathfrak{q} + \mathfrak{q}_i = A$, donc après produit il vient

$\mathfrak{q} + \mathfrak{q}_1^{f_1} \cdots \mathfrak{q}_s^{f_s} = A$ pour toute famille d'entiers $f_1, \cdots, f_s$. Il s'ensuit que $\mathfrak{q}_1^{f_1} \cdots \mathfrak{q}_s^{f_s} A_\mathfrak{q}$ n'est pas inclus dans l'idéal maximal $\mathfrak{q}A_\mathfrak{q}$ de $A_\mathfrak{q}$, donc est l'idéal unité de $A_\mathfrak{q}$, et finalement que $v_\mathfrak{q}(\mathfrak{q}^{f_0}\mathfrak{q}_1^{f_1} \cdots \mathfrak{q}_s^{f_s}) = v_\mathfrak{q}(\mathfrak{q}^{f_0}) = f_0$.

3) Il découle de 1) et 2) que l'ensemble $\{\mathfrak{p} \in \mathrm{Max}(A),\, v_\mathfrak{p}(I) \neq 0\}$ est fini et que $I = \prod_{\mathfrak{p} \in \mathrm{Max}(A)} \mathfrak{p}^{v_\mathfrak{p}(I)}$. □

Voici quelques conséquences immédiates du théorème.

Conséquences. – Soient I, J deux idéaux fractionnaires non nuls de A de Dedekind.

i) $I \subset J \Leftrightarrow (\forall \mathfrak{p} \in \mathrm{Max}(A), v_\mathfrak{p}(I) \geqslant v_\mathfrak{p}(J))$. Ceci améliore la propriété *iv)* avant le théorème.

ii) $I = \bigcap_{\mathfrak{p} \in \mathrm{Max}(A)} IA_\mathfrak{p}$. (En effet, $IA_\mathfrak{p} = \{x \in A,\, v_\mathfrak{p}(x) \geqslant v_\mathfrak{p}(I)\}$, donc ii) découle de i)).

iii) Le théorème des restes Chinois nous dit que

$$A/I \xrightarrow{\sim} \prod_{\mathfrak{p} \in \mathrm{Max}(A)} A/\mathfrak{p}^{v_\mathfrak{p}(I)}.$$

En effet, pour tout $\mathfrak{p} \in \mathrm{Max}(A)$, on a $\mathfrak{p}^{v_\mathfrak{p}(I)} + \prod_{\mathfrak{q} \neq \mathfrak{p}} \mathfrak{q}^{v_\mathfrak{q}(I)} = A$ comme dans la preuve ci-dessus. Cette décomposition peut aussi s'exprimer comme un résultat *d'approximation simultanée* : soient $\mathfrak{p}_1, \cdots, \mathfrak{p}_r \in \mathrm{Max}(A)$ deux à deux distincts, $e_1, \cdots, e_r \in \mathbb{N}$ et $x_1, \cdots, x_n \in A$. *Alors il existe* $x \in A$ *tel que* $v_{\mathfrak{p}_i}(x - x_i) \geqslant e_i$ *pour tout* $i = 1, \cdots, r$.

iv) Deux idéaux I, J non nuls sont premiers entre eux (ie $I + J = A$) si et seulement si ils n'ont pas de facteur premier commun.

Exercice. – i) Soient $\mathfrak{p}_1, \cdots, \mathfrak{p}_r \in \mathrm{Max}(A)$ deux à deux distincts et $e_1, \cdots, e_r \in \mathbb{N}$. Montrer qu'il existe $x \in A$ tel que $v_{\mathfrak{p}_i}(x) = e_i$ pour $i = 1, \cdots, r$.

ii) Soit maintenant I un idéal non nul de A. Trouver $x \in A$ tel que $(x) = IJ$ avec J et I premiers entre eux.

iii) En utilisant l'isomorphisme $I/IJ = I/(I \cap J) \xrightarrow{\sim} (I + J)/J$, en déduire que I est engendré par 2 éléments.

Comme on l'a vu, un anneau de Dedekind n'est pas nécessairement principal. On mesure son défaut de principalité par son groupe de classes.

3.3.5 *Groupe des classes.* Soit A un anneau de Dedekind. Notons $\mathfrak{Z}^1(A)$ le groupe abélien libre de base les idéaux maximaux [3] de A . et $\mathfrak{Z}^1_{\mathrm{prin}}(A)$, le sous-groupe engendré par les sommes $\sum_i a_i \mathfrak{p}_i$ telles que l'idéal $\prod_i \mathfrak{p}_i^{a_i}$ soit *principal.* On définit alors

$$\mathcal{C}\ell(A) := \mathfrak{Z}^1(A)/\mathfrak{Z}^1_{\mathrm{prin}}(A).$$

3. Pour une définition générale, il faut remplacer "idéaux maximaux" par "idéaux premiers de hauteur 1" dans cette définition, ce qui correspond géométriquement aux cycles de codimension 1

On remarquera que le théorème de factorisation unique des idéaux nous dit que $\mathcal{C}\ell(A) = \mathrm{Pic}(A)$.[4] De plus, par définition, on voit que A est principal si et seulement si $\mathcal{C}\ell(A) = 0$.[5] Nous verrons plus tard une manière de borner l'ordre du groupe des classes d'un anneau de nombres $\mathcal{O}_K$, qui dans certains cas permet de le calculer.

3.3.6 *Structure des modules de type fini.* Même lorsque A n'est pas principal, la structure des A-modules de type fini est raisonnablement simple. Nous l'expliquons ici, mais nous ne démontrerons que le nécessaire pour la suite, et laisserons le reste "en exercice".

Notons $K := \mathrm{Frac}(A)$. Soit M un A-module de type fini. On a une suite exacte

$$0 \longrightarrow M_{\mathrm{tors}} \longrightarrow M \longrightarrow M/M_{\mathrm{tors}} \longrightarrow 0$$

où $M_{\mathrm{tors}} = \{m \in M, \exists a \in A \setminus \{0\}, am = 0\} = \mathrm{Ker}(M \longrightarrow K \otimes_A M)$ est un module *de torsion* et $M/M_{\mathrm{tors}} = \mathrm{Im}(M \longrightarrow K \otimes_A M)$ est un module *sans torsion.*

Fait. – *Pour A anneau de Dedekind, cette suite exacte est scindée (non canoniquement). On peut donc écrire $M = M_{\mathrm{tors}} \oplus M'$ avec M' sans torsion.*

Explication. Un A-module de type fini sans torsion est *localement libre* (pour tout $\mathfrak{p}$, le $A_\mathfrak{p}$-module sans torsion $A_\mathfrak{p} \otimes_A M$ est libre car $A_\mathfrak{p}$ est principal) donc *projectif.* □

Ceci nous ramène à étudier séparément les modules de torsion et les modules sans torsion. Pour M sans torsion, on pose $\mathrm{rg}(M) := \dim_K(K \otimes_A M)$. Si $\mathrm{rg}(M) = 1$, M est donc isomorphe à un idéal fractionnaire non nul, donc inversible, de A. Plus généralement :

Proposition. – *Soit M un A-module sans torsion de rang n.*

i) Il existe des idéaux fractionnaires inversibles $I_1, \cdots, I_n$ tels que $M \simeq I_1 \oplus \cdots \oplus I_n$.

ii) Pour toute autre collection $I'_1, \cdots, I'_n$, on a $M \simeq I'_1 \oplus \cdots \oplus I'_n$ si et seulement si $\prod_i I_i = \prod_i I'_i$ dans $\mathcal{C}\ell(A)$.

Démonstration. i) On a déjà vu le cas $n = 1$. Pour $n > 1$ soit $\pi : (K \otimes_A M) \longrightarrow K$ une forme K-linéaire non nulle. On en déduit une suite exacte $(M \cap \mathrm{Ker}(\pi)) \hookrightarrow M \twoheadrightarrow \mathrm{Im}(\pi)$. Comme $\mathrm{Im}(\pi)$ est sans torsion de rang 1, il est isomorphe à un idéal inversible. Ce dernier est projectif, donc la suite se scinde et on conclut par récurrence sur n.

ii) Regardons le cas $n = 1$. Si $I = I'$ dans $\mathcal{C}\ell(A)$ alors $I^{-1}I'$ est principal, disons engendré par $x \in K$, et la multiplication par x induit un isomorphisme $I \xrightarrow{\sim} I'$. Réciproquement, si $\varphi : I \xrightarrow{\sim} I'$ est un isomorphisme, il s'étend en un isomorphisme $I \otimes_A K = K \xrightarrow{\sim} J \otimes_A K = K$, lequel est donné par la multiplication par un $x \in K$. Ce x engendre donc $I^{-1}I'$.

Pour $n > 1$, notons que $\prod_i I_i$ est le déterminant de M (l'image de $M \otimes \cdots \otimes M$ dans $\bigwedge^n(K \otimes_A M)$). Donc la condition "$\prod_i I_i = \prod_i I'_i$ dans $\mathcal{C}\ell(A)$", qui équivaut à la condition "$\prod_i I_i \simeq \prod_i I'_i$", est nécessaire. Pour voir qu'elle est suffisante, il suffit de prouver que $I_1 \oplus \cdots \oplus I_n \simeq A^{n-1} \oplus \prod_i I_i$. Par récurrence, il suffit de traiter le cas $n = 2$, *ie* $I \oplus J \simeq A \oplus IJ$. Soient alors $a, b \in K$ tels que $aI + bJ = A$ (cf lemme ci-dessous), puis soient i, j tels que $ai + bj = 1$. Alors la matrice

4. Plus généralement, si A est noethérien et localement factoriel, $\mathcal{C}\ell(A)$ coïncide avec $\mathrm{Pic}(A)$.
5. Plus généralement, une anneau A noethérien normal est factoriel si et seulement si $\mathcal{C}\ell(A) = 0$.

$\begin{pmatrix} a & b \\ -abj & abi \end{pmatrix}$ est dans $\mathrm{GL}_2(K)$ et envoie le sous-module $I \oplus J$ de $K \oplus K$ dans le sous-module $A \oplus abIJ$ qui est isomorphe à $A \oplus IJ$. □

LEMME. – *Soient I, J deux idéaux fractionnaires inversibles. Alors il existe $a, b \in K$ tels que $aI + bJ = A$.*

Démonstration. On peut supposer que I et J sont dans A. Si I et J sont premiers entre eux, on a $I + J = A$, et on n'a rien à faire. Sinon, soit x un élément de A tel que $v_\mathfrak{p}(x) = v_\mathfrak{p}(I)$ pour tout $\mathfrak{p}$ tel que $v_\mathfrak{p}(J) > 0$. Alors $x^{-1}I$ et J n'ont plus de facteur premier en commun ($v_\mathfrak{p}(I)v_\mathfrak{p}(J) = 0$ pour tout $\mathfrak{p}$), *mais* $x^{-1}I$ n'est plus un idéal. Choisissons donc y tel que $v_\mathfrak{q}(y) = -v_\mathfrak{q}(x^{-1}I)$ pour tout $\mathfrak{q}$ tel que $v_\mathfrak{q}(x^{-1}I) < 0$ *et* $v_\mathfrak{p}(y) = 0$ pour tout $\mathfrak{p} \supset J$. Alors yxI est un idéal premier à J, donc $xyI + J = A$. □

Remarque. – Pour $I = J$ on retrouve le fait que I^{-1} est engendré par deux éléments.

Intéressons-nous maintenant aux modules de torsion. A est toujours un anneau de Dedekind.

PROPOSITION. – *Soit M un A-module de type fini de torsion. Pour $\mathfrak{p} \in \mathrm{Max}(A)$, posons $M_{\mathfrak{p}-\mathrm{tors}} := \{m \in M,\ \exists k \in \mathbb{N},\ \mathfrak{p}^k m = 0\}$.*

i) Alors $M = \bigoplus_{\mathfrak{p} \in \mathrm{Max}(A)} M_{\mathfrak{p}-\mathrm{tors}}$ (et en particulier, $\{\mathfrak{p} \in \mathrm{Max}(A), M_{\mathfrak{p}-\mathrm{tors}} \neq 0\}$ est fini).

ii) Pour chaque $\mathfrak{p}$ tel que $M_{\mathfrak{p}-\mathrm{tors}} \neq 0$ il existe une unique suite d'entier $n_1 \leqslant n_2 \leqslant \cdots \leqslant n_r$ telle que $M_{\mathfrak{p}-\mathrm{tors}} \simeq A/\mathfrak{p}^{n_1} \oplus \cdots \oplus A/\mathfrak{p}^{n_r}$.

Exercice. – En déduire que tout module de torsion M admet une unique décomposition de la forme $M = A/I_1 \oplus A/I_2 \oplus \cdots \oplus A/I_r$ avec $I_1 | I_2 | \cdots | I_r$.

Démonstration. i) Pour $m \in M$, l'idéal annulateur $\mathrm{Ann}(m) = \{a \in A, am = 0\}$ est non nul. Puisque M est de type fini, il existe donc un idéal I qui annule M (*i.e.* $I.M = 0$), par exemple l'intersection des annulateurs d'une famille génératrice.

Maintenant, si $M_{\mathfrak{p}-\mathrm{tors}} \neq 0$, alors $\mathfrak{p} \supset I$. En effet, dans le cas contraire, l'égalité $\mathfrak{p}^k + I = A$ montre que $\mathfrak{p}^k m = 0 \Rightarrow m = 0$. Par ailleurs, pour $\mathfrak{p} \supset I$, on a $\mathfrak{p}^{v_\mathfrak{p}(I)} M_{\mathfrak{p}-\mathrm{tors}} = 0$.

Considérons l'idéal $\sum_{\mathfrak{p} \supset I} I.\mathfrak{p}^{-v_\mathfrak{p}(I)}$. Il n'est contenu dans aucun idéal maximal car les $I\mathfrak{p}^{-v_\mathfrak{p}(I)}$ n'ont pas de facteur commun. C'est donc l'idéal unité et on peut écrire $1 = \sum_{\mathfrak{p} \supset I} x_\mathfrak{p}$ avec $x_\mathfrak{p} \in I\mathfrak{p}^{-v_\mathfrak{p}(I)}$. Pour tout $m \in M$, on a $\mathfrak{p}^{v_\mathfrak{p}(I)}.(x_\mathfrak{p} m) = 0$ donc $x_\mathfrak{p} m \in M_{\mathfrak{p}-\mathrm{tors}}$. L'égalité $m = \sum_{\mathfrak{p} \supset I} x_\mathfrak{p} m$ montre alors que $M = \sum_\mathfrak{p} M_{\mathfrak{p}-\mathrm{tors}}$. De plus, si $\mathfrak{q} \neq \mathfrak{p}$ est un autre idéal contenant I, alors $x_\mathfrak{p} M_{\mathfrak{q}-\mathrm{tors}} = 0$. Il s'ensuit que la somme est directe, car si l'on se donne des éléments $(m_\mathfrak{p})_{\mathfrak{p} \supset I}$ tels que $\sum_\mathfrak{p} m_\mathfrak{p} = 0$, on a $m_\mathfrak{p} = x_\mathfrak{p}(\sum_\mathfrak{p} m_\mathfrak{p}) = 0$.

ii) peut se démontrer de manière élémentaire. Mais nous allons le déduire de la structure connue des modules de type fini sur un anneau principal, en prouvant que $M_{\mathfrak{p}-\mathrm{tors}}$ s'identifie au localisé de M en $\mathfrak{p}$. □

LEMME. – *(Ici A peut être un anneau commutatif quelconque). Soit $\mathfrak{m}$ un idéal maximal de A, et M un A-module de $\mathfrak{m}$-torsion,* i.e. *annulé par une puissance de $\mathfrak{m}$. Alors*

i) L'application $M \longrightarrow M_\mathfrak{m} = A_\mathfrak{m} \otimes_A M$ est bijective.

ii) Pour tout idéal maximal $\mathfrak{n}$ *distinct de* $\mathfrak{m}$*, on a* $M_{\mathfrak{n}} = 0$*.*

Démonstration. i) *Injectivité.* Par définition de la localisation on a $\mathrm{Ker}(M \longrightarrow M_{\mathfrak{m}}) = \{m \in M, \exists s \in A \setminus \mathfrak{m}, sm = 0\}$. Soit donc $m \in M$ annulé par $s \in A \setminus \mathfrak{m}$. On a $(s) + \mathfrak{m} = A$ donc $(s) + \mathfrak{m}^k = A$ pour tout $k \in \mathbb{N}$. Choisissons k tel que $\mathfrak{m}^k$ annule m. On voit que A annule m et donc $m = 0$.

Surjectivité. Soit $x = \frac{m}{s}$ un élément de $M_{\mathfrak{m}}$, avec $m \in M$ et $s \in A \setminus \mathfrak{m}$. Choisissons encore k tel que $\mathfrak{m}^k$ annule m, et t tel que $st \in 1 + \mathfrak{m}^k$. Alors l'image de $tm \in M$ dans $M_{\mathfrak{m}}$ est $x = \frac{m}{s}$.

ii) Tout élément $s \in \mathfrak{m} \setminus \mathfrak{n}$ agit de manière nilpotente sur M, donc $S^{-1}M = 0$ dès que $s \in S$, et en particulier $M_{\mathfrak{n}} = 0$. □

Le i) signifie qu'on peut considérer M comme un $A_{\mathfrak{m}}$-module, ce qui à certains égards est pratique, car $A_{\mathfrak{m}}$ est local.

Corollaire. – *(Ici* A *est à nouveau de Dedekind). Soit* M *un* A*-module de type fini de torsion. Alors pour tout* $\mathfrak{p} \in \mathrm{Max}(A)$ *l'application* $M \longrightarrow M_{\mathfrak{p}}$ *induit un isomorphisme* $M_{\mathfrak{p}-\mathrm{tors}} \xrightarrow{\sim} M_{\mathfrak{p}}$ *et l'application produit* $M \xrightarrow{\sim} \bigoplus_{\mathfrak{p} \in \mathrm{Max}(A)} M_{\mathfrak{p}}$ *est un isomorphisme.*

Preuve du ii) de la proposition précédente. Puisque $A_{\mathfrak{p}}$ est un anneau principal, on sait qu'il existe une unique suite d'entiers $n_1 \leqslant n_2 \leqslant \cdots \leqslant n_r$ telle que $M_{\mathfrak{p}} \simeq A_{\mathfrak{p}}/(\mathfrak{p}A_{\mathfrak{p}})^{n_1} \oplus \cdots \oplus A_{\mathfrak{p}}/(\mathfrak{p}A_{\mathfrak{p}})^{n_r}$. Reste alors à appliquer à nouveau le lemme ci-dessus pour voir que $A/\mathfrak{p}^e \xrightarrow{\sim} A_{\mathfrak{p}} \otimes_A (A/\mathfrak{p}^e) = A_{\mathfrak{p}}/(\mathfrak{p}A_{\mathfrak{p}})^e$. □

Remarque. (*"Rappel" sur les modules de longueur finie*) – Soit A un anneau commutatif. Un A-module est dit "de longueur finie" s'il est à la fois noethérien (toute suite croissante de sous-modules stationne) et artinien (toute suite décroissante de sous-modules stationne). Dans ce cas, il existe des chaînes $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_l = M$ de A-sous-modules de longueur l maximale. Noter qu'une chaîne est de longueur maximale si et seulement si les quotients successifs M_i/M_{i-1} sont des A-modules simples. On montre alors que de telles chaines ont toutes la même longueur, appelée longueur de M. Il s'ensuit facilement que dans une suite exacte $M_1 \hookrightarrow M_2 \twoheadrightarrow M_3$ on a $\mathrm{long}(M_2) = \mathrm{long}(M_1) + \mathrm{long}(M_3)$.

Soit $M := A/\mathfrak{p}^n$. On a une filtration finie $M \supset \mathfrak{p}M \supset \cdots \supset \mathfrak{p}^{n-1}M \supset \{0\}$ dont les sous-quotients successifs sont de la forme $\mathfrak{p}^i/\mathfrak{p}^{i+1}$. Chaque $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ est un $A/\mathfrak{p}$-espace vectoriel de dimension finie. Il s'ensuit que $A/\mathfrak{p}^n$ est un A-module de longueur finie. En fait, si $x \in A$ est tel que $v_{\mathfrak{p}}(x) = i$, la multiplication par x induit un morphisme $A/\mathfrak{p} \longrightarrow \mathfrak{p}^i/\mathfrak{p}^{i+1}$.

Lemme. – *Ce morphisme est un isomorphisme. En conséquence* $\mathrm{long}_A(A/\mathfrak{p}^n) = n$*.*

Démonstration. Comme dans le lemme précédent l'application $\mathfrak{p}^i/\mathfrak{p}^{i+1} \longrightarrow (\mathfrak{p}^i/\mathfrak{p}^{i+1})_{\mathfrak{p}} = (\mathfrak{p}A_{\mathfrak{p}})^i/(\mathfrak{p}A_{\mathfrak{p}})^{i+1}$ est un isomorphisme. On est donc ramené au cas où A est un AVD. Dans ce cas, $\mathfrak{p}^i = (\varpi^i)$ et $x \in \varpi^i A^\times$, et l'assertion est claire. □

Exercice. – Montrer plus généralement que $A/I \simeq J/IJ$ pour I, J idéaux non nuls.

3.3.7 DÉFINITION.– *Soit M un A-module de type fini de torsion. On note $[M]$ l'idéal*

$$[M] = [M]_A = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{long}_A(M_\mathfrak{p})}$$

où $\mathrm{long}_A(M_\mathfrak{p})$ est la longueur du A-module artinien $M_\mathfrak{p}$.

Propriétés. – i) Pour I idéal non nul de A, on a $[A/I]_A = I$.

ii) Si $M_1 \hookrightarrow M_2 \twoheadrightarrow M_3$ est une suite exacte de modules de torsion, on a $[M_2] = [M_1][M_3]$.

iii) Si $A = \mathbb{Z}$, alors $[M]$ est (l'idéal engendré par) le cardinal de M.

iv) Pour tout $\mathfrak{p}$ on a $[M]_A A_\mathfrak{p} = [M_\mathfrak{p}]_{A_\mathfrak{p}}$.

3.3.8 DÉFINITION.– *Si $N \subset M$ sont deux modules sans torsion de même rang, on définit* l'indice $(M : N) = (M : N)_A := [M/N]_A$.

Propriétés. – i) Pour tout $\mathfrak{p}$, on a $(M : N)A_\mathfrak{p} = (M_\mathfrak{p} : N_\mathfrak{p})_{A_\mathfrak{p}}$.

ii) Si $A = \mathbb{Z}$, $(M : N)$ est l'idéal engendré par l'indice au sens usuel.

iii) Si $L \subset N \subset M$, on a $(M : L) = (M : N)(N : L)$. Ceci permet d'étendre la définition à deux sous-modules M, N de rang n dans K^n en posant

$$(M : N) := (M : M \cap N)(N : M \cap N)^{-1}.$$

C'est un idéal fractionnaire de A.

iv) Avec cette définition étendue, si M est de rang n dans K^n et $\alpha \in \mathrm{GL}_n(K)$, alors $(M : \alpha(M)) = \det(\alpha)A$. (Utiliser i) pour se ramener au cas principal).

3.4 Décomposition des idéaux premiers dans une extension

On se place ici dans la situation suivante : A est un anneau de Dedekind, L une extension séparable finie de $K = \mathrm{Frac}(A)$ et B la clôture intégrale de A dans L. Pour $\mathfrak{p} \in \mathrm{Max}(A)$, on s'intéresse aux propriétés de la décomposition $\mathfrak{p}B = \prod_i \mathfrak{P}_i^{e_i}$ de $\mathfrak{p}B$ en produit d'idéaux premiers de B.

Notation. – Si $\mathfrak{p} \in \mathrm{Max}(A)$ et $\mathfrak{P} \in \mathrm{Max}(B)$ sont tels que $\mathfrak{P} \supset \mathfrak{p}$, alors $B/\mathfrak{P}$ est une extension finie du corps $A/\mathfrak{p}$. On note :

- $f(\mathfrak{P}/\mathfrak{p}) := \dim_{A/\mathfrak{p}}(B/\mathfrak{P})$ le *degré résiduel* de $\mathfrak{P}$ sur $\mathfrak{p}$.
- $e(\mathfrak{P}/\mathfrak{p}) := \mathrm{long}_B(B/\mathfrak{p}B)_\mathfrak{P}$ l'*indice de ramification* de $\mathfrak{P}$ sur $\mathfrak{p}$.

3.4.1 PROPOSITION.– *Avec les notations ci-dessus, on a*

$$B/\mathfrak{p}B \simeq \prod_{\mathfrak{P} \in \mathrm{Max}(B), \mathfrak{P} \cap A = \mathfrak{p}} B/\mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}.$$

En conséquence on a :

i) $\mathfrak{p}B = [B/\mathfrak{p}B]_B = \prod_{\mathfrak{P}\cap A=\mathfrak{p}} \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}$, *et*
ii) $[L:K] = \dim_{A/\mathfrak{p}}(B/\mathfrak{p}B) = \sum_{\mathfrak{P}\cap A=\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$.

Démonstration. i) Pour $\mathfrak{Q} \in \mathrm{Max}(B)$ on a $(B/\mathfrak{p}B)_{\mathfrak{Q}} \neq 0 \Rightarrow \mathfrak{p} \subset \mathfrak{Q} \Rightarrow \mathfrak{p} \subset \mathfrak{Q} \cap A$. Comme $\mathfrak{p}$ est maximal dans A et $1 \notin \mathfrak{Q}$, ceci implique $\mathfrak{p} = \mathfrak{Q} \cap A$. On peut donc écrire

$$B/\mathfrak{p}B = \prod_{\mathfrak{P}\cap A=\mathfrak{p}} (B/\mathfrak{p})_{\mathfrak{P}} = \prod_{\mathfrak{P}\cap A=\mathfrak{p}} B_{\mathfrak{P}}/\mathfrak{p}B_{\mathfrak{P}} = \prod_{\mathfrak{P}\cap A=\mathfrak{p}} B_{\mathfrak{P}}/\mathfrak{P}^{v_{\mathfrak{P}}(\mathfrak{p}B)}B_{\mathfrak{P}}.$$

Or, le dernier lemme nous dit que $v_{\mathfrak{P}}(\mathfrak{p}B)$ est aussi la longueur du $B_{\mathfrak{P}}$-module monogène $B_{\mathfrak{P}}/\mathfrak{p}B_{\mathfrak{P}}$, c'est-à-dire $e(\mathfrak{P}/\mathfrak{p})$ par définition.

ii) On a $B/\mathfrak{p}B = (A/\mathfrak{p}) \otimes_A B = (A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}) \otimes_A B = (A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}) \otimes_{A_{\mathfrak{p}}} (A_{\mathfrak{p}} \otimes_A B)$ Or B est sans torsion de rang $[L:K]$ sur A, donc $A_{\mathfrak{p}} \otimes_A B$ est libre de rang $[L:K]$ sur $A_{\mathfrak{p}}$ et finalement $B/\mathfrak{p}B$ est de dimension $[L:K]$ sur $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} = A/\mathfrak{p}$. La deuxième égalité de l'énoncé ii) découle du i). □

On notera simplement "$\mathfrak{P}|\mathfrak{p}$" pour "$\mathfrak{P} \cap A = \mathfrak{p}$" (ce qui équivaut à $\mathfrak{P} \supset \mathfrak{p}$).

Remarque. – L'anneau $B_{\mathfrak{p}} = B \otimes_A A_{\mathfrak{p}}$ s'identifie à la clôture intégrale de $A_{\mathfrak{p}}$ dans L. C'est donc un anneau de Dedekind, et il est libre de rang $[L:K]$ sur $A_{\mathfrak{p}}$. Il est *semi-local* (nombre fini d'idéaux maximaux), et ses idéaux maximaux sont les $\mathfrak{P}B_{\mathfrak{p}}$ pour $\mathfrak{P}|\mathfrak{p}$. On a donc aussi $B_{\mathfrak{p}} = \bigcap_{\mathfrak{P}|\mathfrak{p}} B_{\mathfrak{P}}$. La proposition nous dit que $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}} \simeq \prod B_{\mathfrak{P}}/\mathfrak{p}B_{\mathfrak{P}}$, mais puisque $B_{\mathfrak{p}}$ est intègre, on ne peut pas relever cette décomposition en un produit des $B_{\mathfrak{P}}$ pour $\mathfrak{P}|\mathfrak{p}$. D'ailleurs $B_{\mathfrak{P}}$ n'est pas fini sur $B_{\mathfrak{p}}$ (qui est normal). On verra plus tard comment obtenir une telle décomposition après *complétion* $\mathfrak{p}$*-adique*.

Terminologie. – On dit que $\mathfrak{p}$ est :
– *ramifié* s'il existe $\mathfrak{P}|\mathfrak{p}$ tel que $e(\mathfrak{P}/\mathfrak{p}) > 1$ [ou que $B/\mathfrak{P}$ soit inséparable sur $A/\mathfrak{p}$] [6],
– *inerte* s'il est non ramifié et si $\mathfrak{p}B$ est premier.
– *totalement décomposé* si $|\{\mathfrak{P}|\mathfrak{p}\}| = [L:K]$, *ie* si $e(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p}) = 1$ pour tout $\mathfrak{P}|\mathfrak{p}$.

Le plus facile à détecter est la ramification ou non-ramification. Cela demande d'adapter la notion de discriminant à B sur A, sachant que B n'est pas nécessairement libre sur A.

3.4.2 *Discriminant d'une extension de Dedekind.* Soit M un sous-A-module de rang $n = [L:K]$ dans L. Notons

$$M^* := \{x \in L, \forall y \in M, \mathrm{Tr}_{L/K}(xy) \in A\}.$$

Propriétés :

i) Si M est libre sur A de base $\omega_1, \cdots, \omega_n$, alors M^* est libre sur la base duale $\omega_1^*, \cdots, \omega_n^*$.

ii) En général, M^* est encore un sous-A-module de rang n. (Découle de i))

6. Dans le cas d'anneaux d'entiers de corps de nombres, les corps résiduels sont finis et toutes les extensions résiduelles sont donc séparables

iii) Si $\mathfrak{p} \in \mathrm{Max}(A)$, on a $(M^*)_\mathfrak{p} = (M_\mathfrak{p})^*$ (le second membre est relatif à $A_\mathfrak{p}$ au lieu de A). Exercice.

On définit maintenant l'idéal *fractionnaire* de A

$$D(M) = D_{L/A}(M) := (M^* : M)_A.$$

Propriétés :

i) Dans le cas où M est libre comme ci-dessus, $D(M)$ est l'idéal fractionnaire principal engendré par le déterminant de la matrice de passage des ω_i^* aux ω_i. Mais cette matrice n'est autre que $(\mathrm{Tr}_{L/K}(\omega_i\omega_j))_{i,j}$. On a donc $D_{L/A}(M) = D_{L/K}(\omega_1, \cdots, \omega_n)A$.

ii) Pour tout $\mathfrak{p} \in \mathrm{Max}(A)$ on a $D_{L/A}(M)A_\mathfrak{p} = D_{L/A_\mathfrak{p}}(M_\mathfrak{p})$.

iii) Si N est un autre sous-module de L de rang n, on a $D(N) = D(M)(M : N)_A^2$. (Utiliser ii) pour se ramener au cas principal).

Définition. – *L'idéal discriminant de B sur A est* $\mathrm{disc}(B/A) := D(B) = (B^*, B)_A$.

Noter que c'est bien un idéal et pas seulement un idéal fractionnaire puisque $\mathrm{Tr}_{L/K}(B) \subset A$. Pour A principal, cette définition est compatible avec l'ancienne. En général, on a

$$\mathrm{disc}(B/A)A_\mathfrak{p} = \mathrm{disc}(B_\mathfrak{p}/A_\mathfrak{p}) \text{ pour tout } \mathfrak{p} \in \mathrm{Max}(A).$$

3.4.3 Théorème.– *Un $\mathfrak{p} \in \mathrm{Max}(A)$ est ramifié dans B si et seulement si $\mathfrak{p}|\mathrm{disc}(B/A)$.*

Démonstration. On vient de voir que $\mathfrak{p}|\mathrm{disc}(B/A) \Leftrightarrow \mathrm{disc}(B_\mathfrak{p}/A_\mathfrak{p}) \subsetneq A_\mathfrak{p}$. Comme $A_\mathfrak{p}$ est local, on peut calculer $\mathrm{disc}(B_\mathfrak{p}/A_\mathfrak{p})$ à l'aide d'une base de $B_\mathfrak{p}$ sur $A_\mathfrak{p}$, et on voit ainsi que l'image de $\mathrm{disc}(B_\mathfrak{p}/A_\mathfrak{p})$ dans $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} = A/\mathfrak{p}$ est le discriminant $\mathrm{disc}((B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p})/(A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p})) = \mathrm{disc}((B/\mathfrak{p}B)/(A/\mathfrak{p}))$. Il s'ensuit que $\mathfrak{p}|\mathrm{disc}(B/A) \Leftrightarrow \mathrm{disc}((B/\mathfrak{p}B)/(A/\mathfrak{p}A)) = 0$. La formule $\mathrm{disc}((B/\mathfrak{p}B)/(A/\mathfrak{p}A)) = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{disc}((B/\mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})})/(A/\mathfrak{p}A))$ (à méditer) montre finalement que

$$\mathfrak{p}|\mathrm{disc}(B/A) \Leftrightarrow \exists \mathfrak{P}|\mathfrak{p},\ \mathrm{disc}((B/\mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})})/(A/\mathfrak{p})) = 0.$$

Pour conclure il reste à invoquer le fait général suivant : *si k est un corps et R une k-algèbre locale de dimension finie, on a* $\mathrm{disc}(R/k) \neq 0$ *si et seulement si R est une extension séparable de k.* On a déjà vu en effet le "si". Pour voir le "seulement si", remarquons d'abord que si R n'est pas un corps, alors son radical de Jacobson $J = \sqrt{(0)}$ est non nul. Soit $0 \neq x \in J$, on a alors $\mathrm{Tr}_{R/K}(xy) = 0$ pour tout $y \in R$ (puisque xy est nilpotent), donc la forme bilinéaire $\theta_{R/K}$ est dégénérée et $\mathrm{disc}(R/k) = 0$. Si maintenant R n'est pas séparable, alors $R \otimes_k R$ a un radical de Jacobson non nul, donc $\mathrm{disc}(R \otimes_k R/R) = \mathrm{disc}(R/k)R = 0$. □

Corollaire. – *L'ensemble des $\mathfrak{p} \in \mathrm{Max}(A)$ ramifiés dans B est fini.*

Exemples. – i) (cas quadratique) Si $K = \mathbb{Q}(\sqrt{d})$ avec d sans facteurs carrés, alors
– Si $d \equiv 2, 3[4]$ on a (p ramifié) $\Leftrightarrow$ ($p|4d$).
– Si $d \equiv 1[4]$ on a (p ramifié) $\Leftrightarrow$ ($p|d$).
Dans chacun des cas, si p est ramifié, sa décomposition est de la forme $p\mathcal{O}_K = \mathfrak{P}^2$.

ii) (Cas p-cyclotomique) Pour $K = \mathbb{Q}(e^{2i\pi/p^r})$, l'unique premier ramifié est p.

iii) (Exemple géométrique) Soit $A = \mathbb{C}[X]$ et $B = \mathbb{C}[\sqrt{X}]$. Ici $\mathrm{Max}(A)$ et $\mathrm{Max}(B)$ sont en bijection ($z \mapsto (X - z)$ ou $z \mapsto (\sqrt{X} - z)$) avec les points de la droite affine sur $\mathbb{C}$, et l'application $\mathfrak{P} \mapsto \mathfrak{P} \cap A$ correspond à $z \mapsto z^2$. Si $z \neq 0$, l'idéal $\mathfrak{p} = (X - z)$ a deux antécédents et se décompose $\mathfrak{p}B = \mathfrak{P}_1\mathfrak{P}_2 = (\sqrt{X} - z_1)(\sqrt{X} + z_1)$. Pour $z = 0$, $\mathfrak{p} = (X)$ n'a qu'un antécédent $\mathfrak{P} = (\sqrt{X})$ et se ramifie en $\mathfrak{p}B = \mathfrak{P}^2$. D'ailleurs le discriminant $\mathrm{disc}(B/A)$ est (X).

Il est aussi possible de caractériser individuellement les $\mathfrak{P}|\mathfrak{p}$ tels que $e(\mathfrak{P}/\mathfrak{p}) > 1$ ou $B/\mathfrak{P}$ inséparable sur $A/\mathfrak{p}$ (on dit alors que $\mathfrak{P}$ est ramifié au-dessus de $\mathfrak{p}$). Pour cela on utilise la *différente* $\mathfrak{D}_{B/A} := (B^*)^{-1}$ qui est un idéal de B.

THÉORÈME. – *$\mathfrak{P}$ est ramifié au-dessus de $\mathfrak{p}$ si et seulement si $\mathfrak{P}|\mathfrak{D}_{B/A}$.*

Exercice. – Si $B = A[\alpha]$, alors $\mathfrak{D}_{B/A} = f'_\alpha(\alpha)B$.

3.4.4 *Une méthode de calcul de la décomposition de $\mathfrak{p}B$.* Ecrivons $L = K(\alpha)$ pour un $\alpha \in B$, et toujours $f_\alpha \in A[X]$ le polynôme minimal de α sur A. On fait l'hypothèse (forte) suivante :

$$\textit{On suppose que } \mathfrak{p} \not| \ (B : A[\alpha])_A$$

Soit $\overline{f}_\alpha \in A/\mathfrak{p}[X]$ l'image de f_α et $\overline{f}_\alpha = \overline{g}_1^{e_1} \cdots \overline{g}_r^{e_r}$ sa décomposition en facteurs irréductibles dans $A/\mathfrak{p}[X]$ (les $\overline{g}_i$ sont premiers entre eux deux à deux). Choisissons ensuite des relèvements moniques $g_i \in A[X]$ des $\overline{g}_i$.

THÉORÈME. – *Avec les notations et hypothèses ci-dessus, on a :*

i) $\forall i = 1, \cdots, r$, *l'idéal* $\mathfrak{P}_i := \mathfrak{p}B + g_i(\alpha)B$ *est maximal et* $[B/\mathfrak{P}_i : A/\mathfrak{p}] = \deg(g_i)$.

ii) $i \neq j \Rightarrow \mathfrak{P}_i \neq \mathfrak{P}_j$ *pour tous* i, j.

iii) $\mathfrak{p}B = \prod_i \mathfrak{P}_i^{e_i}$.

Démonstration. On a $(\mathfrak{p} \not| (B : A[\alpha])_A) \Leftrightarrow (B/A[\alpha])_\mathfrak{p} = 0 \Leftrightarrow B_\mathfrak{p} = A_\mathfrak{p}[\alpha]$, et ceci implique que $B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} \simeq (A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p})[X]/(\overline{f}_\alpha)$. Avec nos notations ci-dessus on a donc

$$B/\mathfrak{p}B \simeq A/\mathfrak{p}[X]/(\overline{f}_\alpha) = \prod_{i=1}^{r} A/\mathfrak{p}[X]/(\overline{g}_i^{e_i}).$$

Chaque facteur du produit est une $A/\mathfrak{p}$-algèbre locale. En comparant avec la décomposition de la proposition 3.4.1, on en déduit une bijection $i \mapsto \mathfrak{P}_i$ entre $\{1, \cdots, r\}$ et $\{\mathfrak{P}|\mathfrak{p}\}$ telle que

$$B/\mathfrak{P}_i^{e(\mathfrak{P}_i/\mathfrak{p})} \simeq A/\mathfrak{p}[X]/(\overline{g}_i^{e_i}).$$

En comparant les longueurs (en tant que modules sur elles-même) de ces deux algèbres locales, on constate que $e(\mathfrak{P}_i/\mathfrak{p}_i) = e_i$. De plus, en quotientant chaque membre par son radical de Jacobson, on obtient un isomorphisme des corps résiduels

$$B/\mathfrak{P}_i \simeq A/\mathfrak{p}[X]/(\overline{g}_i),$$

donc en particulier une égalité des degrés : $f(\mathfrak{P}_i/\mathfrak{p}) = \deg(g_i)$. Enfin, on peut réécrire le terme de droite sous la forme

$$A/\mathfrak{p}[X]/(\overline{g}_i) = A[X]/(\mathfrak{p}A[X] + (f_\alpha(X)) + (g_i(X))) = A[\alpha]/(\mathfrak{p}A[\alpha] + (g_i(\alpha))).$$

Il s'ensuit que $\mathfrak{P}_i = \mathfrak{p}B + g_i(\alpha)B$. □

Remarque. – La formule $\mathrm{disc}(f_\alpha)A = \mathrm{disc}(B/A)(B : A[\alpha])^2$ nous dit que si $\mathfrak{p} \not| \mathrm{disc}(f_\alpha)$ alors $\mathfrak{p} \not| (B : A[\alpha])$ et $\mathfrak{p}$ est non ramifié.

Exemple. (Corps quadratiques) – Regardons le cas $K = \mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteur carré et $\alpha = \sqrt{d}$, de sorte que $f_\alpha(X) = X^2 - d$. On a vu précédemment que $(\mathcal{O}_K : \mathbb{Z}[\sqrt{d}]) = 1$ ou 2. Soit p un nombre premier.

i) Supposons $p \neq 2$. On a alors les possibilités suivantes :
   - $(X^2 - d$ irréductible dans $\mathbb{F}_p[X]) \Leftrightarrow (p$ inerte dans $\mathcal{O}_K)$.
   - $(X^2 - d = (X - \overline{a})(X + \overline{a})$ dans $\mathbb{F}_p[X]) \Leftrightarrow (p$ totalement décomposé et $(p) = \mathfrak{P}_1\mathfrak{P}_2$ avec $\mathfrak{P}_1 = (p, \sqrt{d} - a)$ et $\mathfrak{P}_2 = (p, \sqrt{d} + a)$ où $a \in \mathbb{Z}$ relève $\overline{a})$.
   - $(X^2 - d = X^2$ dans $\mathbb{F}_p[X]) \Leftrightarrow (p$ est ramifié et $(p) = \mathfrak{P}^2$ où $\mathfrak{P} = (p, \sqrt{d}).)$

ii) Supposons $p = 2$.
   - Si $d \equiv 2, 3[4]$, on sait que $2 \not| (\mathcal{O}_K : \mathbb{Z}[\sqrt{d}])$ et que 2 est ramifié. On a alors $(2) = \mathfrak{P}^2$ avec $\mathfrak{P} = (2, \sqrt{d})$ si $d \equiv 2[4]$ et $\mathfrak{P} = (2, \sqrt{d} - 1)$ si $d \equiv 3[4]$.
   - Supposons $d \equiv 1[4]$. On sait déjà que 2 est non ramifié. On sait aussi que $2|(\mathcal{O}_K : \mathbb{Z}[\sqrt{d}])$ mais on peut écrire $\mathcal{O}_K = \mathbb{Z}[\alpha]$ avec $\alpha = \frac{1-\sqrt{d}}{2}$. On a alors $f_\alpha(X) = X^2 - X + \frac{1-d}{4}$ et deux cas se présentent :
     - Si $d \equiv 1[8]$ alors $\overline{f}_\alpha = X(X - 1)$, donc 2 est décomposé et $(2) = \mathfrak{P}_1\mathfrak{P}_2$ avec $\mathfrak{P}_1 = (2, \alpha)$ et $\mathfrak{P}_2 = (2, \alpha - 1)$.
     - Si $d \equiv 5[8]$ alors $\overline{f}_\alpha = X^2 - X - 1$ est irréductible, donc 2 est inerte.

Exemple. (Cas Eisenstein) – Un polynôme $f(X) = X^n + a_0X^{n-1} + \cdots + a_n \in A[X]$ est dit "d'Eisenstein en $\mathfrak{p} \in \mathrm{Max}(A)$" si $v_\mathfrak{p}(a_i) > 0$ pour tout i et $v_\mathfrak{p}(a_n) = 1$. Comme dans le cas $A = \mathbb{Z}$, un tel polynôme est irréductible dans $K[X]$. De plus, si, avec les notations du théorème, f_α est d'Eisenstein en $\mathfrak{p}$, alors on montre comme dans le cas $A = \mathbb{Z}$ que $\mathfrak{p} \not| (B : A[\alpha])$. On peut donc appliquer le théorème, et puisque $\overline{f}_\alpha = X^n$, on constate qu'on a $\mathfrak{p}B = \mathfrak{P}^n$ où $\mathfrak{P} = \mathfrak{p}B + (\alpha)$. On dit que $\mathfrak{p}$ est "totalement" ramifié.

Exemple. (Cas p-cyclotomique) – Regardons la décomposition de p dans l'extension $K = \mathbb{Q}(\zeta_r)$ où $\zeta_r = e^{2i\pi/p^r}$. On a donc $f_{\zeta_r} = \Phi_{p^r}$. C'est un cas particulier du cas précédent puisque $f_{\zeta_r}(1 + X)$ est Eisenstein en p. On a donc $(p) = \mathfrak{P}^{\varphi(p^r)}$ avec $\mathfrak{P} = (p, \zeta_r - 1)$. On peut améliorer cette expression en remarquant que

$$p = \Phi_{p^r}(1) = \prod_{a \in (\mathbb{Z}/p^r\mathbb{Z})^\times} (1 - \zeta_r^a) \in (1 - \zeta_r)^{\varphi(p^r)}\mathbb{Z}[\zeta_r]^\times,$$

(exercice : vérifier que $\frac{1-\zeta_r^a}{1-\zeta_r}$ et $\frac{1-\zeta_r}{1-\zeta_r^a}$ sont dans $\mathbb{Z}[\zeta_r]$), et donc que $\mathfrak{P} = (1 - \zeta_r)$.

3.4.5 THÉORÈME. (Corps cyclotomiques)– *Pour $n > 1$ entier, posons $\zeta_n := e^{2i\pi/n}$ et notons $\Phi_n(X)$ le n-ème polynôme cyclotomique. Alors si $n \not\equiv 2[4]$, on a :*

i) $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ *(et donc Φ_n est irréductible et $\chi_{n,\mathbb{Q}} : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longrightarrow \mathbb{Z}/n\mathbb{Z}^\times$ est un isomorphisme).*

ii) $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$

iii) Pour p premier, (p ramifié dans $\mathbb{Q}(\zeta_n)$) $\Leftrightarrow$ $p|n$.

iv) Pour p premier, écrivons $n = n'p^r$ avec $(n', p) = 1$. Alors dans $\mathbb{Z}[\zeta_n]$ on a $(p) = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{\varphi(p^r)}$ où tous les $f(\mathfrak{P}_i/\mathfrak{p})$ sont égaux à l'ordre de p dans $(\mathbb{Z}/n'\mathbb{Z})^\times$.

Démonstration. On prouve d'abors i), ii) et iii) par récurrence sur le nombre k de facteurs premiers de n. On a déjà traité le cas $k = 1$, donc on peut supposer $k > 1$, choisir un diviseur premier p de n et écrire $n = n'p^r$ avec $(n', p) = 1$. Remarquons alors que $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n'}, \zeta_{p^r}) = \mathbb{Q}(\zeta_{n'})(\zeta_{p^r}) = \mathbb{Q}(\zeta_{n'})\mathbb{Q}(\zeta_{p^r})$ (corps composé).

i) L'hypothèse de récurrence nous dit que $\mathcal{O}_{\mathbb{Q}(\zeta_{n'})} = \mathbb{Z}[\zeta_{n'}]$ et que si $\mathfrak{P} \in \mathrm{Max}(\mathbb{Z}[\zeta_{n'}])$ divise (p) alors $e(\mathfrak{P}/p) = v_{\mathfrak{P}}(p) = 1$. Il s'ensuit que dans $\mathbb{Z}[\zeta_r][X]$, le polynôme $\Phi_{p^r}(1 + X)$ est d'Eisenstein en $\mathfrak{P}$, donc irréductible, et on a donc

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{n'})(\zeta_{p^r}) : \mathbb{Q}(\zeta_{n'})][\mathbb{Q}(\zeta_{n'}) : \mathbb{Q}] = \varphi(p^r)\varphi(n') = \varphi(n).$$

ii) Regardons l'égalité d'idéaux de $\mathbb{Z}[\zeta_{n'}]$

$$\mathrm{disc}(\mathbb{Z}[\zeta_n]/\mathbb{Z}[\zeta_{n'}]) = \mathrm{disc}(\mathcal{O}_{\mathbb{Q}(\zeta_n)}/\mathbb{Z}[\zeta_{n'}])(\mathcal{O}_{\mathbb{Q}(\zeta_n)} : \mathbb{Z}[\zeta_n])^2_{\mathbb{Z}[\zeta_{n'}]}.$$

En remarquant que $\mathbb{Z}[\zeta_n] = \mathbb{Z}[\zeta_{n'}][\zeta_{p^r}]$, on voit que le terme de gauche est l'idéal $(\mathrm{disc}(\Phi_{p^r})) = (p)^{m(r)}$ pour un certain entier $m(r)$. Il s'ensuit que pour $\mathfrak{P} \in \mathrm{Max}(\mathbb{Z}[\zeta_{n'}])$ on a

$$\mathfrak{P}|(\mathcal{O}_{\mathbb{Q}(\zeta_n)} : \mathbb{Z}[\zeta_n])_{\mathbb{Z}[\zeta_{n'}]} \Rightarrow \mathfrak{P}|(p)$$

Or on a vu que $\Phi_{p^r}(1 + X)$ est Eisenstein en tout $\mathfrak{P}$ divisant (p), donc comme dans le cas $A = \mathbb{Z}$, le théorème 2.5.5 et le lemme 2.5.6 montrent que $\mathfrak{P}$ ne divise pas $(\mathcal{O}_{\mathbb{Q}(\zeta_n)} : \mathbb{Z}[\zeta_n])_{\mathbb{Z}[\zeta_{n'}]}$ et finalement que $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.

iii) On a maintenant l'égalité $(\mathrm{disc}(\Phi_{p^r})) = (p)^{m(r)} = \mathrm{disc}(\mathcal{O}_{\mathbb{Q}(\zeta_n)}/\mathbb{Z}[\zeta_{n'}])$. Elle montre que si $\mathfrak{P} \in \mathrm{Max}(\mathbb{Z}[\zeta_{n'}])$ se ramifie dans $\mathbb{Z}[\zeta_n]$ alors $\mathfrak{P}|(p)$, comme voulu.

La récurrence est maintenant achevée. Il nous reste à prouver iv).

iv) On vient de voir que p est non ramifié dans $\mathbb{Z}[\zeta_{n'}]$, donc $p\mathbb{Z}[\zeta_{n'}]$ est de la forme $p\mathbb{Z}[\zeta_{n'}] = \mathfrak{p}_1 \cdots \mathfrak{p}_g$ (avec les $\mathfrak{p}_i \in \mathrm{Max}(\mathbb{Z}[\zeta_{n'}])$ 2 à 2 distincts) et l'anneau

$$\mathbb{Z}[\zeta_{n'}]/(p) = \mathbb{F}_p[X]/(\Phi_{n'})$$

est un produit de corps (*i.e.* le polynôme $\Phi_{n'}$ est séparable dans $\mathbb{F}_p[X]$). Chacun des facteurs de ce produit est engendré par une racine primitive n'-ème de l'unité, donc isomorphe au sous-corps $\mathbb{F}_p(\mu_{n'})$ de $\overline{\mathbb{F}}_p$. Donc

$$\mathbb{Z}[\zeta_{n'}]/(p) = \mathbb{F}_p[X]/(\Phi_{n'}) \simeq \mathbb{F}_p(\mu_{n'})^g.$$

Il reste à déterminer le degré f de $\mathbb{F}_p(\mu_{n'})$ sur $\mathbb{F}_p$. Or, pour tout $k \geqslant 1$, on voit que

$$\mu_{n'} \subset \mathbb{F}_{p^k}^\times \Leftrightarrow n' | (p^k - 1)$$

Donc f est le plus petit k tel que $n'|(p^k-1)$, *i.e.* l'ordre de p dans $(\mathbb{Z}/n'\mathbb{Z})^\times$.

Maintenant, comme le polynôme Φ_{p^r} est d'Eisenstein en chaque $\mathfrak{p}_i$, les $\mathfrak{p}_i$ sont totalement ramifiés dans $\mathbb{Z}[\zeta_n]$, c'est à dire qu'on a $\mathfrak{p}_i\mathbb{Z}[\zeta_n] = \mathfrak{P}_i^{\varphi(p^r)}$ pour un $\mathfrak{P}_i \in \mathrm{Max}(\mathbb{Z}[\zeta_n])$. □

Remarque. – On voit que le type de décomposition de p dans $\mathbb{Z}[\zeta_n]$ est déterminé par la classe de p modulo n. Par exemple :

– p est totalement décomposé si et seulement si $p \equiv 1[n]$,

– p est inerte si et seulement si p engendre $\mathbb{Z}/n\mathbb{Z}^\times$.

Ceci tient au fait que l'équation $\Phi_n(x) = 0$ est facile à résoudre dans les corps finis. Dans le cas des corps quadratiques, que nous traiterons plus loin, l'équation $X^2 - d$ n'est pas facile à résoudre et c'est la *loi de réciprocité quadratique* qui nous permet de passer à des conditions de congruences.

Exercice. – Trouver n tel que *aucun* premier p n'est inerte dans $\mathbb{Z}[\zeta_n]$.

3.5 Action de Galois. Groupes de décomposition et d'inertie

On continue avec le contexte précédent (A est un anneau de Dedekind, L une extension séparable finie de $K = \mathrm{Frac}(A)$ et B la clôture intégrale de A dans L) et on suppose de plus que L est *Galoisienne* sur K. On notera le groupe de Galois

$$G = G_{L/K} := \mathrm{Gal}(L/K).$$

3.5.1 Proposition.– *Avec les notations ci-dessus, on a*

i) $\forall \sigma \in G,\ \sigma(B) \subset B$ *et* $B^G = A$,

ii) $\forall \mathfrak{p} \in \mathrm{Max}(A)$, G *agit transitivement sur* $\{\mathfrak{P} \in \mathrm{Max}(B), \mathfrak{P}|\mathfrak{p}\}$.

Démonstration. i) On a $f_{\sigma(x)} = f_x$ pour tout $x \in L$, donc $x \in B \Rightarrow \sigma(x) \in B$. De plus, $B^G = B \cap L^G = B \cap K = A$.

ii) Tout d'abord il est clair que pour $\mathfrak{P} \in \mathrm{Max}(B)$ on a $\sigma(\mathfrak{P}) \in \mathrm{Max}(B)$, et que si $\mathfrak{P}|\mathfrak{p}$ alors $\sigma(\mathfrak{P})|\sigma(\mathfrak{p}) = \mathfrak{p}$. Donc G agit bien sur l'ensemble de l'énoncé. Supposons maintenant que cette action ne soit pas transitive, et soient $\mathfrak{P}, \mathfrak{P}'$ dans deux orbites disjointes. On peut alors trouver (lemme d'approximation ou lemme Chinois) un élément $b \in B$ tel que

$$\forall \sigma \in \mathfrak{P},\ b \in \sigma(\mathfrak{P}) \text{ et } b - 1 \in \sigma(\mathfrak{P}').$$

Mais alors $N_{L/K}(b) = \prod_{\sigma \in G} \sigma(b)$ est à la fois égal à 0 et à 1 modulo $\mathfrak{p}$. Contradiction. □

3.5.2 Corollaire.– *Soit* $\mathfrak{p} \in \mathrm{Max}(A)$, *et* $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ *avec les* $\mathfrak{P}_i$ *distincts 2 à 2. Alors* $e_1 = e_2 = \cdots = e_g =: e$, $f_1 = f_2 = \cdots = f_g =: f$, *et* $efg = n$ $(= [L : K])$.

3.5.3 DÉFINITION.– *Le stabilisateur* $D_{\mathfrak{P}} = \{\sigma \in G, \sigma(\mathfrak{P}) = \mathfrak{P}\}$ *d'un* $\mathfrak{P} \in \mathrm{Max}(B)$ *est appelé* groupe de décomposition en $\mathfrak{P}$.

Propriétés. – i) On a $D_{\sigma(\mathfrak{P})} = \sigma D_{\mathfrak{P}} \sigma^{-1}$ pour tout $\sigma \in G$.

ii) $|D_{\mathfrak{P}}| = ef$ (avec la notation du corollaire ci-dessus.) En effet, le ii) de la proposition nous dit que $|G|/|D_{\mathfrak{P}}| = g$.

iii) p totalement décomposé $\Leftrightarrow D_{\mathfrak{P}} = \{1\}$ (pour un $\mathfrak{P}|\mathfrak{p}$ ou pour tous, c'est équivalent.)

iv) Si $K \subset L'$ est une extension Galoisienne contenue dans L, B' la normalisation de A dans L' et $\mathfrak{P}' := \mathfrak{P} \cap B'$, alors $D_{\mathfrak{P}'}$ est l'image de $D_{\mathfrak{P}}$ par la surjection $\pi : G_{L/K} \twoheadrightarrow G_{L'/K}$. Plus précisément, π induit une suite exacte

$$D_{\mathfrak{P}/\mathfrak{P}'} \hookrightarrow D_{\mathfrak{P}} \twoheadrightarrow D_{\mathfrak{P}'}.$$

En effet, il est clair que $\pi(D_{\mathfrak{P}}) \subset D_{\mathfrak{P}'}$. Réciproquement, si $\sigma' \in D_{\mathfrak{P}'}$ et $\sigma \in \pi^{-1}(\sigma')$ alors $\sigma(\mathfrak{P}) \cap B' = \mathfrak{P}'$ donc par le ii) de la proposition il existe $\tau \in G_{L/L'}$ tel que $\tau\sigma(\mathfrak{P}) = \mathfrak{P}$. Or on a $\pi(\tau\sigma) = \sigma'$, donc $\sigma' \in \pi(D_{\mathfrak{P}'})$. Enfin on a bien $\mathrm{Ker}(\pi_{|D_{\mathfrak{P}}}) = D_{\mathfrak{P}} \cap G_{L/L'} = D_{\mathfrak{P}/\mathfrak{P}'}$ (le groupe de décomposition en $\mathfrak{P}$ pour l'extension $L \supset L'$).

Puisque $D_{\mathfrak{P}}$ stabilise B et $\mathfrak{P}$, il agit par automorphismes d'anneaux sur le quotient $B/\mathfrak{P}$, et de façon $A/\mathfrak{p}$ linéaire, si $\mathfrak{p} = \mathfrak{P} \cap A$. D'où un homomorphisme $D_{\mathfrak{P}} \longrightarrow \mathrm{Aut}_{A/\mathfrak{p}-alg}(B/\mathfrak{P})$. Dans la suite nous noterons

$$k_{\mathfrak{P}} := B/\mathfrak{P} \text{ et } k_{\mathfrak{p}} := A/\mathfrak{p} \quad \text{les corps résiduels.}$$

3.5.4 PROPOSITION.– *L'extension* $k_{\mathfrak{P}} \supset k_{\mathfrak{p}}$ *est normale et l'homomorphisme ci-dessus* $D_{\mathfrak{P}} \longrightarrow \mathrm{Aut}_{k_{\mathfrak{p}}-\mathrm{alg}}(k_{\mathfrak{P}})$ *est surjectif.*

Démonstration. La première assertion est claire si A est un anneau d'entiers d'un corps de nombres, car les corps résiduels sont alors finis et toute extension de corps finis est normale. Dans le cas général, soit $\overline{b} \in k_{\mathfrak{P}}$. Il faut voir que toutes les racines de $f_{\overline{b}} \in k_{\mathfrak{p}}[X]$ sont dans $k_{\mathfrak{P}}$. Choisissons un relèvement $b \in B$ de $\overline{b}$. Puisque L est normale, toutes les racines de $f_b \in A[X]$ sont dans B et donc celles de $\overline{f}_b$ sont dans $k_{\mathfrak{P}}$. Or $\overline{f}_b(\overline{b}) = 0$, donc $f_{\overline{b}} | \overline{f}_b$.

Passons à la seconde assertion et notons $k^s_{\mathfrak{P}}$ la clôture séparable de $k_{\mathfrak{p}}$ dans $k_{\mathfrak{P}}$. Choisissons un générateur $\overline{b}$ (élément primitif) de $k^s_{\mathfrak{P}}$ sur $k_{\mathfrak{p}}$. Tout automorphisme $\tau \in \mathrm{Aut}_{k_{\mathfrak{p}}-\mathrm{alg}}(k_{\mathfrak{P}}) = \mathrm{Gal}(k^s_{\mathfrak{P}}/k_{\mathfrak{p}})$ est déterminé par $\tau(\overline{b})$ qui est une racine de $f_{\overline{b}}$. Il nous suffit donc de montrer que toute racine de $f_{\overline{b}}$ est de la forme $\overline{\sigma(b)}$ pour un relèvement $b \in B$ de $\overline{b}$ et un élément $\sigma \in D_{\mathfrak{P}}$.

Pour cela, choisissons b tel que $\forall \sigma \in G \backslash D_{\mathfrak{P}},\ b \in \sigma(\mathfrak{P})$ et posons $f(X) = \prod_{\sigma}(X - \sigma(b)) \in A[X]$. Alors $\overline{f}(X) = X^{|G \backslash D_{\mathfrak{P}}|} \prod_{\sigma \in D_{\mathfrak{P}}}(X - \overline{\sigma(b)})$. Puisque $\overline{f}(\overline{b}) = 0$, ceci montre que toute racine de $f_{\overline{b}}$ est de la forme $\overline{\sigma(b)}$ pour un $\sigma \in D_{\mathfrak{P}}$. □

Remarque. – Le cas qui nous intéresse est celui où A est l'anneau des entiers d'un corps de nombres. Dans ce cas les corps résiduels sont finis, donc l'extension $k_{\mathfrak{P}} \supset k_{\mathfrak{p}}$ est

Galoisienne, et on a donc un morphisme surjectif $D_{\mathfrak{P}} \twoheadrightarrow \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$. On notera

$$N\mathfrak{p} := |A/\mathfrak{p}| \text{ de sorte que } k_{\mathfrak{p}} \simeq \mathbb{F}_{N\mathfrak{p}} \text{ et } N\mathfrak{P} = (N\mathfrak{p})^f.$$

Le groupe de Galois $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$ est cyclique d'ordre f, engendré par le Frobenius relatif à $k_{\mathfrak{p}}$, qui est donné par $x \mapsto x^{N\mathfrak{p}}$.

3.5.5 Définition.– *Le noyau $I_{\mathfrak{P}}$ de la surjection $D_{\mathfrak{P}} \longrightarrow \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$ est appelé* sous-groupe d'inertie en $\mathfrak{P}$

Propriétés. – i) On a $I_{\sigma(\mathfrak{P})} = \sigma I_{\mathfrak{P}} \sigma^{-1}$.

ii) $|I_{\mathfrak{P}}| = e$.

iii) p non ramifié $\Leftrightarrow I_{\mathfrak{P}} = \{1\}$ (pour un $\mathfrak{P}|\mathfrak{p}$, ce qui équivaut à pour tous).

iv) p totalement ramifié $\Leftrightarrow I_{\mathfrak{P}} = G_{L/K}$ (il n'y a alors qu'un seul $\mathfrak{P}|\mathfrak{p}$).

v) p inerte $\Leftrightarrow (I_{\mathfrak{p}} = \{1\}$ et $D_{\mathfrak{P}} = G_{L/K})$.

vi) Si $K \subset L'$ est une extension Galoisienne contenue dans L, B' la normalisation de A dans L' et $\mathfrak{P}' := \mathfrak{P} \cap B'$, alors $I_{\mathfrak{P}'}$ est l'image de $I_{\mathfrak{P}}$ par la surjection $\pi : G_{L/K} \twoheadrightarrow G_{L'/K}$. Plus précisément, π induit une suite exacte

$$I_{\mathfrak{P}/\mathfrak{P}'} \hookrightarrow I_{\mathfrak{P}} \twoheadrightarrow I_{\mathfrak{P}'}.$$

En effet, il est clair que $\pi(I_{\mathfrak{P}}) \subset I_{\mathfrak{P}'}$. Réciproquement, si $\sigma' \in I_{\mathfrak{P}'}$ et $\sigma \in \pi^{-1}(\sigma') \cap D_{\mathfrak{P}}$ alors σ induit un automorphisme $\overline{\sigma}$ $k_{\mathfrak{P}'}$-linéaire de $k_{\mathfrak{P}}$. Un tel automorphisme peut se relever en un élément $\tau \in D_{\mathfrak{P}/\mathfrak{P}'}$ et on a alors $\tau^{-1}\sigma \in I_{\mathfrak{P}}$. Or on a aussi $\pi(\tau^{-1}\sigma) = \sigma'$, donc $\sigma' \in \pi(I_{\mathfrak{P}'})$. Enfin on a bien $\mathrm{Ker}(\pi_{|I_{\mathfrak{P}}}) = I_{\mathfrak{P}} \cap G_{L/L'} = I_{\mathfrak{P}/\mathfrak{P}'}$ (le groupe d'inertie en $\mathfrak{P}$ pour l'extension $L \supset L'$).

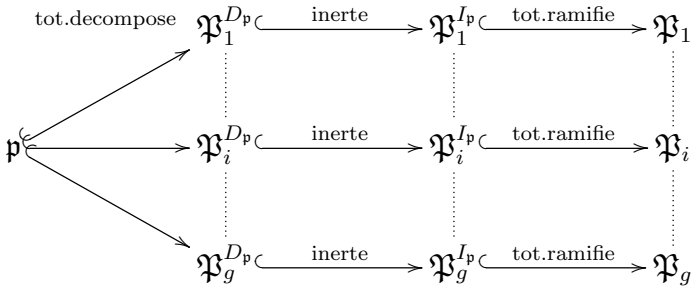
Le diagramme suivant résume les propriétés des groupes introduits.

$$K = L^G \xhookrightarrow{\deg.g} L^{D_{\mathfrak{P}}} \xhookrightarrow{\deg.f} L^{I_{\mathfrak{P}}} \xhookrightarrow{\deg.e} L$$

$$\begin{array}{ccccccc}
\mathfrak{p} = \mathfrak{P}^G & \hookrightarrow & \mathfrak{P}^{D_{\mathfrak{P}}} & \xhookrightarrow{\text{inerte}} & \mathfrak{P}^{I_{\mathfrak{P}}} & \xhookrightarrow{\text{tot.ramifie}} & \mathfrak{P} \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
A = B^G & \hookrightarrow & B^{D_{\mathfrak{P}}} & \hookrightarrow & B^{I_{\mathfrak{P}}} & \hookrightarrow & B \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
k_{\mathfrak{p}} & \xhookrightarrow{\sim} & k_{\mathfrak{P}^{D_{\mathfrak{P}}}} & \xhookrightarrow{\deg.f} & k_{\mathfrak{P}^{I_{\mathfrak{P}}}} & \xhookrightarrow{\sim} & k_{\mathfrak{P}}
\end{array}$$

Noter que $L \supset L^{I_{\mathfrak{P}}}$ est Galoisienne de groupe $I_{\mathfrak{P}}$, et que $L^{I_{\mathfrak{P}}} \supset L^{D_{\mathfrak{P}}}$ est Galoisienne de groupe isomorphe à $D_{\mathfrak{P}}/I_{\mathfrak{P}} \simeq \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$. Par contre en général $L^{D_{\mathfrak{P}}} \supset L$ n'est pas Galoisienne. Elle l'est si et seulement si $D_{\mathfrak{P}}$ est distingué dans G. Dans ce cas $\mathfrak{p}$ est *totalement décomposé* dans $L^{D_{\mathfrak{P}}}$, puisque $f_{L^{D_{\mathfrak{P}}}/K} = f(\mathfrak{P}^{D_{\mathfrak{P}}}|\mathfrak{p}) = 1 = e(\mathfrak{P}^{D_{\mathfrak{P}}}|\mathfrak{p}) = e_{L^{D_{\mathfrak{P}}}/K}$.

Cas particulier où $G_{L/K}$ est abélien. Dans ce cas, $D_{\mathfrak{P}}$ est indépendant de $\mathfrak{P}$, tout comme $I_{\mathfrak{P}}$, et on peut les noter respectivement $D_{\mathfrak{p}}$ et $I_{\mathfrak{p}}$. On peut alors schématiser la décomposition de $\mathfrak{p}$ par le diagramme.



Exemple. (Corps cyclotomiques) – Prenons $K = \mathbb{Q}$ et $L = \mathbb{Q}(\zeta_n)$, et fixons un idéal $\mathfrak{p} = (p)$ de $\mathbb{Z}$, où p est un nombre premier. Comme le groupe de Galois est abélien, on est dans la situation ci-dessus. Écrivons $n = n'p^r$ avec $(n', p) = 1$. Le théorème 3.4.5 nous dit que

$$I_p = G_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n'})} \quad \text{et} \quad L^{I_p} = \mathbb{Q}(\zeta_{n'}).$$

Via l'isomorphisme $\chi_{n,\mathbb{Q}} : G_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$ et la décomposition canonique (lemme chinois) $(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/n'\mathbb{Z})^\times \times (\mathbb{Z}/p^r\mathbb{Z})^\times$ on a donc $\chi_{n,\mathbb{Q}}(I_p) = (\mathbb{Z}/p^r\mathbb{Z})^\times$. De plus, on a $\chi_n(D_p) = \chi_{n'}(D'_p) \times (\mathbb{Z}/p^r\mathbb{Z})^\times$ où $D'_p = D_p/I_p$ est le groupe de décomposition de p dans $\mathbb{Q}(\zeta_{n'})$. Voir ci-dessous pour un calcul de $\chi_{n',\mathbb{Q}}(D'_p)$.

3.5.6 *Substitutions de Frobenius et symbole d'Artin.* On suppose dorénavant que L et K sont des corps de nombres (et donc $A = \mathcal{O}_K$ et $B = \mathcal{O}_L$). Soit $\mathfrak{p} \in \mathrm{Max}(A)$ un premier *non ramifié* dans B et soit $\mathfrak{P} \in \mathrm{Max}(B)$ contenant $\mathfrak{p}$. On a donc $I_{\mathfrak{P}} = \{1\}$ et $D_{\mathfrak{P}} \xrightarrow{\sim} G_{k_{\mathfrak{P}}/k_{\mathfrak{p}}}$. L'élément $\sigma_{\mathfrak{P}} \in D_{\mathfrak{P}}$ correspondant au Frobenius $x \mapsto x^{N\mathfrak{p}}$ est appelé *substitution de Frobenius en* $\mathfrak{P}$. C'est donc un élément d'ordre $f(\mathfrak{P}|\mathfrak{p})$, caractérisé par la propriété suivante :

$$\forall b \in B,\ \sigma_{\mathfrak{P}}(b) - b^{N\mathfrak{p}} \in \mathfrak{P}.$$

Lorsqu'on change $\mathfrak{P}$ on obtient un conjugué. Plus précisément :

$$\forall \tau \in G_{L/K},\ \sigma_{\tau(\mathfrak{P})} = \tau\sigma_{\mathfrak{P}}\tau^{-1}.$$

Il s'ensuit que si $G_{L/K}$ est *abélien*, alors $\sigma_{\mathfrak{P}}$ ne dépend que de $\mathfrak{p}$ et pas de $\mathfrak{P}|\mathfrak{p}$. On le note alors simplement $\sigma_{\mathfrak{p}}$ ou encore par son *symbole d'Artin* $\left(\frac{L/K}{\mathfrak{p}}\right)$.

Plus généralement, si $I = \prod_i \mathfrak{p}_i^{e_i}$ avec chaque $\mathfrak{p}_i$ non ramifié, on pose $\left(\frac{L/K}{I}\right) = \prod_i \left(\frac{L/K}{\mathfrak{p}_i}\right)^{e_i}$.

Exemple. (Corps cyclotomiques) – Prenons $K = \mathbb{Q}$ et $L = \mathbb{Q}(\zeta_n)$, et fixons un nombre premier p *tel que* $(p, n) = 1$. On sait alors que (p) est non ramifié dans $\mathbb{Q}(\zeta_n)$. Avec la notation maintenant habituelle $\chi_{n,\mathbb{Q}} : G_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$, on a

$$\chi_{n,\mathbb{Q}}\left(\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{p}\right) = p, \text{ et donc } \chi_{n,\mathbb{Q}}(D_p) = \langle \text{ss-gr de } (\mathbb{Z}/n\mathbb{Z})^\times \text{ engendré par } p\rangle.$$

En effet, notons $\sigma' := \chi_{n,\mathbb{Q}}^{-1}(p)$. Par définition on a $\sigma'(\zeta_n) = \zeta_n^p$ et donc a fortiori $\sigma'(\zeta_n) - \zeta_n^p \in \mathfrak{P}$ si $\mathfrak{P}|p$. Puisque $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ est engendré par ζ_n, on en déduit $\sigma'(b) - b^p \in \mathfrak{P}$ pour tout $b \in \mathcal{O}_{\mathbb{Q}(\zeta_n)}$ et on reconnait là la propriété caractéristique de $\sigma = \left(\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{p}\right)$.

Exemple. (Corps quadratiques) – Ici $K = \mathbb{Q}$ et $L = \mathbb{Q}(\sqrt{d})$ pour $d \in \mathbb{Z} \setminus \{1, 0\}$ sans facteur carré. On a un isomorphisme

$$\psi_d : G_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}} \xrightarrow{\sim} \{\pm 1\}, \quad \sigma \mapsto \sigma(\sqrt{d})/\sqrt{d}.$$

Soit maintenant $p \not| 4d$ (qui est donc non ramifié) et $\mathfrak{P}|p$. On voit que

$$\left(\frac{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}{p}\right) = 1 \Leftrightarrow k_{\mathfrak{P}} = \mathbb{F}_p \Leftrightarrow d \in (\mathbb{F}_p^\times)^2 \Leftrightarrow \left(\frac{d}{p}\right) = 1$$

où le dernier terme est le symbole de Legendre. On en conclut qu'on a toujours

$$\psi_d \left(\frac{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}{p}\right) = \left(\frac{d}{p}\right),$$

et que le symbole d'Artin est une (vaste) généralisation de celui de Legendre.

Exercice. – Soient $L \supset L' \supset K$ des extensions abéliennes et $\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_K)$ non ramifié dans $\mathcal{O}_L$.

i) Vérifier que $\mathfrak{p}$ est non ramifié dans $\mathcal{O}_{L'}$ et que tout $\mathfrak{P}'|\mathfrak{p}$ dans $\mathrm{Max}(\mathcal{O}_{L'})$ est non ramifié dans $\mathcal{O}_L$.

ii) Montrer que $\left(\frac{L'/K}{\mathfrak{p}}\right) = \pi\left(\frac{L/K}{\mathfrak{p}}\right)$ où $\pi : G_{L/K} \twoheadrightarrow G_{L'/K}$.

iii) Montrer que si $\mathfrak{P}'|\mathfrak{p}$ dans $\mathrm{Max}(\mathcal{O}_{L'})$, alors $\left(\frac{L/L'}{\mathfrak{p}}\right) = \left(\frac{L/K}{\mathfrak{p}}\right)^{f(\mathfrak{P}'/\mathfrak{p})}$.

3.5.7 *Application : loi de réciprocité quadratique.* Soient p et q deux nombres premiers impairs distincts. Nous voulons montrer que

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Cette "loi" nous dit que le type de décomposition de p dans $\mathbb{Q}(\sqrt{q})$ (i.e. le fait que q soit un carré dans $\mathbb{F}_p^\times$ ou non) ne dépend que de la classe de p modulo q (et modulo 4). Cela donne aussi un algorithme efficace pour calculer les symboles de Legendre.

Rappelons que $\mathrm{disc}(\Phi_q) = (-1)^{\frac{q-1}{2}} q^{q-2}$. Par la formule $\mathrm{disc}(\Phi_q) = \prod_{i<j}(\zeta_q^i - \zeta_q^j)^2$, on voit que $\mathrm{disc}(\Phi) \in \mathbb{Q}(\zeta_q)^2$ et donc que $\mathbb{Q}(\zeta_q) \supset \mathbb{Q}(\sqrt{q^*})$ où on a posé $q^* := (-1)^{\frac{q-1}{2}} q$. Puisque $p \neq q$, on sait que p est non ramifié dans $\mathbb{Q}(\zeta_q)$ (et a fortiori dans $\mathbb{Q}(\sqrt{q^*})$). On a

alors un diagramme :

$$\begin{array}{ccccc} G_{\mathbb{Q}(\zeta_q)/\mathbb{Q}(\sqrt{q^*})} & \hookrightarrow & G_{\mathbb{Q}(\zeta_q)/\mathbb{Q}} & \xrightarrow{\pi} & G_{\mathbb{Q}(\sqrt{q^*})/\mathbb{Q}} \\ \downarrow \sim & & \downarrow \chi_{q,\mathbb{Q}} & & \downarrow \psi_{q^*} \\ (\mathbb{F}_q^\times)^2 & \hookrightarrow & \mathbb{F}_q^\times & \xrightarrow[a\mapsto\left(\frac{a}{q}\right)]{} & \{\pm 1\} \end{array}$$

En effet, comme $\mathbb{F}_q^\times$ est cyclique, il possède un unique sous-groupe d'indice 2, à savoir $(\mathbb{F}_q^\times)^2$, et par conséquent la flèche en bas à droite est donnée par le symbole de Legendre. On en déduit (cf exercice ci-dessus pour la deuxième égalité) :

$$\left(\frac{q^*}{p}\right) = \psi_{q^*}\left(\frac{\mathbb{Q}(\sqrt{q^*})/\mathbb{Q}}{p}\right) = \psi_{q^*} \circ \pi \left(\frac{\mathbb{Q}(\zeta_q)/\mathbb{Q}}{p}\right) = \left(\frac{a}{q}\right)$$

avec

$$a = \chi_{q,\mathbb{Q}}\left(\frac{\mathbb{Q}(\zeta_q)/\mathbb{Q}}{p}\right) = p.$$

On a donc obtenu

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Pour calculer $\left(\frac{-1}{p}\right)$, on peut remarquer que $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\zeta_4)$ et utiliser, comme on l'a vu plus haut, le fait que p est totalement décomposé dans $\mathbb{Q}(\zeta_4)$ si et seulement si $p \equiv 1[4]$. On en déduit dans ce cas que $\left(\frac{-1}{p}\right) = 1$ et finalement que, en général, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

3.5.8 *Vers d'autres lois de réciprocités.* Soit K un sous-corps d'un $\mathbb{Q}(\zeta_n)$. C'est une extension abélienne de $\mathbb{Q}$ (inversement le théorème de Kronecker-Weber nous dit que toute extension abélienne de $\mathbb{Q}$ se plonge dans un corps cyclotomique). Soit $p \not| n$ un nombre premier. Il est donc non ramifié dans K. On s'intéresse à son type de décomposition, c'est à dire au degré résiduel f_p commun à tout $\mathfrak{P} \in \mathrm{Max}(\mathcal{O}_K)$ contenant p. On aimerait voir que ce type de décomposition *ne dépend que de propriétés de congruences de* p.

Pour cela, remarquons que f_p est l'ordre de $\left(\frac{K/\mathbb{Q}}{p}\right)$ dans $G_{K/\mathbb{Q}}$. On a un diagramme

$$\begin{array}{ccccc} G_{\mathbb{Q}(\zeta_n)/K} & \hookrightarrow & G_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} & \xrightarrow{\pi} & G_{K/\mathbb{Q}} \\ & \searrow^{\chi_{n,K}} & \downarrow \chi_{n,\mathbb{Q}} & & \sim \downarrow \\ & & (\mathbb{Z}/n\mathbb{Z})^\times & \twoheadrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times / \mathrm{Im}(\chi_{n,K}) \end{array}$$

qui nous montre que le problème est de déterminer l'image de $\chi_{n,K}$. Par exemple p est totalement décomposé ($f_p = 1$) si et seulement si $\left(\frac{K/\mathbb{Q}}{p}\right) \in \mathrm{Im}(\chi_{n,K})$. Pour cela, on a le théorème suivant, qui sera prouvé dans le cours fondamental :

THÉORÈME. – *Soit L/K une extension Galoisienne de corps de nombres. Alors $G_{L/K}$ est engendré par les substitutions de Frobenius.*

Dans notre cas, $G_{\mathbb{Q}(\zeta_n)/K}$ est donc engendré par les $\left(\frac{\mathbb{Q}(\zeta_n)/K}{\mathfrak{P}}\right) = \left(\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{p}\right)^{f_p}$ (où $\mathfrak{P}|p$) pour p premier à n. Il s'ensuit que $\mathrm{Im}(\chi_{n,K})$ est engendré par les p^{f_p} où p est premier.

Contrairement aux apparences, on ne tourne pas en rond. En effet, comme $\mathrm{Im}(\chi_{n,K})$ est fini, il suffit d'un nombre fini de p pour l'engendrer. On doit donc déterminer "à la main" f_p pour un nombre fini de p, puis tous les autres f_p seront donnés par la classe de p mod n.

4 Valeurs absolues et complétions

4.1 Valeurs absolues et places des corps de nombres

4.1.1 *Définitions.* Une *valeur absolue* sur un corps K est une application $|.| : K \longrightarrow \mathbb{R}_+$ telle que pour tout x, y on a

i) $|x| = 0 \Leftrightarrow x = 0$.

ii) $|xy| = |x||y|$

iii) $|x + y| \leqslant |x| + |y|$

Certains auteurs parlent de *norme multiplicative*, et certains auteurs anglo-saxons de *valuations*. Nous adoptons ici la terminologie de Bourbaki.

La valeur absolue est dite *non-archimédienne* si elle vérifie l'axiome plus fort

iii)' $|x + y| \leqslant \max(|x|, |y|)$

LEMME. – *On a équivalence entre :*

i) $|.|$ *est non archimédienne,*

ii) $\forall n \in \mathbb{Z}$, $|n| \leqslant 1$ *(en notant encore n l'image de n dans K)*

iii) $\exists M > 0$, $\forall n \in \mathbb{Z}$, $|n| \leqslant M$

Démonstration. i)⇒ ii). En effet $|n| = |1 + 1 + \cdots + 1| \leqslant \max(1, 1, \cdots, 1) = 1$

ii) ⇒ iii) est tautologique.

iii) ⇒ i). On a $|x+y|^n = |\sum_{k=0}^n \binom{n}{k} x^k y^{n-k}| \leqslant M \sum_{k=0}^n |x^k y^{n-k}| \leqslant M(n+1)\max(|x|, |y|)^n$ d'où $|x + y| \leqslant \lim_{n\to\infty}(M(n + 1))^{1/n} \max(|x|, |y|) = \max(|x|, |y|)$ □

Conséquences. – Si K est de caractéristique > 0, toutes ses valeurs absolues sont non-archimédiennes.

Remarque. – Si $|.|$ est une v.a. non archimédienne sur K, alors :
– $\mathcal{O} := \{x \in K, |x| \leqslant 1\}$ est un anneau, et
– $\mathfrak{m} := \{x \in K, |x| < 1\}$ en est son unique idéal maximal.

Exemples. – i) La valeur absolue triviale : $|x| = 1, \forall x \in K^\times$.

ii) Le module $z \mapsto |z| = \sqrt{z\overline{z}}$ sur $\mathbb{C}$.

iii) Si $v : K \longrightarrow \mathbb{R} \cup \{\infty\}$ est une valuation alors $x \mapsto \rho^{-v(x)}$ est une valeur absolue non-archimédienne pour tout réel $\rho > 1$.

Corps de nombres.– Soit K un corps de nombres.
– À tout plongement $\sigma : K \hookrightarrow \mathbb{C}$ on associe la v.a. *archimédienne* $|x|_\sigma := |\sigma(x)|$.
– À tout $\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_K)$, on associe la v.a. *non-archimédienne* $|x|_\mathfrak{p} = N\mathfrak{p}^{-v_\mathfrak{p}(x)}$.

4.1.2 *Topologie définie par une valeur absolue.* C'est la topologie engendrée par les boules ouvertes $B(x,r) := \{y \in K, |x-y| < r\}$ pour $x \in K$ et $r > 0$, *i.e.* la topologie métrique associée à la distance $d(x,y) := |x-y|$. La multiplication et l'addition de K sont continues ; on dit que K est un *corps topologique.*

Particularités du cas non-archimédien. Dans ce cas, la distance d est ultramétrique, d'où les curiosités suivantes :
– Tout point d'une boule en est le centre : $\forall y \in B(x,r)$, $B(x,r) = B(y,r)$.
– Si deux boules B_1, B_2 ont une intersection non vide, alors $B_1 \subset B_2$ ou $B_2 \subset B_1$.

Particularité d'une valeur absolue discrète. Si $|K^\times|$ est un sous-groupe discret de $\mathbb{R}_+^\times$, alors les boules ouvertes sont aussi fermées, et les boules fermées de rayon non nul sont ouvertes. La topologie est donc *totalement discontinue* (les seules parties connexes sont les singletons).

Exemple. – Si K est un corps de nombres et $\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_K)$, la topologie associée à $|.|_\mathfrak{p}$ est appelée *topologie $\mathfrak{p}$-adique.* Une base d'ouverts est donnée par les $x+\mathfrak{p}^i = B(x,(N\mathfrak{p})^{-i})$, pour $x \in K$, et $i \in \mathbb{N}$.

Lemme. – *Pour deux valeurs absolues $|.|_1$ et $|.|_2$ non-triviales, on a équivalence entre*

i) $|.|_1$ *et* $|.|_2$ *définissent la même topologie.*

ii) $\forall x \in K$, $|x|_1 \leqslant 1 \Rightarrow |x|_2 \leqslant 1$.

iii) $\exists a > 0$, $|.|_2 = |.|_1^a$.

Démonstration. i)⇒ ii). Clair puisque $|x| < 1 \Leftrightarrow \lim_{n\to\infty} x^n = 0$.

ii)⇒ iii). Puisque $|.|_1$ est non triviale, soit $y \in K$ tel que $|y|_1 > 1$. On a alors $|y|_2 > 1$ et il existe un (unique) $a > 0$ tel que $|y|_2 = |y|_1^a$. Soit maintenant $x \in K$ quelconque et b tel que $|x|_1 = |y|_1^b$. On doit montrer que $|x|_2 = |y|_2^b$. Or, soit $r = \frac{m}{n} \geqslant b$. On a $|x|_1 \leqslant |y|_1^r$, donc $|x^n/y^m|_1 \leqslant 1$, donc $|x^n/y^m|_2 \leqslant 1$ et finalement $|x|_2 \leqslant |y|_2^r$. En passant à la limite, on obtient $|x|_2 \leqslant |y|_2^b$. De même on montre $|x|_2 \geqslant |y|_2^b$.

iii)⇒ i). Sous iii), les deux v.a. définissent les mêmes boules ouvertes. □

Définition. – *Lorsque les propriétés du lemme sont satisfaites, on dit que $|.|_1$ et $|.|_2$ sont* équivalentes. *Une classe d'équivalence de valeurs absolues non triviales sur K est appelée* place de K.

4.1.3 THÉORÈME. (Ostrowski)– *Sur $\mathbb{Q}$, les valeurs absolues non triviales sont équivalentes à la valeur absolue usuelle $|.|_\infty$ ou à une valeur absolue p-adique $|.|_p$ pour p premier.*

Démonstration. Soit $|.|$ une valeur absolue non triviale sur $\mathbb{Q}$, et soient $(a,b) \in \mathbb{N}$ avec $a > 1$. Ecrivons b en base a.

$$\exists! m \in \mathbb{N} \text{ et } \exists!(b_0, \cdots, b_m) \in \{0, \cdots, a-1\}^m \text{ tels que } b = b_0 + b_1 a + \cdots b_m a^m.$$

Noter que $m \leqslant \frac{\log(b)}{\log(a)}$. En posant $M_a := \max\{|1|, |2|, \cdots, |a-1|\}$, on obtient

$$|b| \leqslant \sum_{i=0}^{m} |b_i||a^i| \leqslant (m+1) M_a \max(1, |a|^m) \leqslant M_a \left(\frac{\log(b)}{\log(a)} + 1\right) \max\left(1, |a|^{\frac{\log(b)}{\log(a)}}\right).$$

En appliquant cette inégalité à b^n on en déduit que

$$|b| \leqslant \lim_{n\to\infty} M_a^{1/n} \left(\frac{n\log(b)}{\log(a)} + 1\right)^{1/n} \max\left(1, |a|^{\frac{\log(b)}{\log(a)}}\right) = \max\left(1, |a|^{\frac{\log(b)}{\log(a)}}\right).$$

Deux cas se présentent alors :

i) $\exists b \in \mathbb{N}$, $|b| > 1$. Dans ce cas, $|a| > 1$ et en inversant les rôles on obtient $|b|^{\frac{1}{\log(b)}} = |a|^{\frac{1}{\log(a)}} =: \rho$. On a alors $|x| = \rho^{\log(x)}$ pour tout $x > 0$ et $|x| = |x|_\infty^{\log(\rho)}$ pour tout $x \in \mathbb{Q}$.

ii) $\forall b \in \mathbb{N}, |b| \leqslant 1$. Dans ce cas, l'anneau $\mathcal{O} = \{b \in \mathbb{Q}, |b| \leqslant 1\}$ est un anneau local contenant $\mathbb{Z}$. Soit $\mathfrak{m} = \{b \in \mathbb{Q}, |b| < 1\}$ son idéal maximal. Alors $\mathbb{Z} \cap \mathfrak{m}$ est un idéal premier, qui est non nul car $|.|$ est non triviale. Il est donc de la forme (p) pour un nombre premier p et on constate que $|x|_p \leqslant 1 \Rightarrow |x| \leqslant 1$ pour tout $x \in \mathbb{Q}$. Par le critère ii) du lemme précédent, on en déduit que $|.|$ est équivalente à $|.|_p$.

□

Remarque. – L'intérêt de la normalisation de $|.|_p$ par $|p|_p = p^{-1}$ est qu'on a la *formule du produit* (en notant $\mathcal{P}$ l'ensemble des nombres premiers)

$$\forall x \in \mathbb{Q}, \prod_{v \in \mathcal{P} \cup \{\infty\}} |x|_v = 1.$$

4.1.4 *Complétions : existence et propriétés.* On sait bien que $\mathbb{Q}$ n'est pas complet pour $|.|_\infty$ et que $\mathbb{R}$ est son complété. De même nous verrons que $\mathbb{Q}$ n'est pas complet pour la topologie p-adique, et qu'il sera intéressant de le compléter. En attendant, voici les définitions et constructions des complétions.

Corps valués. Un couple $(K, |.|)$ avec K un corps et $|.|$ une valeur absolue sera appelé *corps valué.* Un morphisme $(K, |.|_K) \longrightarrow (L, |.|_L)$ de corps valués est un morphisme de corps σ tel que $|\sigma(x)|_L = |x|_K$ pour tout $x \in K$. On dit que le corps valué $(K, |.|)$ est *complet* si toute suite de Cauchy pour la distance induite par $|.|$ admet une limite dans K.

DÉFINITION. – *Une complétion d'un corps valué $(K, |.|)$ est un couple $((\hat{K}, |.|), \iota)$ où $(\hat{K}, |.|)$ est un corps valué complet et $\iota : (K, |.|) \hookrightarrow (\hat{K}, |.|)$ un morphisme de corps valués qui possède la propriété universelle suivante : pour tout corps valué complet $(L, |.|_L)$, et tout morphisme $\sigma : (K, |.|) \longrightarrow (L, |.|_L)$ de corps valués, il existe un unique $\hat{\sigma} : (\hat{K}, |.|) \longrightarrow (L, |.|_L)$ tel que $\sigma = \hat{\sigma} \circ \iota$.*

En d'autres termes, le morphisme $\iota : (K, |.|) \hookrightarrow (\hat{K}, |.|)$ est universel parmi les morphismes de $(K, |.|)$ vers un corps valué complet. Cette universalité garantit qu'une complétion, si elle existe, est unique à isomorphisme unique près.

PROPOSITION. – *Tout corps valué $(K, |.|)$ possède une complétion $((\hat{K}, |.|), \iota)$. De plus,*

i) ι est (à isomorphisme près) l'unique morphisme de corps valués de $(K, |.|)$ vers un corps complet dont l'image soit dense.

ii) La topologie de $\hat{K}$ ne dépend que de celle de K. Plus précisément, la complétion de $(K, |.|^a)$ est $((\hat{K}, |.|^a), \iota)$.

Démonstration. La construction de $\hat{K}$ est la même que celle de $\mathbb{R}$. On pose

$$\hat{K} := \{\text{suites de Cauchy de } K\}_{/\sim} \text{ où } (x_n)_n \sim (y_n)_n \text{ si } \lim_{n\to\infty} |x_n - y_n| = 0,$$

et la norme est donnée par $|(x_n)_n| := \lim_{n\to\infty} |x_n|$. Le morphisme ι envoie x sur la suite constante $(x_n = x)_n$. On voit aisément que la propriété universelle annoncée est satisfaite et que K est dense dans $\hat{K}$. Si $(K', |.|')$ est un corps valué complet dans lequel K est dense, le morphisme $(\hat{K}, |.|) \longrightarrow (K', |.|')$ de la propriété universelle est un isomorphisme. Enfin le ii) vient du fait que deux normes équivalentes ont les mêmes suites de Cauchy. □

Exemple. – La complétion de $(\mathbb{Q}, |.|_\infty)$ est $(\mathbb{R}, |.|)$ muni de l'inclusion naturelle. La complétion de $(\mathbb{Q}, |.|_p)$ est notée $(\mathbb{Q}_p, |.|_p)$, et appelée corps des *nombres p-adiques*. Nous l'étudierons en détail plus loin.

4.1.5 THÉORÈME.– *Sur un corps de nombres K, toute valeur absolue non triviale est équivalente à une valeur absolue $|.|_\sigma$ pour un $\sigma : K \hookrightarrow \mathbb{C}$ ou à $|.|_\mathfrak{p}$ pour $\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_K)$. De plus, parmi ces dernières, les seules équivalentes sont $|.|_\sigma$ et $|.|_{c\circ\sigma}$ où c désigne la conjugaison complexe.*

Démonstration. Soit $|.|$ une valeur absolue non triviale sur K.

i) Supposons que $|.|$ est non archimédienne. Il nous suffira alors de montrer que $\forall x \in \mathcal{O}_K, |x| \leqslant 1$. En effet, dans ce cas, en notant $\mathfrak{p} := \{x \in \mathcal{O}_K,\ |x| < 1\}$ et en choisissant une uniformisante ϖ de $\mathcal{O}_{K,\mathfrak{p}}$, on aura $|x| = |\varpi|^{v_\mathfrak{p}(x)}$ pour tout $x \in K$.

Soit donc $x \in \mathcal{O}_K$ et $f_x = X^n + a_0 X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ son polynôme minimal. Puisque $|.|$ est non-archimédienne on a $|a_i| \leqslant 1$ pour tout i. On en déduit $|x|^n \leqslant \max(1, |x|^{n-1})$ ce qui implique $|x| \leqslant 1$.

ii) Supposons maintenant $|.|$ archimédienne. Soit $\iota : K \hookrightarrow \hat{K}$ la complétion de K pour $|.|$. Puisque $|.|_{|\mathbb{Q}} \sim |.|_\infty$, l'inclusion $\mathbb{Q} \hookrightarrow K$ induit une inclusion continue $\mathbb{R} \hookrightarrow \hat{K}$. Soit alors $\alpha \in K$ tel que $K = \mathbb{Q}[\alpha]$. Considérons le sous-corps $\mathbb{R}[\iota(\alpha)]$ de $\hat{K}$. Il est algébrique

sur $\mathbb{R}$, donc de degré au plus 2. La valeur absolue de $\hat{K}$ induit une valeur absolue $|.|$ de $\mathbb{R}[\iota(\alpha)]$, qui est aussi une norme de $\mathbb{R}$-espace vectoriel ; il s'ensuit que $\mathbb{R}[\iota(\alpha)]$ est complet, puisque de dimension finie sur $\mathbb{R}$, et que la valeur absolue $|.|$ induit la topologie de $\mathbb{R}$-ev de dimension finie sur $\mathbb{R}[\iota(\alpha)]$, donc est équivalente à la valeur absolue usuelle de $\mathbb{R}[\iota(\alpha)]$ (qu'il soit isomorphe à $\mathbb{R}$ ou $\mathbb{C}$). Puisque complet, $\mathbb{R}[\iota(\alpha)]$ est fermé dans $\hat{K}$. Or il contient $\iota(K)$ qui est dense, donc finalement $\mathbb{R}[\iota(\alpha)] = \hat{K}$.

On a donc prouvé que l'extension $\mathbb{R} \hookrightarrow \hat{K}$ est de degré 1 ou 2. Si elle est de degré 1, c'est un isomorphisme topologique et ι fournit donc le plongement continu $\sigma : K \hookrightarrow \mathbb{R}$ cherché. Si elle est de degré 2, alors on peut choisir un isomorphisme $\mathbb{R}$-linéaire continu $\hat{K} \xrightarrow{\sim} \mathbb{C}$ d'où, après composition avec ι, le plongement continu $\sigma : K \hookrightarrow \mathbb{C}$ cherché.

iii) Reste à étudier les équivalences entre ces normes. Dans le cas non-archimédien, on retrouve $\mathfrak{p}$ à partir de $|.|_\mathfrak{p}$ puisque $\mathfrak{p} = \{x \in \mathcal{O}_K, |x| < 1\}$. Dans le cas archimédien, il est clair que σ et $c \circ \sigma$ induisent la même topologie sur K puisque $c : \mathbb{C} \longrightarrow \mathbb{C}$ est continu. Réciproquement, supposons $|.|_\sigma \sim |.|_{\sigma'}$. Cela signifie qu'il existe un isomorphisme *K-linéaire* de corps *topologiques* de la complétion K_σ de K pour $|.|_\sigma$ vers son homologue $K_{\sigma'}$. Notons que K_σ s'identifie à l'adhérence de $\sigma(K)$ dans $\mathbb{C}$. On a donc un diagramme

$$\begin{array}{ccccc} K & \xhookrightarrow{\sigma} & K_\sigma & \hookrightarrow & \mathbb{C} \\ & \searrow^{\sigma'} & \downarrow \exists f \simeq & & \\ & & K_{\sigma'} & \hookrightarrow & \mathbb{C} \end{array}$$

Deux cas se présentent :

(a) si $K_\sigma = \mathbb{R}$, alors on doit aussi avoir $K_{\sigma'} = \mathbb{R}$, mais le seul automorphisme continu de $\mathbb{R}$ est l'identité, donc $\sigma = \sigma'$.

(b) si $K_\sigma = \mathbb{C}$, alors on doit aussi avoir $K_{\sigma'} = \mathbb{C}$, mais les seuls automorphismes continus de $\mathbb{C}$ sont l'identité et la conjugaison complexe, donc $\sigma = \sigma'$ ou $\sigma' = c \circ \sigma$. □

4.1.6 *Places d'un corps de nombres.* D'après le théorème précédent on a

$$\{\text{places de } K\} \leftrightarrow \mathrm{Max}(\mathcal{O}_K) \cup \{\text{plongements } K \hookrightarrow \mathbb{C}\}_{/\mathrm{conj}}.$$

Une place est typiquement notée v, et la complétion de K associée est notée K_v. Les places non-archimédiennes sont aussi appelées *places finies*. On note $v|p$ si v correspond à $\mathfrak{p} = \mathfrak{p}_v|(p)$. On dit aussi que v est une place p-adique dans ce cas, et on note aussi $K_\mathfrak{p} = K_v$. Les places archimédiennes sont aussi appelées *places infinies* et on note $v|\infty$. On note aussi $K_\sigma = K_v$ lorsque v correspond au plongement σ. On dit que la place est réelle si $K_v \simeq \mathbb{R}$, et complexe sinon. Pour chaque place, il est utile de choisir soigneusement une valeur absolue normalisée :

- Si v est finie, on prend $|.|_v = |.|_{\mathfrak{p}_v}$.
- Si v est réelle et correspond à $\sigma : K \hookrightarrow \mathbb{R}$, on prend $|.|_v = |.|_\sigma$.
- Si v est complexe et correspond à $\{\sigma, c \circ \sigma\}$ on prend $|.| = |.|_\sigma \times |.|_{c\circ\sigma}$.

Dans ce dernier cas, $|.|_v$ n'est pas vraiment une valeur absolue car elle ne vérifie pas l'inégalité triangulaire. Mais cela permet d'avoir la formule du produit.

4.1.7 PROPOSITION.– *Avec les normalisations ci-dessus, si $\alpha \in K$ on a :*

$$\prod_{v|\infty} |\alpha|_v = |N_{K/\mathbb{Q}}(\alpha)|_\infty, \quad \prod_{v|p} |\alpha|_v = |N_{K/\mathbb{Q}}(\alpha)|_p, \quad \textit{et donc} \prod_v |\alpha|_v = 1$$

Démonstration. i) On a par définition $\prod_{v|\infty} |\alpha|_v = \prod_{\sigma:K\hookrightarrow\mathbb{C}} |\sigma(\alpha)| = |N_{K/\mathbb{Q}}(\alpha)|$.

ii) On a $\prod_{v|p} |\alpha|_v = \prod_{\mathfrak{p}|p} N\mathfrak{p}^{-v_\mathfrak{p}(\alpha)} = |\mathcal{O}_{K,\mathfrak{p}}/(\alpha)|^{-1}$ (ici $|.|$ signifie "cardinal" et cette égalité vient de la décomposition $\mathcal{O}_{K,\mathfrak{p}}/(\alpha) = \prod_{\mathfrak{p}|p} \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}^{v_\mathfrak{p}(\alpha)}$).

Or, $|\mathcal{O}_{K,\mathfrak{p}}/(\alpha)| = |(\mathcal{O}_K/(\alpha))_p|$ est la partie p-primaire de $|\mathcal{O}_K/(\alpha)| = |N_{K/\mathbb{Q}}(\alpha)|$, et donc $|\mathcal{O}_{K,\mathfrak{p}}/(\alpha)|^{-1} = |N_{K/\mathbb{Q}}(\alpha)|_p$.

□

Remarque. – L'isomorphisme ii) de la page 14 se réinterprète en :

$$K \otimes_\mathbb{Q} \mathbb{R} \simeq \prod_{v|\infty} K_v.$$

Un isomorphisme semblable existe pour les places finie. Soit p un nombre premier. Si $\mathfrak{p}|p$ dans $\mathrm{Max}(\mathcal{O}_K)$, l'inclusion $\mathbb{Q} \hookrightarrow K$ induit, par propriété universelle des complétions, un plongement continu $\mathbb{Q}_p \hookrightarrow K_\mathfrak{p}$ puisque la restriction de $|.|_\mathfrak{p}$ à $\mathbb{Q}$ est équivalente à $|.|_p$. On a donc un morphisme canonique $K \otimes_\mathbb{Q} \mathbb{Q}_p \longrightarrow K_\mathfrak{p}$, $x \otimes y \mapsto xy$. Si on écrit $K = \mathbb{Q}[\alpha]$, on voit que la norme de $K_\mathfrak{p}$ induit une norme du $\mathbb{Q}_p$-e.v. de dimension finie $\mathbb{Q}_p[\iota(\alpha)] \subset K_\mathfrak{p}$, et donc que ce dernier est complet. Comme il contient K on a $\mathbb{Q}_p[\iota(\alpha)] = K_\mathfrak{p}$ et $K_\mathfrak{p}$ est donc de dimension finie sur $\mathbb{Q}_p$. Considérons maintenant le morphisme

$$K \otimes_\mathbb{Q} \mathbb{Q}_p \longrightarrow \prod_{\mathfrak{p}|p} K_\mathfrak{p}.$$

Le lemme d'approximation (conséquence iii) du théorème 3.3.4) nous dit que l'image de K dans le terme de droite est *dense* (exercice). Il s'ensuit que l'image est un $\mathbb{Q}_p$-sev dense du terme de droite, donc égal au terme de droite, puisque tout espace vectoriel de dimension finie sur un corps valué complet est complet. Ainsi : *le morphisme produit ci-dessus est surjectif.*

Nous démontrerons plus tard que ce morphisme est un isomorphisme. En fait, la description explicite de $K_\mathfrak{p}$ permettra de voir que les dimensions sur $\mathbb{Q}_p$ sont égales.

4.1.8 *Situation relative.* Supposons donnée une extension $L \supset K$ de corps de nombres. Par restriction, on obtient une application $w \mapsto v$ de l'ensemble des places de L dans celui de K. On note $w|v$ pour "w divise v" ou "w est au-dessus de v". Bien-sûr, dans ce cas w est non-archimédienne si et seulement si v l'est et on a alors $\mathfrak{P}_w|\mathfrak{p}_v$. Les formules de la proposition précédente se généralisent en (voir plus loin) :

$$\forall \alpha \in L, \prod_{w|v} |\alpha|_w = |N_{L/K}(\alpha)|_v$$

$$L \otimes_K K_v \xrightarrow{\sim} \prod_w L_w.$$

4.2 Complétion dans le cas non-archimédien

4.2.1 *Généralités.* Soit $(K, |.|)$ un corps valué non-archimédien, $\mathcal{O}$ son anneau de valuation et $\mathfrak{m}$ l'idéal maximal de celui-ci.

Sa complétion $((\hat{K}, |.|), \iota)$ est aussi non-archimédienne (puisque $|.|$ reste bornée sur les entiers, par exemple). Notons $\hat{\mathcal{O}}$ son anneau de valuation et $\hat{\mathfrak{m}}$ l'idéal maximal.

On a alors $\iota(\mathcal{O}) \subset \hat{\mathcal{O}}$ et le couple $(\hat{\mathcal{O}}, \iota)$ est une complétion de $\mathcal{O}$ pour la métrique induite par la valeur absolue $|.|$.

Supposons maintenant que $|K^\times|$ est discret. (ou de manière équivalente que $\mathcal{O}$ est un AVD). On a alors les propriétés suivantes :

i) $|\hat{K}^\times| = |K^\times|$ (clair sur la construction avec les suites de Cauchy), donc $\hat{\mathcal{O}}$ est aussi un AVD, et toute uniformisante ϖ de $\mathfrak{m}$ est une uniformisante de $\hat{\mathfrak{m}}$ (puisque ϖ est uniformisante ssi $|\varpi|$ engendre $|K^\times|$).

ii) La topologie de $\mathcal{O}$ associée à $|.|$ est la "topologie ϖ-adique" engendrée par les ensembles de la forme $x + \mathfrak{m}^i = x + \varpi^i\mathcal{O}$, où $x \in \mathcal{O}$ et $i \in \mathbb{N}$. En effet $x + \mathfrak{m}^i$ est la boule ouverte $B(x, |\varpi|^{i+\varepsilon})$ pour tout $1 > \varepsilon > 0$.

iii) De même, la topologie de $\hat{\mathcal{O}}$ associée à $|.|$ est la "topologie ϖ-adique" engendrée par les ensembles de la forme $x + \hat{\mathfrak{m}}^i = x + \varpi^i\hat{\mathcal{O}}$, où $x \in \mathcal{O}$ et $i \in \mathbb{N}$.

iv) *L'inclusion ι induit des isomorphismes $\mathcal{O}/\varpi^n\mathcal{O} \xrightarrow{\sim} \hat{\mathcal{O}}/\varpi^n\hat{\mathcal{O}}$.* En effet,
   - on a $\varpi^n\hat{\mathcal{O}} \cap \mathcal{O} = \{x \in \mathcal{O}, |x| \leqslant |\varpi^n|\} = \varpi^n\mathcal{O}$ d'où l'injectivité.
   - La densité de $\mathcal{O}$ dans $\hat{\mathcal{O}}$ pour la topologie ϖ-adique donne la surjectivité.

Considérons maintenant l'anneau

$$\lim_{\longleftarrow n} \mathcal{O}/\varpi^n\mathcal{O} := \left\{ (x_n)_{n\in\mathbb{N}} \in \prod_n \mathcal{O}/\varpi^n\mathcal{O},\ x_n = \bar{x}_m, \forall m > n \right\}.$$

On le munit de la topologie induite par la topologie produit des topologies discrètes sur chaque $\mathcal{O}/\varpi^n\mathcal{O}$. On obtient un anneau topologique (addition et multiplication sont continues). Le point iv) ci-dessus nous fournit des morphismes d'anneaux $\hat{\mathcal{O}} \longrightarrow \mathcal{O}/\varpi^n\mathcal{O}$ qui, par le point iii), sont continus pour la topologie discrète de $\mathcal{O}/\varpi^n\mathcal{O}$. Le produit cartésien de ces morphismes induit donc un homomorphisme continu $\mathcal{O}$-linéaire d'anneaux topologiques

$$\hat{\mathcal{O}} \longrightarrow \lim_{\longleftarrow n} \mathcal{O}/\varpi^n\mathcal{O}, \quad x \mapsto (\overline{x})_n.$$

4.2.2 Proposition.– *Sous les hypothèses précédentes ($|K^\times|$ discret dans $\mathbb{R}_+^\times$), le morphisme ci-dessus est un isomorphisme $\hat{\mathcal{O}} \xrightarrow{\sim} \lim_{\longleftarrow n} \mathcal{O}/\varpi^n\mathcal{O}$ d'anneaux topologiques.*

Démonstration. Injectivité. Par le point iv) ci-dessus, on peut remplacer la cible du morphisme étudié par $\lim_{\longleftarrow n} \hat{\mathcal{O}}/\varpi^n\hat{\mathcal{O}}$. On voit alors que le noyau de ce morphisme est $\bigcap_n \varpi^n\hat{\mathcal{O}}$ donc est nul, puisque ϖ est uniformisante de l'A.V.D. $\hat{\mathcal{O}}$.

Surjectivité. Si $(x_n)_n$ est une suite dans le terme de doite, et $(\tilde{x}_n)_n$ une suite de relèvements dans $\mathcal{O}^{\mathbb{N}}$, alors $(\tilde{x}_n)$ est une suite de Cauchy dans $\mathcal{O}$ pour la métrique associée à $|.|$. Cette suite admet donc une limite x dans $\hat{\mathcal{O}}$, dont l'image est justement $(x_n)_n$.

Homéomorphie. La continuité a déjà été expliquée. Il reste à voir que ce morphisme est ouvert. Or il envoie $x+\mathfrak{m}^i$ sur l'image réciproque de $\{\overline{x}\}$ via la projection $\varprojlim(\hat{\mathcal{O}}/\varpi^n\hat{\mathcal{O}}) \longrightarrow \hat{\mathcal{O}}/\varpi^i\hat{\mathcal{O}}$. Mais cette projection est continue et $\{\overline{x}\}$ est ouvert dans $\hat{\mathcal{O}}/\varpi^i\hat{\mathcal{O}}$, donc l'image de $x+\mathfrak{m}^i$ est bien ouverte. □

Cette proposition donne une construction algébrique de la complétion. Concrètement, si R est l'image d'une section ensembliste $\mathcal{O}/\varpi\mathcal{O} \hookrightarrow \mathcal{O}$ de la projection naturelle, alors tout élément de $\mathcal{O}$ *s'écrit de manière unique* comme une série $x = \sum_{n\in\mathbb{N}} a_n\varpi^n$ avec $a_n \in R$. Cependant, l'addition et la multiplication ne sont pas faciles à décrire dans ces termes.

Exemple. – On note $\mathbb{Z}_p$ l'anneau de valuation de $\mathbb{Q}_p$. C'est donc la "complétion p-adique" de $\mathbb{Z}$, donnée par

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \left\{ \sum_{n\in\mathbb{N}} a_n p^n,\ (a_n)_n \in \{0,\cdots,p-1\}^{\mathbb{N}} \right\}.$$

On remarque que $\mathbb{N}$, qui s'identifie aux éléments tels que $a_n = 0$ pour $n >> 0$, est dense dans $\mathbb{Z}_p$. Les règles habituelles de multiplication et addition en base p (avec retenues, etc.) se prolongent à $\mathbb{Z}_p$. Par exemple, -1 s'écrit $-1 = \sum_{n\in\mathbb{N}}(p-1)p^n$. Par ailleurs, comme $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$, on obtient aussi des développement en "série"

$$\mathbb{Q}_p = \left\{ \sum_{n\in\mathbb{Z}} a_n p^n,\ (a_n)_n \in \{0,\cdots,p-1\}^{\mathbb{N}} \text{ et } a_{-n} = 0 \text{ pour } n >> 0 \right\}.$$

Exemple. – Un exemple plus facile est celui de $\mathbb{F}_p[X]$ pour la valuation X-adique. Dans ce cas le complété est

$$\mathbb{F}_p[[X]] = \varprojlim_n \mathbb{F}_p[X]/(X^n) = \left\{ \sum_{n\in\mathbb{N}} a_n X^n,\ (a_n)_n \in \mathbb{F}_p^{\mathbb{N}} \right\}.$$

Mais ici, l'addition et la multiplication sont beaucoup plus faciles à voir : ce sont les opérations usuelles sur les séries formelles. Le corps des fractions est noté $\mathbb{F}_p((X))$.

4.2.3 Corollaire.– *Si K est un corps valué complet non-archimédien, alors on a équivalence entre*

i) K est localement compact

ii) $\mathcal{O}$ est compact

iii) $|K^\times|$ est discret dans $\mathbb{R}^\times$ et le corps résiduel $\mathcal{O}/\mathfrak{m}$ est fini.

Démonstration. i) $\Rightarrow$ ii) car si K est localement compact, ses boules fermées sont compactes et $\mathcal{O}$ est une boule fermée.

iii) $\Rightarrow$ i) découle de la proposition précédente, car tous les $\mathcal{O}/\varpi^n\mathcal{O}$ sont alors finis, donc leur produit est compact et la limite projective est fermée dans le produit.

ii) $\Rightarrow$ iii). Comme $\mathfrak{m}$ est ouvert, la projection $\mathcal{O} \longrightarrow \mathcal{O}/\mathfrak{m}$ est continue pour la topologie discrète de $\mathcal{O}/\mathfrak{m}$. Elle est aussi surjective, donc $\mathcal{O}/\mathfrak{m}$ est compact et discret et par conséquent fini. Soit maintenant $0 < r < 1$ et $I_r := \{x \in \mathcal{O}, |x| < r\}$. C'est un idéal ouvert donc, comme ci-dessus, $\mathcal{O}/I_r$ est fini. Cela implique que $|K^\times| \cap]r, 1]$ est fini, et donc que le sous-groupe $|K^\times|$ de $\mathbb{R}_+^\times$ est discret. □

Exemple. – L'anneau $\mathbb{Z}_p$ est compact et $\mathbb{Q}_p$ est localement compact. Plus généralement, si K est un corps de nombres et $\mathfrak{p}|p$, alors $K_\mathfrak{p}$ est un corps localement compact et de degré fini sur $\mathbb{Q}_p$ (déjà vu plus haut). De même $\mathbb{F}_p((X))$ est localement compact.

Ces exemples de corps non archimédiens localement compacts sont en fait typiques :

Proposition. – *Tout corps non archimédien localement compact est une extension finie d'un $\mathbb{Q}_p$ ou isomorphe à un $\mathbb{F}_q[[X]]$.*

Nous montrerons plus loin que, inversement, toute extension finie de $\mathbb{Q}_p$ possède une valeur absolue qui en fait un corps valué localement compact, et nous montrerons aussi qu'une telle extension finie provient de la complétion d'un corps de nombres.

Démonstration. Supposons K de caractéristique 0 et soit p la caractéristique du corps fini $\mathcal{O}/\mathfrak{m}$. Alors $|p| < 1$ et la restriction de $|.|$ à $\mathbb{Q}$ est p-adique, si bien que K contient $\mathbb{Q}_p$ et $\mathcal{O}$ contient $\mathbb{Z}_p$. Nous allons montrer que $\mathcal{O}$ est de type fini sur $\mathbb{Z}_p$. On sait que $\mathcal{O}/p\mathcal{O}$ est fini. Fixons une $\mathbb{F}_p$-base $\overline{x}_1, \cdots, \overline{x}_m$ de $\mathcal{O}/p\mathcal{O}$ et des relèvements $x_1, \cdots, x_m$ dans $\mathcal{O}$. Nous allons montrer que $x_1, \cdots, x_m$ est une $\mathbb{Z}_p$ base de $\mathcal{O}$.

S'il existe une relation de dépendence $\mathbb{Z}_p$-linéaire non nulle $\sum_i a_i x_i = 0$, il en existe une pour laquelle $v_p(a_1) = 0$. Mais alors la projection dans $\mathcal{O}/p\mathcal{O}$ donne une relation de dépendence linéaire non nulle sur les $\overline{x}_i$: contradiction. La famille $(x_1, \cdots, x_n)$ est donc libre sur $\mathbb{Z}_p$.

Soit maintenant $x \in \mathcal{O}$. On peut trouver $a_1^1, \cdots, a_m^1 \in \mathbb{Z}_p$ tels que $x - \sum_i a_i^1 x_i \in p\mathcal{O}$. Par récurrence on peut trouver $a_1^n, \cdots, a_m^n \in \mathbb{Z}_p$ tels que $x - \sum_i a_i^n x_i \in p^n\mathcal{O}$ et $v_p(a_i^n - a_i^{n-1}) \geqslant n$. Les suites $(a_i^n)_{n\in\mathbb{N}}$ sont donc de Cauchy et convergent vers des éléments $a_i \in \mathbb{Z}_p$. Par construction $x - \sum_i a_i x_i \in \bigcap_n p^n\mathcal{O} = \{x \in \mathcal{O}_K, |x| < |p|^n \forall n\} = \{0\}$.

Ainsi la famille $(x_1, \cdots, x_m)$ est une base de $\mathcal{O}$ sur $\mathbb{Z}_p$, et donc une base de K sur $\mathbb{Q}_p$ (exercice).

Le cas où K est de caractéristique positive est laissé au lecteur. □

4.2.4 *Complétion et extension d'anneaux de Dedekind.* Revenons à un contexte maintenant familier : soit A un anneau de Dedekind, $K = \mathrm{Frac}(A)$, L une extension séparable finie de K et B la clôture intégrale de A dans L. On sait que B est de type fini comme A-module. Enfin, soit $\mathfrak{p} \in \mathrm{Max}(A)$. Nous avons vu que $B_\mathfrak{p} := A_\mathfrak{p} \otimes_A B$ s'identifie, via

l'application $a \otimes b \mapsto ab \in L$ au sous anneau $A_{\mathfrak{p}}B$ de L qui n'est autre que la clôture intégrale de $A_{\mathfrak{p}}$ dans L. C'est un anneau semi-local tel que $\mathrm{Max}(B_{\mathfrak{p}}) \leftrightarrow \{\mathfrak{P} \in \mathrm{Max}(B), \mathfrak{P}|\mathfrak{p}\}$. Cet anneau est intègre, mais le résultat suivant montre comment sa complétion $\mathfrak{p}$-adique permet de le scinder en un produit d'anneaux locaux complets.

THÉORÈME. – *Avec les notations ci-dessus, on a un isomorphisme d'anneaux topologiques*

$$\hat{A}_{\mathfrak{p}} \otimes_A B \xrightarrow{\sim} \prod_{\mathfrak{P}|\mathfrak{p}} \hat{B}_{\mathfrak{P}}.$$

De plus, $\hat{B}_{\mathfrak{P}}$ est libre de rang $e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$ sur $\hat{A}_{\mathfrak{p}}$ et s'identifie à la clôture intégrale de $\hat{A}_p$ dans le complété $\hat{L}_{\mathfrak{P}}$ de L pour toute valeur absolue $\mathfrak{P}$-adique.

Démonstration. Par définition le terme de gauche est $\hat{A}_{\mathfrak{p}} \otimes_A B = (\varprojlim_n A/\mathfrak{p}^n) \otimes_A B = (\varprojlim_n A_{\mathfrak{p}}/\mathfrak{p}^n A_{\mathfrak{p}}) \otimes_{A_{\mathfrak{p}}} B_{\mathfrak{p}}$. Comme $B_{\mathfrak{p}}$ est libre de rang fini, on peut le rentrer dans la limite projective (puisqu'une limite projective d'une somme directe de systèmes projectifs est la somme directe des limites). Le terme de gauche devient alors $\varprojlim_n (A_{\mathfrak{p}}/\mathfrak{p}^n A_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} B_{\mathfrak{p}}) = \varprojlim_n (A/p^n \otimes_A B) = \varprojlim_n B/\mathfrak{p}^n B$. Or,pour tout n, on a avec les notations usuelles

$$B/\mathfrak{p}^n B = \prod_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{ne(\mathfrak{P}/\mathfrak{p})}.$$

On en déduit l'isomorphisme du théorème en prenant la limite projective, sachant que si $[(M_n)_n, (\rho_{m,n} : M_m \longrightarrow M_n)_{n \leqslant m}]$ est un système projectif, et si $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ est une application strictement croissante, alors $\varprojlim_n M_n \xrightarrow{\sim} \varprojlim_n M_{\varphi(n)}$.

$\hat{B}_{\mathfrak{P}}$ est libre sur $\hat{A}_{\mathfrak{p}}$, puisque qu'il est facteur direct d'un libre et puisque $\hat{A}_{\mathfrak{p}}$ est principal (A.V.D). Son rang est celui de $\hat{B}_{\mathfrak{P}}/\mathfrak{p}\hat{B}_{\mathfrak{P}} = \hat{B}_{\mathfrak{p}}/\mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}\hat{B}_{\mathfrak{P}} = B_{\mathfrak{p}}/\mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}B_{\mathfrak{P}} = B/\mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})}$ sur $A/\mathfrak{p}$, à savoir $e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$.

Munissons maintenant L d'une valeur absolue $\mathfrak{P}$-adique (du type $|x| = \rho^{-v_{\mathfrak{P}}(x)}$ pour $\rho > 1$). La restriction à K est une valeur absolue $\mathfrak{p}$-adique, d'où un plongement continu des complétés $\hat{K}_{\mathfrak{p}} \hookrightarrow \hat{L}_{\mathfrak{P}}$. On a vu que $\hat{A}_{\mathfrak{p}}$ s'identifie à l'anneau de valuation de $\hat{K}_{\mathfrak{p}}$ et de même pour $\hat{B}_{\mathfrak{P}}$ dans $\hat{L}_{\mathfrak{P}}$. En particulier, $\hat{B}_{\mathfrak{P}}$ est un A.V.D, donc est normal et son corps des fractions est $\hat{L}_{\mathfrak{P}}$. Comme il est de type fini sur $\hat{A}_{\mathfrak{p}}$, c'en est la clôture intégrale dans $\hat{L}_{\mathfrak{P}}$. □

Exemple. – Soit K un corps de nombres, on obtient : $\mathcal{O}_K \otimes \mathbb{Z}_p \xrightarrow{\sim} \prod_{\mathfrak{p}|p} \mathcal{O}_{K_{\mathfrak{p}}}$. En inversant p, on en déduit l'isomorphisme

$$K \otimes_{\mathbb{Q}} \mathbb{Q}_p \xrightarrow{\sim} \prod_{\mathfrak{p}[p} K_{\mathfrak{p}}.$$

Plus généralement, si $L \supset K$ est une extension de corps de nombres et v une place finie de K, on obtient une décomposition

$$L \otimes_K K_v \xrightarrow{\sim} \prod_{w|v} L_w.$$

4.2.5 *Extension de valuations.* On s'intéresse à la question suivante : étant donné un corps valué $(K, |.|)$ et une extension L de K. Peut-on prolonger la valeur absolue de K à L ? Nous y répondons sous l'hypothèse que K est non-archimédien complet et $|K^\times|$ est discret. Le résultat peut s'énoncer de manière algébrique ou plus "analytique". Voici l'énoncé algébrique.

COROLLAIRE. – *Soient A, K, B, L comme au paragraphe précédent. Si A est un A.V.D complet, alors B est un A.V.D complet.*

Démonstration. L'isomorphisme du théorème précédent devient :

$$B \xrightarrow{\sim} \prod_{\mathfrak{P} \in \mathrm{Max}(B)} \hat{B}_{\mathfrak{P}}.$$

Or B est intègre, donc $\mathrm{Max}(B)$ est un singleton $\{\mathfrak{P}\}$ et $B = \hat{B}_{\mathfrak{P}}$ est bien un AVD complet. □

Voici la version plus analytique.

COROLLAIRE. – *Soit $(K, |.|_K)$ un corps valué complet non archimédien, tel que $|K^\times|$ est discret dans $\mathbb{R}_+^\times$, et soit L une extension séparable finie de degré n. Alors il existe une unique valeur absolue $|.|_L$ sur L prolongeant $|.|_K$, donnée par*

$$\forall x \in L,\ |x|_L = |N_{L/K}(x)|_K^{1/n}.$$

Démonstration. L'existence d'un prolongement résulte du corollaire précédent appliqué à $A = \mathcal{O} = \{x \in K, |x| \leqslant 1\}$. En effet, écrivons $|x|_K = \rho^{-v(x)}$ où v est la valuation de A et $\rho = |\varpi|^{-1}$ avec ϖ uniformisante de A. Soit v' la valuation de la clôture intégrale B de A dans L. Alors $x \mapsto \rho^{-\frac{v'(x)}{v'(\varpi)}}$ définit une valeur absolue sur L qui prolonge $|.|_K$.

Montrons l'unicité. Soit $|.|_L$ un prolongement. C'est une valeur absolue non archimédienne dont l'anneau contient A et donc aussi la clôture intégrale B de A. On a donc $|B^\times|_L = 1$. Vu la décomposition $L^\times = \bigsqcup_n \varpi_B^n B^\times$, on voit que $|.|_L$ est déterminé par $|\varpi_B|_L$. Soit e tel que $\varpi B = \varpi_B^e B$ (ie $e = v'(\varpi)$) on doit avoir $|\varpi_B|_L^e = |\varpi|_K$, ce qui finalement détermine $|.|_L$ complètement.

Pour voir la formule annoncée, on peut montrer directement que $v(N_{L/K}(x)) = \frac{n}{e} v'(x)$ (exercice). On peut aussi fixer une clôture Galoisienne $\tilde{L}$ de L sur K et remarquer que, par unicité, on a $|x|_L = |\sigma(x)|_{\tilde{L}}$ pour tout plongement $\sigma : L \hookrightarrow \tilde{L}$, ce qui donne

$$|x|_L^n = \prod_{\sigma : L \hookrightarrow \tilde{L}} |\sigma(x)|_{\tilde{L}} = |N_{L/K}(x)|_K.$$

□

Application : soit $\overline{\mathbb{Q}}_p$ une clôture algébrique de $\mathbb{Q}_p$. Il existe un unique prolongement $|.|_p$ à $\overline{\mathbb{Q}}_p$ de la valeur absolue $|.|_p$, et le groupe de Galois agit par isométries :

$$\forall \sigma \in G_{\overline{\mathbb{Q}}_p/\mathbb{Q}_p}, \forall x \in \overline{\mathbb{Q}}_p,\ \ |\sigma(x)|_p = |x|_p.$$

Si K est un corps de nombres, tout plongement $K \hookrightarrow \overline{\mathbb{Q}}_p$ fournit une valeur absolue p-adique de K donnée par $|x|_\sigma := |\sigma(x)|_p$. Deux plongements conjugués sous $G_{\overline{\mathbb{Q}}_p/\mathbb{Q}_p}$ donnent la même valeur absolue, et cela induit une bijection

$$\{\sigma : K \hookrightarrow \overline{\mathbb{Q}}_p\}/_{G_{\overline{\mathbb{Q}}_p/\mathbb{Q}_p}} \leftrightarrow \{\text{places } v \text{ } p\text{-adiques}\}.$$

Le complété $K_\sigma = K_v$ s'identifie, via σ, au sous-corps composé $\sigma(K)\mathbb{Q}_p$ de $\overline{\mathbb{Q}}_p$, qui est aussi l'adhérence de $\sigma(K)$ dans $\overline{\mathbb{Q}}_p$. La situation est maintenant très similaire à la situation archimédienne.

Remarque. – La valeur absolue de $\overline{\mathbb{Q}}_p$ n'est plus discrète ! En fait on a $|\overline{\mathbb{Q}}_p^\times|_p = p^{\mathbb{Q}}$. L'inclusion $|\overline{\mathbb{Q}}_p^\times|_p \subset p^{\mathbb{Q}}$ découle de la formule du corollaire (avec la norme), et l'autre inclusion se voit en remarquant que si $\alpha^n = p$ alors $|\alpha| = p^{-1/n}$. En particulier, $\overline{\mathbb{Q}}_p$ n'est pas complet. Son complété est généralement noté $\mathbb{C}_p$. On peut montrer qu'il est encore algébriquement clos.

Exercice. – Soit $F \supset \mathbb{Q}_p$ une extension finie. On dit qu'elle est "ramifiée" ou "non ramifiée" si l'unique $\mathfrak{P}|(p)$ l'est. On note aussi $e = e(\mathfrak{P}/p)$ (indice de ramification) et $f = f(\mathfrak{P}/p)$ (degré rédiduel). On a $[F : \mathbb{Q}_p] = ef$.

i) Montrer que F est non ramifiée si et seulement si $|F^\times|_p = |\mathbb{Q}_p^\times|_p$.

ii) Montrer que si F est totalement ramifiée (ie $f = 1$) si et seulement si pour toute uniformisante ϖ_F de $\mathcal{O}_F$, la norme $N_{F/\mathbb{Q}_p}(\varpi_F)$ est une uniformisante de $\mathbb{Z}_p$.

Mise en garde.– Sur $F \supset \mathbb{Q}_p$, il ne faut pas confondre la valeur absolue $|.|_p$ obtenue ci-dessus et la valeur absolue $|.|_{\mathfrak{p}_F}$ normalisée comme dans le cas des corps de nombres. Si v est la valuation normalisée de $\mathcal{O}_F$, alors on a

$$\forall x \in F, \quad |x|_p = p^{\frac{-v(x)}{e}} \quad \text{et} \quad |x|_{\mathfrak{p}_E} = p^{-fv(x)}.$$

4.2.6 *Action de Galois.* On reprend le contexte A, K, B, L des paragraphes précédents, et on suppose de plus que L est Galoisienne sur K. Soit $\mathfrak{P} \in \mathrm{Max}(B)$ et $\mathfrak{p} = A \cap \mathfrak{P}$. Le groupe de décomposition $D_\mathfrak{P} \subset G_{L/K}$ agit sur chaque $B/\mathfrak{P}^i$, donc agit sur la limite projective $\hat{B}_\mathfrak{P}$, et donc sur le corps des fractions $\hat{L}_\mathfrak{P} = \mathrm{Frac}(\hat{B}_\mathfrak{P})$, qui est aussi le complété de L pour toute valeur absolue $\mathfrak{P}$-adique. Cette action se fait par automorphismes de corps et préserve A, donc $\hat{A}_\mathfrak{p}$, et donc $\hat{K}_\mathfrak{p} \subset \hat{L}_\mathfrak{P}$.

PROPOSITION. – *L'homomorphisme $D_\mathfrak{P} \longrightarrow G_{\hat{L}_\mathfrak{P}/\hat{K}_\mathfrak{p}}$ ainsi obtenu est bijectif.*

Démonstration. Puisque $K \subset \hat{K}_\mathfrak{p}$ et $L \subset \hat{L}_\mathfrak{P}$ on a aussi, par restriction, un morphisme $G_{\hat{L}_\mathfrak{P}/\hat{K}_\mathfrak{p}} \xrightarrow{res} G_{L/K}$. Il est clair que la composée de *res* avec le morphisme de l'énoncé est l'identité de $D_\mathfrak{P}$. Ceci prouve l'injectivité du morphisme de l'énoncé. Comme $|D_\mathfrak{P}| = ef = [\hat{L}_\mathfrak{P} : \hat{K}_\mathfrak{g}]$, on en déduit la surjectivité. On constate aussi que *res* est l'isomorphisme inverse. □

4.3 Lemme de Hensel

4.3.1 Théorème. (Lemme de Hensel)– *Soit A un A.V.D complet de corps résiduel k, et soit $f \in A[X]$ unitaire d'image $\overline{f} \in k[X]$. Supposons qu'on ait une factorisation $\overline{f} = g_0 h_0$ dans $k[X]$ avec $(g_0, h_0) = 1$. Alors il existe une unique paire $(g, h) \in A[X]^2$ telle que $f = gh$, $\overline{g} = g_0$, $\overline{h} = h_0$ et $\deg(g) = \deg(g_0)$, $\deg(h) = \deg(h_0)$.*

Exemple d'application : Considérons $A = \mathbb{Z}_p$ et $f(X) = X^{p-1} - 1$. Le polynôme résiduel $\overline{f}$ est scindé (et séparable) dans $\mathbb{F}_p[X]$. Le lemme de Hensel implique donc que f est aussi scindé, *i.e.* que $\mathbb{Q}_p$ contient les racines $p-1$-èmes de l'unité.

Remarque. – On prendra garde au fait que l'hypothèse $(g_0, h_0) = 1$ est cruciale pour pouvoir relever la factorisation. Par exemple dans $\mathbb{Z}_p[X]$, le polynôme $f(X) = X^n - p$ est irréductible (critère d'Eisenstein), bien que sa réduction $\overline{f}(X) = X^n$ soit réductible.

4.3.2 *Preuve algébrique.* La preuve usuelle consiste à construire par récurrence des paires $(g_n, h_n) \in A[X]$ de polynômes de degré $\deg(g_0)$ et $\deg(h_0)$ respectivement, et telles que

- $f - g_n h_n \in \varpi^n A[X]$,
- $g_n - g_{n-1} \in \varpi^n A[X]$ et $h_n - h_{n-1} \in \varpi^n A[X]$.

On en déduit l'existence de g et h par passage à la limite puisque A est complet. Voir par exemple les notes de Milne pour les détails, ou faire l'exercice.

Voici une approche légèrement différente. Soit, plus généralement, A un anneau local noetherien d'idéal maximal $\mathfrak{m}$, et B une A-algèbre B de type fini comme A-module. La projection $B \twoheadrightarrow B/\mathfrak{m}$ induit une application

$$\{\text{idempotents de } B\} \longrightarrow \{\text{idempotents de } B/\mathfrak{m}B\}.$$

On dit que A est *Henselien* si pour toute A-algèbre finie B, l'application ci-dessus est *surjective*. On vérifie facilement (exercice) qu'elle est alors *bijective*. [Si $\varepsilon \equiv \varepsilon'[\mathfrak{m}]$, alors le lemme de Nakayama montre que $\varepsilon(1-\varepsilon') = 0 = \varepsilon'(1-\varepsilon)$]

Proposition. – *Dans un anneau local Henselien normal, le lemme de Hensel est vrai.*

Démonstration. Soient f, g_0, h_0 comme dans l'énoncé du lemme de Hensel ci-dessus. Posons $B := A[X]/(f)$. On a donc $B/\mathfrak{m}B = k[X]/(g_0) \times k[X]/(h_0)$ (lemme Chinois) d'où un idempotent ε tel que $\varepsilon(B/\mathfrak{m}B) = k[X]/(g_0)$ et $(1-\varepsilon)(B/\mathfrak{m}) = k[X]/(h_0)$. Concrètement, si $u, v \in k[X]$ sont tels que $uh_0 + vg_0 = 1$, alors ε est l'image de uh_0 dans $B/\mathfrak{m}B = k[X]/(\overline{f})$. Inversement, on a $h_0 = \text{p.g.c.d}(\overline{f}, \overline{f}_\varepsilon)$ où $\overline{f}_\varepsilon \in k[X]$ représente $\varepsilon \in k[X]/(f)$.

Puisque A est Henselien, on peut relever ε en un idempotent $\tilde{\varepsilon}$ de B. Soit $f_{\tilde{\varepsilon}} \in A[X]$ représentant ε dans B. Posons $h := \text{p.g.c.d}(f, f_{\tilde{\varepsilon}})$ et $g := \text{p.g.c.d}(f, 1 - f_{\tilde{\varepsilon}})$ (les pgcd étant pris dans l'anneau principal $K[X]$, où $K = \text{Frac}(A)$, et moniques). Il est clair que $(g, h) = 1$ et que $gh | f$, et on a finalement $gh = f$ grâce à $f_{\tilde{\varepsilon}}(1 - f_{\tilde{\varepsilon}}) \in (f)$. Comme A est normal, g et h sont dans $A[X]$, et par construction $\overline{g} | g_0$ et $\overline{h} | h_0$. Mais puisque $\overline{g}\overline{h} = \overline{f}$, on a bien $\overline{g} = g_0$ et $\overline{h} = h_0$.

L'unicité de la paire (g, h) découle de l'unicité du relèvement $\tilde{\varepsilon}$. □

THÉORÈME. – *Un anneau local noethérien complet est Hensélien.*

Ici "complet" signifie "séparé et complet pour la topologie $\mathfrak{m}$-adique" engendrée par les $x + \mathfrak{m}^i$ où $x \in A$ et $i \in \mathbb{N}$.

Démonstration. Ecrivons $1 = (X + (1-X))^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} X^{2n-k}(1-X)^k$, et posons

$$f_n(X) := \sum_{k=0}^{n} \binom{2n}{k} X^{2n-k}(1-X)^k.$$

On vérifie alors par le calcul les propriétés suivantes :

i) $f_n(X) \equiv f_n(X)^2 \quad [X^n(1-X)^n]$,

ii) $f_n(X) \equiv f_{n-1}(X) \quad [X^{n-1}(1-X)^{n-1}]$,

iii) $f_1(X) \equiv X \quad [X(1-X)]$.

Soit maintenant $(A, \mathfrak{m})$ local complet, B finie sur A et ε un idempotent dans $B/\mathfrak{m}B$. Le point crucial est que B est *complet* (et séparé) pour la topologie $\mathfrak{m}$-adique (engendrée par les $x + \mathfrak{m}^i B$ où $x \in B$ et $i \in \mathbb{N}$), car il est fini sur A qui est noethérien complet.

Choisissons donc $b \in B$ tel que $\overline{b} = \varepsilon$, et considérons la suite $(f_n(b))_{n\in\mathbb{N}}$. Puisque $b(1-b) \in \mathfrak{m}B$, le point ii) nous dit que c'est une suite de Cauchy pour la topologie $\mathfrak{m}$-adique. Elle a donc une limite $\tilde{\varepsilon}$ dans B. Le point i) nous dit par passage à la limite que $\tilde{\varepsilon}^2 = \tilde{\varepsilon}$, et le point iii) que $\overline{\tilde{\varepsilon}} = \overline{b} = \varepsilon$. □

Remarque. – L'intérêt de cette approche par les idempotents est que la preuve ci-dessus fonctionne également lorsque B est non-commutative. Par exemple, elle permet de montrer que pour un groupe fini G, les idempotents de $\mathbb{F}_l[G]$ se relèvent à $\mathbb{Z}_l[G]$.

4.3.3 *Méthode de Newton.* Soit $(K, |.|)$ un corps valué complet non archimédien d'anneau $\mathcal{O}$. Fixons un polynôme $f \in \mathcal{O}[X]$ unitaire. Lorsque la valeur absolue est discrète, le lemme de Hensel montre qu'une racine isolée de $\overline{f}$ se relève en une racine de f. La méthode de Newton permet de donner une construction précise et algorithmique d'une telle racine, et qui ne nécessite pas que la valeur absolue soit discrète.

THÉORÈME. – *Avec les notations ci-dessus, soit $x_0 \in \mathcal{O}$ tel que $|f(x_0)| < |f'(x_0)|^2$. Alors il existe un unique $x \in \mathcal{O}$ tel que $f(x) = 0$ et $|x - x_0| \leqslant \frac{|f(x_0)|}{|f'(x_0)|}$.*

La preuve est similaire au cas usuel sur $\mathbb{R}$. Pour l'existence, en posant $\delta := \frac{|f(x_0)|}{|f'(x_0)|^2} < 1$, on montre que la suite récurrente $x_n := x_{n-1} - \frac{f(x_{n-1})}{f'(x_{n-1})}$ vérifie pour tout n :

i) $|f(x_n)| \leqslant \delta |f(x_{n-1})|$.

ii) $|f'(x_n)| = |f'(x_{n-1})|$ (et donc la suite est bien définie),

c'est donc une suite de Cauchy et sa limite x a les propriétés voulues.

5 Géométrie des nombres

5.1 Réseaux euclidiens et théorème de Minkowski

5.1.1 Définition.– *Un* réseau euclidien *est la donnée*
– *d'un groupe abélien libre de rang fini L et*
– *d'un produit scalaire euclidien $\langle .,. \rangle$ sur $V = \mathbb{R} \otimes_{\mathbb{Z}} L$.*

Soit n le rang de L. Le quotient $V/L \simeq (\mathbb{R}/\mathbb{Z})^n$ est compact : on dit que L est cocompact.

Exercice. – Soit $(V, \langle .,. \rangle)$ un espace euclidien de dimension finie, et L un sous-groupe de V. Alors on a équivalence entre :

i) L est un réseau (euclidien) dans V,

ii) L est discret et cocompact dans V,

iii) L contient une base de V et pour tout ensemble borné B, $B \cap L$ est fini.

Si $(e_1, \cdots, e_n)$ est une base orthonormée de V, donnant donc un isomorphisme $\mathbb{R}^n \xrightarrow{\sim} V$, on munit V de la mesure de Lebesgue de $\mathbb{R}^n$. Cette mesure ne dépend pas du choix de la base orthonormée (le Jacobien d'un changement de base orthogonal est 1).

Comme la projection $V \longrightarrow V/L$ est un homéomorphisme local, cela induit une mesure sur le quotient V/L, et puisque ce dernier est compact, son volume $\mathrm{vol}(V/L)$, appelé *covolume* de L et noté $\mathrm{covol}(L)$, est fini.

5.1.2 Lemme.– *Soit $v_1, \cdots, v_n$ une base de L, alors on a* $\mathrm{covol}(L)^2 = \det\left(\langle v_i, v_j \rangle\right)_{i,j}$.

Démonstration. Par définition de la mesure quotient, le covolume de L est égal au volume $\mathrm{vol}(D)$ d'un domaine fondamental D pour L dans V (ie un ensemble mesurable D tel que $V = \bigsqcup_{x \in L}(x + D)$). Le parallélépipède

$$D = \prod_{i=1}^{n} [0,1[v_i = \left\{ v = \sum_i \lambda_i v_i \in V,\ 0 \leqslant \lambda_i < 1 \right\}$$

est clairement un domaine fondamental, et son volume est donnée par

$$\mathrm{vol}(D) = |\det(P)| = \sqrt{\det({}^tPP)} \quad \text{où} \quad P = \left(\langle e_i, v_j \rangle\right)_{i,j}$$

est la matrice de passage des e_i aux v_j. Or, on a ${}^tPP = \left(\langle v_i, v_j \rangle\right)_{i,j}$. □

5.1.3 Théorème. (Minkowski)– *Soit $(L, \langle .,. \rangle)$ un réseau euclidien et $B \subset V = \mathbb{R} \otimes L$ un sous-ensemble borné,* convexe *et* symétrique *de V tel que l'une des deux conditions soit satisfaite :*

(a) $\mathrm{vol}(B) > 2^n \mathrm{covol}(L)$

(b) $\mathrm{vol}(B) \geqslant 2^n \mathrm{covol}(L)$ *et B fermé.*

Alors $(B \cap L) \setminus \{0\} \neq \emptyset$.

Démonstration. (a) Regardons la projection $\pi : V \twoheadrightarrow V/2L$ et remarquons que $2^n \mathrm{covol}(L) = \mathrm{covol}(2L)$. Ainsi l'hypothèse (a) implique que $\pi_{|B}$ n'est pas injective, d'où l'existence de $x \neq y \in B$ tels que $x - y \in 2L$. Mais alors $\frac{1}{2}(x-y)$ appartient à B (convexe et symétrique) et à L et est non nul.

(b) D'après (a), pour tout $m \in \mathbb{N}$ l'ensemble $L \cap (1 + \frac{1}{m})B \setminus \{0\}$ est non vide. Comme par ailleurs il est fini, et que la suite de ces ensembles est décroissante, leur intersection est non vide. Comme B est fermé, tout élément de cette intersection est dans B. □

5.2 Finitude du nombre de classes

Soit K un corps de nombres de degré n sur $\mathbb{Q}$. Fixons un ensemble Σ de représentants des classes de conjugaison de plongements de K dans $\mathbb{C}$, et notons $\Sigma = \Sigma_1 \sqcup \Sigma_2$ la partition en plongements réels et non réels. Rappelons la décomposition

$$K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \prod_{\sigma \in \Sigma} K_\sigma = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

où $r_1 = |\Sigma_1|$ est le nombre de plongements réels, et $r_2 = |\Sigma_2|$ le nombre de plongements complexes non réels modulo conjugaison. On munit $K_{\mathbb{R}}$ de l'involution $\mathbb{R}$-linéaire $x \mapsto \overline{x}$ qui sur chaque facteur $\mathbb{R}$ est l'identité et sur chaque facteur $\mathbb{C}$ est la conjugaison complexe. On peut alors définir le produit scalaire suivant pour $x = (x_\sigma)_{\sigma\in\Sigma}$ et $y = (y_\sigma)_{\sigma\in\Sigma}$:

$$\langle x, y\rangle := \mathrm{Tr}_{K_{\mathbb{R}}/\mathbb{R}}(x\overline{y}) = \sum_{\sigma\in\Sigma} \mathrm{Tr}_{K_\sigma/\mathbb{R}}(x_\sigma \overline{y}_\sigma).$$

On remarquera que $(x, y) \in \mathbb{C}^2 \mapsto \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(x\overline{y})$ est le double du produit scalaire usuel sur $\mathbb{C}$, ce qui permet d'écrire

$$(*) \qquad \forall x, y \in K \subset K_{\mathbb{R}}, \ \ \langle x, y\rangle = \sum_{\sigma : K \hookrightarrow \mathbb{C}} \sigma(x)\overline{\sigma(y)},$$

où la somme porte vraiment sur tous les plongements, et en particulier

$$(**) \qquad \forall x \in K \subset K_{\mathbb{R}}, \ \ ||x||^2 = \sum_{\sigma : K \hookrightarrow \mathbb{C}} |\sigma(x)|^2.$$

5.2.1 Proposition.– *En plus des notations ci-dessus, posons* $D_K := \mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) \in \mathbb{Z}$.

i) L'image de $\mathcal{O}_K$ *dans* $K_{\mathbb{R}}$ *est un réseau euclidien de covolume* $\sqrt{|D_K|}$.

ii) L'image d'un idéal fractionnaire I *de* $\mathcal{O}_K$ *dans* $K_{\mathbb{R}}$ *est un réseau euclidien de covolume*

$$\mathrm{covol}(I) = (\mathcal{O}_K : I)\sqrt{|D_K|}.$$

Démonstration. i) $\mathcal{O}_K$ contient une $\mathbb{Q}$-base de K, donc une $\mathbb{R}$-base de $K_{\mathbb{R}}$. Soit $B_r := \{x \in K_{\mathbb{R}}, \ ||x|| \leqslant r\}$ pour $r > 0$. Par un exercice vu plus haut, il nous suffit de prouver que $B_r \cap \mathcal{O}_K$ est fini. D'après $(**)$ ci-dessus,

$$x \in \mathcal{O}_K \cap B_r \Rightarrow |\sigma(x)| \leqslant r, \forall \sigma : K \hookrightarrow \mathbb{C}.$$

Pour un tel x, le polynôme caractéristique

$$\chi_{K/\mathbb{Q},x}(T) = \prod_{\sigma:K\hookrightarrow\mathbb{C}} (T - \sigma(x))$$

est de degré $[K : \mathbb{Q}]$ et à coefficients entiers et bornés en fonction de r. Il n'y a qu'un nombre fini de tels polynômes, donc un nombre fini de tels x.

Soit maintenant $\omega_1, \cdots, \omega_n$ une base de $\mathcal{O}_K$ sur $\mathbb{Z}$. On a $\mathrm{covol}(\mathcal{O}_K)^2 = \det\left(\langle\omega_i, \omega_j\rangle\right)_{i,j}$. Introduisons la matrice $M := (\sigma_i(\omega_j))_{i,j}$ où $\sigma_1, \cdots, \sigma_n$ sont les plongements de K dans $\mathbb{C}$. D'après $(*)$ ci-dessus, $\langle\omega_i, \omega_j\rangle = \sum_k \sigma_k(\omega_i)\overline{\sigma_k(\omega_j)}$, donc

$$\mathrm{covol}(\mathcal{O}_K)^2 = \det({}^tM\overline{M}) = |\det(M)|^2.$$

Par ailleurs on a vu que

$$\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) = D_{\mathcal{O}_K/\mathbb{Z}}(\omega_1, \cdots, \omega_n) = \det({}^tMM) = \det(M)^2.$$

On en déduit la formule du covolume $\mathrm{covol}(\mathcal{O}_K) = \sqrt{|D_K|}$.

ii) Si $I \subset \mathcal{O}_K$, ii) découle de i) puisque I est d'indice fini $(\mathcal{O}_K : I)$ dans $\mathcal{O}_K$. □

Lemme. – *Si $m \in \mathbb{N}$, l'ensemble des idéaux I d'indice $\leqslant m$ dans $\mathcal{O}_K$ est fini.*

Démonstration. Si $(\mathcal{O} : I) \leqslant m$ alors $m!$ annule le groupe fini $\mathcal{O}_K/I$, donc $I \supset m!\mathcal{O}_K$. Or, $\mathcal{O}_K/m!\mathcal{O}_K$ est fini. □

5.2.2 Théorème.– *Pour tout idéal fractionnaire J de $\mathcal{O}_K$ il existe un idéal $I \subset \mathcal{O}_K$ tel que IJ est principal et $(\mathcal{O}_K : I) \leqslant \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|D_K|}$.*

Avant de prouver le théorème, énonçons tout de suite le corollaire qui nous intéresse, et qui utilise aussi le lemme précédent.

Corollaire. – *Le groupe de classes $\mathcal{C}\ell(\mathcal{O}_K)$ est fini.*

Démonstration du théorème. Commençons par réinterpréter l'énoncé. L'idéal I cherché est de la forme $(\alpha)J^{-1}$ pour un $\alpha \in K^\times$ et comme $I \subset \mathcal{O}_K$, on doit avoir $\alpha \in J$. On a aussi

$$(\dagger) \qquad (\mathcal{O}_K : I) = (\mathcal{O}_K : \alpha\mathcal{O}_K)(\mathcal{O}_K : J)^{-1} = |N_{K/\mathbb{Q}}(\alpha)|_\infty . \mathrm{covol}(J)^{-1}.\sqrt{|D_K|}$$

On voit donc que le problème est de trouver $\alpha \in J$ *non nul* avec $|N_{K/\mathbb{Q}}(\alpha)|_\infty$ aussi petit que possible. Remarquons maintenant que

$$(\dagger\dagger) \qquad |N_{K/\mathbb{Q}}(\alpha)|_\infty = \prod_{\sigma\in\Sigma} |\sigma(\alpha)|^{[K_\sigma:\mathbb{R}]}.$$

Considérons alors, pour $c = (c_\sigma)_{\sigma\in\Sigma} \in (\mathbb{R}_+^\times)^\Sigma$ le produit de boules $B(c)$ suivant :

$$B(c) := \{x = (x_\sigma)_{\sigma\in\Sigma} \in K_\mathbb{R},\ |x_\sigma| \leqslant c_\sigma, \forall\sigma \in \Sigma\}.$$

Ainsi, $B(c)$ est fermé, symétrique, convexe et son volume est

$$\mathrm{vol}(B(c)) = \prod_{\sigma\in\Sigma_1}(2c_\sigma) \times \prod_{\sigma\in\Sigma_2}(2\pi c_\sigma^2) = 2^n\left(\frac{\pi}{2}\right)^{r_2}\prod_{\sigma\in\Sigma} c_\sigma^{[K_\sigma:\mathbb{R}]}$$

où $\Sigma = \Sigma_1 \sqcup \Sigma_2$ est la partition en plongements réels et non réels. Chosissons alors c tel que $N(c) := \prod_{\sigma\in\Sigma} c_\sigma^{[K_\sigma:\mathbb{R}]} = \left(\frac{2}{\pi}\right)^{r_2}\mathrm{covol}(J)$. D'après le théorème de Minkowski, il existe un élément α non nul dans $B(c)\cap J$. Pour un tel élément, (††) nous dit que $|N_{K/\mathbb{Q}}(\alpha)| \leqslant N(c)$ et (†) nous donne la majoration voulue sur $(\mathcal{O} : I)$. □

On peut, par la même méthode mais en utilisant l'inégalité arithmético-géométrique, améliorer la constante en facteur qui majore $(\mathcal{O} : I)$ dans le théorème. Le nombre suivant

$$M_K := \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}$$

est appelé *constante de Minkowski.*

5.2.3 Théorème.– *Pour tout idéal fractionnaire J de $\mathcal{O}_K$ il existe un idéal $I \subset \mathcal{O}_K$ tel que IJ est principal et $(\mathcal{O}_K : I) \leqslant M_K\sqrt{|D_K|}$.*

Démonstration. L'inégalité arithmético-géométrique et la formule (††) nous donnent

$$|N_{K/\mathbb{Q}}(\alpha)|_\infty = \prod_{\sigma\in\Sigma}|\sigma(\alpha)|^{[K_\sigma:\mathbb{R}]} \leqslant \left(\frac{1}{n}\sum_{\sigma\in\Sigma}[K_\sigma:\mathbb{R}]|\sigma(\alpha)|\right)^n.$$

Ceci invite à considérer, pour $r > 0$, l'ensemble borné, symétrique et fermé

$$B'(r) := \left\{x = (x_\sigma)_{\sigma\in\Sigma}, \sum_{\sigma\in\Sigma}[K_\sigma:\mathbb{R}]|x_\sigma| \leqslant r\right\}.$$

On peut montrer que son volume est : $\mathrm{vol}(B'(r)) = 2^{r_1}\pi^{r_2}\frac{r^n}{n!}$. Choisissons alors r tel que $\mathrm{vol}(B'(r)) = 2^n\mathrm{covol}(J)$, d'où l'existence de α non nul dans $B'(r)\cap J$. On a alors

$$|N_{K/\mathbb{Q}}(\alpha)|_\infty \leqslant \left(\frac{r}{n}\right)^n = M_K.\mathrm{covol}(J).$$

D'après l'égalité (†) de la preuve précédente, il s'ensuit que pour l'idéal $I := \alpha J^{-1}$, on a $(\mathcal{O}_K : I) \leqslant M_K\sqrt{|D_K|}$. □

Ce théorème a bien-sûr un rôle important pour estimer le nombre de classes d'un corps de nombre, voire pour calculer le groupe de classes dans des cas de petit discriminant. Mais voici auparavant une conséquence plus inattendue :

Corollaire. – *Pour tout corps de nombres K, il existe au moins un nombre premier qui se ramifie dans $\mathcal{O}_K$.*

Démonstration. Il faut voir que $D_K \neq \pm 1$. Le point de départ est que, comme il y a au moins 1 classe d'idéaux, le théorème précédent assure que $M_K\sqrt{|D_K|} \geqslant 1$. Ceci implique

$$\sqrt{|D_K|} \geqslant \left(\frac{\pi}{4}\right)^{r_2} \frac{n^n}{n!} \geqslant \frac{\pi^{n/2}}{2} > 1$$

où on a utilisé que $r_2 \leqslant n/2$ et $n^n \geqslant 2^{n-1}n!$, et enfin que $n > 1$. □

Passons maintenant aux applications plus naturelles.

Exemple. – Calculons le groupe de classes $\mathcal{C}\ell(\mathcal{O}_K)$ pour $K = \mathbb{Q}[\sqrt{-5}]$. On a $n = 2$, $r_2 = 1$ et $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) = -20$ donc $M_K < 3$. Donc toute classe d'idéaux contient un représentant I d'indice $\leqslant 2$ dans $\mathcal{O}_K$. Si $(\mathcal{O}_K : I) = 1$ alors $I = \mathcal{O}_K$.

Si $(\mathcal{O}_K : I) = 2$ alors $2 \in I$. On sait que 2 est ramifié dans $\mathcal{O}_K$ donc il existe $\mathfrak{p} \in \mathrm{Max}(\mathcal{O}_K)$ tel que $2\mathcal{O}_K = \mathfrak{p}^2$. On a alors $(\mathcal{O}_K : \mathfrak{p}^2) = 4$ donc $(\mathcal{O}_K : \mathfrak{p}) = 2$ et $I = \mathfrak{p}$.

Reste à savoir si $\mathfrak{p}$ est principal. Mais $\mathfrak{p} = (\alpha)$ implique $|N_{K/\mathbb{Q}}(\alpha)| = 2$. Ecrivant $\alpha = a + b\sqrt{-5}$, on a $|N_{K/\mathbb{Q}}(\alpha)| = a^2 + 5b^2$ qui ne peut pas être égal à 2. On a donc montré que $\mathcal{C}\ell(\mathcal{O}_K) = \mathbb{Z}/2\mathbb{Z}$.

Application. Expliquons comment montrer que l'équation diophantienne $y^2 + 5 = x^3$ n'a pas de solutions entières. Supposons qu'on ait une solution $(x, y) \in \mathbb{Z}^2$. Alors on a une factorisation d'idéaux de $\mathcal{O}_K$ $(y + \sqrt{-5})(y - \sqrt{-5}) = (x)^3$ qui montre, puisque $(y + \sqrt{-5})$ et $(y - \sqrt{-5})$ sont premiers entre eux [En effet, si $\mathfrak{q}$ premier divise les deux, il divise $(2\sqrt{-5})$. Mais il est clair que $(\sqrt{-5})$ ne divise pas $(y + \sqrt{-5})$ car $y \neq 0$, et si l'idéal $\mathfrak{p}$ (tel que $\mathfrak{p}^2 = (2)$) divisait $(y + \sqrt{-5})$, alors 2 diviserait x et nécessairement y serait impair. Or, ceci est impossible car en réduisant $y^2 + 5 = x^3$ modulo 4 on obtiendrait $1 + 5 = 0(\mathrm{mod}4)$.], qu'il existe un idéal $I \subset \mathcal{O}_K$ tel que $(y + \sqrt{-5}) = I^3$ et $(y - \sqrt{-5}) = \overline{I}^3$ (conjugué sous Galois). *Puisque* $\mathcal{C}\ell(\mathcal{O}_K) = \mathbb{Z}/2\mathbb{Z}$, $I^3 \sim 1 \Rightarrow I \sim 1$ donc I est principal, disons $I = (\alpha)$. On a alors $y + \sqrt{-5} = \pm\alpha^3$. Mais il est élémentaire de montrer qu'il n'existe pas de tel α.

5.3 Théorème des unités de Dirichlet

On s'intéresse ici à la structure du groupe des unités $\mathcal{O}_K^\times$ d'un anneau d'entiers de corps de nombres. Commençons par un critère de reconnaissance d'unités :

5.3.1 Proposition.– *Soit $\alpha \in \mathcal{O}_K$. On a $\alpha \in \mathcal{O}_K^\times$ si et seulement si $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

Démonstration. Si $\alpha \in \mathcal{O}_K^\times$, alors $N(\alpha)N(\alpha^{-1}) = 1$ donc $N(\alpha) \in \mathbb{Z}^\times = \{\pm 1\}$. Réciproquement, on a $N(\alpha) = \pm a_0$ dans l'expression $f_\alpha(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0$. Ainsi, si $N(\alpha) = \pm 1$, le polynôme $g(X) = X^m + a_0^{-1}a_1X^{m-1} + \cdots + a_0^{-1}a_{n-1}X + a_0^{-1}$ est dans $\mathbb{Z}[X]$ et annule α^{-1}, donc $\alpha \in \mathcal{O}_K^\times$. □

5.3.2 *Le sous-groupe de torsion.* Le sous-groupe $(\mathcal{O}_K^\times)_{tors}$ formé des éléments de torsion est l'ensemble $\mu(K)$ de toutes les racines de l'unité dans K.

Lemme. – *$\mu(K)$ est fini, donc cyclique.*

Démonstration. La finitude découle de l'irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$. En effet $\zeta_n \in \mu(K) \Rightarrow \varphi(n)|[K:\mathbb{Q}]$. La cyclicité est un résultat classique : tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique. □

Remarque. – Si K admet un plongement réel (*ie* $r_1 \neq 0$), alors $\mu(K) = \{\pm 1\}$.

Exemple. (Corps quadratiques) – Si $\zeta_n \in \mu(\mathbb{Q}[\sqrt{d}])$, alors $\varphi(n) \leqslant 2$, ce qui laisse comme possibilités $n = 2, 3, 4$, ou 6. Par ailleurs, on constate facilement que $\zeta_3 \in \mathbb{Q}[\sqrt{d}] \Leftrightarrow d = -3$ et $\zeta_4 \in \mathbb{Q}[\sqrt{d}] \Leftrightarrow d = -1$. On en conclut que

$$\mu(\mathbb{Q}[\sqrt{d}]) = \begin{cases} \mu_6 \text{ si } d = -3 \\ \mu_4 \text{ si } d = -1 \\ \mu_2 \text{ si } d \neq -1, -3 \end{cases}$$

Proposition. – *Soit $\alpha \in K$ tel que pour tout $\sigma : K \hookrightarrow \mathbb{C}$ on a $|\sigma(\alpha)| = 1$. Alors $\alpha \in \mu(K)$.*

Démonstration. Plus généralement on a le résultat suivant : soit $m, M > 0$. Alors l'ensemble suivant est fini :

$$E_{m,M} := \{\alpha \in \overline{\mathbb{Z}}, \deg(f_\alpha) \leqslant m \text{ et } |\sigma(\alpha)| \leqslant M, \ \ \forall \sigma : K \hookrightarrow \mathbb{C}\}.$$

Ceci est clair puisque les coefficients (entiers) de f_α sont alors bornés en fonction de M. Maintenant, il suffit de remarquer que si α est comme dans l'énoncé, alors $\{\alpha^n, n \in \mathbb{N}\} \subset E_{[K:\mathbb{Q}],1}$. □

5.3.3 *La partie libre.* Le *rang* du groupe abélien $\mathcal{O}_K^\times$ est par définition la dimension du $\mathbb{Q}$-espace vectoriel $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_K^\times$. Il n'est pas clair a priori qu'il soit fini. Notons que c'est aussi le rang du quotient $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)_{tors}$ qui est un groupe abélien sans torsion.

Soit Σ comme dans la section précédente. On définit une application

$$\begin{array}{rccc} \mathcal{L} : & K_{\mathbb{R}}^\times = \prod_{\sigma\in\Sigma} K_\sigma^\times & \to & \mathbb{R}^\Sigma \\ & (x_\sigma)_{\sigma\in\Sigma} & \mapsto & \left(\log(|x_\sigma|^{[K_\sigma:\mathbb{R}]})\right)_{\sigma\in\Sigma} \end{array}.$$

L'image $\mathcal{L}(\mathcal{O}_K^\times)$ de $\mathcal{O}_K^\times$ (plongé diagonalement dans $K_{\mathbb{R}}^\times$) est un sous-groupe additif de $\mathbb{R}^\Sigma$, et la formule du produit nous dit qu'elle est contenue dans l'hyperplan

$$H := \left\{ (a_\sigma)_{\sigma\in\Sigma} \in \mathbb{R}^\Sigma, \sum_{\sigma\in\Sigma} a_\sigma = 0 \right\}.$$

Théorème. (Dirichlet) – *Avec les notations ci-dessus,*

i) $\mathrm{Ker}(\mathcal{L}) \cap \mathcal{O}_K^\times = \mu(K) = (\mathcal{O}_K)_{tors}$,

ii) $\mathcal{L}(\mathcal{O}_K^\times)$ *est un réseau (ie discret cocompact) dans* H.

En particulier $\mathcal{O}_K^\times$ est de rang fini égal à $r_1 + r_2 - 1$

Démonstration. i) $\alpha \in \mathrm{Ker}(\mathcal{L}) \cap \mathcal{O}_K^\times \Leftrightarrow |\sigma(\alpha)| = 1, \forall \sigma$, donc la proposition précédente cela équivaut aussi à $\alpha \in \mu(K)$.

ii) (a) Montrons d'abord que $\mathcal{L}(\mathcal{O}_K^\times)$ est discret. Si B est un ensemble ouvert borné de H, alors $\mathcal{L}^{-1}(B)$ est ouvert borné dans $K_\mathbb{R}^\times$ et donc $\mathcal{L}^{-1}(B) \cap \mathcal{O}_K$ est fini puique $\mathcal{O}_K$ est discret dans $K_\mathbb{R}^\times$. Il s'ensuit que $B \cap \mathcal{L}(\mathcal{O}_K^\times)$ est fini. *A ce stade on sait que le rang de $\mathcal{O}_K^\times$ est fini.*

(b) Reste à montrer que $\mathcal{L}(\mathcal{O}_K^\times)$ est cocompact dans H. Ceci donnera le rang égal à $\dim(H) = r_1 + r_2 - 1$. Il suffit de montrer que $\mathcal{O}_K^\times$ est cocompact dans

$$\mathcal{H} := \mathcal{L}^{-1}(H) = \left\{ x = (x_\sigma)_{\sigma\in\Sigma} \in K_\mathbb{R}^\times, N(x) := \prod_{\sigma\in\Sigma} |x_\sigma|^{[K_\sigma:\mathbb{R}]} = 1 \right\},$$

au sens où il existe un compact C de $K_\mathbb{R}^\times$ tel que $\mathcal{H} = \mathcal{O}_K^\times(\mathcal{H} \cap C)$.

Comme dans la preuve du théorème 5.2.2, considérons, pour $c = (c_\sigma)_{\sigma\in\Sigma} \in (\mathbb{R}_+^\times)^\Sigma$ le produit de boules

$$B(c) := \{x = (x_\sigma)_{\sigma\in\Sigma} \in K_\mathbb{R},\ |x_\sigma| \leqslant c_\sigma, \forall \sigma \in \Sigma\},$$

et choisissons c tel que $\mathrm{vol}(B(c)) = 2^n \mathrm{covol}(\mathcal{O}_K)$. Cela fixe la valeur de $N(c) := \prod_\sigma c_\sigma^{[K_\sigma:\mathbb{R}]}$ (peu importe cette valeur).

Maintenant, pour $x \in \mathcal{H}$, le volume de $x^{-1}B(c)$ est $N(x^{-1})\,\mathrm{vol}(B(c)) = \mathrm{vol}(B(c)) = 2^n \mathrm{covol}(\mathcal{O}_K)$ donc le théorème de Minkowski nous fournit un $\alpha \in \mathcal{O}_K \cap x^{-1}B(c)$ non nul. On a alors

$$|N_{K/\mathbb{Q}}(\alpha)| \leqslant N(x^{-1})N(c) = N(c).$$

Puisque $\{I \subset \mathcal{O}_K, (\mathcal{O} : I) \leqslant N(c)\}$ est fini, il existe $\alpha_1, \cdots, \alpha_N$ tels que

$$\forall a \in \mathcal{O}_K,\ |N_{K/\mathbb{Q}}(a)| \leqslant N(c) \Rightarrow \exists j,\ \ (\alpha) = (\alpha_j).$$

Il existe donc un j tel que $(\alpha) = (\alpha_j)$, *i.e.* $\alpha \in \mathcal{O}_K^\times \alpha_j$, et on en déduit que $x \in \mathcal{O}_K^\times \alpha_j^{-1} B(c)$. Posons alors $C := \bigcup_{j=1,\cdots,N} \alpha_j^{-1} B(c)$, qui est visiblement compact. Nous venons de montrer que $\mathcal{H} = \mathcal{O}_K^\times.(\mathcal{H} \cap C)$. □

Le théorème implique que $\mathcal{O}_K^\times \simeq (\mathcal{O}_K^\times)_{tors} \times \mathbb{Z}^{r_1+r_2-1}$. Un problème en général difficile est de trouver un *système d'unités fondamentales*, c'est-à-dire une famille $(\varepsilon_1, \cdots, \varepsilon_{r_1+r_2-1})$ d'unités dont l'image dans $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)_{tors}$ en soit une $\mathbb{Z}$-base.

Exemple. – Dans le cas $\mathbb{Q}(\sqrt{d})$ avec $d > 0$, la partie libre est de rang 1. Les unités $\varepsilon = x + y\sqrt{d}$ (lorsque $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$) satisfont l'équation de Pell-Fermat $N(\varepsilon) = x^2 - dy^2 = \pm 1$ dont la résolution utilise la fraction continue de $\sqrt{d}$.

Exercices

Exercice. (On veut montrer la transitivité des normes) – Les données sont un endomorphisme u d'un module libre de rang fini M sur un anneau B lui-même libre de rang fini sur A. On veut alors prouver l'égalité dans A

$$\mathcal{E}(A, B, M, u) : \quad \det_A(u) = N_{B/A}(\det_B(u)).$$

i) Vérifier cette égalité lorsque $B = A \times A \times \cdots \times A$.

ii) Soit $f : A \longrightarrow A'$ un morphisme d'anneaux. Posons $B' := A' \otimes_A B$, $M' := A' \otimes_A M = B' \otimes_B M$ et $u' := \mathrm{id} \otimes u$. Montrer :

   (a) $\mathcal{E}(A, B, M, u) \Rightarrow \mathcal{E}(A', B', M', u')$,

   (b) si f est injectif alors $\mathcal{E}(A', B', M', u') \Rightarrow \mathcal{E}(A, B, M, u)$.

iii) Utiliser i) et ii)(b) pour montrer $\mathcal{E}(A, B, M, u)$ lorsque A est un corps et B une algèbre séparable sur A. En déduire alors le cas où B est un anneau intègre et de caractéristique nulle (c'est essentiellement tout ce dont on a besoin pour ce cours).

iv) On traite maintenant le cas où $B = A[X]/(f)$ avec $f \in A[X]$ monique.

   (a) Montrer que le cas particulier $A = \mathbb{Z}[\alpha_1, \cdots, \alpha_m][a_{ij}^{(0)}, \cdots a_{ij}^{(m-1)}]_{1 \leqslant i,j, \leqslant n}$ et $f = X^m + \alpha_1 X^{m-1} + \cdots + \alpha_m$ est justiciable du iii).

   (b) Par un argument de spécialisation utilisant ii)(a), en déduire le cas général de iv). On pourra, dans la situation de iv)(a) considérer $M = B^n$ et u donné par la matrice $(b_{ij})_{i,j}$ avec $b_{ij} = \sum_{k=0}^{m-1} a_{ij}^{(k)} \bar{X}^k$.

v) De iv), déduire $\mathcal{E}(A, B, M, u)$ lorsque B est un corps (on pourra considérer des extensions monogènes intermédiaires entre A et B). Puis en déduire le cas où B est intègre.