Théorie des nombres

François Charles

17 janvier 2020

Table des matières

Chapitre 1

Théorie générale des corps de nombres

1.1 Algèbres à division, algèbres simples centrales

Dans cette section, on va montrer les théorèmes de finitude du nombre de classe et du groupe des unités pour les ordres dans les algèbres à division sur $\mathbb{Q}$.

1.1.1 Généralités

Soit k un corps. Dans ce qui suit, une k-algèbre sera par définition associative et unitaire, mais pas nécessairement commutative. Si A est une k-algèbre, l'injection naturelle $k \to A, x \mapsto x.1$ permet de considérer k comme une sous-algèbre de A.

Définition 1.1.1. *Une k-algèbre est de dimension finie si elle est de dimension finie comme espace vectoriel sur k.*

Rappelons qu'une k-algèbre A est de type fini si A est engendré *comme k-algèbre* par un nombre fini d'éléments : on peut trouver $x_1, \ldots, x_n$ dans A tels que le morphisme de k-algèbres $k[X_1, \ldots, X_n] \to A, X_i \mapsto x_i$ est surjective.

L'algèbre de polynômes $k[X_1, \ldots, X_n]$ est de type fini sur k, mais n'est pas de dimension finie. C'est la géométrie algébrique qui s'occupe de l'étude des algèbres (commutatives) de type fini. Dans ce cours, on étudiera des algèbres de dimension finie sur $\mathbb{Q}$ et leurs ordres (en fait, on considérera surtout des corps de nombres et de leurs anneaux d'entiers). Géométriquement, cela signifie que nous étudierons la géométrie des *courbes arithmétiques*. La *géométrie arithmétique* est l'étude sous cet angle de schémas de type fini sur $\mathbb{Z}$ et forme une large généralisation de ce cours.

Exemple 1.1.1.1. *(i) Si n est un entier naturel, l'algèbre des matrices carrées de taille n $M_n(k)$ est une k-algèbre de dimension n^2.*

(ii) Soit P un élément non-nul de $k[X]$. Soit (P) l'idéal de $k[X]$ engendré par P. Alors $k[X]/(P)$ est une k-algèbre commutative de dimension finie. Quelle est sa dimension ?

Soit A une algèbre de dimension finie sur k. À un élément a de A, on peut associer l'endomorphisme du k-espace vectoriel A

$$L_a : A \to A, x \mapsto ax.$$

On a bien sûr $L_a L_b = L_{ab}$.

Définition 1.1.2. *La trace de a, notée $Tr_{A/k}(a)$, est la trace de L_a. La norme de a, notée $N_{A/k}(a)$, est le déterminant de L_a.*

On pourrait aussi définir une trace et une norme à droite – qui sont en général distinctes de leurs homologues à gauche. On verra plus bas que si tout élément de A est inversible (et plus généralement, si A est une algèbre simple centrale), ce problème ne se pose pas.

Voici les propriétés de base de la norme et de la trace, qui suivent des définitions.

Proposition 1.1.3. *Soit A une k-algèbre de dimension finie. Soient $a, b \in A$, et soit $\lambda \in k$.*

(i) $Tr_{A/k}(1) = \dim_k(A)$;

(ii) $Tr_{A/k}(\lambda a + b) = \lambda Tr_{A/k}(a) + Tr_{A/k}(b)$;

(iii) $N_{A/k}(\lambda) = \lambda^{\dim_k(A)}$;

(iv) $N_{A/k}(ab) = N_{A/k}(a)N_{A/k}(b)$.

Exemple 1.1.1.2. *Si $A = M_n(k)$, et si $M \in A$, on vérifie*

$$Tr_{A/k}(M) = nTr(M);$$

$$N_{A/k}(M) = (det(M))^n.$$

Plus généralement, si P est le polynôme caractéristique de la multiplication à gauche par M, et χ_M le polynôme caractéristique de M, alors

$$P = (\chi_M)^n.$$

Définition 1.1.4. *Soit A une k-algèbre, et soit a un élément de A. On dit que a est inversible à gauche (resp. à droite) s'il existe b dans A tel que $ba = 1$ (resp. $ab = 1$). On dit que a est inversible s'il est inversible à gauche et à droite.*

Si a est inversible à gauche et à droite, ses inverses à gauche et à droite coïncident – il s'agit de l'inverse de x, noté a^{-1}.

Proposition 1.1.5. *Soit A une k-algèbre de dimension finie, et soit a un élément de A. Les conditions suivantes sont équivalentes.*

(i) *a est inversible dans A ;*

(ii) *a est inversible à gauche ;*

(iii) *a est inversible à droite ;*

(iv) *$N_{A/k}(a) \in k^*$.*

Démonstration. Supposons a inversible à gauche, et soit b tel que $ba = 1$. Alors $L_b L_a = \mathrm{Id}_A$. En particulier, puisque A est de dimension finie sur k, L_a est inversible et $N_{A/k}(a) \in k^*$.

Supposons maintenant $N_{A/k}(a) = det(L_a) \in k^*$. Alors L_a est inversible, donc bijectif, et on peut trouver b tel que $L_a(b) = 1$, ce qui signifie que b est un inverse à droite de a.

Ce qui précède montre que si a est inversible à gauche, alors a est inversible à droite. Par symétrie, la réciproque est vraie. On a montré toutes les implications nécessaires à la preuve de la proposition. □

On va introduire deux classes importantes d'algèbres de dimension finie sur k. Commençons par un rappel sur les idéaux.

Définition 1.1.6. *Soit A un anneau (associatif, unitaire). Un idéal à gauche (resp. à droite) de A est un sous-groupe I de $(A, +)$ stable par multiplication à gauche (resp. à droite) par les éléments de A :*

$$\forall x \in A, i \in I, xi \in I.$$

Un idéal bilatère de A est un sous-groupe de $(A, +)$ qui est un idéal à gauche et à droite.

Exemple 1.1.1.3. *Si $f : A \to B$ est un morphisme de k-algèbres, alors le noyau de f est un idéal bilatère de A. Réciproquement, si I est un idéal bilatère de A, le quotient A/I – au sens des groupes abéliens – est naturellement muni d'une structure de k-algèbre, et I est le noyau du morphisme d'algèbres $A \to A/I$.*

Exemple 1.1.1.4. *Soit V un k-espace vectoriel, et soit A la k-algèbre des endomorphismes de V. Si W est un sous-espace de V, l'ensemble des $f \in A$ tel que $W \subset \mathrm{Ker}(f)$ (resp. $\mathrm{Im}(f) \subset W$) est un idéal à gauche (resp. à droite) de A.*

Définition 1.1.7. *Soit A une k-algèbre. Le centre de A, noté $Z(A)$, est l'ensemble*

$$Z(A) = \{a \in A, \forall b \in A, ab = ba\}.$$

Définition 1.1.8. *Soit A une k-algèbre.*

(i) On dit que A est simple si $A \neq 0$ et A n'a pas d'idéal bilatère autre que 0 et A ;

(ii) on dit que A est centrale si $Z(A) = k$;

(iii) on dit que A est une algèbre à division si $A \neq 0$ et si tout élément non-nul de A est inversible.

Si A est une algèbre à division, on vérifie que le centre Z de A est un corps. Par ailleurs, il est immédiat de vérifier que A est simple (comme k-algèbre ou Z-algèbre, c'est équivalent). Ainsi, une algèbre à division est une algèbre simple centrale sur son centre.

Remarque 1.1.9. *(i) Une k-algèbre à division qui est commutative est un corps qui est une extension de k.*

(ii) On parle aussi de corps non commutatif au lieu d'algèbre à division. En anglais, on dit aussi skew field (corps gauche).

On va donner des exemples dans la partie suivante, mais on commence d'abord par développer un peu la théorie.

Rappelons – ou signalons – d'abord que l'on peut faire un peu d'algèbre linéaire dans ce cadre. Si A est une k-algèbre, un A-module M (à gauche) est un groupe additif muni d'une action à gauche de A par endomorphismes : pour tout $a \in A$, on dispose de

$$M \to M, m \mapsto am$$

tels que $a(bm) = (ab)m$ pour tous a, b, m. De même, un A-module à droite N est un k-espace vectoriel N muni d'une action à droite de A par endomorphismes : pour tout $a \in A$, on dispose de

$$M \to M, m \mapsto ma$$

tels que $(ma)b = m(ab)$ pour tous a, b, m.

Exemple 1.1.1.5. *Si A est une k-algèbre, on note A^{opp} l'algèbre opposée de A, qui a même sous-espace vectoriel sous-jacent que A, mais où la multiplication est définie par*

$$a^{opp}b^{opp} = ba,$$

où a^{opp}, b^{opp} sont les éléments de A^{opp} correspondant à a, b.

Si M est un A-module à gauche, M est muni d'une structure naturelle de A^{opp}-module à droite via $ma^{opp} = am$.

Si A est une algèbre à division, la théorie de la dimension marche comme d'habitude. En particulier, si un A-module à gauche M est engendré par un nombre fini d'éléments, on peut trouver une base de M comme A-module, qui fournit un isomorphisme $A^n \to M$. On dit encore que n est la dimension de M comme A-module. Si

A est en outre de dimension finie sur k, et si M est un A-module, alors M est de dimension finie comme A-module si et seulement M est de dimension finie comme k-espace vectoriel, et

$$\dim_k(M) = \dim_A(M)\dim_k(A).$$

Dans la situation ci-dessus, on dispose encore de l'algèbre $\mathrm{End}_A(M)$ des endomorphismes A-linéaires de M. La description usuelle se généralise à notre situation en un isomorphisme

$$\mathrm{End}_A(M) \simeq M_n(A^{opp}),$$

où n est la dimension de M comme A-module, et A^{opp} étant l'algèbre opposée à A – l'algèbre des matrices carrées $M_n(A)$ étant définie comme d'habitude. On l'obtient en faisant agir $f \in M_n(A^{opp})$ par multiplication à droite par la transposée de f – considérer le cas où $M = A$ est important.

Proposition 1.1.10. *Soit A une k-algèbre de dimension finie n.*

(i) A est une algèbre à division si et seulement si $A \neq 0$ et $\forall a \in A, N_{A/k}(a) \neq 0$.

(ii) Supposons que A est une algèbre à division, et soit $a \in A$. Soit $K = k[a]$ le sous-corps de A engendré par a, et notons r sa dimension sur k. Alors r divise n et

$$Tr_{A/k}(a) = \frac{n}{r} Tr_{K/k}(a)$$

et

$$N_{A/k}(a) = N_{K/k}(a)^{n/r}.$$

En particulier, le second énoncé montre que la trace d'un élément dans une algèbre à division peut être définie indifféremment par la multiplication à droite ou à gauche, puisque c'est bien le cas dans le corps K.

Démonstration. Le premier énoncé est un cas particulier de la Proposition 1.1.5.

Prouvons le second énoncé, et soit $a \in A$. La multiplication à gauche par les éléments de K fait de A un K-espace vectoriel de dimension finie d. On a bien sûr $n = dr$, ce qui prouve la divisibilité attendue. Soit $e_1, \ldots, e_d$ une base de A sur K :

$$A = \bigoplus_{i=1}^{d} Ke_i.$$

La multiplication à gauche par a laisse invariants les sous-espaces Ke_i, qui sont isomorphes à K comme K-modules à gauche. Cela prouve les énoncés. □

Remarque 1.1.11. *Avec les notations précédentes, soit P le polynôme minimal de a. Alors*

$$P(X) = X^r - Tr_{K/k}(a)X^{r-1} + \ldots + (-1)^r N_{K/k}(a).$$

En effet, on a $K \simeq k[X]/(P)$ et la matrice de la multiplication par a dans la base $1, X, \ldots, X^{r-1}$ est la matrice compagnon de polynôme caractéristique P.

1.1.2 Le théorème de Wedderburn, premiers exemples

C'est un fait plus ou moins bien connu que si n est un entier positif, la k-algèbre $M_n(k)$ est simple centrale. On va généraliser ce résultat. On commence par quelques résultats préliminaires très utiles.

Proposition 1.1.12. *Soit D une k-algèbre à division, et soit n un entier positif. Alors la k-algèbre $M_n(D)$ est simple, de centre $Z(D)$.*

Démonstration. Pour montrer que $M_n(D)$ est simple, il suffit de montrer que si M est un élément non nul de $M_n(D)$, l'idéal bilatère $I = M_n(D)MM_n(D)$ engendré par M est égal à $M_n(D)$ tout entier.

Pour $1 \leq i, j \leq n$, soit E_{ij} la matrice élémentaire dont les coefficients vérifient

$$(E_{ij})_{kl} = \delta_{ij}^{kl}.$$

Les E_{ij} formant une base du D-module $M_n(D)$, il suffit de montrer que tous les E_{ij} sont dans I. Au vu de l'identité

$$E_{kl} = E_{ki}E_{ij}E_{jl},$$

il suffit de montrer qu'il existe i, j tels que E_{ij} appartient à I. Enfin, on a

$$E_{ii}ME_{jj} = M_{ij}E_{ij}.$$

Puisque M est non nulle, on peut trouver i, j tels que $M_{ij} \neq 0$, et

$$E_{ij} = M_{ij}^{-1}E_{ii}ME_{jj},$$

ce qui montre bien $I = M_n(D)$.

Soit M un élément du centre de $M_n(D)$. Alors, pour tous i, j, on a

$$E_{ij}M = ME_{ij},$$

ce qui implique, comme dans le cas commutatif, que M est de la forme $\lambda\mathrm{Id}$ avec $\lambda \in D$. Puisque M commute aux homothéties, λ doit appartenir au centre de D. □

Rappelons qu'un A-module (à gauche ou à droite) simple est un A-module non nul sans sous-module non trivial.

Lemme 1.1.13. *Soit A une algèbre. Soit* $\mathrm{End}(A)$ *l'algèbre des endomorphismes de A considéré comme A-module à gauche. Alors la multiplication à droite par les éléments de A induit un isomoprhisme*

$$\mathrm{End}(A) \simeq A^{opp}.$$

Démonstration. Soit f un endomorphisme de A vu comme A-module à gauche. Alors, pour $a \in A$, $f(a) = f(a.1_A) = af(1_A)$. Finalement, f est la multiplication à droite par $f(1_A)$, et $\mathrm{End}_A(A) = A^{opp}$. □

Lemme 1.1.14. *Soit A une k-algèbre de dimension finie, et soit M un A-module à gauche simple. On suppose que l'action de A sur M est fidèle. Alors il existe un entier n tel que A, vu comme A-module à gauche, est isomorphe à M^n. En particulier, M est isomorphe à un idéal à gauche de A.*

Démonstration. Puisque M est simple, il est engendré sur A par un élément (considérer sinon le A-module engendré par un élément non nul), donc est de dimension finie sur k. Comme A agit fidèlement sur M, on peut trouver $m_1, \ldots, m_n \in M$ tel que $\{a \in A | am_1 = \ldots = am_n = 0\} = 0$ – choisir par exemple une k-base de M. Choisissons n minimal, et notons, pour $0 \leq r \leq n$,

$$A_r = \{a \in A | am_1 = \ldots = am_r = 0\}.$$

C'est un idéal à gauche de A. On a par définition $0 = A_n \subset A_{n-1} \subset \ldots \subset A_0 = A$. La minimalité de n garantit que la suite des A_r est strictement décroissante. On dispose de flèches injectives

$$p_r : A_r/A_{r+1} \to M, [a] \mapsto am_{r+1}.$$

Puisque M est simple, les p_r sont surjectives, ce sont donc des isomorphismes. En particulier, $p_{n-1} : A_{n-1} \to M, a \mapsto am_n$ définit un isomorphisme de A-modules entre M et l'idéal à gauche A_{n-1} de A. Par récurrence, on montre que pour tout i entre 1 et n, le morphisme de A-modules à gauche

$$A_{n-i} \to M^i, a \mapsto (am_{n-i+1}, \ldots, am_n)$$

est un isomorphisme. En particulier, le morphisme de A-modules à gauche

$$A \to M^n, a \mapsto (am_1, \ldots, am_n)$$

est un isomorphisme. □

Proposition 1.1.15. *Soit A une k-algèbre de dimension finie, M un A-module à gauche simple, $D = \mathrm{End}_A(M)$. Alors D est une algèbre à division et la flèche naturelle*

$$A \to \mathrm{End}_D(M), a \mapsto (m \mapsto am)$$

est surjective.

Démonstration. Soit f un élément non nul de D. Le noyau de f est un sous-D-module de I, donc il est nul, ce qui prouve que f est inversible – au moins comme k-endomorphisme, mais l'inverse est automatiquement D-linéaire. Ainsi, D est une algèbre à division.

Soit $\phi : A \to \mathrm{End}_D(M)$ la flèche de l'énoncé. Notons que pour tout $f \in D = \mathrm{End}_A(M)$, et tous a, m dans A et D, on a

$$f(am) = af(m),$$

ce qui signifie bien que a est D-linéaire.

Le noyau de la flèche $\phi : A \to \mathrm{End}_D(M)$ est l'idéal I des $a \in A$ agissant trivialement sur M. Quitte à remplacer A par A/I, on peut supposer que ϕ est injective, autrement dit que A agit fidèlement sur M. En particulier, le lemme 1.1.14 montre que A est isomorphe à M^n comme A-module à gauche, où n est un entier positif.

Le lemme 1.1.13 montre l'égalité $\mathrm{End}_A(A) = A^{opp}$. Par ailleurs,

$$\mathrm{End}_A(A) = \mathrm{End}_A(M^n) = M_n(D).$$

On en tire $A \simeq M_n(D^{opp})$, ce qui montre que A est simple grâce à la proposition précédente.

Identifions M à un idéal I de A comme ci-dessus. Comme A est simple, I est bilatère et $IA = A$.

On remarque la chose suivante : soit $i \in I$. Alors $I \to I, x \mapsto xi$ est un endomorphisme A-linéaire de I, et appartient donc à D. En particulier, si f est un endomorphisme D-linéaire de I, on a, pour tout $x \in I, f(xi) = f(x)i$. Finalement,

$$\forall x \in I, f\phi(x) = \phi(f(x)).$$

Puisque A est simple, on a $IA = A$. Écrivons donc

$$1 = \sum_k i_k a_k.$$

Soit $f \in \mathrm{End}_D(I)$, et soit $x \in I$. On écrit

$$f(x) = \sum_k f(i_k a_k x) = (\sum_k f(i_k) a_k) x,$$

ce qui montre que f est dans l'image de I. □

Voici le théorème de Wedderburn.

Théorème 1.1.16 (Wedderburn)**.** *Soit A une algèbre simple de dimension finie sur un corps k. On peut trouver un entier positif n, et une algèbre à division de dimension finie D, telle que A est isomorphe à $M_n(D)$. Le centre de A est $Z(D)$. Réciproquement, si D est une algèbre à division sur k, $M_n(D)$ est simple.*

Démonstration. Montrons le premier énoncé du théorème. Soit A une algèbre simple centrale de dimension finie sur k. Soit I un idéal à gauche non nul de A, minimal pour l'inclusion – il suffit de prendre I non nul de dimension minimale. Le A-module à gauche I est simple par définition : il n'admet pas de sous-module non nul. Soit $D = End_A(I)$. La proposition 1.1.15 montre que D est une algèbre à division et que le morphisme naturel de k-algèbres

$$\phi : A \to \mathrm{End}_D(I)$$

est surjectif. Le noyau de ϕ est un idéal bilatère de A. Comme A est simple et $\phi \neq 0$, ϕ est injective. Il s'agit donc d'un isomorphisme.

Les rappels d'algèbre linéaire sur les algèbres à division donnés plus haut montre que le D-module I est de la forme D^n pour un certain n, ce qui montre que $\mathrm{End}_D(I)$ s'identifie à l'algèbre de matrices $M_n(D^{opp})$.

Le second énoncé est la proposition 1.1.12. □

Corollaire 1.1.17. *Si k est algébriquement clos, alors toute algèbre simple centrale de dimension finie sur k est isomorphe à $M_n(k)$ pour un certain n.*

Démonstration. Il suffit de montrer qu'il n'existe pas d'algèbre à division de dimension finie sur k autre que k lui-même. Soit D une telle algèbre à division contenant strictement k, et soit $a \in D \setminus k$. Alors $k[a]$ est une extension finie de k contenant strictement k, ce qui contredit le fait que k est algébriquement clos. □

Corollaire 1.1.18. *Le centre d'une k-algèbre simple de dimension finie est un corps.*

Démonstration. Le théorème de Wedderburn nous permet de ne considérer que le cas d'une algèbre à division, que nous avons déjà traité. □

On termine cette section par des compléments sur $M_n(D)$.

Proposition 1.1.19. *Soit D une algèbre à division sur k, et soit n un entier positif. Soit I_k l'idéal à gauche de $A = M_n(D)$ constitué des matrices dont toutes les colonnes sauf la k-ième sont nulles. Alors les I_k sont des A-modules à gauche simples, deux à deux isomorphes, et tout A-module simple est isomorphe à I_1.*

Démonstration. Montrons d'abord que I_1 est simple. Cela revient à montrer que I_1 est minimal pour l'inclusion parmi les idéaux à gauche non nuls de A. Soit I un idéal à gauche de A, non nul, inclus dans I_1. Il faut montrer que $I = I_1$, c'est-à-dire que les matrices élémentaires E_{i1} sont toutes dans i. Écrivant

$$E_{j1} = E_{ji}E_{i1},$$

on voit comme plus haut qu'il suffit de montrer qu'il existe un i tel que E_{i1} est dans I_1. Par ailleurs, si M est dans I_1, on a toujours

$$E_{i1}M = M_{i1}E_{i1},$$

donc choisissant i tel que $M_{i1} \neq 0$, on a

$$E_{i1} = M_{i1}^{-1}E_{i1}M \in I_1,$$

ce qui conclut la preuve de la simplicité de I_1.

On a bien sûr

$$I_k = I_1E_{1k},$$

ce qui montre que I_k est isomorphe à I_1 comme A-module à gauche. En particulier, I_k est simple.

Soit maintenant M un A-module simple. Soit $m \in M \setminus \{0\}$. La flèche

$$A \to M, a \mapsto am$$

est non nulle, donc surjective car M est simple. Comme A-module à gauche, on a bien sûr par ailleurs

$$A = \bigoplus_{k=1}^{n} I_k,$$

d'où une surjection de A-modules

$$\bigoplus_{k=1}^{n} I_k \to M.$$

Une des flèches $I_k \to M$ est non nulle. C'est donc un isomorphisme car I_k et M sont simples. □

Le théorème de Wedderburn nous permet de déduire le corollaire suivant.

Corollaire 1.1.20. *Soit A une algèbre simple de dimension finie sur k. Alors il existe, à isomorphisme près, un unique A-module à gauche simple.*

Démonstration. Si A est centrale, c'est une conséquence de la proposition précédente. Mais si K est le centre de A, A est une K-algèbre simple centrale, ce qui prouve le résultat. □

Corollaire 1.1.21. *Soient D et D' deux algèbres à division de dimension finie sur k, et soit n, n' deux entiers positifs. Alors les k-algèbres $M_n(D)$ et $M_{n'}(D')$ sont isomorphes si et seulement si $n = n'$ et $D \simeq D'$.*

Démonstration. Soit $A = M_n(D)$, et soit M l'unique A-module simple de A, à isomorphisme près. La preuve du théorème de Wedderburn montre que D^{opp} s'identifie à $\mathrm{End}_A(M)$, ce qui montre que D est déterminé par A. Pour des raisons de dimension, n aussi est déterminé par A. □

1.1.3 Produits tensoriels et groupe de Brauer d'un corps

Pour exploiter le théorème de Wedderburn, il est pratique – via le corollaire ci-dessus – de pouvoir changer le corps de base. C'est ce que l'on appelle l'extension des scalaires. Expliquons de quoi il s'agit.

Soit A une k-algèbre de dimension finie (ce n'est pas nécessaire mais supposons-le pour fixer les idées), et soit K une extension de k. Le K-espace vectoriel $B = A \otimes_k K$ est muni d'une structure de K-algèbre naturelle via

$$(a \otimes x)(b \otimes y) = ab \otimes xy.$$

Via $a \mapsto a \otimes 1$, on peut voir A comme une sous-k-algèbre de B. On dit que B est obtenue par extension des scalaires de k à K.

On peut rendre explicite cette construction : soit $e_1, \ldots, e_n$ une base de A sur k. La multiplication sur A est donnée par la table

$$e_i e_j = \sum_k \omega_{ij}^k e_k.$$

On dit que les ω_{ij}^k sont les *constantes de structure* de A, elles déterminent la structure d'algèbre de A par bilinéarité. L'associativité de A se traduit par des relations explicites sur les ω_{ij}^k. Avec cette donnée, $A \otimes_k K$ est la K-algèbre déterminée elle aussi par la base e_i et les constantes de structure ω_{ij}^k.

Par construction, la norme et la trace sont invariantes par extension des scalaires.

Exemple 1.1.3.1. *(i) Soit L une extension finie séparable de k. Le théorème de l'élément primitif permet d'écrire $L = k[a]$ pour un certain $a \in L$. Si P est le polynôme minimal de a, on a un isomorphisme d'algèbres $L \simeq k[X]/(P)$, et $L \otimes_k K \simeq K[X]/(P)$. Notons*

$$P = \Pi_i P_i$$

la décomposition de P en facteurs irréductibles sur K. Le lemme chinois montre que l'on a

$$L \otimes_k K \simeq \Pi_i K[X]/(P_i).$$

(ii) Soit L une extension galoisienne de k de groupe G. On a un isomorphisme

$$L \otimes_k L \simeq L^G, x \otimes y \mapsto (\sigma(x)y)_{\sigma \in G}.$$

(iii) On a $M_n(k) \otimes_k K \simeq M_n(K)$.

(iv) Plus généralement, on a $M_n(D) \otimes_k K \simeq M_n(D \otimes_k K)$.

On peut considérer plus généralement le produit tensoriel $A \otimes_k B$, où A et B sont deux k-algèbres. Il est encore muni d'une structure de k-algèbre naturelle définie de manière unique par la propriété

$$(a \otimes b)(a' \otimes b') = (aa') \otimes (bb')$$

et la distributivité.

L'algèbre $A \otimes_k B$ contient les sous-algèbres $A \simeq A \otimes_k 1_B$ et $B \simeq 1_A \otimes_k B$ – au moins dès que A et B sont toutes deux non-nulles. Remarquons que A et B commutent :

$$(a \otimes 1)(1 \otimes b) = a \otimes b = (1 \otimes b)(a \otimes 1).$$

Nous laissons au lecteur le soin de montrer la propriété universelle suivante : si C est une k-algèbre contenant A et B comme sous-algèbres qui commutent, alors il existe un unique morphisme

$$A \otimes_k B \to C$$

préservant A et B.

Les k-algèbres $A \otimes_k B$ et $B \otimes_k A$ sont isomorphes – la propriété universelle ci-dessus rend par exemple évidente la symétrie entre A et B, et l'on a aussi $A \otimes_k (B \otimes_k C) \simeq (A \otimes_k B) \otimes_k C$, de manière canonique. On peut expliciter là encore et écrire des constantes de structure de $A \otimes_k B$ en fonction de constantes de structure de A et de B.

Exemple 1.1.3.2. *On a $M_n(A) \otimes_k B \simeq M_n(A \otimes_k B)$. On a $M_n(k) \otimes_k M_m(k) \simeq M_{mn}(k)$.*

Voyons comment démontrer le premier isomorphisme ci-dessus. La propriété d'associativité du produit tensoriel nous ramène à montrer l'isomorphisme $M_n(k) \otimes_k B \simeq M_n(B)$. Une base du k-espace vectoriel $M_n(k)$ est donnée par les matrices E_{ij} avec $1 \leq i, j \leq n$. La mutliplication est donnée par les formules usuelles. Par conséquent, le B-module (à droite) $M_n(k) \otimes_k B$ est libre de base les $E_{ij} \otimes 1_B$. La loi de multiplication est donnée par la formule

$$(E_{ij} \otimes 1_B)(E_{kl} \otimes 1_B) = \delta_k^j E_{il} \otimes 1_B.$$

L'algèbre $M_n(B)$ est munie d'une base comme B-module qui satisfait les mêmes identités, d'où l'isomorphisme annoncé.

Le centre du produit tensoriel est facile à calculer.

Proposition 1.1.22. *Soient A et B deux k-algèbres. On a*

$$Z(A \otimes_k B) = Z(A) \otimes_k Z(B).$$

Démonstration. On a bien sûr une inclusion

$$Z(A) \otimes_k Z(B) \subset Z(A \otimes_k B).$$

Soit $(e_i)_{i \in I}$ une base de A comme k-espace vectoriel. Alors $(e_i \otimes 1_B)_{i \in I}$ est une base de $A \otimes_k B$ comme B-module à droite. Les éléments de $A \otimes_k B$ s'écrivent donc de manière unique comme somme de $e_i \otimes b_i$.

Supposons qu'une somme finie $x = \sum_i e_i \otimes b_i$ soit dans le centre de $A \otimes_k B$. En particulier, x commute à tous les $1_A \otimes b$, $b \in B$, ce qui signifie

$$\sum_i e_i \otimes (bb_i) = \sum_i e_i \otimes (b_i b).$$

L'unicité des écritures ci-dessus garantit que l'on a $bb_{i=}b_i b$ pour tout $i \in I$, $b \in B$, ce qui signifie que les b_i sont tous dans le centre de B. Autrement dit, on a montré

$$Z(A \otimes_k B) \subset A \otimes_k Z(B).$$

Appliquant ce résultat en échangeant les facteurs, on trouve

$$Z(A \otimes_k B) \subset Z(A) \otimes_k Z(B),$$

ce qui conclut. □

On passe au comportement de la simplicité par produit tensoriel. Soit A une k-algèbre de dimension finie, A^{opp} son algèbre opposée. Notons $\mathrm{End}_k(A)$ la k-algèbre des automorphismes du k-espace vectoriel A.

On dispose de morphismes d'algèbres

$$A \to \mathrm{End}_k(A), a \mapsto (x \mapsto ax)$$

et

$$A^{opp} \to \mathrm{End}_k(A), b \mapsto (x \mapsto xb),$$

d'où un morphisme naturel de k-algèbres

$$\phi : A \otimes_k A^{opp} \to \mathrm{End}_k(A)$$

qui envoie $a \otimes b$ sur $x \mapsto axb$.

Les dimensions sur k de $A \otimes_k A^{opp}$ et $\mathrm{End}_k(A)$ sont égales, de sorte que ϕ est un isomorphisme si et seulement si ϕ est injectif ou surjectif.

Proposition 1.1.23. *Avec les notations précédentes, A est simple centrale si et seulement si ϕ est un isomorphisme.*

Démonstration. Supposons que A n'est pas simple, et soit I un idéal bilatère de A, distinct de 0 et A. Pour tout f dans l'image de ϕ, la propriété d'idéal bilatère signifie précisément que $f(I) \subset I$, de sorte que ϕ ne peut pas être surjective.

De même, supposons que A n'est pas centrale, et soit K le centre de A. Alors ϕ envoie A dans $\mathrm{End}_K(A)$, donc ϕ ne peut pas être surjective.

Supposons donc que A est simple centrale. Notons B la k-algèbre $A \otimes_k A^{opp}$. On note M le B-module de k-vectoriel sous-jacent A muni de l'action de B donnée par ϕ. Puisque A est simple, M est un B-module simple – c'est équivalent.

Calculons $\mathrm{End}_B(M)$. Soit $f : M \to M$ B-linéaire. Alors pour tout a, x, b dans A, on a $f(axb) = af(x)b$. En particulier, $f(x) = xf(1_A)$, et pour tout $x \in M$, $f(x) = f(1_A)x = xf(1_A)$. Cela montre que $f(1_A)$ appartient au centre de A, d'où l'égalité

$$\mathrm{End}_B(M) = k.$$

Le lemme 1.1.15 montre que la flèche naturelle $\phi : B \to \mathrm{End}_k(M)$ est surjective. Les dimensions de B et de $\mathrm{End}_k(M)$ sur k sont égales, ce qui prouve que ϕ est un isomorphisme. □

Voici des conséquences importantes de la proposition ci-dessus.

Corollaire 1.1.24. *Soit A une k-algèbre de dimension finie.*

(i) Soit K un corps contenant k. Alors A est simple centrale si et seulement si la K-algèbre $A \otimes_k K$ est simple centrale.

(ii) A est simple centrale si et seulement s'il existe une extension K de k telle que la K-algèbre $A \otimes_k K$ est isomorphe à une algèbre de matrices carrées. Il existe une telle extension qui est finie, et l'on peut prendre pour K n'importe quelle extension algébriquement close de k.

Remarque 1.1.25. *On pourrait montrer dans le deuxième énoncé que K peut être choisi séparable sur k.*

Remarque 1.1.26. *On dit que A est* déployée *par K si $A \otimes_k K$ est une algèbre de matrices.*

Démonstration. Prouvons (i). La proposition 1.1.22 garantit que A est centrale si et seulement si $A \otimes_k K$ l'est.

Supposons que A n'est pas simple, et soit I un idéal bilatère de A distinct de 0 et A. Alors $I \otimes_k K$ est un idéal bilatère de $A \otimes_k K$ distinct de 0 et A, par exemple pour des raisons de dimension, donc $A \otimes_k K$ n'est pas simple.

Finalement, supposons que A est simple centrale. Alors la flèche naturelle $A \otimes_k A^{opp} \to \mathrm{End}_k(A)$ est un isomorphisme donc, après tensorisation par K, la flèche naturelle

$$(A \otimes_k K) \otimes_K (A^{opp} \otimes_k K) \to \mathrm{End}_K(A \otimes_k K)$$

est un isomorphisme, ce qui prouve que $A \otimes_k K$ est simple centrale.

Prouvons (ii). D'après (i) et le corollaire 1.1.17, si L est algébriquement clos, $A \otimes_k L$ est isomorphe à une algèbre de matrices. D'après (i), il reste seulement à montrer que l'on peut trouver une extension finie K de k telle que $A \otimes_k K$ est isomorphe à une algèbre de matrices. Soit L une clôture algébrique de k. choisissons un isomorphisme

$$A \otimes_k L \to M_n(L).$$

Se donner un tel isomorphisme, c'est se donner, pour une base e_i de A sur k, des matrices à coefficients dans L, satisfaisant des identités qui traduisent la préservation des lois d'algèbre et le caractère injectif du morphisme. Ces identités sont indépendantes du corps de base, et les coefficients des matrices en question engendrent une extension finie K de k, qui satisfait bien la propriété désirée. □

Remarque 1.1.27. *Dans le second énoncé, on pourrait choisir K séparable sur k.*

Corollaire 1.1.28. *La dimension d'une k-algèbre simple centrale de dimension finie est un carré parfait.*

Démonstration. La dimension est invariante par extension des scalaires, il suffit donc de traiter le cas de $M_n(k)$, dont la dimension est n^2. □

Théorème 1.1.29. *Soit A une k-algèbre de dimension finie, et soit B une k-algèbre simple centrale. Soient $f, g : A \to B$ deux morphismes de k-algèbres. Alors il existe un élément inversible b de B tel que $f = b^{-1}gb$. En particulier, les automorphismes de B sont tous intérieurs.*

Démonstration. Supposons d'abord $B = M_n(k)$. L'action naturelle de B sur k^n induit, via f et g, deux actions de A sur k^n. □

Corollaire 1.1.30. *Soit A une algèbre simple centrale de dimension finie et de dimension n^2 sur un corps parfait k. Pour tout $a \in A$, il existe un unique polynôme unitaire P_a de degré n à coefficients dans k, tel que P_a^n est le polynôme caractéristique de la multiplication à gauche par a.*

Remarque 1.1.31. *Le résultat vaut même si k n'est pas supposé parfait.*

Avant de prouver le corollaire, on commence par un résultat de théorie des corps.

Lemme 1.1.32. *Soit K/k une extension de corps finie séparable. Soit P et Q deux polynômes unitaires dans $K[X]$ et $k[X]$ respectivement, tels que $Q = P^n$. Alors P appartient à $k[X]$.*

Démonstration. On peut supposer K/k galoisienne. On vérifie immédiatement qu'un polynôme unitaire $P \in K[X]$ tel que $P^n = Q$ est unique. En particulier, P est invariant sous le groupe de Galois de l'extension K/k, donc $P \in k[X]$ car K/k est séparable. □

Démonstration du corollaire 1.1.30. Vu le lemme ci-dessus et puisque k est parfait, l'énoncé est invariant par extension finie du corps de base. D'après le corollaire 1.1.24, on peut donc supposer que A est la k-algèbre $M_n(k)$, et le résultat suit de l'exemple 1.1.1.2. □

Définition 1.1.33. *Soit A une algèbre simple centrale de dimension finie sur un corps, et soit $a \in A$. Soit*

$$P = X^n - a_{n-1}X^{n-1} + \ldots + (-1)^n a_n$$

le polynôme fourni par le corollaire 1.1.30. La trace réduite de a, notée $Trd_{A/k}(a)$ est le coefficient a_{n-1} de P. La norme réduite de a, notée $Nrd_{A/k}(a)$, est le coefficient a_n.

La proposition qui vient suit des définitions et des propriétés de la norme.

Proposition 1.1.34. *Soit A une algèbre simple centrale de dimension finie n^2 sur un corps, et soit $a \in A$. Les normes et traces réduites sont invariantes par extension des scalaires. On a :*

(i) $Tr_{A/k}(a) = nTrd_{A/k}(a)$;

(ii) $N_{A/k}(a) = Nrd_{A/k}(a)^n$;

(iii) *a est inversible si et seulement si* $Nrd_{A/k}(a) \neq 0$.

Remarque 1.1.35. *En caractéristique positive, il est possible que la trace réduite d'un élément soit non-nulle alors que sa trace est nulle.*

On peut comprendre trace et norme réduite un peu mieux. Soit en effet A une k-algèbre simple centrale de dimension finie, et soit $e_1, \ldots, e_{n^2}$ une base de A comme k-espace vectoriel. Un élément a de A s'écrit de manière unique sous la forme

$$a = \sum_{i=1}^{n^2} x_i e_i$$

pour certains $x_i \in k$.

Proposition 1.1.36. *Dans la situation précédente, il existe des polynôme $T, N \in k[X_1, \ldots, X_{n^2}]$ tels que pour tous $x_1, \ldots, x_{n^2} \in k$,*

$$Trd_{A/k}(\sum_{i=1}^{n^2} x_i e_i) = T(x_1, \ldots, x_{n^2})$$

et

$$Nrd_{A/k}(\sum_{i=1}^{n^2} x_i e_i) = N(x_1, \ldots, x_{n^2}).$$

Le polynôme T est homogène de degré 1 et N est homogène de degré n.

Démonstration. Soit K le corps $k(X_1, \ldots, X_{n^2})$. L'extension des scalaires $A \otimes_k K$ est une K-algèbre simple centrale. Notons $g = \sum_{i=1}^{n^2} X_i e_i \in A \otimes_k K$. Le polynôme caractéristique de la multiplication à gauche par g est un élément de $K[T]$, unitaire. C'est en fait un élément χ de $k[X_1, \ldots, X_{n^2}, T]$. Par construction, χ a la propriété suivante : pour tous $a_1, \ldots, a_{n^2} \in k$, $\chi_T(a_1, \ldots, a_{n^2}, T)$ est le polynôme caractéristique de la multiplication à gauche par $\sum_{i=1}^{n^2} a_i e_i \in A$. Tout cela est par exemple une conséquence de l'expression explicite de χ en fonction des constantes de structure de A.

On applique le corollaire 1.1.30 à l'élément g de $A \otimes_k K$ pour trouver un unique $P \in K[T]$, unitaire, tel que $P^n = \chi$. Comme χ est un élément de $k[X_1, \ldots, X_{n^2}, T]$, il en va de même de P. D'après ce qui précède, si $a_1, \ldots, a_n$ sont des éléments de k, alors $P(a_1, \ldots, a_{n^2}, T)$ est un polynôme unitaire dont la puissance n-ième est égale au polynôme caractéristique de la multiplication à gauche par $\sum_{i=1}^{n^2} a_i e_i \in A$. C'est donc le polynôme P_a du corollaire 1.1.30. Prenant les coefficients en T, la proposition est démontrée – l'assertion sur les degrés d'homogénéité suivant des propriétés d'homogénéité du déterminant et de la trace usuels. □

Le résultat suivant, conséquence lui aussi de la proposition 1.1.23, permet la définition du groupe de Brauer.

Proposition 1.1.37. *Soient A et B deux k-algèbres simples de dimension finie. Si A est centrale, alors $A \otimes_k B$ est une k-algèbre simple de dimension finie. Si A et B sont centrales, alors $A \otimes_k B$ est une k-algèbre simple centrale de dimension finie.*

Démonstration. Supposons d'abord A et B simples centrales. On applique le corollaire 1.1.24 : soit K une extension algébriquement close de k. Alors $A \otimes_k K \simeq M_n(K)$ et $B \otimes_k K \simeq M_m(K)$ pour deux entiers positifs m et n. On a donc

$$(A \otimes_k B) \otimes_k K \simeq (A \otimes_k K) \otimes_K (B \otimes_k K) \simeq M_n(K) \otimes_K M_m(K) \simeq M_{mn}(K).$$

On conclut par la réciproque du corollaire 1.1.24.

Supposons maintenant A simple centrale, et B seulement simple. Soit K le centre de B – c'est un corps par le Corollaire 1.1.18. On a un isomorphisme d'algèbres

$$A \otimes_k B \simeq (A \otimes_k K) \otimes_K B.$$

Le membre de droite est une K-algèbre simple centrale, c'est donc une k-algèbre simple. □

Remarque 1.1.38. *On pourrait directement utiliser la proposition 1.1.23.*

Définition 1.1.39. *Soit k un corps. Le groupe de Brauer de k, noté $Br(k)$, est l'ensemble des classes d'équivalences des k-algèbres simples centrales de dimension finie pour la relation d'équivalence*

$$A \sim B \iff \exists m, n, A \otimes_k M_n(k) \simeq B \otimes_k M_m(k),$$

muni de la loi de groupe abélien $[A] + [B] = [A \otimes_k B]$.

Il faut bien entendu vérifier que la définition ci-dessus a un sens, et qu'elle définit bien un groupe abélien.

La relation $\sim$ est bien une relation d'équivalence : symétrie et réflexivité sont évidentes. Pour la transitivité, si

$$A \otimes_k M_p(k) \simeq B \otimes_k M_q(k)$$

et

$$B \otimes_k M_r(k) \simeq C \otimes_k M_s(k),$$

alors, par commutatitivité du produit tensoriel et l'identité $M_{mn}(k) \simeq M_m(k) \otimes_k M_n(k)$,

$$A \otimes_k M_{pr}(k) \simeq B \otimes_k M_{qr}(k) \simeq C \otimes_k M_{qs}(k).$$

Que la loi de composition soit bien définie suit de la proposition 1.1.37. Son associativité et sa commutativité suivent des propriétés analogues du produit tensoriel. La formule

$$A \otimes_k A^{opp} \simeq M_n(k),$$

montre que $[A^{opp}]$ est l'opposé de $[A]$ dans $Br(k)$.

Ce qui suit est une conséquence immédiate du théorème de Wedderburn et du corollaire 1.1.21.

Proposition 1.1.40. *Soit k un corps. Tout élément de $Br(k)$ est représenté par une unique algèbre à division.*

Notons par ailleurs la fonctorialité suivante du groupe de Brauer : si K est un corps contenant k, associer à une k-algèbre simple centrale A la K-algèbre simple centrale $A \otimes_k K$ induit un morphisme de groupes $Br(k) \to Br(K)$.

Le groupe de Brauer d'un corps est un invariant arithmétique profond. Avec un peu plus de géométrie algébrique, on peut comprendre sa définition de manière géométrique. Le groupe de Brauer paramètre des objets qui, après extension finie (séparable, donc étale), deviennent isomorphe à une algèbre de matrices. D'après le théorème de Skolem-Noether, le groupe des automorphismes de la k-algèbre $M_n(k)$ est $PGL_n(k)$, agissant par conjugaison. On peut exprimer le groupe de Brauer directement à partir des groupes $PGL_n(k)$ et, comme ce sont les groupes d'automorphismes des espaces projectifs, montrer que le groupe de Brauer paramètre les fibrés projectifs sur $\mathrm{Spec}(k)$ qui sont *localement triviaux pour la topologie étale*.

1.1.4 Exemples de groupes de Brauer

Proposition 1.1.41. *Soit k un corps algébriquement clos. Alors $Br(k) = 0$.*

Démonstration. C'est une reformulation du corollaire 1.1.17. □

Le cas des corps finis est plus intéressant.

Théorème 1.1.42 (Wedderburn)**.** *Le groupe de Brauer d'un corps fini est trivial.*

Via la proposition 1.1.40, c'est le fait que toute algèbre à division finie est un corps. Donnons-en une preuve qui utilise la théorie développée jusqu'ici. On commence par l'énoncé suivant d'intérêt indépendant.

Théorème 1.1.43 (Chevalley-Warning)**.** *Soient p un nombre premier, q une puissance de p, et $\mathbb{F}_q$ le corps fini à q éléments. Soit $P \in k[X_1, \ldots, X_n]$ un polynôme de degré total strictement inférieur à n. Alors le nombre de solutions dans $\mathbb{F}_q^n$ de l'équation $P(x_1, \ldots, x_n) = 0$ est divisible par p. En particulier, si P est homogène, alors cette équation a une solution non-nulle.*

Démonstration. L'observation clé est que pour x dans $\mathbb{F}_q$, x^{q-1} vaut 1 si x est non-nul et 0 sinon : l'élévation à la puissance $q-1$ est la fonction indicatrice de $\mathbb{F}_q^*$. Le nombre de solution de l'équation qui nous intéresse est donc congru modulo p à

$$N = \sum_{\underline{x} \in \mathbb{F}_q^n} \big(1 - P(\underline{x})^{q-1}\big).$$

Le degré du polynôme $1 - P(X_1, \ldots, X_n)^{q-1}$ est strictement inférieur à $(q-1)n$. Considérons l'un de ses monômes non nuls $aX_1^{a_1} \ldots X_n^{a_n}$. Alors l'un des a_i vérifie $a_i < q-1$. En particulier, $\sum_{x \in \mathbb{F}_q} x^{a_i} = 0$ (multiplier cette expression par un $x_0^{a_i} \neq 0, 1$). On a donc $N = 0$, ce qui conclut. □

Démonstration du théorème 1.1.42. Soit D une algèbre à division sur $\mathbb{F}_q$, centrale. Il faut montrer que $D = \mathbb{F}_q$. Soit n^2 la dimension de D. Soit $e_1, \ldots, e_{n^2}$ une base de D sur k. La proposition 1.1.36 fournit un polynôme $N \in k[X_1, \ldots, X_{n^2}]$ homogène de degré n, tel que

$$\forall x_1, \ldots, x_{n^2} \in F_q, N(x_1, \ldots, x_{n^2}) = Nrd(\sum_{i=1}^{n^2} x_i e_i).$$

Raisonnons par l'absurde et supposons $n > 1$. Le théorème de Chevalley-Warning s'applique et nous donne $x_1, \ldots, x_{n^2}$ non tous nuls tels que $N(x_1, \ldots, x_{n^2}) = 0$. L'élément $\sum_{i=1}^{n^2} x_i e_i$ est un élément non nul de D qui n'est pas inversible, ce qui contredit le fait que D est une algèbre à division. □

Remarque 1.1.44. *Des arguments (un peu) similaires permettent de montrer que le groupe de Brauer de $\mathbb{C}(X)$ est trivial (théorème de Tsen).*

Définition 1.1.45. *Soit k un corps de caractéristique différente de 2, et soient a, b deux éléments non nuls de k. L'algèbre de quaternions (a, b) est la k-algèbre de dimension 4, de base $1, i, j, ij$ telle que*

$$i^2 = a, j^2 = b, ij = -ji.$$

Exemple 1.1.4.1. *Les quaternions de Hamilton sont donnés par*

$$\mathbb{H} = (-1, -1).$$

Proposition 1.1.46. *Conservons les notations précédentes.*

(i) L'algèbre de quaternions (a, b) est simple centrale. Il s'agit soit d'une algèbre à division, soit de $M_2(k)$.

(ii) Soit $a = x + yi + zj + tij$. La trace réduite de a est $2x$, la norme réduite de a est $x^2 - ay^2 - bz^2 + abt^2$.

(iii) L'algèbre de quaternions (a, b) est une algèbre à division si et seulement si l'équation $ax^2 + by^2 = 1$ n'a pas de solution dans k.

(iv) Toute algèbre simple centrale de dimension 4 sur k est une algèbre de quaternions.

Démonstration. On prouve les énoncés dans l'ordre.

(i) Si $a = a'^2$, remplacer i par $\frac{1}{a'}i$ permet de supposer $a = 1$. On vérifie que l'algèbre $(1, b)$ est isomorphe à $M_2(k)$ via l'isomorphisme qui envoie i sur $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et j sur $\begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$. Si a n'est pas un carré, soit $K = k[\sqrt{a}]$. D'après ce qui précède, $(a, b) \otimes_k K$ est une algèbre de matrices, donc (a, b) est simple centrale.

Si (a, b) n'est pas une algèbre à division, le théorème de Wedderburn garantit que $(a, b) \simeq M_n(D)$ pour une certaine algèbre à division D. Comparant les dimensions, on trouver $4 = n^2 D$, et $n > 1$, ce qui implique $n = 2$ et $D = k$.

(ii) Cf TD – c'est une conséquence de la proposition 1.1.10.

(iii) Si $ax^2 + by^2 = 1$, alors la norme réduite de $1 + xi + yj$ est nulle, donc $1 + xi + yj$ n'est pas inversible et (a, b) n'est pas une algèbre à division. Réciproquement, supposons que (a, b) n'est pas une algèbre à division. Alors $(a, b) \simeq M_2(k)$.

Remarquons que tout sous-espace vectoriel de dimension 3 de $M_2(k)$ contient une matrice inversible non nulle (considérer le noyau de $M \mapsto M.(1, 0)$), donc on peut trouver λ, x, y non tous les trois nuls tels que $ax^2 + by^2 = \lambda^2$. Si $\lambda \neq 0$, il suffit de diviser par λ^2 pour trouver une solution à l'équation en question. Si

$\lambda = 0$, alors $ax^2 + by^2 = 0$ et l'on peut supposer, quitte à remplacer i par $\frac{1}{x}i$ et j par $\frac{1}{y}j$, que l'on a $a = -b$. On a dans ce cas

$$1 = a(\frac{1 + 1/a}{2})^2 - a(\frac{1 - 1/a}{2})^2,$$

ce qui conclut.

(iv) Soit A une algèbre simple centrale de dimension 4 sur k. Tout élément de $A \setminus k$ engendre une sous-algèbre finie de A contenant k dont le degré divise 4. Si ce degré est 4, A est commutative, ce qui contredit sa centralité. Tout élément de $A \setminus k$ engendre donc une k-algèbre de degré 2. On peut donc trouver $i \in A \setminus k$ tel que $a := i^2$ appartient à k. Considérons l'application k-linéaire

$$c_i : x \mapsto i^{-1}xi$$

. On a $c_i^2 = \mathrm{Id}_A$, donc les valeurs propres de c_i sont 1 et -1. Comme i n'est pas dans le centre de A, on peut trouver un vecteur propre j de c_i associé à la valeur propre -1. On a donc $ij = -ji$, et $ij^2 = j^2i$. Le commutant de j^2 contient $1, i$ et j. Comme c'est une sous-algèbre de A, il est de dimension 4 et j^2 appartient au centre de A. On peut donc trouver $b \in k$ tel que $j^2 = b$.

□

Corollaire 1.1.47. *Soient $a, b \in k^*$. L'algèbre de quaternions (a, b) est déployée par $k[\sqrt{a}]$.*

Démonstration. Il faut montrer que si a est un carré dans k, alors (a, b) est déployée. C'est clair par le point *(iii)* de la proposition précédente. □

Voici quelques manipulations de base sur les algèbres de quaternions.

Proposition 1.1.48. *Soient $a, b, b', x, y \in k^*$. On dispose des isomorphismes suivants :*

(i) $(a, b) \simeq (b, a)$;

(ii) $(a, b) \simeq (x^2a, y^2b)$;

(iii) $(1, b) \simeq M_2(k)$;

(iv) $(a, b) \otimes_k (a, b') \simeq (a, bb') \otimes M_2(k)$.

Remarque 1.1.49. *En particulier, la classe d'une algèbre de quaternions dans le groupe de Brauer est d'ordre 2. C'est un théorème profond de Merkurjev que toute classe d'ordre 2 est produit de classes d'algèbres de quaternions.*

Démonstration. Les trois premières formules ont été prouvées au cours de la preuve précédente. Montrons la dernière. On pourrait donner un isomorphisme explicite mais on va raisonner autrement.

Si a est un carré dans k, toutes les algèbres de quaternions qui apparaissent sont isomorphes à $M_2(k)$. On suppose donc que a n'est pas un carré. Soit $K = k[\sqrt{a}]$, que l'on considère comme un sous-corps de (a, b'). Soit ρ son k-automorphisme non-trivial, qui envoie $\sqrt{a}$ sur son opposé. Le Corollaire 1.1.47 montre que (a, b) est déployée par K. L'inclusion de K dans (a, b') fournit donc une inclusion de $M_2(K) \simeq (a, b) \otimes_k K$ dans $(a, b) \otimes_k (a, b')$. Le k-automorphisme ρ agit sur la K-algèbre $M_2(K)$, et son algèbre des invariants est $M \simeq M_2(k) \subset A = (a, b) \otimes_k (a, b')$.

Considérons la sous-algèbre N de A engendrée par $1 \otimes_k K$ et $x = j \otimes j'$. Elle est bien sûr isomorphe à (a, bb'). Par construction, $1 \otimes_k K$ commute à M. Par ailleurs, la conjugaison par x agit comme ρ, donc agit sur $M_2(K)$ comme ρ. En particulier, x commute à M, donc M et N commutent.

Le morphisme d'algèbres

$$M \otimes_k N \simeq M_2(k) \otimes_k (a, bb') \to (a, b) \otimes_k (a, b')$$

est surjectif : son image contient $(a, b) \otimes_K$ et $j \otimes j'$, qui engendrent une k-algèbre dont la dimension est au moins 9 et divise 16, donc vaut 16. Il s'agit donc d'un isomorphisme. □

On conclut cette section par le calcul du groupe de Brauer de $\mathbb{R}$.

Théorème 1.1.50 (Frobenius)**.** *Le groupe de Brauer de $\mathbb{R}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Son élément non-trivial est la classe de l'algèbre des quaternions de Hamilton $\mathbb{H} = (-1, -1)$.*

Démonstration. Il faut montrer que $\mathbb{H}$ est la seule algèbre à division centrale sur $\mathbb{R}$, distincte de $\mathbb{R}$. Soit D une telle algèbre à division. Sa dimension est au moins 4.

Un élément x de $D \setminus k$ engendre une extension de $\mathbb{R}$, nécessairement isomorphe à $\mathbb{C}$. Choisissons donc $x \in D$ tel que $x^2 = -1$. Comme plus haut, la conjugaison par x dans D a carré Id_D. On écrit $D = D^+ \oplus D^-$, où D^+ est le commutant de x et D^- le sous-espace des éléments de D qui anticommutent à x. Comme D est centrale et $x \notin k$, $D^- \neq 0$. Pour tout y dans D^-, la multiplication par y échange D^+ et D^-, qui sont donc de la même dimension.

Par ailleurs, D^+ est une sous-algèbre intègre de D contenant un sous-corps isomorphe à $\mathbb{C}$. C'est donc un $\mathbb{C}$-algèbre à division. On a déjà vu que cela implique $D^+ = \mathbb{C}$. Finalement, D^+ et D^- sont tous deux de dimension 2 sur $\mathbb{R}$, et D est de dimension 4 sur $\mathbb{R}$: c'est une algèbre de quaternions.

Finalement, soit $A = (a, b)$ une algèbre de quaternions sur $\mathbb{R}$ qui est une algèbre à division. On peut modifier (a, b) en les multipliant par des réels strictement positifs de sorte que $(a, b) = (\pm 1, \pm 1)$. La proposition précédente garantit que A est une algèbre à division si et seulement s'il s'agit de $(-1, -1)$. □

1.1.5 Algèbres cycliques, définitions et exemples

Donnons une construction assez générale d'algèbres simples centrales, dûe à Dickson. Rappelons qu'une extension finie de corps est *cyclique* si elle est galoisienne de groupe de Galois cyclique.

Définition 1.1.51. *Soit k un corps. Soient K une extension cyclique de degré n de k, σ un générateur du groupe de Galois de K sur k, et a un élément non nul de k. On définit l'algèbre cyclique associée à σ et a comme la k-algèbre engendrée par K et un élément α, soumis aux relations*

$$\alpha^n = a, x\alpha = \alpha\sigma(x)$$

pour tout $x \in K$. On note (σ, a) cette algèbre.

Notons qu'il suit de la définition l'égalité, pour tout $x \in K$,

$$x\alpha^i = \alpha^i\sigma^i(x).$$

Proposition 1.1.52. *La k-algèbre (σ, a) est une algèbre simple centrale de dimension n^2, déployée par K.*

Démonstration. Il suffit de montrer que $(\sigma, a) \otimes_k K$ est isomorphe à $M_n(k)$. Remarquons tout d'abord que la multiplication à gauche par les éléments de K fait de (σ, a) un K-espace vectoriel de dimension n, donc que (σ, a) a dimension n^2 sur K.

Rappelons que $K \otimes_k K$ est isomorphe comme K-algèbre à K^G, l'action de G étant donnée par $g.(x_h)_{h\in G} = (x_{gh})$. Autrement dit, $K \otimes_k K$ est isomorphe à K^n, l'action de σ étant donnée par $\sigma.(x_1, \ldots, x_n) = (x_2, x_3, \ldots, x_1)$. Finalement, l'algèbre $(\sigma, a) \otimes_k K$ est engendrée comme K-algèbre par K^n et un élément α, soumis à la relation

$$(x_1, \ldots, x_n)\alpha = \alpha(x_2, x_3, \ldots, x_1),\ \alpha^n = a$$

Dans l'algèbre de matrices $M_n(K)$, soit $M(x_1, \ldots, x_n)$ la matrice diagonale de coefficients $x_1, \ldots, x_n$. Notons

$$M(\alpha) = \begin{pmatrix} 0 & 0 & \cdots & 0 & a \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

On a $M(\alpha)^n = aI_n$, et $M(x_1, \ldots, x_n)M(\alpha) = M(\alpha)M(x_2, x_3, \ldots, x_1)$, d'où un morphisme de k-algèbres $(\sigma, a) \otimes_k K \to M_n(K)$, dont on vérifie sans peine qu'il est surjectif. Comme les deux algèbres en jeu ont la même dimension sur K, ce morphisme est un isomorphisme. □

Remarque 1.1.53. *L'automorphisme σ de K agit sur $M_n(K)$ par l'action naturelle. Via l'isomorphisme $M_n(K) \simeq (\sigma, b) \otimes_k K$, le calcul précédent montre qu'il agit par $c_\alpha \otimes \sigma$, où c_α^{-1} est la conjugaison par α.*

On va donner un cas particulier d'algèbres cycliques, qui généralise directement les algèbres de quaternions. Soit n un entier premier à la caractéristique de k, et supposons que k contient toutes les racines n-ièmes de l'unité. Dans ce qui suit, on fixe une racine primitive n-ième de l'unité $\omega \in k$.

Définition 1.1.54. *Soient $a, b \in k^*$. On définit l'algèbre $(a, b)_\omega$ comme la k-algèbre engendrée par deux éléments x, y tels que $x^n = a$, $y^n = b$ et $\omega xy = yx$.*

La théorie de Kummer nous montre que les extensions cycliques d'ordre n de k sont exactement les $k(b^{1/n})$ où b est un élément d'ordre n dans $k^*/(k^*)^n$.

Remarque 1.1.55. *Pour $n = 2$, on retrouve les algèbres de quaternions.*

Remarque 1.1.56. *On a $(a, b)_\omega \simeq (b, a)_{\omega^{-1}}$.*

Proposition 1.1.57. *Soit K une extension cyclique d'ordre n de k, et soit σ un générateur de $Gal(K/k)$. On peut trouver $b \in k^*$ tel que $K = k(b^{1/n})$ et une racine primitive n-ième de l'unité $\omega \in k$ telle que $\sigma(b^{1/n}) = \omega b^{1/n}$.*

Pour tout $a \in k^*$, on a un isomorphisme

$$(\sigma, a) \simeq (a, b)_\omega.$$

Démonstration. L'algèbre (σ, a) est engendrée sur k par $y = b^{1/n}$ et un élément x tel que $x^n = a$ et $yx = \omega xy$. Cela prouve le résultat. □

Proposition 1.1.58. *Avec les notations précédentes, on a $(a, 1)_\omega \simeq (1, b)_\omega \simeq M_n(k)$ pour tous $a, b \in k^*$. Plus généralement, si $b \in (k^*)^n$, alors $(a, b)_\omega \simeq M_n(k)$.*

Démonstration. Pour tout $t \in k^*$, on a un isomorphisme $(a, b)_\omega \simeq (a, t^n b)_\omega$. Il suffit donc, prenant en compte la remarque 1.1.56, de montrer que l'on a $(a, 1)_\omega \simeq M_n(k)$. Dans $M_n(k)$, considérons la matrice

$$X = \begin{pmatrix} 0 & 0 & \cdots & 0 & a \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Soit Y la matrice diagonale de coefficients $(\omega, \ldots, \omega^i, \ldots, 1)$. Alors $X^n = a$, $Y^n = 1$ et

$$YX = \omega XY.$$

On a donc un morphisme naturel

$$(a,1)_\omega \longrightarrow M_n(k).$$

Comme X et Y engendrent $M_n(k)$ comme k-algèbre (exercice !), il s'agit d'un isomorphisme pour des raisons de dimension. □

Corollaire 1.1.59. *Pour tous $a, b \in k^*$, la k-algèbre (a,b) est simple centrale.*

Démonstration. Après changement de base à une extension de k dans laquelle a est une puissance n-ième, la proposition précédente montre que $(a,b)_\omega$ devient isomorphe à une algèbre de matrices, ce qui prouve le résultat. □

Proposition 1.1.60. *Supposons n inversible dans k, et soit $\omega \in k$ une racine primitive n-ième de l'unité. Alors, pour tous $a, a', b, b' \in k^*$, on a*

$$(a,b)_\omega \otimes_k (a',b)_\omega \simeq (aa',b)_\omega \otimes_k M_n(k)$$

et

$$(a,b)_\omega \otimes_k (a,b')_\omega \simeq (a,bb')_\omega \otimes_k M_n(k).$$

Démonstration. La remarque 1.1.56 permet de ne prouver que le premier énoncé. On raisonne comme dans la proposition 1.1.48, (iv). Il s'agit de trouver dans $(a,b)_\omega \otimes_k (a',b)_\omega$ deux sous-algèbres respectivement isomorphes à (aa',b) et $M_n(k)$ qui commutent.

On note x, y, x', y' des générateurs de $(a,b)_\omega$ et $(a',b)_\omega$ tels que

$$x^n = x'^n = a,\ y^n = b,\ y'^n = b',\ xy\omega = yx,\ \omega x'y' = y'x'.$$

Soient

$$z = x \otimes x',\ t = y \otimes 1$$

et

$$z' = 1 \otimes x',\ t' = y^{-1} \otimes 1.$$

On laisse au lecteur le soin de vérifier que la k-algèbre engendrée par z, t est isomorphe à (aa',b) et que la k-algèbre engendrée par z', t' est isomorphe à $(a,1) \simeq M_n(k)$. De plus, ces deux sous-algèbres commutent. Le morphisme induit

$$(a,bb')_\omega \otimes_k M_n(k) \longrightarrow (a,b)_\omega \otimes_k (a',b)_\omega$$

n'est pas nul, il est donc injectif car le membre de gauche est simple – c'est un produit d'algèbres simples centrales – et c'est un isomorphisme pour des raisons de dimension. □

1.1.6 Algèbres cycliques, propriétés générales

Pour mieux comprendre les algèbres cycliques, donnons quelques résultats généraux. On commence par un résultat important de la théorie des algèbres simples centrales.

Théorème 1.1.61. *Soit A une algèbre simple centrale de dimension finie sur k, et soit B une k-algèbre simple. Soient $f, g : B \to A$ deux morphismes de k-algèbres. Alors on peut trouver $x \in A^*$ tel que $f = xgx^{-1}$. En particulier, tous les automorphismes de A sont intérieurs.*

Démonstration. Notons que f et g sont injectifs car B est simple, donc B est de dimension finie sur k.

Soit M un A-module à gauche simple, et soit $D = \mathrm{End}_A(M)$. Alors D est une k-algèbre à division de centre k (voir la preuve du théorème de Wedderburn : on a $A \simeq M_n(D^{opp})$ pour un certain $n \geq 0$). Sur M, on peut mettre deux structures de $B \otimes_k D$-module à gauche via

$$(b \otimes d).m = f(b)d(m)$$

et

$$(b \otimes d).m = g(b)d(m).$$

On les note M_f et M_g respectivement.

La proposition 1.1.37 montre que l'algèbre $B \otimes_k D$ est simple. En particulier, M_f et M_g sont isomorphes car ils ont la même dimension (cf TD).

Soit $\phi : M_f \to M_g$ un isomorphisme de $B \otimes_k D$-modules. Alors ϕ est un automorphisme de M qui commute à M, donc ϕ est la multiplication par un élément x de A par la proposition 1.1.15. La linéarité de ϕ par rapport à B se traduit par

$$\forall b \in B, \forall m \in M, f(b)xm = xg(b)m,$$

soit $f = xgx^{-1}$. □

Proposition 1.1.62. *Soit A une algèbre simple centrale de dimension n^2 sur k, et soit K une extension galoisienne de k incluse dans A. Alors $[K : k] \leq n$. Si $[K : k] = n$, alors le commutant de K dans A est K lui-même.*

Démonstration. Soit L une extension de k contenant K et déployant A. Alors $A \otimes_k L \simeq M_n(L)$, et $M_n(L)$ contient la L-algèbre $K \otimes_k L \simeq L^{[K:k]}$. En particulier, $M_n(L)$ contient une famille de $[K : k]$ projecteurs deux à deux orthogonaux, ce qui implique $[K : k] \leq n$.

Si de plus $[K : k] = n$, alors les projecteurs orthogonaux ci-dessus sont les projecteurs sur les droites d'une base de L^n, donc $K \otimes_k L$ s'identifie, après changement de base, à l'algèbre des matrices diagonales, et son commutant est bien $K \otimes_k L$. Le commutant de K dans A est donc l'ensemble des invariants sous Galois dans $K \otimes_k L$ soit K lui-même. □

Proposition 1.1.63. *Soit K/k une extension cyclique de degré n, et soit σ un générateur du groupe de Galois de K sur k. Soit A une algèbre simple centrale de dimension n^2 sur k, contenant K comme sous k-algèbre. Alors A est une algèbre cyclique (σ, a) pour un certain $a \in k^*$. En particulier, A est déployée par K.*

Démonstration. D'après le théorème de Noether-Skolem appliqué à l'inclusion de K dans A et à sa précomposition avec σ, on peut trouver un élément $\alpha \in A^*$ tel que

$$\forall x \in K, x\alpha = \alpha\sigma(x).$$

Pour tout entier i, et tout $x \in K$, on a

$$x\alpha^i = \alpha^i\sigma^i(x).$$

L'indépendance linéaire des caractères montre que les α^i forment une K-base de A. En particulier, α^n commute à K, donc à tous les $x\alpha^i$, $x \in K$, et donc à A tout entier, ce qui montre que $\alpha^n \in k$. Comme α est inversible, α^n est dans k^*, ce qui conclut. □

Remarque 1.1.64. *La réciproque est vraie : si A est déployée par K, alors A est cyclique, associée à un sous-corps de K.*

On peut généraliser aux algèbres cycliques certaines propriétés des algèbres de quaternions.

Proposition 1.1.65. *Soit $a \in k^*, x \in K^*$). Alors on a un isomorphisme*

$$(\sigma, a) \simeq (\sigma, N_{K/k}(x)a).$$

Démonstration. Écrivons (σ, a) comme l'algèbre engendrée par K et un élément α tel que $\alpha^n = a$ et $y\alpha = \alpha\sigma(y)$ pour tout $y \in K$. Soit $\beta = \alpha x$. Alors

$$\beta^n = N_{K/k}(x)a$$

et, pour tout $y \in K$, on a

$$y\beta = y\alpha x = \alpha\sigma(y)x = \alpha x\sigma(y).$$

L'algèbre (σ, a) est engendrée par K et β, donc $(\sigma, a) \simeq (\sigma, N_{K/k}(x)a)$. □

Proposition 1.1.66. *Avec les notations précédentes, on a, pour tous $a, b \in k^*$,*

$$(\sigma, a) \otimes_K (\sigma, b) \simeq M_n(k) \otimes_k (\sigma, ab).$$

En particulier, prenant les classes dans le groupe de Brauer, on a

$$[(\sigma, a)][(\sigma, b)] = [(\sigma, ab)].$$

Démonstration. Il s'agit de l'analogue en dimension supérieure de la proposition 1.1.48, (iv). On en copie essentiellement la démonstration. Il s'agit là encore de trouver dans $(\sigma, a) \otimes_k (\sigma, b)$ deux sous-algèbres respectivement isomorphes à $M_n(k)$ et (σ, ab), qui commutent.

L'inclusion de K dans (σ, b) induit une inclusion de

$$M_n(K) \simeq (\sigma, a) \otimes_k K$$

dans $(\sigma, a) \otimes_k (\sigma, b)$. Le k-automorphisme σ agit sur la K-algèbre $M_n(K)$, et sont algèbre des invariants est $M \simeq M_n(k)$. Par construction, $1 \otimes_k K$ commute à M. Par ailleurs, avec des notations évidentes, l'élément $\alpha \otimes \beta$ commute à M grâce au calcul de la proposition 1.1.48. L'algèbre N engendrée par $1 \otimes_k K$ et $\alpha \otimes \beta$ est isomorphe à (σ, ab), ce qui conclut. □

Corollaire 1.1.67. *Avec les notations précédentes, on a*

$$(\sigma, 1) \simeq M_n(k).$$

Démonstration. Pour tout $a \in k^*$, la proposition précédente montre l'égalité dans $Br(k)$

$$[(\sigma, 1)] + [(\sigma, a)] = [(\sigma, a)],$$

ce qui montre que $[(\sigma, 1)] = 0$. □

Proposition 1.1.68. *Soit K/k une extension cyclique, et soit σ un générateur de $Gal(K/k)$. L'application*

$$a \mapsto [(\sigma, a)]$$

induit un isomorphisme de groupes

$$k^*/N_{K/k}(K^*) \longrightarrow Br(K/k),$$

où $Br(K/k)$ est le sous-groupe de $Br(k)$ constitué des éléments déployés par K.

Remarque 1.1.69. *Nous allons seulement montrer que $k^*/N_{K/k}(K^*) \longrightarrow Br(K/k)$ est un morphisme de groupes injectif.*

Démonstration. La proposition 1.1.66 montre que

$$a \mapsto [(\sigma, a)]$$

induit un morphisme de groupes $k^* \to Br(k)$, dont l'image est contenue dans $Br(K/k)$ par la proposition 1.1.52.

La proposition 1.1.65 montre que l'on a $(\sigma, N_{L/K}(x)) \simeq (\sigma, 1)$. Le corollaire précédent montre que $[(\sigma, N_{L/K}(x))] = 0$ dans $Br(k)$. On obtient donc bien un morphisme de groupes $\phi : k^*/N_{K/k}(K^*) \longrightarrow Br(K/k)$.

Montrons que ϕ est injective. Soit donc $a \in k^*$ et supposons $A = (\sigma, a)$ déployée. Alors $(\sigma, a) \simeq (\sigma, 1)$. Fixons un plongement de K dans A et un élément α de A tel que $\alpha^n = 1$ et $x\alpha = \alpha\sigma(x)$ pour tout $x \in K$. D'après le théorème de Noether-Skolem, on peut trouver $\gamma \in A$ et $\beta \in A$ tels que $\beta^n = 1$ et

$$x\alpha = \alpha\sigma(x)$$

pour tout $x \in \gamma K \gamma^{-1}$. Alors $(\gamma^{-1}\beta\gamma)\alpha^{-1}$ commute à K, donc est un élément x de K par la proposition 1.1.62. On en déduit

$$a = \alpha^n = \beta^{-n} N_{K/k}(x) = N_{K/k}(x).$$

Nous n'utiliserons pas la surjectivité de ϕ, que nous ne montrerons pas. □

1.1.7 Dépendance en σ

Passons maintenant aux questions de fonctorialité en fonction de σ, plus difficiles. Voici un résultat élémentaire.

Proposition 1.1.70. *Soit m un entier premier à n, et soit $a \in k^*$. Alors on a un isomorphisme*

$$(\sigma, a) \simeq (\sigma^m, a^m).$$

En particulier, on a

$$[(\sigma, a)] = m[(\sigma^m, a)]$$

dans $Br(k)$.

Démonstration. Écrivons (σ, a) comme l'algèbre engendrée par K et un élément α tel que $\alpha^n = a$ et $x\alpha = \alpha\sigma(x)$ pour tout $x \in K$. Soit $\beta = \alpha^m$. Alors $\beta^n = a^m$, et $x\beta = \beta\sigma^m(x)$ pour tout $x \in K$. Puisque m est premier à $n = [K : k]$, σ^m est un générateur de $Gal(K/k)$, ce qui prouve le résultat. □

On étudie maintenant la situation de deux extensions cycliques disjointes.

Proposition 1.1.71. *Soient K_1 et K_2 deux extensions cycliques de k de degré n_1 et n_2 respectivement, σ_1 et σ_2 deux générateurs des groupes de Galois de K_1/k et K_2/k respectivement. On suppose que n_1 et n_2 sont premiers entre eux. Alors K_1 et K_2 disjointes.*

Soit K le corps $K_1 \otimes_k K_2$. On identifie le groupe de Galois de K/k à $Gal(K_1/k) \times Gal(K_2/k)$. Alors $\sigma = (\sigma_1, \sigma_2)$ est un générateur de $Gal(K/k)$ et l'on a un isomorphisme, pour tout $a \in k^*$,

$$(\sigma_1, a) \otimes_k (\sigma_2, a) \simeq (\sigma, a^{n_1+n_2}).$$

Démonstration. Que K_1 et K_2 soient disjointes, que $K = K_1K_2 = K_1 \otimes_k K_2$ soit un corps et que σ engendre $Gal(K/k)$ suit de la théorie de Galois de base.

Pour $i = 1, 2$, l'algèbre (σ_i, a) est engendrée par K_i et un élément α_i tel que $\alpha_i^{n_i} = a$ et $x\alpha_i = \alpha_i\sigma_i(x)$ pour tout $x \in K_i$. Alors $(\sigma_1, a) \otimes_k (\sigma_2, a)$ est engendré par $K = K_1 \otimes_k K_2$ et l'élément $\beta = \alpha_1 \otimes \alpha_2$, tel que $\beta^{n_1n_2} = a^{n_1+n_2}$ et $x\beta = \beta\sigma(x)$ pour tout $x \in K$. Cela prouve le résultat. □

On peut traiter d'autre cas d'extensions cycliques disjointes – voici un exemple. La preuve de l'énoncé suivant est semblable à celle de la proposition 1.1.66. On ne l'utilisera pas dans la suite.

Proposition 1.1.72. *Soient K_1 et K_2 deux extensions cycliques de k de degré n_1 et n_2 respectivement, σ_1 et σ_2 deux générateurs des groupes de Galois de K_1/k et K_2/k respectivement. On suppose que n_1 divise n_2, et on écrit $n_2 = rn_1$.*

Supposons K_1 et K_2 disjointes, et soit L le corps $K_1 \otimes_k K_2$. On identifie le groupe de Galois de L/k à $Gal(K_1/k) \times Gal(K_2/k)$. Soit K le sous-corps de L fixé par $(\sigma_1, \sigma_2^{-r})$. Alors $\sigma = (1, \sigma_2)$ est un générateur de $Gal(K/k)$ et l'on a un isomorphisme, pour tout $a \in k^*$,

$$(\sigma_1, a) \otimes_k (\sigma_2, a) \simeq (\sigma, a) \otimes_k M_{n_1}(k).$$

Démonstration. La théorie de Galois usuelle garantit que $L = K_1 \otimes_k K_2 = K_1K_2$ est une extension galoisienne de k de groupe de Galois le produit de groupes cycliques $Gal(K_1/k) \times Gal(K_2/k)$. En particulier, L est de degré $n_1n_2 = rn_1^2$ sur k. L'ordre de $(\sigma_1, \sigma_2^{-r})$ est n_1, donc le degré de K sur k est n_2, et l'on vérifie immédiatement que $\sigma = (1, \sigma_2)$ est un générateur de $Gal(K/k)$. Notons enfin que K est disjointe de K_1 : un élément de $K \cap K_1$ est fixé par $(1, \sigma_2)$ et $(\sigma_1, \sigma_2^{-r})$, donc est dans k.

Pour $i = 1, 2$, l'algèbre (σ_i, a) est engendrée par K_i et un élément α_i tel que $\alpha_i^{n_i} = a$ et $x\alpha_i = \alpha_i\sigma_i(x)$ pour tout $x \in K_i$.

Soit A l'algèbre simple centrale

$$A = (\sigma_1, a) \otimes_k (\sigma_2, a).$$

Alors A contient $L = K_1 \otimes_k K_2$, et $K \subset L$ est un sous-corps de A. L'élément $\beta = 1 \otimes \alpha_2$ vérifie $\beta^{n_2} = a$ et $x\beta = \beta\sigma(x)$ pour tout $x \in K$. Le corps K et β engendrent donc une sous-algèbre A_1 de A isomorphe à (σ, a).

De même, $K_1 \subset L$ est un sous-corps de A. L'élément $\gamma = \alpha_1 \otimes \alpha_2^{-r}$ vérifie $\gamma^{n_1} = 1$ et $x\gamma = \gamma\sigma_1(x)$ pour tout $x \in K_1$. Le corps K_1 et γ engendrent donc une sous-algèbre A_2 de A isomorphe à $(\sigma_1, 1) \simeq M_{n_1}(k)$.

Nous laissons au lecteur le soin de vérifier que A_1 et A_2 commutent. On obtient donc un morphisme de k-algèbres simples

$$A_1 \otimes_k A_2 \longrightarrow A,$$

qui est un isomorphisme pour des raisons de dimension, ce qui prouve le résultat. □

On considère enfin la situation de deux extensions cycliques contenues l'une dans l'autre.

Proposition 1.1.73. *Soit L une extension cyclique de k contenant K, et notons $r = [L : K]$. Soit σ un générateur du groupe de Galois de L sur k. Alors, pour tout $a \in k^*$, on a*

$$(\sigma, a^r) \simeq (\sigma_{|K}, a) \otimes_k M_r(k).$$

En particulier, on a

$$r[(\sigma, a)] \simeq [(\sigma_{|K}, a)]$$

dans $Br(k)$.

Démonstration. Notons A la k-algèbre simple centrale (σ, a^r). Alors A est engendrée par le corps L, de degré nr sur k, et un élément α tel que $\alpha^{nr} = a^r$ et $x\alpha = \alpha\sigma(x)$ pour tout $x \in L$.

Soit P le polynôme dans $\mathbb{Z}[X]$ tel que

$$X^{nr} - a^r = (X^n - a)P(X^n),$$

et soit I l'idéal à gauche de A

$$I = AP(\alpha^n).$$

On commence par construire une injection

$$(\sigma_{|K}, a) \hookrightarrow \mathrm{End}_A(I).$$

Pour ce faire, écrivons $(\sigma_{|K}, a)$ comme la k-algèbre engendrée par K et un élément β tel que $\beta^n = a$ et $x\beta = \beta\sigma(x)$ pour tout $x \in K$.

On commence par remarquer que, dans (σ, a^r), α^n commute à K. Le corps K agit donc par multiplication à droite sur I. Par ailleurs, comme α commute à tout polynôme en α, α agit par multiplication à droite sur I. Notons de plus que l'on a

$$P(\alpha^n)(\alpha^n - a) = \alpha^{nr} - a^r = 0,$$

soit

$$P(\alpha^n)\alpha^n = aP(\alpha).$$

Plus généralement, pour tout $i \in I$, on a

$$i\alpha^n = ai.$$

L'action de K et α par multiplication à droite sur I s'étend donc en une action à droite de $(\sigma_{|K}, a)$ sur I. Autrement dit, I est muni d'une structure de $(\sigma_{|K}, a)^{opp}$-module à gauche. Comme $(\sigma_{|K}, a)^{opp}$ est simple centrale, c'est une somme directe de copies de

l'unique $(\sigma_{|K}, a)^{opp}$-module simple (cf TD). Calculons sa dimension comme k-espace vectoriel, soit la dimension du L-espace vectoriel

$$A_L P(\alpha^n).$$

Après identification de A_L avec $M_n(L)$, on peut identifier α à une matrice compagnon de polynôme minimal $X^{nr} - a^r$. L'algèbre linéaire élémentaire montre que $A_L P(\alpha^n)$ est l'idéal des matrices s'annulant sur le noyau de $P(\alpha^n)$, qui est de dimension $n(r-1)$. Cet idéal a donc dimension

$$n^2r^2 - nr\big(n(r-1)\big) = n^2 r.$$

Finalement, la dimension sur k de I est $n^2 r$, donc il est isomorphe à $(\sigma_{|K}, a)^r$ comme $(\sigma_{|K}, a)^{opp}$-module. En particulier, on a

$$\mathrm{End}_{(\sigma_{|K},a)^{opp}}(I) \simeq M_r((\sigma_{|K}, a)).$$

Soit $B = \mathrm{End}_A(I)$. Le lemme de Rieffel ci-dessous montre que l'on a un isomorphisme

$$A \simeq \mathrm{End}_B(I).$$

Comme $(\sigma_{|K}, a)$ est simple, l'action de $(\sigma_{|K}, a)^{opp}$ sur I donne par ailleurs une injection

$$(\sigma_{|K}, a)^{opp} \hookrightarrow B.$$

On obtient ainsi une injection

$$\mathrm{End}_B(I) \hookrightarrow \mathrm{End}_{(\sigma_{|K},a)^{opp}}(I) \simeq M_r((\sigma_{|K}, a)^{opp}).$$

Comme

$$\dim_k(A) = n^2 r^2 = \dim_k M_r((\sigma_{|K}, a)),$$

on trouve enfin

$$A \simeq M_r((\sigma_{|K}, a)),$$

ce qui conclut. □

Nous avons utilisé dans la preuve la variante suivante de la proposition 1.1.15. La preuve, similaire, en sera vue en TD.

Lemme 1.1.74 (Lemme de Rieffel)**.** *Soit A une k-algèbre simple, et soit I un idéal à gauche non-nule de A Soit $B = \mathrm{End}_A(I)$, Alors la flèche naturelle*

$$A \longrightarrow \mathrm{End}_B(I)$$

est un isomorphisme.

1.1.8 Aparté : le groupe de Galois absolu d'un corps et sa topologie

On rappelle brièvement, sans donner aucune preuve (qui se déduisent toutes de la théorie de Galois usuelle), quelques éléments de théorie de Galois des extensions infinies. On fixe un corps k.

Définition 1.1.75. *Soit K une extension algébrique de k. On dit que K est une extension* galoisienne *de k si K est réunion de ses sous-extensions galoisiennes finies de k. Le* groupe de Galois *de K/k, noté $Gal(K/k)$, est le groupe des k-automorphismes de k.*

Remarque 1.1.76. *Si K/k est une extension finie, on trouve la topologie discrète.*

La principale différence entre la théorie de Galois des extensions arbitraires et celle des extensions finies est la présence d'une topologie sur le groupe de Galois $Gal(K/k)$.

Définition 1.1.77. *Avec les notations précédentes, la* topologie de Krull *de $Gal(K/k)$ est l'unique topologie sur $Gal(K/k)$ qui en fait un groupe topologique dont les sous-groupes ouverts sont les $Gal(K/K')$ où K' est une extension finie de k contenue dans K.*

Il faut bien sûr prouver que la définition fournit un groupe topologique. On peut comprendre un peu différemment cette topologie. On munira toujours les groupes de Galois de leur topologie de Krull dans la suite.

Proposition 1.1.78. *Avec les notations précédentes, soit K' une extension galoisienne de k contenue dans K. L'application de restriction*

$$Gal(K/k) \longrightarrow Gal(K'/k)$$

est continue et surjective. L'application continue induite

$$Gal(K/k) \longrightarrow \lim_{K'} Gal(K'/k)$$

où K' parcourt les extensions finies galoisiennes de k contenues dans K, est un isomorphisme de groupes topologiques.

On dit que $Gal(K/k)$ est un *groupe profini* : c'est une limite projective de groupes finis munis de la topologie discrète. En particulier, c'est un groupe compact.

On discutera plus en détail des limites projectives d'espaces topologiques (finis, discrets) quand on considérera les nombres p-adiques. À ce stade, nous retiendrons surtout de l'énoncé ci-dessus la continuité et la surjectivité des applications de restriction, et le fait qu'il est équivalent de se donner un k-automorphisme de K, et une famille compatible d'automorphismes des K'/k, où K' parcourt les extensions

finies galoisiennes de k contenues dans K – ce dernier énoncé étant une conséquence formelle du fait que K est réunion de ses sous-extensions galoisiennes finies.

La correspondance de Galois pour les extensions pas nécessairement finies prend la forme suivante.

Théorème 1.1.79. *Avec les notations précédentes, les applications*

$$K' \mapsto Gal(K/K')$$

et

$$H \mapsto K^H$$

induisent une bijection entre l'ensemble des sous-corps de K contenant k et les sous-groupes fermés de $Gal(K/k)$. De plus, K^H/K est galoisienne si et seulement si H est distingué, et dans ce cas on a un isomorphisme canonique

$$Gal(K^H/k) \simeq Gal(K/k)/H.$$

Remarque 1.1.80. *Il n'est pas vrai que tout sous-groupe d'indice fini de $Gal(K/k)$ est fermé. Les sous-groupes fermés d'indices finis de $Gal(K/k)$ sont exactement les $Gal(K/K')$, où K' est une extension finie de k contenue dans K. Ils sont ouverts.*

Soit $\mathbb{U}$ le groupe multiplicatif des nombres complexes de module 1 muni de sa topologie naturelle. On considère $\mathbb{Q}/\mathbb{Z}$ comme un sous-groupe topologique de $\mathbb{U}$ via

$$x \mapsto e^{2i\pi x}.$$

Soit G un groupe abélien localement compact. On note $\widehat{G}$ le *groupe dual*

$$\widehat{G} = \mathrm{Hom}_{cont}(G, \mathbb{U})$$

des morphismes continus de G vers $\mathbb{U}$, muni de la topologie de la convergence uniforme sur les compacts, engendrée par les $\{\chi \in \widehat{G}, \chi(K) \subset U\}$ où K parcourt les compacts de G et U les ouverts de $\mathbb{U}$. Les éléments de $\widehat{G}$ sont les *caractères* de G.

Proposition 1.1.81. *Soit G un groupe profini. Alors tout caractère de G est d'image finie et*

$$\widehat{G} = \mathrm{Hom}_{cont}(G, \mathbb{Q}/\mathbb{Z})$$

est un groupe abélien de torsion, muni de la topologie discrète.

Démonstration. Soit $\chi : G \to \mathbb{U}$ un caractère de G. Par définition de la topologie de G, G a une base $(G_i)_{i\in I}$ de voisinage de 0 formée de sous-groupes de G d'indice fini dans G. Pour tout voisinage U de 0 dans $\mathbb{U}$, on peut trouver un G_i tel que $\chi(G_i) \subset U$. Si U est suffisamment petit, alors U ne contient pas de sous-groupe de $\mathbb{U}$ différent de

$\{1\}$, ce qui prouve que l'on peut trouver $i \in I$ tel que $G_i \subset \operatorname{Ker}\chi$. Cela montre que χ se factorise par un quotient d'indice fini de G, et que χ est de torsion. En particulier, χ est à valeurs dans $\mathbb{Q}/\mathbb{Z}$.

Il reste à montrer que $\widehat{G}$ est un groupe discret. Comme G est compact, pour tout ouvert U de $\mathbb{U}$, le sous-ensemble de G

$$V = \{\chi \in \widehat{G}, \chi(G) \subset U\}$$

est ouvert dans $\widehat{G}$. Si U est suffisamment petit, le seul sous-groupe de $\mathbb{U}$ contenu dans U est $\{1\}$, donc $V = \{0\}$, ce qui prouve que $\widehat{G}$ est discret. □

Remarque 1.1.82. *La proposition précédente montre que $\widehat{G}$ s'identifie aux morphismes de G dans $\mathbb{Q}/\mathbb{Z}$ muni de sa topologie discrète.*

Une partie de la proposition précédente se reformule comme suit dans le cas des groupes de Galois.

Corollaire 1.1.83. *Avec les notations précédentes, soit $G = Gal(K/k)$. Si χ est un caractère de G, on peut trouver une extension finie cyclique K'/k de k contenue dans K telle que χ induise un isomorphisme de $Gal(K'/k)$ sur son image.*

Démonstration. La proposition précédente montre que le noyau de χ est un sous-groupe d'indice fini de G. Par ailleurs, l'image de χ est un sous-groupe de $\mathbb{Q}/\mathbb{Z}$, nécessairement cyclique. Cela prouve le résultat. □

Dans ce qui suit, si $\overline{k}$ est une clôture séparable de k, on note $G_k = Gal(\overline{k}/k)$. C'est le *groupe de Galois absolu de k*. On note $X(k)$ le groupe dual de G_k.

1.1.9 Groupe de Brauer et groupe de Galois absolu d'un corps

On va reformuler les résultats de fonctorialité pour les algèbres cycliques de manière plus agréable.

Soit comme précédemment

$$X(k) = \operatorname{Hom}(G_k, \mathbb{Q}/\mathbb{Z})$$

le groupe des morphismes continus du groupe de Galois absolu G_k d'un corps k vers $\mathbb{Q}/\mathbb{Z}$ (muni de sa topologie usuelle ou discrète).

Soit χ un élément de $X(k)$. Son image est de la forme $1/n\mathbb{Z}/\mathbb{Z}$ pour un certain $n \geq 1$. À χ sont associés une extension cyclique K – le sous-corps de $\overline{k}$ fixé par le noyau de χ – et un générateur σ distingué de $Gal(K/k)$ tel que $\chi(\sigma) = 1$.

Si a est un élément de k^*, on note $(\chi, a) \in Br(k)$ la classe de l'algèbre cyclique (σ, a). Les calculs que nous avons fait sur les algèbres cycliques se résument comme suit.

On commence par quelques résultats préliminaires.

Lemme 1.1.84. *Soit D une algèbre à division centrale de dimension n^2 sur k. Soit K une extension de k de degré d premier à n. Alors $D \otimes_k K$ est une algèbre à division sur K.*

Démonstration. Écrivons $D \otimes_k K = M_r(D')$, où D' est une K-algèbre à division de dimension n'^2. Alors $n = rn'$ et D'^r est muni d'une structure de D-module à droite via l'inclusion $D \subset D \otimes_k K$.

Comme D est une algèbre à division, tout D-module est isomorphe à une somme de copies de D. En particulier, $n^2 = \dim_k D$ divise $\dim_k D'^r = drn'^2 = dnn'$, ce qui signifie, puisque d est premier à n, que n divise n', soit $r = 1$. □

Proposition 1.1.85. *Soit A une algèbre simple centrale de dimension n^2 sur k. Soit K une extension de k de degré premier à n. Alors $A \otimes_k K$ est déployée si et seulement si A est déployée.*

Démonstration. On écrit $A = M_r(D)$, où D est une k-algèbre à division. Le lemme 1.1.84 montre que $D \otimes_k K$ est une algèbre à division. Finalement, $A \otimes_k K$ est déployée si et seulement si $D \otimes_k K = K$, i.e. si et seulement si A est déployée. □

Lemme 1.1.86. *Soit K une extension finie de k, contenue dans $\overline{k}$. Soit $\chi \in X(k)$, $a \in k^*$. Notons χ_K la restriction de χ à $G_K \subset G_k$. Alors dans $Br(K)$ on a l'égalité*

$$(\chi, a) \otimes_k K = (\chi_K, a).$$

Démonstration. Soient L l'extension cyclique de k et σ le générateur de $Gal(L/k)$ associés à χ. On note $n = [L : k]$. On peut traiter séparément le cas où K est disjoint de L et celui où K est inclus dans L.

Supposons d'abord K disjoint de L. Alors LK est une extension cyclique de degré n de K, et σ s'identifie à un générateur σ' de $Gal(LK/K)$. On a de manière évidente

$$(\chi, a) \otimes_k K = (\sigma', a).$$

On laisse au lecteur le soin de vérifier que la restriction de χ à G_K induit un isomorphisme de LK/K qui envoie σ' sur $1/n\mathbb{Z}/\mathbb{Z}$, ce qui conclut ce premier cas.

Supposons maintenant K inclus dans L. Soit $r = [K : k]$. On vérifie immédiatement

$$(\chi_K, a) = (\sigma^r, a).$$

Considérons par ailleurs la K-algèbre $A = (\sigma, a) \otimes_k K$. Elle est engendrée par $L \otimes_k K$ et un élément α tel que $\alpha^n = a$ et $x\alpha = \alpha\sigma(x)$ pour tout $x \in L$.

On a un isomorphisme canonique de K-algèbres

$$L \otimes_k K \simeq L^r,\ x \otimes y \mapsto (xy, \sigma(x)y, \dots, \sigma^{r-1}(x)y).$$

Le groupe $Gal(L/k)$ agit sur $L \otimes_k K$ par automorphismes K-linéaires, donc sur L^r par l'isomorphisme ci-dessus. L'action est donnée par

$$\sigma.(x_1, \dots, x_r) = (x_2, x_3, \dots, \sigma^r(x_1)).$$

Autrement dit, A est engendrée par L^r et un élément α tel que $\alpha^n = a$ et

$$(x_1, \dots, x_r)\alpha = \alpha(x_2, x_3, \dots, x_r, \sigma^r(x_1)).$$

La K-algèbre (σ^r, a) a dimension n^2/r^2. Elle est engendrée par L et un élément β tel que $\beta^{n/r} = a$ et $x\beta = \beta\sigma^r(x)$ pour tout $x \in L$. Dans l'algèbre $M_r((\sigma^r, a))$, on trouve L^r plongé de manière diagonale et une matrice

$$\gamma = \begin{pmatrix} 0 & 0 & \cdots & 0 & \beta \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Alors $\gamma^n = a$ et

$$(x_1, \dots, x_r)\gamma = \gamma(x_2), x_3, \dots, x_r, \sigma^r(x_1))$$

pour tous $x_1, \dots, x_r$ dans L. On en déduit un morphisme

$$A \longrightarrow M_r((\sigma^r, a)) \simeq (\sigma^r, a) \otimes_K M_r(K).$$

Ce morphisme est injectif car A est simple. C'est un isomorphisme pour des raisons de dimension. □

Lemme 1.1.87. *Soit $\chi \in X(k)$, et soit $a \in k^*$. Alors, pour tout entier d, on a*

$$(d\chi, a) = d(\chi, a).$$

Démonstration. Soient K l'extension cyclique de k et σ le générateur de $Gal(K/k)$ associés à χ. On note $n = [K : k]$. On peut traiter séparément le cas où d est premier à n et celui où d divise n.

Si d est premier à n, l'énoncé suit de la proposition 1.1.70.

Supposons que d divise n. L'énoncé suit de la proposition 1.1.73. □

Nous pouvons combiner les preuves de la Proposition 1.1.73 et de la Proposition 1.1.71 pour obtenir les énoncés suivants [1].

1. Merci à Tongmu He pour avoir suggéré un énoncé similaire !

Lemme 1.1.88. *Soient K_1 et K_2 deux extensions cycliques de k de degré n_1 et n_2 respectivement, toutes deux contenues dans $\overline{k}$. On suppose que n_1 divise n_2, et on écrit $n_2 = rn_1$. On suppose $r > 1$ ou n_2 impair. Soit $K = K_1 \cap K_2$, $L = L_1L_2$.*

Soient σ_1 et σ_2 des générateurs de $Gal(K_1/k)$ et $Gal(K_2/k)$ dont les restrictions à K coïncident, et soient χ_1 et χ_2 les éléments de $X(k)$ correspondant. On identifie $Gal(L/k)$ au sous-groupe de $Gal(K_1/k)\times Gal(K_2/k)$ dont les éléments sont les couples (σ, τ) sont ceux dont les restrictions à K coïncident.

Alors le caractère $\chi_1+\chi_2$ a pour noyau $Gal(\overline{k}/K_3)$, où K_3 est l'extension cyclique de degré n_2 de k fixée par $(\sigma_1, \sigma_2^{-r})$, et (σ_1, σ_2) est un générateur du groupe de Galois de K_3/k.

Démonstration. L'image de $\chi_1 + \chi_2$ est contenue dans $1/n_2\mathbb{Z}/\mathbb{Z}$. Par ailleurs,

$$(\chi_1 + \chi_2)(\sigma_1, \sigma_2) = \frac{r+1}{n_2},$$

qui est un générateur de $1/n_2\mathbb{Z}/\mathbb{Z}$. L'image de $\chi_1+\chi_2$ est donc égale à $1/n_2\mathbb{Z}/\mathbb{Z}$. Cela prouve que K_3 est de degré n_2 sur k, et que (σ_1, σ_2) est un générateur du groupe de Galois de K_3/k.

L'image de (σ_1^a, σ_2^b) par $\chi_1 + \chi_2$ est $\frac{ar+b}{n_2}$, qui est nul dans $\mathbb{Q}/\mathbb{Z}$ si et seulement si $b = -ar$ modulo n_2, ce qui prouve la dernière assertion.

□

Lemme 1.1.89. *Avec les notations du lemme précédent, soit $\sigma = (\sigma_1, \sigma_2)$, considéré comme un élément de $Gal(K_3/k)$. Alors, pour tout $a \in k^*$, on a*

$$(\sigma_1, a) \otimes_k (\sigma_2, a) \simeq (\sigma, a^{1+r}) \otimes M_{n_1}(k),$$

soit

$$(\chi_1, a) + (\chi_2, a) = (\chi_1 + \chi_2, a).$$

Démonstration. Que la première formule implique la seconde est une conséquence du précédent lemme que nous laissons au lecteur. On va prouver la première.

Soit A_i la k-algèbre simple centrale (σ_1, a). Elle est engendrée par K_i et un élément α_i tel que $\alpha_i^{n_i} = a$. Soit $A = A_1 \otimes_k A_2$. Soit $\beta = \alpha_1 \otimes \alpha_2 \in A$. Alors $\beta^{n_2} = a^{1+r}$.

Soit $\gamma = \alpha_1 \otimes \alpha_2^{-r}$. Alors $\gamma^{n_1} = 1$. Soit P le polynôme tel que

$$X^n - 1 = (X - 1)P(X)$$

et soit I l'idéal de A

$$I = AP(\gamma).$$

Les arguments de la Proposition 1.1.73 montre que I a dimension $n_1n_2^2$ sur K (étendre les scalaires à L, et travailler sous forme matricielle), et que $(\sigma, a^{1+r})^{opp}$ agit sur I (plonger K_3 dans $K_1 \otimes_k K_2$ et considérer la multiplication à droite par K_3 et β). On conclut de la même manière. □

Théorème 1.1.90. *L'application*

$$X(k) \times k^* \to Br(k)$$

est bilinéaire. Si χ est un élément de $X(k)$ associé à une extension cyclique K/k, alors le morphisme de groupes

$$k^* \longrightarrow Br(k), a \mapsto (\chi, a)$$

induit un isomorphisme

$$k^*/N_{K/k}(K^*) \longrightarrow Br(K/k).$$

Enfin, si K est une extension finie de k, l'application de restriction naturelle $X(k) \to X(K)$, l'inclusion $k^* \subset K^*$ et l'extension des scalaires $Br(k) \to Br(K)$ induisent un diagramme commutatif

$$\begin{array}{ccc} X(k) \times k^* & \longrightarrow & Br(k) \\ \downarrow & & \downarrow \\ X(K) \times K^* & \longrightarrow & Br(K) \end{array}$$

Remarque 1.1.91. *Comme précédemment, nous prouvons seulement que le noyau de $k^* \longrightarrow Br(k), a \mapsto (\chi, a)$ est le groupe de normes $N_{K/k}(K^*)$.*

Démonstration. D'après ce qui précède, la seule égalité à prouver est la suivante : soient χ_1 et χ_2 deux éléments de $X(k)$, et soit $a \in k^*$. Alors

$$(\chi_1 + \chi_2, a) = (\chi_1, a) + (\chi_2, a).$$

On commence par se ramener au cas où les ordres respectifs de χ_1 et χ_2 sont des puissances de nombres premiers. Pour ce faire, soit n_1 et n_2 les ordres de χ_1 et χ_2 respectivement. On écrit

$$n_1 = p_1^{r_1} \dots p_a^{r_a}$$

et

$$n_2 = q_1^{s_1} \dots q_b^{s_b}$$

pour les décompositions en facteur premier. Alors les

$$\chi_{1,i} = n_1/p_i^{r_i}\chi_1$$

et les

$$\chi_{2,j} = n_2/q_j^{s_j}\chi_2$$

sont d'ordre une puissance d'un nombre premier. Si pour tout i, j, on a

$$(\chi_{1,i} + \chi_{2,j}, a) = (\chi_{1,i}, a) + (\chi_{2,j}, a),$$

alors, écrivant χ_1 comme combinaison linéaire à coefficients entiers des $\chi_{1,i} = n_1/p_i^{r_i}\chi_1$, et sembablement pour χ_2, on trouve le résultat.

On suppose donc que les ordres respectifs de χ_1 et χ_2 sont des puissances de nombres premiers. Si ces nombres premiers sont différents, les extensions cycliques de k déterminées par χ_1 et χ_2 sont cycliques d'ordres premiers entre eux et la proposition 1.1.71 montre le résultat.

Supposons χ_1 et χ_2 tous les deux d'ordre une puissance de p. Le lemme **??** permet de conclure si p est impair ou si les ordres sont différents. Nous laissons au lecteur le soin de compléter la preuve dans le cas restant, dont les seules complications sont notationnelles. □

1.1.10 Résultats plus avancés

On peut formuler les principaux résultats de la théorie du corps de classe via le groupe de Brauer. Donnons-les brièvement – nous supposons ici connue l'existence des corps $\mathbb{Q}_p$, où p est un nombre premier.

Ce qui suit n'est pas très loin du corps de classe local.

Théorème 1.1.92. *Soit p un nombre premier. Il existe un isomorphisme canonique*

$$Br(\mathbb{Q}_p) \simeq \mathbb{Q}/\mathbb{Z}.$$

De plus, toute algèbre simple centrale sur $\mathbb{Q}_p$ est cyclique.

Remarque 1.1.93. *Il existe un unique élément de degré 2 dans $\mathbb{Q}/\mathbb{Z}$, ce qui signifie qu'il existe une unique algèbre de quaternion non-déployée sur $\mathbb{Q}_p$.*

La théorie du corps de classe global est essentiellement équivalente au résultat suivant (ou mieux, à sa variante sur un corps de nombre arbitraire).

Théorème 1.1.94 (Albert-Brauer-Hasse-Noether)**.** *Les flèches naturelles $Br(\mathbb{Q}) \to Br(\mathbb{Q}_p), [A] \mapsto [A \otimes_{\mathbb{Q}} \mathbb{Q}_p]$, où p est un nombre premier, et $Br(\mathbb{Q}) \to Br(\mathbb{R}), [A] \mapsto [A \otimes_{\mathbb{Q}} \mathbb{R}]$ induisent une suite exacte*

$$0 \to Br(\mathbb{Q}) \to \Big(\bigoplus_p \mathbb{Q}/\mathbb{Z}\Big) \oplus Z/2\mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \to 0$$

où la dernière application est la somme.

Remarque 1.1.95. *Le seul fait que la flèche $Br(\mathbb{Q}) \to \big(\bigoplus_p \mathbb{Q}/\mathbb{Z}\big) \oplus Z/2\mathbb{Z}$ soit bien définie n'est pas trivial. Appliqué aux algèbres de quaternions, le fait que la suite $Br(\mathbb{Q}) \to \big(\bigoplus_p \mathbb{Q}/\mathbb{Z}\big) \oplus Z/2\mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \to 0$ soit exacte généralise la loi de réciprocité quadratique.*

Remarque 1.1.96. *Appliqué aux algèbres de quaternions, le résultat ci-dessus permet de retrouver le théorème de Hasse-Minkowski – on le verra plus loin.*

On peut montrer comme conséquence de ce qui précède :

Théorème 1.1.97. *Soit A une algèbre simple centrale sur un corps de nombres. Alors A est cyclique.*

1.2 Ordres dans les algèbres à division sur $\mathbb{Q}$ – finitudes

1.2.1 Ordres et idéaux dans les $\mathbb{Q}$-algèbres, énoncés

Soit R un anneau principal, et soit K son corps des fractions.

Définition 1.2.1. *Soit A une K-algèbre de dimension finie. Un R-ordre de A est une sous-R-algèbre $\mathcal{O}$ de A telle que*

(i) $\mathcal{O}$ est un R-module de type fini ;

(ii) la flèche naturelle $\mathcal{O} \otimes_R K \to A$ est un isomorphisme.

On dit que $\mathcal{O}$ est maximal s'il est maximal pour l'inclusion.

On parlera souvent d'ordre sans référence à R si le contexte est clair. En particulier, on considèrera souvent le cas $R = \mathbb{Z}$.

Exemple 1.2.1.1. *Si n est un entier, la $\mathbb{Z}$-algèbre $\mathbb{Z} + in\mathbb{Z}$ est un ordre de $\mathbb{Q}[i]$.*

Remarque 1.2.2. *La propriété (ii) peut se reformuler de manière plus simple. Soit en effet $\mathcal{O}$ une sous-R-algèbre de A, finie comme R-module. Alors $\mathcal{O}$ est sans torsion car A l'est, et la flèche naturelle $\mathcal{O} \otimes_R K \to A$ est injective comme on le voit par exemple en prenant une base de $\mathcal{O}$, d'image le sous-K-espace vectoriel de A engendré par $\mathcal{O}$. La propriété (ii) signifie donc*

$$\forall a \in A, \exists c \in R \setminus \{0\}, ca \in \mathcal{O}.$$

Autrement dit, $\mathcal{O}$ engendre A comme K-espace vectoriel.

Proposition 1.2.3. *Soit A une K-algèbre de dimension finie.*

(i) Soit $\mathcal{O}$ une sous-R-algèbre de A. Alors $\mathcal{O}$ est un ordre de A si et seulement si $\mathcal{O}$ est isomorphe à $R^{\dim_K A}$ comme R-module.

(ii) Il existe au moins un ordre dans A.

(iii) Soit B une sous-R-algèbre de rang fini de A. Alors B est contenue dans un ordre.

(iv) *Un élément x de A est contenu dans un ordre de A si et seulement si il est entier sur R. En particulier, sa norme et sa trace sont dans R.*

(v) *Si A est commutative, il existe au plus un ordre maximal de A : c'est l'ensemble des éléments de A qui sont entiers sur R.*

Démonstration. (i) L'anneau R est principal, donc tout R-module de type fini sans torsion est libre. En particulier, un ordre $\mathcal{O}$ est un R-module libre, de rang $\dim_K(\mathcal{O} \otimes_R K) = \dim_K(A)$. Réciproquement, supposons que $\mathcal{O}$ est une sous-R-algèbre de A de rang $\dim_K(A)$ comme R-module. Il s'agit de montrer que la flèche naturelle $\mathcal{O} \otimes_R K \to A$ est un isomorphisme. Le lemme précédent garantit qu'elle est injective, d'où la conclusion par égalité des dimensions.

(ii) Soit $(e_i)_{1 \leq i \leq n}$ une base de A sur K, avec $e_1 = 1$. Quitte à multiplier les e_i, $i > 1$ par des éléments de R, on peut supposer que les $e_i.e_j$ sont dans $\sum_i Re_i$. Alors $\sum_i Re_i$ est un ordre de A par le point précédent.

(iii) Soit B une sous-algèbre de A, de type fini comme R-module. Soit $\mathcal{O}$ un ordre de A. Soit $M = \mathcal{O}.B$ le R-module engendré par les ab, $a \in \mathcal{O}$, $b \in B$. C'est un sous R-module de A, de type fini, tel que $M \otimes_R K = A$. Alors

$$\mathcal{O}' := \{x \in A, Mx \subset M\}$$

est un ordre de A qui contient B : il est clair que $\mathcal{O}'$ contient B et engendre A comme K-espace vectoriel. Un calcul explicite montre que $\mathcal{O}'$ est bien de type fini.

(iv) Par définition, l'élément x de A est entier si et seulement si $R[x]$ est un R-module de type fini, ce qui conclut par le point précédent.

(v) Soit $\mathcal{O}$ un ordre de A. Si x est entier, alors l'algèbre engendrée par $\mathcal{O}$ et x est de type fini car engendrée comme algèbre par un nombre fini d'entiers, ce qui conclut.

□

Proposition 1.2.4. *Supposons $K = \mathbb{Q}$, $R = \mathbb{Z}$, et soit A une algèbre simple sur $\mathbb{Q}$. Alors il existe un ordre maximal dans A.*

Démonstration. Considérons l'application bilinéaire

$$\phi : A \times A \to K, (a, b) \mapsto Tr_{A/K}(ab).$$

Alors ϕ est non-dégénérée – se ramener au cas d'une algèbre de matrices. Si x est entier, alors $Tr_{A/K}(x)$ est dans $\mathbb{Z}$, donc en particulier, si $\mathcal{O}$ est un ordre de A, la trace sur $\mathcal{O}$ est à valeurs entières. Si le discriminant de $\mathcal{O}$ est de valeur absolue minimale, alors $\mathcal{O}$ est maximal. □

Remarque 1.2.5. *L'argument s'applique aussi à $K = \mathbb{Q}_p$, $A = \mathbb{Z}_p$.*

Voici quelques exemples. On suppose $R = \mathbb{Z}$, $K = \mathbb{Q}$.

(i) $\mathbb{Z}$ est un ordre dans $\mathbb{Q}$.

(ii) $\mathbb{Z}[i]$ est un ordre dans $\mathbb{Q}[i]$ – ce sont les entiers de Gauss.

(iii) Soit α un élément entier sur $\mathbb{Q}$ qui n'est pas dans $\mathbb{Q}$. Alors $\mathbb{Z}[\alpha]$ est un ordre dans $\mathbb{Q}[\alpha]$. En particulier, pour tout $n \neq 0$, $\mathbb{Z}[n\alpha]$ est un ordre dans $\mathbb{Q}[\alpha]$, qui n'est pas maximal si $n \neq \pm 1$.

(iv) $\mathbb{Z} + \frac{1+\sqrt{5}}{2}\mathbb{Z}$ est un ordre dans $\mathbb{Q}[\sqrt{5}]$.

(v) $M_n(\mathbb{Z})$ est un ordre dans $M_n(\mathbb{Q})$. Il est maximal. Tout conjugué de $M_n(\mathbb{Z})$ est un ordre maximal.

(vi) Soit (a, b) une algèbre de quaternions sur $\mathbb{Q}$, de base standard i, j, k. Alors $\mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$ est un ordre dans (a, b). Ce n'est pas nécessairement un ordre maximal : en effet, considérons dans les quaternions de Hamilton $(-1, -1)$ sur $\mathbb{Q}$ le sous-anneau constitué des $a + bi + cj + dk$ tels que a, b, c, d sont tous soit dans $\mathbb{Z}$, soit dans $\frac{1}{2} + \mathbb{Z}$.

(vii) Soit G un groupe fini, $\mathbb{Q}[G]$ son algèbre de groupe. Alors $\mathbb{Z}[G]$ est un ordre dans $\mathbb{Q}[G]$.

Remarque 1.2.6. *Il est faux en général qu'un ordre (même maximal) dans un anneau d'entiers de corps de nombres soit engendré comme $\mathbb{Z}$-algèbre par un unique élément.*

Proposition 1.2.7. *Soit A une K-algèbre simple centrale, et soit $\mathcal{O}$ un ordre de A. Soit $x \in \mathcal{O}$. Alors x est inversible dans $\mathcal{O}$ si et seulement si $N_{A/k}(x)$ est inversible dans R.*

Démonstration. Si x est inversible, sa norme est inversible par multiplicativité.

Réciproquement, supposons que la norme de x est inversible dans R. Soit $e_1, \ldots, e_n$ une base de $\mathcal{O}$ sur R. La matrice de la multiplication à gauche par x est à coefficients dans R, et son déterminant est $N_{A/k}(x)$. Comme il est inversible dans R, cette matrice est inversible dans $GL_n(R)$, donc x est inversible à gauche dans $\mathcal{O}$. De même – comme A est simple centrale, $N_{A/k}(x)$ est définie aussi bien par la multiplication à gauche qu'à droite – x est inversible à droite, ce qui conclut. □

On va maintenant se restreindre pour fixer les idées au cas d'une algèbre à division D sur $K = \mathbb{Q}$, et de $R = \mathbb{Z}$. Soit $\mathcal{O}$ un ordre dans D.

Définition 1.2.8. *Soient I et J des idéaux à gauche non-nuls de $\mathcal{O}$. On dit que I et J sont équivalents, et on note $I \sim J$, s'il existe $\alpha \in D$ tel que $I\alpha = J$. On note $Cl(\mathcal{O})$ l'ensemble des classes d'équivalence d'idéaux à gauche non-nuls de A. C'est* l'ensemble des classes d'idéaux *de $\mathcal{O}$.*

Proposition 1.2.9. *Un idéal à gauche de $\mathcal{O}$ est un $\mathcal{O}$-sous-module à gauche de type fini de $\mathcal{O}$. Si I est non-nul, on a $I \otimes_{\mathbb{Z}} \mathbb{Q} = D$. Réciproquement, tout $\mathcal{O}$-module M de type fini sans torsion tel que $M \otimes_{\mathbb{Z}} \mathbb{Q} \simeq D$ comme D-modules à gauche est isomorphe à un idéal de $\mathcal{O}$.*

Démonstration. La première assertion est claire. La seconde suit de la Remarque 1.2.2.

Réciproquement, soit M comme dans l'énoncé de la proposition. Choisissons un isomorphisme de D-modules à gauche

$$\phi : M \otimes_{\mathbb{Z}} \mathbb{Q} \to D.$$

Quitte à multiplier ϕ par un entier non nul, on peut supposer que ϕ envoie M dans $\mathcal{O}$. L'image de M est alors un idéal de $\mathcal{O}$. □

Remarque 1.2.10. *La même preuve montrerait que tout $\mathcal{O}$-module de type fini à gauche M sans torsion tel que $M \otimes_{\mathbb{Z}} \mathbb{Q} \simeq D^n$ est isomorphe à un sous $\mathcal{O}$-module de $\mathcal{O}^n$.*

Proposition 1.2.11. *Soient I et J deux idéaux à gauche non-nuls de $\mathcal{O}$. Alors $I \sim J$ si et seulement si I et J sont isomorphes comme $\mathcal{O}$-modules.*

Démonstration. Soit $\alpha \in D$, nécessairement non-nul, tel que $I\alpha = J$. Alors l'application

$$x \mapsto x\alpha$$

est un isomorphisme de $\mathcal{O}$-modules de I vers J.

Réciproquement, soit

$$\phi : I \to J$$

un isomorphisme de $\mathcal{O}$-modules. Il s'étend en un isomorphisme de D-modules

$$D = I \otimes_{\mathbb{Z}} \mathbb{Q} \to J \otimes_{\mathbb{Z}} \mathbb{Q} = D,$$

nécessairement donné par la multiplication par un $\alpha \in D$. □

Exemple 1.2.1.2. *Si D est commutative – autrement dit, si D est un corps – alors idéaux à gauche et à droite coïncident, et le produit de deux idéaux non nuls est un idéal non nul. La relation d'équivalence est compatible au produit et l'ensemble des classes d'idéaux de $\mathcal{O}$ est un monoïde abélien, que l'on peut aussi définir comme le monoïde des idéaux de $\mathcal{O}$ modulo le sous-monoïde des idéaux principaux.*

Remarque 1.2.12. *On verra plus tard que si $\mathcal{O}$ est maximal et D commutatif – autrement dit, $\mathcal{O}$ est l'anneau des entiers d'un corps de nombres grâce à la proposition 1.2.3 – le monoïde des idéaux modulo équivalence est en fait un groupe : le groupe de classes.*

Remarque 1.2.13. *Si $\mathcal{O}$ est un anneau principal, alors tous les idéaux non nuls sont équivalents.*

Donnons un exemple. Soit $n \geq 1$, et $d \geq 1$. Soit $\mathcal{O}_n$ l'ordre $\mathbb{Z} + ni\sqrt{d}\mathbb{Z}$ dans $\mathbb{Q}[i\sqrt{d}]$. Un idéal de $\mathcal{O}_n$ est un sous-réseau [2] de $\mathcal{O}_n$ dans $\mathbb{C}$, stable par multiplication par $ni\sqrt{d}$. Deux idéaux sont équivalents si et seulement si ils sont envoyés l'un sur l'autre par une similitude du plan.

Si $n = 1$ et $d = 1$, on peut expliciter : un idéal de $\mathbb{Z}[i]$ est sous-réseau de $\mathbb{Z}^2 = \mathbb{Z}+\mathbb{Z}i$ stable par la multiplication par i –la rotation d'angle $\pi/2$. Un tel réseau est toujours de la forme $\mathbb{Z}\alpha + \mathbb{Z}i\alpha$, où α est un élément de plus petite norme du réseau. Tous les tels réseaux sont équivalents sous l'action des similitudes du plan. On en déduit ce qui suit.

Proposition 1.2.14. *L'anneau $\mathbb{Z}[i]$ est principal.*

Voici un exemple classique d'application : soit p un nombre premier congru à 1 modulo 4. On sait que -1 est un carré dans $\mathbb{F}_p$. Autrement dit, on peut trouver a dans $\mathbb{Z}$ tel que $a^2 + 1$ est divisible par p. Soit I l'idéal

$$I = (a + i, p)$$

dans $\mathbb{Z}[i]$. On peut trouver α tel que $I = \alpha\mathbb{Z}[i]$. Comme p est dans I, on peut trouver β tel que $\alpha\beta = p$. En particulier, on a $p^2 = N(\alpha)N(\beta)$, N désignant la norme de $\mathbb{Q}[i]$, de sorte que trois cas peuvent se présenter :

1. $N(\alpha) = p^2$, $N(\beta) = 1$. Alors β est inversible et l'on peut supposer $\alpha = p$, $I = p\mathbb{Z}[i]$, contradiction car $a + i$ n'est pas divisible par p ;
2. $N(\alpha) = 1$, $N(\beta) = p^2$. De même, $I = \mathbb{Z}[i]$, ce qui contredit le fait que pour tout $x + iy$ dans I, $x^2 + y^2$ est divisible par p.
3. $N(\alpha) = N(\beta) = p$, donc, notant $\alpha = x + iy$, on a $x^2 + y^2 = p$.

On a finalement montré, la réciproque étant claire :

Proposition 1.2.15 (Fermat)**.** *Soit p un nombre premier. Alors p est somme de deux carrés d'entiers si et seulement si $p = 2$ ou p est congru à 1 modulo 4.*

Le même genre d'arguments permet de trouver facilement des exemples non principaux. Prenons $d = 5$, et $\mathcal{O} = \mathbb{Z}[i\sqrt{5}]$. L'élément de plus petite norme de $\mathcal{O}$ est 1, l'élément de plus petite norme qui lui est linéairement indépendant est $i\sqrt{-5}$. Ces deux éléments forment une base orthogonale, et tout réseau de $\mathcal{O}$ qui est semblable à $\mathcal{O}$ vérifie la même propriété. Soit $I = 2\mathbb{Z} + (1 + i\sqrt{5})\mathbb{Z}$. C'est bien un idéal de $\mathcal{O}$. Son élément de plus petite norme est 2, le plus petit qui lui est linéairement indépendant est $1 + i\sqrt{5}$. Ces deux vecteurs ne sont pas orthogonaux, donc I n'est pas principal.

Énonçons maintenant les deux principaux théorèmes de finitude. On énoncera le premier dans le cadre un peu plus général des algèbres semi-simples.

2. ici, un sous $\mathbb{Z}$-module de rang 2

Définition 1.2.16. *Soit A une algèbre de dimension finie sur un corps. On dit que A est semi-simple si A est produit d'algèbres simples.*

Nous introduisons cette définition afin d'incorporer l'exemple de l'algèbre d'un groupe fini, qui est semi-simple (nous ne démontrons pas ce fait, pas très difficile).

Théorème 1.2.17 (Jordan-Zassenhaus)**.** *Soit A une algèbre semi-simple de dimension finie sur $\mathbb{Q}$, et soit $\mathcal{O}$ un $\mathbb{Z}$-ordre de A. Soit M_A un A-module de type fini sans torsion. Alors l'ensemble de classes d'isomorphismes de $\mathcal{O}$-modules à gauche M de type fini tels que $M \otimes_{\mathbb{Z}} \mathbb{Q} \simeq M_A$ est fini.*

Théorème 1.2.18. *Soit D une algèbre à division de dimension finie sur $\mathbb{Q}$, et soit $\mathcal{O}$ un $\mathbb{Z}$-ordre de D. Alors $\mathcal{O}^*$ est cocompact dans*

$$D^1_{\mathbb{R}} := \{x \in D_{\mathbb{R}}, N_{D_{\mathbb{R}}/\mathbb{R}}(x) = \pm 1\}.$$

Un cas particulier important du théorème 1.2.17 correspond au cas où A est une algèbre à division et $M_A = A$. Via les résultats précédents, on trouve :

Théorème 1.2.19. *Soit D une algèbre à division de dimension finie sur $\mathbb{Q}$, et soit $\mathcal{O}$ un $\mathbb{Z}$-ordre de D. Alors l'ensemble des classes d'idéaux de $\mathcal{O}$ est fini.*

Voici quelques rappels autour du théorème 1.2.18. Soit G un groupe topologique séparé, localement compact, et soit Γ un sous-groupe discret de G (autrement dit, Γ est localement fini dans G). On dit que Γ est *cocompact* dans G si l'espace topologique quotient G/Γ est compact. Remarquons que le quotient de G par un groupe discret est toujours séparé.

Comme G/Γ et $\Gamma\backslash G$ sont homéomorphes par $x\Gamma \mapsto \Gamma x^{-1}$, Γ est cocompact si et seulement si $\Gamma\backslash G$ est compact.

Proposition 1.2.20. *Le groupe Γ est cocompact dans G si et seulement si il existe un compact F dans G tel que $G = F\Gamma$.*

Démonstration. Si F est comme dans l'énoncé, la projection de F vers le quotient G/Γ est continue surjective, donc le quotient est compact comme image d'un compact.

Réciproquement, supposons G/Γ compact. La projection $\pi : G \to G/\Gamma$ est un homéomorphisme local car Γ est discret. On recouvre G/Γ par un nombre fini de compacts K_i tels qu'il existe K_i' dans G pour lesquels $\pi_{|K_i'}$ est un isomorphisme vers K_i. Alors les K_i' sont compacts et leur union F satisfait les propriétés désirées. □

Exemple 1.2.1.3. *Soit V un espace vectoriel réel de dimension finie. Les sous-groupes discrets cocompacts de V sont les réseaux de V : les sous-groupes discrets qui engendrent V comme espace vectoriel réel.*

Le proposition 1.2.7 garantit que les éléments de $\mathcal{O}^*$ sont exactement les éléments de $\mathcal{O}$ dont la norme vaut ± 1. Le groupe $\mathcal{O}^*$ est donc bien un sous-groupe de $D^1_{\mathbb{R}}$. Comme $\mathcal{O}$ est discret dans $D_{\mathbb{R}}$, $\mathcal{O}^*$ est discret dans $D^*_{\mathbb{R}}$.

Le théorème 1.2.18 est faux si D n'est pas une algèbre à division, comme le montre ce qui suit.

Proposition 1.2.21. *Le groupe $SL_n(\mathbb{Z})$ n'est pas cocompact dans $SL_n(\mathbb{R})$ si $n > 1$.*

Démonstration. Raisonnons par l'absurde et supposons $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$ compact. Pour $k > 0$, considérons M_k la matrice diagonale de coefficients $(1/k, k, 1, \ldots, 1)$. L'image du vecteur e_1 par M_k est $\frac{1}{k}e_1$. Soit M un élément de $SL_n(\mathbb{R})$ dont l'image dans le quotient est une valeur d'adhérence de la suite des images des M_k. Pour k suffisamment grand dans une sous-suite, M_k est proche de MN_k, avec N_k dans $SL_n(\mathbb{Z})$. En particulier, $\frac{1}{k}e_1$ est proche de $M(v_k)$ pour un certain v_k dans $\mathbb{Z}^n \setminus \{0\}$, ce qui signifie que v_k tend vers 0, contradiction. □

1.2.2 Applications

Soit K un corps de nombre, c'est-à-dire une extension finie de $\mathbb{Q}$. Donnons une forme explicite du théorème 1.2.18 pour $D = K$. Soit $d = [K : \mathbb{Q}]$. Dans ce contexte, le théorème est le théorème des unités de Dirichlet.

Proposition 1.2.22. *Soit r_1 le nombre de plongements de K dans $\mathbb{R}$, et r_2 le nombre de plongements de K dans $\mathbb{C}$ qui n'envoient pas K dans $\mathbb{R}$, à conjugaison complexe près. Alors $d = r_1 + 2r_2$ et l'on a un isomorphisme de $\mathbb{R}$-algèbres*

$$K_{\mathbb{R}} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

Démonstration. Le nombre de plongements de K dans $\mathbb{C}$ est égal à d. Par définition de r_1 et r_2, il vaut $r_1 + 2r_2$.

Le théorème de l'élément primitif nous permet d'écrire $K = \mathbb{Q}[X]/(P)$, où P est un polynôme unitaire irréductible sur $\mathbb{Q}$. Les plongements de K dans $\mathbb{R}$ sont en bijection avec les racines réelles de P, et les couples de plongements complexes conjugués de K dans $\mathbb{C}$ sont en bijection avec les couples de racines complexes conjuguées de P. Couplant cette remarque à la factorisation de P sur $\mathbb{R}$ et au théorème des restes chinois, on conclut. □

Remarquons que si $\sigma_1, \ldots, \sigma_{r_1}$ sont les plongements de K dans $\mathbb{R}$, et si $\tau_1, \ldots, \tau_{r_2}$ sont des représentants des autres plongements de K dans $\mathbb{C}$ à conjugaison complexe près, alors l'isomorphisme de la proposition (au choix des τ_i près) est induit par

$$K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, x \mapsto (\sigma_1(x), \ldots, \sigma_{r_1}(x), \tau_1(x), \ldots, \tau_{r_2}(x)).$$

En particulier, via cet isomorphisme, la norme d'un élément x de $K_{\mathbb{R}}$ identifié à $(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2})$, est

$$N_{K_{\mathbb{R}}/\mathbb{R}}(x) = x_1 \ldots x_{r_1} |z_1|^2 \ldots |z_{r_2}|^2.$$

Soit $\mathbb{S}$ le cercle unité dans $\mathbb{C}$. On a un isomorphisme naturel de groupes topologiques

$$K_{\mathbb{R}}^* \simeq \{\pm 1\}^{r_1} \times \mathbb{S}^{r_2} \times \mathbb{R}^{r_1+r_2}.$$

Via cet isomorphisme, le groupe $K_{\mathbb{R}}^1$ des éléments de norme ± 1 s'identifie au noyau de $s \circ p$, où p est la projection sur $\mathbb{R}^{r_1+r_2}$ et s l'application somme des coordonnées. Au final, $K_{\mathbb{R}}^1$ est le produit

$$\{\pm 1\}^{r_1} \times \mathbb{S}^{r_2} \times \mathrm{Ker}(s),$$

où le dernier facteur est un espace vectoriel réel de dimension $r_1 + r_2 - 1$.

Soit $\mathcal{O}$ un ordre de K. Le théorème 1.2.18 signifie que l'on a une suite exacte de groupes abéliens

$$1 \to \mathcal{O}^* \cap \mathrm{Ker}(p) \to \mathcal{O}^* \to p(\mathcal{O}^*) \to 0,$$

où le premier terme est discret dans le groupe compact $\{\pm 1\}^{r_1} \times \mathbb{S}^{r_2}$ – donc fini – et le dernier est un réseau dans $\mathrm{Ker}(s)$ – c'est en particulier un groupe abélien libre de rang $r_1 + r_2 - 1$.

Le premier terme est exactement l'ensemble des éléments de $\mathcal{O}^*$ dont la norme après tout plongement dans $\mathbb{C}$ est 1. Comme c'est un groupe fini, ces éléments sont tous des racines de l'unité – c'est le théorème de Kronecker.

Exemple 1.2.2.1 (Équation de Pell-Fermat)**.** *On considère $\mathcal{O} = \mathbb{Z} + \sqrt{d}\mathbb{Z}$, où d est un entier positif qui n'est pas un carré. Alors $\mathcal{O}^*$ s'identifie à l'ensemble des $(x, y) \in \mathbb{Z}^2$ tels que*

$$x^2 - dy^2 = \pm 1.$$

Il s'agit d'après ce qui précède du produit de $\{\pm 1\}$ – le groupe des unités de $\mathcal{O}$ – par un groupe abélien libre de rang 1.

Dans le cas non-commutatif, on obtient des groupes intéressants. Voici un cas particulier.

Proposition 1.2.23. *Soit D une algèbre de quaternions non déployée sur $\mathbb{Q}$, déployée sur $\mathbb{R}$. Soit $\mathcal{O}$ un ordre de D. Alors $\Gamma = \mathcal{O}^* N_{D/Q}^{-1}(1)$ est un sous-groupe discret cocompact de $D_{\mathbb{R}}^1 \simeq SL_2(\mathbb{R})$.*

Le groupe $SL_2(\mathbb{R})$ agit par homographies sur le demi-plan de Poincaré $\mathbb{H}$. Le stabilisateur de i est le groupe $SO_2(\mathbb{R})$. Le quotient $SL_2(\mathbb{R})/SO_2(\mathbb{R})$ s'identifie donc

à $\mathbb{H}$. Si Γ est de plus sans torsion – ce qui est le cas après passage à un sous-groupe d'indice fini, il agit donc sur $\mathbb{H}$ de sorte que le quotient $\Gamma\backslash\mathbb{H}$ soit une surface de Riemann compacte.

On donne une application du théorème de Jordan-Zassenhaus à la théorie des groupes finis.

Théorème 1.2.24. *Soit G un groupe fini, et soit V une représentation de G dans un $\mathbb{Q}$-espace vectoriel de dimension fini. Il existe un nombre fini de représentations de G dans un $\mathbb{Z}$-module libre de type fini qui deviennent isomorphe à V après extension des scalaires à $\mathbb{Q}$.*

Démonstration. Il s'agit exactement du théorème de Jordan-Zassenhaus appliqué à l'algèbre de groupe $\mathbb{Q}[G]$ et à son ordre $\mathbb{Z}[G]$. En effet, une représentation V est un $\mathbb{Q}[G]$-module à gauche, et une représentation de G dans un $\mathbb{Z}$-module libre de type fini M correspond à une structure de $\mathbb{Z}[G]$-module à gauche sur M. □

Corollaire 1.2.25. *Soit n un entier strictement positif. Il n'existe qu'un nombre fini de classes de conjugaison de sous-groupes fini dans $GL_n(\mathbb{Z})$.*

Démonstration. On sait (ou on admet) que les sous-groupes finis de $GL_n(\mathbb{Z})$ s'injectent dans $GL_n(\mathbb{Z}/3\mathbb{Z})$. En particulier, il n'y en a qu'un nombre fini à isomorphisme près.

Soit maintenant G un groupe fini. Se donner un plongement de G dans $GL_n(\mathbb{Z})$, c'est se donner une action de G sur $\mathbb{Z}^n$. Deux telles actions sont isomorphes si et seulement si les plongements correspondants de G dans $GL_n(\mathbb{Z})$ sont conjugués. Ainsi, pour montrer le résultat, le théorème de Jordan-Zassenhaus nous ramène à montrer qu'un groupe fini G n'a qu'un nombre fini de représentations de dimension finie donnée sur $\mathbb{Q}$, ce qui est bien connu. □

1.2.3 Géométrie des nombres

Soit V un espace vectoriel réel de dimension finie n, munie de sa topologie naturelle. Un réseau de V est un sous-groupe L discret cocompact de V. La discrétude de L est équivalente au fait que $L \cap K$ est fini pour tout compact K de L, ou encore que 0 est point isolé de L.

On laisse la proposition suivante en exercice.

Proposition 1.2.26. *Soit L un sous-groupe de V.*

(i) Si L est discret, alors L est un groupe libre de rang $r \leq n$, et $V/L \simeq (\mathbb{R}/\mathbb{Z})^r \times \mathbb{R}^{n-r}$. En particulier, L est alors un réseau si et seulement si L est libre de rang n.

(ii) *L est un réseau si et seulement si L admet une famille génératrice qui est une $\mathbb{R}$-base de V.*

(iii) *L est un réseau si et seulement si il existe un isomorphisme $f : V \to \mathbb{R}^n$ tel que $f(L) = \mathbb{Z}^n$.*

Soit L un réseau dans V, et soit μ une mesure de Lebesgue sur V, i.e. une mesure borélienne non nulle, finie sur les compacts, invariante par translation. On sait qu'une telle mesure est unique à multiplication par un scalaire près, et qu'elle est toujours égale à la mesure de Lebesgue sur $\mathbb{R}^n$ après choix d'un isomorphisme $V \simeq \mathbb{R}^n$.

L'application quotient

$$p : V \to V/L$$

est un homéomorphisme local, et préserve donc les ensembles mesurables.

Définition 1.2.27. *Un domaine fondamental D est un sous-ensemble mesurable de V tel que $p_{|V} : D \to V/L$ est un isomorphisme.*

Autrement dit, tout élément de V s'écrit de manière unique sous la forme $\lambda + x$, $x \in D$.

Il existe des domaines fondamentaux : si $e_1, \ldots, e_n$ est une base de L, alors

$$\sum_{i=1}^{n} [0, 1[e_i$$

est un domaine fondamental.

Lemme 1.2.28. *Soient D et D' deux domaines fondamentaux, et soit E un sous-ensemble mesurable de V/L. Alors*

$$\mu(p^{-1}(E) \cap D) = \mu(p^{-1}(E) \cap D').$$

Démonstration. L'ensemble $p^{-1}(E) \cap D$ est réunion disjointe des $p^{-1}(E) \cap D \cap (D' + \lambda)$, $\lambda \in L$. L'invariance par translation de la mesure μ garantit l'égalité

$$\mu(p^{-1}(E) \cap D \cap (D' + \lambda)) = \mu(p^{-1}(E) \cap (D - \lambda) \cap D').$$

Sommer sur tous les λ donne l'égalité cherchée. □

Le lemme ci-dessus montre en particulier que la mesure d'un domaine fondamental est un invariant du réseau L.

Définition 1.2.29. *Le covolume de L (dans L, relativement à μ), noté* $\mathrm{covol}(L)$*, est la mesure d'un domaine fondamental pour L.*

Le covolume de L dépend du choix de la mesure μ. Le lemme ci-dessus permet de définir une mesure, encore notée μ, sur le quotient V/L, par la formule

$$\mu(E) = \mu(p^{-1}(E) \cap D),$$

où D est un domaine fondamental pour L dans V.

Exemple 1.2.3.1. *Soit L' un sous-réseau de L. Si D est un domaine fondamental de L dans V, et si $\lambda_1, \ldots, \lambda_r$ est un système de représentants de L/L' dans L. Alors l'union disjointe des $\lambda_i + D$ est un domaine fondamental de L' dans V, ce qui donne en particulier*

$$\mathrm{covol}(L') = \mathrm{covol}(L)[L : L'].$$

Ce qui suit est une conséquence immédiate de la formule du changement de variable.

Proposition 1.2.30. *Soit $e_1, \ldots, e_n$ une base de V sur $\mathbb{R}$, telle que $\mu(\sum_{i=1}^n [0,1[e_i) = 1$. Soient $\lambda_1, \ldots, \lambda_n$ des éléments de L. Les λ_i forment une base de L si et seulement si le déterminant des λ_i dans la base $e_1, \ldots, e_n$ est égal à $\mathrm{covol}(L)$ en valeur absolue.*

Énonçons maintenant les deux théorèmes fondamentaux de géométrie des nombres.

Théorème 1.2.31 (Blichtfeld)**.** *Soit V un espace vectoriel réel de dimension finie, et soit L un réseau de V. Soit μ une mesure de Lebesgue sur V.*

(i) Soit X une partie mesurable de V. Si $\mu(X) > \mathrm{covol}(L)$, alors

$$\exists (x, y) \in X^2, x - y \in L \setminus \{0\}.$$

(ii) Soit X une partie compacte de V. Si $\mu(X) \geq \mathrm{covol}(L)$, alors

$$\exists (x, y) \in X^2, x - y \in L \setminus \{0\}.$$

Démonstration. (i) Il faut montrer que la restriction de $p : V \to V/L$ à X n'est pas injective. Soit D un domaine fondamental pour L. On écrit X comme réunion disjointe des $X \cap (\lambda + D)$, $\lambda \in L$. Alors $\mu(X)$ est somme des $\mu(X \cap (\lambda + D))$, soit, comme μ est invariante par translation, somme des $\mu((X + \lambda) \cap (D))$.

Si la restriction de p à X est injective, les $(X+\lambda)\cap D$ sont deux à deux disjoints, ce qui montre que la somme des $\mu((X+\lambda)\cap(D))$ est inférieure ou égale à $\mu(D)$, i.e. au covolume de L, ce qui est la contradiction attendue.

(ii) On applique le résultat à un système de voisinages ouverts de X dans V et on conclut par compacité.

□

Théorème 1.2.32 (Minkowski)**.** *Soient V, L et μ comme dans le théorème précédent, et soit n la dimension de V. Soit X une partie mesurable de V, convexe et symétrique.*

(i) Si $\mu(X) > 2^n \mathrm{covol}(L)$, alors $X \cap (L \setminus \{0\})$ est non-vide.

(ii) Si X est compact et $\mu(X) \geq 2^n \mathrm{covol}(L)$, alors $X \cap (L \setminus \{0\})$ est non-vide.

Démonstration. Il suffit d'appliquer le théorème de Blichtfeld à $Y = \frac{1}{2}X$. □

Un cas particulièrement utile du théorème de Minkowski est celui où V est muni d'une norme euclidienne $||.||$. Dans ce cas, on prend pour μ la mesure de Lebesgue pour laquelle, si $e_1, \ldots, e_n$ est une base orthonormée de V, on a

$$\mu(\sum_{i=1}^{n} [0,1[e_i) = 1.$$

Soit V_n le volume de la boule unité dans V – on utilisera plus tard dans le cours sa valeur précise, mais ce n'est pas nécessaire pour le moment. Appliqué à X la boule unité fermée de rayon $R > 0$, le théorème de Minkowski nous donne l'estimée suivante.

Théorème 1.2.33. *Soit L un réseau dans V muni de la norme euclidienne $||.||$. Il existe un élément λ de $L \setminus \{0\}$ tel que*

$$||\lambda||^n \leq \frac{2^n}{V_n} \mathrm{covol}(L).$$

Ce qui suit est une variante qui donne un résultat plus général, mais implique des constantes moins bonnes.

Théorème 1.2.34 (Hermite)**.** *Soit L un réseau dans V muni de la norme euclidienne $||.||$. Il existe des éléments $\lambda_1, \ldots, \lambda_n$ de L, linéairement indépendants, tels que*

$$||\lambda_1|| \ldots ||\lambda_n|| \leq C_n \mathrm{covol}(L),$$

où C_n est une constante ne dépendant que de n.

Remarque 1.2.35. *La preuve ci-dessous précise une valeur possible de la constante C_n.*

Démonstration. On raisonne par récurrence sur la dimension n de V. Si $n = 0$, il n'y a rien à démontrer et le résultat est clair si $n = 1$. On suppose le théorème prouvé en dimension au plus $n - 1$. Soit λ_1 non-nul de norme minimal.

On considère maintenant le réseau $L/\mathbb{Z}\lambda_1$ dans $V/\mathbb{R}\lambda_1$ muni de la norme euclidienne induite. On vérifie immédiatement (compléter λ_1 en une base de L et calculer

sur le domaine fondamental standard) l'égalité $\mathrm{covol}(L) = \mathrm{covol}(L/\mathbb{Z}\lambda_1)||\lambda_1||$. Appliquant l'hypothèse de récurrence, on trouve $\gamma_2, \ldots, \gamma_n$ dans $L/\mathbb{Z}\lambda_1$, linéairement indépendants, tels que

$$||\gamma_2|| \ldots ||\gamma_n|| \leq C_{n-1} \frac{1}{||\lambda_1||} \mathrm{covol}(L),$$

soit

$$||\lambda_1|| \, ||\gamma_2|| \ldots ||\gamma_n|| \leq C_{n-1} \mathrm{covol}(L).$$

Soit maintenant, pour $2 \leq i \leq n$, un élément λ_i de L relevant γ_i. Si $\lambda_{i,\mathbb{R}} \in V$ est le relèvement orthogonal de γ_i, alors $||\lambda_{i,\mathbb{R}}|| = ||\gamma_i||$ et λ_i est de la forme $\lambda_{i,\mathbb{R}} + x\lambda_1$, $x \in \mathbb{R}$. On peut supposer $-1/2 \leq x < 1/2$. Alors

$$||\lambda_i|| \leq ||\gamma_i|| + 1/2||\lambda_1|| \leq ||\gamma_i|| + 1/2||\lambda_i||.$$

Finalement, on a

$$||\lambda_i|| \leq 2||\gamma_i||.$$

Cela complète la preuve. □

1.2.4 Preuve des théorèmes de finitude

On prouve les théorèmes 1.2.17 et 1.2.18. Pour simplifier – et parce que c'est suffisant pour les applications à la suite du cours – on ne prouve le théorème 1.2.17 que pour les algèbres à division. On peut ramener (mais ce n'est pas facile) le cas général à cette situation.

Quelques généralités pour commencer : soit D une algèbre à division sur $\mathbb{Q}$ de dimension n. On choisit une norme euclidienne $||.||$ sur $D_\mathbb{R}$, μ la mesure de Lebesgue associée sur $D_\mathbb{R}$, $\mathcal{O}$ un ordre de D. Soit $N = N_{D_\mathbb{R}/\mathbb{R}}$. Bien sûr, $D_\mathbb{R}$ n'est pas en général une algèbre à division.

Commençons tout d'abord par remarquer que $\mathcal{O}$ est un réseau dans D : c'est une conséquence de la proposition 1.2.26.

Voici d'abord comment la norme est liée aux calculs de volumes.

Proposition 1.2.36. *(i) Soit $X \subset D_\mathbb{R}$ mesurable, et $x \in D_\mathbb{R}$. Alors $\mu(xX) = |N(x)|\mu(X)$.*

(ii) Soit L un réseau dans $D_\mathbb{R}$, $x \in A_\mathbb{R}^*$. Alors xL est un réseau de $D_\mathbb{R}$ de covolume $|N(x)|\mathrm{covol}(L)$.

(iii) Soit x un élément non nul de $\mathcal{O}$. Alors $|N(x)| = |\mathcal{O}/x\mathcal{O}|$.

Démonstration. La norme de x est le déterminant de la multiplication par x. Le premier énoncé est donc une conséquence de la formule du changement de variable pour les transformations linéaires.

Prouvons (ii). Il est clair que xL est un réseau de $D_{\mathbb{R}}$: si $(e_i)_i$ est une base de L qui est une base du $\mathbb{R}$-espace vectoriel $D_{\mathbb{R}}$, alors $(xe_i)_i$ est une base de xL qui est une base du $\mathbb{R}$-espace vectoriel $D_{\mathbb{R}}$. Soit F un domaine fondamental de L. Alors xF est un domaine fondamental de xL et

$$\text{covol}(xL) = \mu(xF) = |N(x)|\mu(F) = |N(x)|\text{covol}(L)$$

d'après ce qui précède.

Soit enfin x un élément non nul de $\mathcal{O}$. Alors

$$\text{covol}(x\mathcal{O}) = |N(x)|\text{covol}(\mathcal{O}) = [\mathcal{O} : x\mathcal{O}]\text{covol}(\mathcal{O})$$

d'après l'exemple 1.2.3.1, ce qui conclut à (iii). □

La proposition ci-dessus est une conséquence formelle du fait que la norme est un polynôme de degré n en les coefficients d'un élément de $D_{\mathbb{R}}$ dans une $\mathbb{R}$-base.

Proposition 1.2.37. *Il existe une constante C telle que*

$$\forall x \in D_{\mathbb{R}}, |N(x)| \leq C||x||^n.$$

On commence par prouver le théorème 1.2.17. Les D-modules de type fini sont tous libres. Il faut donc montrer qu'il n'existe qu'un nombre fini de $\mathcal{O}$-modules (à gauche) M sans torsion tel que $M \otimes_{\mathbb{Z}} \mathbb{Q} \simeq D^r$.

Soit donc M un tel $\mathcal{O}$-module. Considérons la flèche – injective car M est sans torsion

$$M \hookrightarrow M \otimes_{\mathbb{Z}} \mathbb{Q} \simeq D^r.$$

Quitte à la multiplier par un entier non nul suffisamment divisible, on peut supposer qu'elle envoie M dans $\mathcal{O}^r$. On considère donc M comme un sous-$\mathcal{O}$-module de $\mathcal{O}^r$. On munit $D_{\mathbb{R}}^r$ (et ses sous-espaces) de la norme euclidienne $||.||$ induite par celle de $D_{\mathbb{R}}$, et de la mesure de Lebesgue correspondante.

Lemme 1.2.38. *On peut trouver $\gamma_1, \ldots, \gamma_r$ dans M, linéairement indépendants sur D, tels que*

$$(||\gamma_1|| \ldots ||\gamma_r||)^n \leq C\text{covol}(M),$$

où C est une constante indépendante de M.

Démonstration. Appliquons le théorème 1.2.34. On trouve $\lambda_1, \ldots, \lambda_{nr}$ dans M, linéairement indépendants, tels que $||\lambda_1|| \leq \ldots \leq ||\lambda_{nr}||$ et

$$||\lambda_1|| \ldots ||\lambda_{nr}|| \leq C\text{covol}(M).$$

Définissons les γ_i de manière inductive de telle sorte que i soit le plus petit indice tel que γ_i n'appartient pas à $\sum_{k=1}^{i-1} D\gamma_k$. Alors $\gamma_i = \lambda_j$ avec $j \leq 1 + (i-1)r$. Les γ_i vérifient la condition du lemme. □

Soit $M' = \sum_{i=1}^{r} \mathcal{O}\gamma_i$. Par construction, M est un $\mathcal{O}$-module libre de rang r.

Lemme 1.2.39. *On a*

$$\mathrm{covol}(M') \leq C'\mathrm{covol}(M),$$

où C' est une constante indépendante de M.

Démonstration. Soit γ un élément non-nul de $\mathcal{O}^r$. Alors $\mathcal{O}\gamma$ est engendré sur $\mathbb{Z}$ par des éléments $e_1, \ldots, e_n$ tels que $||e_i|| \leq C'||\gamma||$ pour une certaine constante C – utiliser que la multiplication par un élément de $\mathcal{O}$ est continue.

Il suit de cette remarque que M' est engendré sur $\mathbb{Z}$ par des éléments e_{ij}, $1 \leq i \leq r$, $1 \leq j \leq n$ tels que

$$||e_{ij}|| \leq C'||\gamma_i||.$$

Considérons le déterminant Δ des e_{ij} dans une base orthonormée de $D^r_{\mathbb{R}}$. Le lemme précédent garantit, développant explicitement le déterminant :

$$\mathrm{covol}(M') = |\Delta| \leq (nr)!\Pi_{i,j}||e_{ij}|| \leq (nr)!(C')^{nr}\Pi_i||\gamma_i||^n \leq (nr)!(C')^{nr}C\,\mathrm{covol}(M),$$

ce qui conclut. □

On a montré que M contient un sous-$\mathcal{O}$-module M', libre de rang r, de covolume borné par $C'\mathrm{covol}(M)$. L'exemple 1.2.3.1 permet d'écrire

$$[M : M'] \leq C'.$$

Reformulant, cela montre que M peut s'écrire comme sous-module de D^r, contenant $\mathcal{O}^r$, tel que

$$[M : \mathcal{O}^r] \leq C'.$$

En particulier, on a

$$\mathcal{O}^r \subset M \subset \frac{1}{C'!}\mathcal{O}^r.$$

Il n'existe qu'un nombre fini de réseaux dans D^r contenus entre les deux réseaux ci-dessus. Cela conclut la preuve du théorème 1.2.17 pour les algèbres à division.

On peut préciser le cas des idéaux – i.e. le cas où $r = 1$ – pour obtenir de meilleurs constantes. Dans le lemme 1.2.38, on applique plutôt le théorème 1.2.33 et l'on trouve $\gamma \neq 0$ tel que

$$||\gamma||^n \leq \frac{2^n}{V_n}\mathrm{covol}(M).$$

En particulier,

$$N(\gamma) \leq C\frac{2^n}{V_n}\mathrm{covol}(M),$$

où C est la constante de la proposition 1.2.37. Finalement, la proposition 1.2.4 garantit que tout idéal de $\mathcal{O}$ contient un idéal principal d'indice au plus

$$C\frac{2^n}{V_n}.$$

On verra plus tard comment contrôler la constante C (et on calculera V_n), et en déduire une borne explicite sur le nombre de classes.

Prouvons maintenant le théorème 1.2.18. Il s'agit de montrer que $\mathcal{O}^*$ est cocompact dans $D^1_{\mathbb{R}}$ – l'ensemble des éléments de $D_{\mathbb{R}}$ de norme ± 1.

Soit x un élément de $D^1_{\mathbb{R}}$. Alors x est inversible dans $D_{\mathbb{R}}$ car sa norme l'est, et la proposition montre que $x\mathcal{O}$ est un réseau de $D_{\mathbb{R}}$, de covolume égal à celui de $\mathcal{O}$. Le théorème 1.2.33 montre l'existence d'un élément non-nul t de $x\mathcal{O}$ tel que $||t|| \leq R$, où

$$R = \frac{2^n}{V_n}\mathrm{covol}(x\mathcal{O}) = \frac{2^n}{V_n}\mathrm{covol}(\mathcal{O})$$

est indépendant de x. Par construction, on peut écrire

$$t = xa, x \in \mathcal{O}, a \in \mathcal{O}, |N(a)| = |N(t)|.$$

Autrement dit, on a

$$D^1_{\mathbb{R}} = \{ta^{-1} | a \in \mathcal{O} \cap D^*, t \in D_{\mathbb{R}}, |N(t)| = |N(a)|, ||t|| \leq R\}.$$

Soit k le plus grand entier qui est valeur absolue d'un $N(t)$ pour un $t \in D_{\mathbb{R}}$ de norme au plus R. On a ainsi

$$D^1_{\mathbb{R}} = \bigcup_{i=1}^{k} \{t \in D_{\mathbb{R}} | \, |N(t)| = i, ||t|| \leq R\}\{a \in \mathcal{O} | \, |N(a)| = i\}^{-1}.$$

Le groupe $\mathcal{O}^*$ agit par multiplication à droite sur $\{a \in \mathcal{O} | \, |N(a)| = i\}^{-1}$, i.e. par multiplication à gauche sur $\{a \in \mathcal{O} | \, |N(a)| = i\}$. Comme les $\{t \in D_{\mathbb{R}} | \, |N(t)| = i, ||t|| \leq R\}$ sont compacts, il suffit de montrer que $\mathcal{O}^* \backslash \{a \in \mathcal{O} | \, |N(a)| = i\}$ est compact.

Appliquons la proposition 1.2.4. Soit a un élément de $\mathcal{O}$ tel que $|N(a)| = i$. Alors $a\mathcal{O}$ est d'indice i dans $\mathcal{O}$. De plus, si a et b sont deux éléments de $\mathcal{O} \cap D^*$ tels que $a\mathcal{O} = b\mathcal{O}$, alors a et b diffèrent par multiplication par un élément de $\mathcal{O}^*$. Cela montre que le quotient $\mathcal{O}^* \backslash \{a \in \mathcal{O} | \, |N(a)| = i\}$ s'envoie de manière injective dans l'ensemble des sous-groupes de $\mathcal{O}$ d'indice i, ce qui conclut.

1.3 Anneaux d'entiers de corps de nombres

On va discuter des propriétés basiques de la structure des anneaux d'entiers de corps de nombres – de manière intrinsèque dans une situation relative. Une partie de la discussion vaudrait pour des ordres plus généraux mais on va se restreindre aux anneaux d'entiers pour simplifier.

On ne traite que le cas de la caractéristique nulle. Le cas des extensions finies de $\mathbb{F}_p[T]$ est largement semblable à celui des corps de nombres, mais on n'hésitera pas à utiliser des arguments spécifiques à la caractéristique nulle quand cela permet de simplifier les arguments.

1.3.1 Anneaux de Dedekind et leurs idéaux

Voici la définition essentielle de ce cours.

Définition 1.3.1. *Un corps de nombres est une extension de degré fini du corps $\mathbb{Q}$ des nombres rationnels.*

Soit K un corps de nombres. En particulier, K est une $\mathbb{Q}$-algèbre simple de dimension finie. D'après les propositions 1.2.3 et 1.2.4, K admet un unique ordre maximal : l'anneau des entiers de K, que l'on note $\mathcal{O}_K$.

Proposition 1.3.2. *Soit $\mathcal{O}$ un ordre dans K. Alors $\mathcal{O}$ est noethérien, et tout idéal premier non-nul de $\mathcal{O}$ est maximal – autrement dit,* $\mathrm{Spec}(\mathcal{O})$ *est un schéma de dimension* 1.

Démonstration. Bien entendu, si $\mathcal{O} = \mathbb{Z}$, le résultat est connu.

L'anneau $\mathcal{O}$ est un groupe abélien de type fini par définition. En particulier, toute chaîne croissante de sous-groupes de $\mathcal{O}$ est stationnaire car $\mathbb{Z}$ est noethérien. A fortiori, toute chaîne croissante d'idéaux de $\mathcal{O}$ est stationnaire, ce qui prouve que $\mathcal{O}$ est un anneau noethérien.

Soit $\mathfrak{p}$ un idéal premier non-nul de $\mathcal{O}$. Alors $\mathfrak{p} \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$. Soit α un élément non-nul de $\mathfrak{p}$. Alors α est algébrique sur $\mathbb{Z}$, ce qui permet d'écrire $P(\alpha) = 0$, où P est un polynôme non-nul à coefficients entiers. On peut par ailleurs supposer $P(0) \neq 0$ car $\alpha \neq 0$. On a alors $P(\alpha) \in \mathfrak{p} \cap \mathbb{Z}$, donc $\mathfrak{p} \cap \mathbb{Z}$ est non-nul. C'est donc un idéal maximal engendré par un nombre premier p. Comme $\mathcal{O}$ est un $\mathbb{Z}$-module de type fini, $\mathcal{O}/\mathfrak{p}$ est un $\mathbb{Z}/p\mathbb{Z}$-module de type fini. Comme $\mathcal{O}/\mathfrak{p}$ est intègre, c'est donc un corps, et $\mathfrak{p}$ est maximal. □

Définition 1.3.3. *Un anneau de Dedekind est un anneau intègre noethérien, intégralement clos, dans lequel tout idéal premier non nul est maximal.*

La définition se traduit de manière agréable du point de vue schématique : Un anneau A est de Dedekind si le schéma $\mathrm{Spec}(A)$ est noethérien, normal, de dimension 1. En dimension 1, la normalité est par ailleurs équivalente à la régularité – et ces deux conditions se vérifient sur les anneaux locaux, on le verra directement plus tard.

Soit $\mathcal{O}'$ un ordre arbitraire de K. Alors $\mathcal{O}_K$ est un $\mathcal{O}'$-module de type fini, et l'on dispose d'un morphisme fini

$$\mathrm{Spec}(\mathcal{O}_K) \to \mathrm{Spec}(\mathcal{O}').$$

Le schéma $\mathrm{Spec}(\mathcal{O}_K)$ est lui aussi noethérien, de dimension 1, et le morphisme induit un isomorphisme au niveau des points génériques – les corps des fractions sont tous les deux K. On peut donc trouver un entier N tel que

$$\mathrm{Spec}(\mathcal{O}_K[1/N]) \to \mathrm{Spec}(\mathcal{O}'[1/N])$$

est un isomorphisme. Concrètement, le morphisme $\mathcal{O}' \to \mathcal{O}_K$ est injectif, induit un isomorphisme au niveau des corps de fractions, donc son conoyau est un groupe fini, tué par un entier N. Le morphisme

$$\mathrm{Spec}(\mathcal{O}_K) \to \mathrm{Spec}(\mathcal{O}')$$

est la *normalisation*.

Théorème 1.3.4. *Soit K un corps de nombres. Alors $\mathcal{O}_K$ est un anneau de Dedekind.*

Démonstration. D'après la proposition 1.3.2, il suffit de montrer que $\mathcal{O}$ est intégralement clos, ce qui est vrai par définition de $\mathcal{O}_K$. □

Les anneaux de Dedekind ne sont pas principaux en général. Cependant, un énoncé d'unique factorisation en premiers reste vrai au niveau des idéaux. Avant de l'énoncer, commençons par trois lemmes.

Lemme 1.3.5. *Soit $\mathcal{O}$ un anneau de Dedekind, et soit I un idéal de $\mathcal{O}$. Il existe des idéaux premiers non-nuls $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ tels que*

$$\mathfrak{p}_1 \ldots \mathfrak{p}_r \subset I.$$

Démonstration. On raisonne par l'absurde. Puisque $\mathcal{O}$ est noethérien, on peut supposer que I est maximal parmi les idéaux qui ne satisfont pas la conclusion du lemme. L'idéal I n'est pas premier. Soient donc $a, b \in \mathcal{O} \setminus I$ tels que $ab \in I$. Par hypothèse, on peut trouver des idéaux premiers non-nuls $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ et $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ tels que

$$\mathfrak{p}_1 \ldots \mathfrak{p}_r \subset I + (a)$$

et

$$\mathfrak{q}_1 \ldots \mathfrak{q}_s \subset I + (b).$$

Alors

$$\mathfrak{p}_1 \ldots \mathfrak{p}_r \mathfrak{q}_1 \ldots \mathfrak{q}_s \subset I,$$

ce qui est une contradiction. □

Lemme 1.3.6. *Soit $\mathcal{O}$ un anneau de Dedekind, et soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}$. Soit K le corps des fractions de $\mathcal{O}$. On définit*

$$\mathfrak{p}^{-1} = \{x \in K | \, x\mathfrak{p} \subset \mathcal{O}\}.$$

Si I est un idéal non-nul de $\mathcal{O}$, alors

$$I \subsetneq I\mathfrak{p}^{-1}.$$

Dans l'énoncé ci-dessus, on a noté $I\mathfrak{p}^{-1}$ l'ensemble

$$\{\sum_i a_i x_i | \, a_i \in I, x_i \in \mathfrak{p}^{-1}\}.$$

Démonstration. Traitons d'abord le cas où $I = \mathcal{O}$. On a certainement $\mathcal{O} \subset \mathfrak{p}^{-1}$, il faut donc trouver un élément x de $K \setminus \mathcal{O}$ tel que $x\mathfrak{p} \subset \mathcal{O}$.

Soit a un élément non-nul de $\mathfrak{p}$. Le lemme précédent nous fournit $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ premiers non-nuls tels que

$$\mathfrak{p}_1 \ldots \mathfrak{p}_r \subset (a) \subset \mathfrak{p}.$$

Les idéaux premiers non-nuls étant maximaux, on peut supposer $\mathfrak{p}_1 = \mathfrak{p}$. On choisit aussi r minimal, donc $\mathfrak{p}_2 \ldots \mathfrak{p}_r$ n'est pas inclus dans (a) : soit donc $b \notin (a)$ tel que $b \in \mathfrak{p}_2 \ldots \mathfrak{p}_r$. Alors $a^{-1}b \notin \mathcal{O}$, mais

$$a^{-1}b\mathfrak{p} = a^{-1}b\mathfrak{p}_1 \subset a^{-1}\mathfrak{p}_1 \ldots \mathfrak{p}_r \subset a^{-1}(a) = \mathcal{O}.$$

Soit maintenant I un idéal non-nul de $\mathcal{O}$, et supposons, en raisonnant par l'absurde,

$$I\mathfrak{p}^{-1} = I.$$

Soit x un élément de $\mathfrak{p}^{-1} \subset K$. La multiplication par x laisse I invariant, et – comme $\mathcal{O}$ est noethérien – I est un $\mathcal{O}$-module de type fini, non-nul, donc un $\mathbb{Z}$-module de type fini. Cela implique que x est entier sur $\mathbb{Z}$, donc que x est dans $\mathcal{O}$ car $\mathcal{O}$ est intégralement clos.

On vient de montrer que $\mathfrak{p}^{-1}$ est inclus dans $\mathcal{O}$, en contradiction avec ce qui précède. □

Lemme 1.3.7. *Soit $\mathcal{O}$ un anneau de Dedekind, et soit $\mathfrak{p}$ un idéal premier non-nul de $\mathcal{O}$. Alors*

$$\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}.$$

Démonstration. Comme $\mathfrak{p}$ est maximal, la suite d'inclusions

$$\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subset \mathcal{O}$$

implique $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. □

Théorème 1.3.8. *Soit $\mathcal{O}$ un anneau de Dedekind, et soit I un idéal non-nul de $\mathcal{O}$. Alors il existe des idéaux premiers non-nuls $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, uniques à permutation près, tels que*

$$I = \mathfrak{p}_1 \ldots \mathfrak{p}_r.$$

Démonstration. Montrons l'existence : soit I un idéal non-nul de $\mathcal{O}$, on veut montrer qu'il est produit d'idéaux premiers – notons que le produit vide est égal à $\mathcal{O}$. Raisonnons par l'absurde et, puisque $\mathcal{O}$ est noethérien, supposons I maximal parmi les idéaux de $\mathcal{O}$ qui ne sont pas produits d'idéaux premiers. Comme $I \neq \mathcal{O}$, on peut trouver un idéal premier $\mathfrak{p}$ qui contient I. Alors

$$I \subsetneq I\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}.$$

Par hypothèse, $I\mathfrak{p}^{-1}$ est produit d'idéaux premier $\mathfrak{p}_1 \ldots \mathfrak{p}_r$. Alors

$$I = I\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}\mathfrak{p}_1 \ldots \mathfrak{p}_r,$$

contradiction.

Montrons l'unicité. Considérons une égalité

$$\mathfrak{p}_1 \ldots \mathfrak{p}_r = \mathfrak{q}_1 \ldots \mathfrak{q}_s,$$

où les $\mathfrak{p}_i, \mathfrak{q}_j$ sont des idéaux premiers non-nuls. Alors $\mathfrak{q}_1 \ldots \mathfrak{q}_s \subset \mathfrak{p}_1$, donc l'un des $\mathfrak{q}_j$ est égal à $\mathfrak{p}_1$. On peut supposer $\mathfrak{p}_1 = \mathfrak{q}_1$. Multipliant par $\mathfrak{p}_1^{-1}$, on obtient

$$\mathfrak{p}_2 \ldots \mathfrak{p}_r = \mathfrak{q}_2 \ldots \mathfrak{q}_s,$$

et l'on conclut par récurrence. □

On peut généraliser un peu les constructions sur les idéaux.

Définition 1.3.9. *Soit $\mathcal{O}$ un anneau de Dedekind, et K son corps des fractions. Un idéal fractionnaire de $\mathcal{O}$ est un sous $\mathcal{O}$-module de type fini, non-nul, de K.*

Si K est un corps de nombres, et si I est un idéal fractionnaire de K, le rang de I comme $\mathbb{Z}$-module – s'il est non nul – est égal au degré de K comme extension de $\mathbb{Q}$. Notons qu'un idéal fractionnaire de K est un idéal de $\mathcal{O}$ si et seulement si il est inclus dans $\mathcal{O}$.

On peut multiplier les idéaux fractionnaires entre eux. Si a est un élément non-nul de K, alors $(a) := a\mathcal{O}$ est un idéal fractionnaire de K – les idéaux obtenus ainsi sont les *idéaux principaux*. Par ailleurs, si I est un idéal fractionnaire, on peut toujours trouver un élément non-nul a de $\mathcal{O}$ tel que aI est un idéal de $\mathcal{O}$.

Définition 1.3.10. *Soit I un idéal fractionnaire de K. L'inverse de I, noté I^{-1}, est l'idéal fractionnaire*

$$I^{-1} = \{x \in K | xI \subset \mathcal{O}\}.$$

Lemme 1.3.11. *Soit I un idéal fractionnaire de K, et soit J un idéal fractionnaire tel que*

$$IJ = \mathcal{O}.$$

Alors $J = I^{-1}$.

Démonstration. On a bien sûr $J \subset I^{-1}$. Par ailleurs,

$$I^{-1} = I^{-1}IJ \subset J,$$

ce qui conclut. □

On généralise le théorème 1.3.8 aux idéaux fractionnaires.

Théorème 1.3.12. *Soit $\mathcal{O}$ un anneau de Dedekind.*

(i) Les idéaux fractionnaires de K forment un groupe pour la multiplication. L'élément neutre est $\mathcal{O}$ et l'inverse d'un idéal fractionnaire I est I^{-1}.

(ii) Tout idéal fractionnaire s'écrit de manière unique comme produit d'idéaux premiers et d'inverses d'idéaux premiers.

Démonstration. Prouvons le premier énoncé. Au vu de ce qui précède, il suffit de montrer que pour tout idéal fractionnaire I de K, on a

$$II^{-1} = \mathcal{O}.$$

Le lemme précédent nous montre qu'il suffit de trouver un idéal fractionnaire J de K tel que $IJ = \mathcal{O}$. Si I est un idéal premier de $\mathcal{O}$, le lemme 1.3.7 fait l'affaire. Si I est un idéal de $\mathcal{O}$, alors I est produit d'idéaux premiers, et le produit des inverses de ces idéaux premiers fournit l'idéal fractionnaire cherché.

Soit enfin I un idéal fractionnaire arbitraire de $\mathcal{O}$. On écrit $I = \frac{1}{a}I'$, où I' est un idéal de $\mathcal{O}$. Alors, si $J = aI'^{-1}$, on a

$$IJ = I'I'^{-1} = \mathcal{O},$$

ce qui conclut.

Prouvons le second énoncé. Il suit de ce qui précède que l'on a toujours $(IJ)^{-1} = I^{-1}J^{-1}$. Un idéal fractionnaire étant toujours de la forme IJ^{-1}, où I et J sont des idéaux non-nuls de $\mathcal{O}$ – l'existence suit. L'unicité est une conséquence de l'unicité de la décomposition en idéaux premiers des idéaux non-nuls de $\mathcal{O}$. □

On note J_K le groupe des idéaux fractionnaires de K. On note P_K le sous-groupe des idéaux principaux, isomorphe à K^*.

Définition 1.3.13. *Le groupe des classes d'idéaux d'un corps de nombre K est le groupe J_K/P_K, quotient du groupe des idéaux fractionnaires par le groupe des idéaux principaux. On le note Cl_K, et on note h_K son cardinal.*

Dans la discussion précédente, il est important de garder en tête le point de vue schématique : les idéaux fractionnaires de $\mathcal{O}_K$ sont exactement les sous-faisceau du faisceau des fonctions méromorphes sur $\operatorname{Spec}\mathcal{O}_K$ de la forme $\mathcal{O}(D)$, où D est un diviseur de Cartier – ici, une combinaison à coefficients entiers de points fermés $\mathfrak{p}$, car $\mathcal{O}_K$ est intégralement clos.

Le groupe des classes d'idéaux est exactement le *groupe de Picard* de $\operatorname{Spec}\mathcal{O}_K$, c'est-à-dire l'ensemble des classes d'isomorphismes de faisceaux localement libres de rang 1 sur $\operatorname{Spec}\mathcal{O}_K$.

Le théorème de Jordan-Zassenhaus a le cas particulier suivant.

Théorème 1.3.14. *Soit K un corps de nombres. Le groupe Cl_K des classes d'idéaux de K est fini.*

Démonstration. Si I est un idéal fractionnaire de K, alors I est isomorphe à $\mathcal{O}_K$ comme $\mathcal{O}_K$-module si et seulement si I est principal. Plus généralement, si I et J sont deux idéaux fractionnaires, alors I et J sont isomorphes comme $\mathcal{O}_K$-modules si et seulement si $I = aJ$ pour un certain $a \in K^*$, i.e. si et seulement si I et J ont la même image dans Cl_K. Le groupe Cl_K s'injecte donc dans l'ensemble des $\mathcal{O}_K$-modules M tels que $M \otimes_{\mathbb{Z}} \mathbb{Q} \simeq K$ – il lui est en fait égal – ce qui conclut par Jordan-Zassenhaus. □

On peut généraliser ce théorème aux schémas réguliers projectifs sur $\mathbb{Z}$, mais c'est beaucoup plus difficile (théorème de Mordell-Weil, essentiellement).

Les notions de divisibilité et d'entiers premiers entre eux se généralisent aux idéaux.

Définition 1.3.15. *Soient I et J deux idéaux fractionnaires d'un anneau $\mathcal{O}$. On dit que I divise J si $J \subset I$.*

Il suit immédiatement des définitions que I divise J si et seulement si J^{-1} divise I^{-1}.

Proposition 1.3.16. *Soient I et J deux idéaux fractionnaire d'un anneau $\mathcal{O}$. Alors I divise J si et seulement si $I^{-1}J$ est un idéal – pas fractionnaire – de $\mathcal{O}$.*

Démonstration. Supposons que I divise J. Alors

$$I^{-1}J \subset I^{-1}I \subset \mathcal{O},$$

donc $I^{-1}J$ est bien un idéal.

Réciproquement, supposons $I^{-1}J \subset \mathcal{O}$. Alors

$$II^{-1}J = J \subset I.$$

□

En particulier, si I et J sont des idéaux, on vérifie que I divise J sur la décomposition en idéaux premiers : la décomposition en facteurs premiers de J doit "contenir" celle de I.

Définition 1.3.17. *Soient $I_1, \ldots, I_k$ des idéaux non-nuls dans un anneau $\mathcal{O}$. On dit que $I_1, \ldots, I_r$ sont premiers entre eux dans leur ensemble si*

$$I_1 + \ldots + I_r = \mathcal{O}.$$

Proposition 1.3.18. *Soient $I_1, \ldots, I_r$ des idéaux non-nuls dans un anneau $\mathcal{O}$. Alors $I_1, \ldots, I_r$ sont premiers entre eux dans leur ensemble si et seulement si pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}$, il existe $k \in \{1, \ldots, k\}$ tel que $\mathfrak{p}$ ne divise pas I_k.*

Démonstration. Supposons qu'il existe un idéal premier $\mathfrak{p}$ tel que pour tout k, $\mathfrak{p}$ divise I_k, i.e. $I_k \subset \mathfrak{p}$. Alors

$$I_k + \ldots + I_r \subset \mathfrak{p}$$

et les I_k ne sont pas premiers entre eux dans leur ensemble.

Réciproquement, supposons que les I_k ne sont pas premiers entre eux dans leur ensemble. Alors on peut trouver un idéal premier $\mathfrak{p}$ tel que

$$I_1 + \ldots + I_r \subset \mathfrak{p}$$

ce qui montre que $\mathfrak{p}$ divise tous les I_k. □

Proposition 1.3.19 (Théorème des restes chinois)**.** *Soit $\mathcal{O}$ un anneau, et soient $I_1, \ldots, I_r$ des idéaux de $\mathcal{O}$, deux à deux premiers entre eux. Soit $I = \bigcap_{k=1}^{r} I_k$. Alors la flèche naturelle*

$$\mathcal{O}/I \to \bigoplus_{k=1}^{r} \mathcal{O}/I_k$$

est un isomorphisme.

Démonstration. Il est clair que la flèche est injective. Il suffit pour montrer la surjectivité de trouver des éléments $e_k \in \mathcal{O}$ tels que

$$\forall j \in \{1, \ldots, r\}, e_k = \delta_j^k \bmod I_j,$$

i.e. de trouver des e_k tels que

$$\forall j \neq k, e_k \in I_j$$

et $e_k - 1 \in I_k$.

Notons $J_k = \bigcap_{j \neq k} I_j$. Pour tout $j \neq k$, on peut écrire

$$1 = x_j + y_j$$

avec $x_j \in I_k$, $y_j \in I_j$. Alors

$$1 = \Pi_{j \neq k}(x_j + y_j) = x'_k + e_k,$$

où $x'_k \in I_k$ et $e_k = \Pi_{j \neq k} y_j \in J_k$. □

1.3.2 Anneaux locaux des anneaux de Dedekind

On ne rappelle pas les propriétés de base de la localisation, qui ont été vues pendant le cours accéléré de géométrie algébrique.

Si $\mathfrak{p}$ est un idéal premier d'un anneau A, on note $A_\mathfrak{p}$ la localisation de A en $\mathfrak{p}$, i.e. la localisation de A par rapport au sous-ensemble multiplicatif $S = A \setminus \mathfrak{p}$. Si A est intègre, de corps des fractions K, on a

$$A_\mathfrak{p} = \{x \in K, \exists y \in A \setminus \mathfrak{p}, xy \in A\}.$$

Il s'agit de l'ensemble des éléments de K qui sont "définis" en $\mathfrak{p}$. En particulier, les éléments de $A_\mathfrak{p}$ s'envoient dans $A/\mathfrak{p}$.

Fixons dans ce qui suit un anneau de Dedekind $\mathcal{O}$, de corps de fractions K. La notion d'anneau de Dedekind est compatible à la localisation.

Proposition 1.3.20. *Soit A un anneau intègre.*

(i) Supposons A intégralement, clos, et soit S un sous-ensemble multiplicatif de A. Alors la localisation $S^{-1}A$ est un anneau intégralement clos.

(ii) Supposons que pour tout idéal premier $\mathfrak{p}$, la localisation de A en $\mathfrak{p}$ est intégralement close. Alors A est intégralement clos.

Démonstration. Admis/connu. □

Rappelons sans preuve comment fonctionnent les idéaux dans les localisés.

Proposition 1.3.21. *Soit $\mathfrak{p}$ un idéal premier dans un anneau A. L'anneau $A_\mathfrak{p}$ est un anneau local : il admet un unique idéal maximal, qui est $\mathfrak{p}A_\mathfrak{p}$. Les idéaux premiers de $A_\mathfrak{p}$ sont en bijection canonique avec les idéaux premiers de A contenus dans $\mathfrak{p}$.*

On dispose d'une injection canonique

$$A/\mathfrak{p} \hookrightarrow A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$$

qui identifie $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ au corps des fractions de $A/\mathfrak{p}$.

Si $\mathfrak{p}$ est maximal, la flèche ci-dessus est un isomorphisme, et l'on a plus généralement, pour tout entier positif n, des isomorphismes canoniques

$$A/\mathfrak{p}^n \to A_{\mathfrak{p}}/(\mathfrak{p}A_p)^n.$$

On comprend bien les anneaux locaux qui sont de Dedekind.

Définition 1.3.22. *Un anneau de valuation discrète est un anneau intègre, local, principal.*

Soit A un anneau de valuation discrète, et soit $\mathfrak{m}$ son idéal maximal. Puisque A est principal, il existe un élément ϖ (on prononce "pi"), unique à multiplication par un élément de A^* près, tel que $\mathfrak{m} = (\varpi)$. On dit que ϖ est une *uniformisante* (uniformizing parameter) de A.

Remarquons qu'un anneau de valuation discrète est un anneau de Dedekind. La théorie des idéaux d'un anneau de valuation discrète est particulièrement simple.

Proposition 1.3.23. *Soit A un anneau de valuation discrète d'idéal maximal $\mathfrak{m}$, de corps des fractions K, et soit ϖ une uniformisante de A.*

(i) Les éléments x de K^* s'écrivent de manière unique sous la forme

$$x = \epsilon\varpi^n,$$

$\epsilon \in A^*, n \in \mathbb{Z}$. L'application

$$K^* \to \mathbb{Z}, x \mapsto n$$

est un morphisme de groupes indépendant du choix de ϖ.

(ii) Les idéaux fractionnaires de A sont exactement les $\mathfrak{m}^n = (\varpi^n)$, pour $n \in \mathbb{Z}$.

Démonstration. Dans un anneau principal, les idéaux premiers non-nuls sont maximaux. Ainsi, $\mathfrak{m}$ est l'unique idéal premier de A. Le théorème de factorisation garantit donc (i) – au moins si $x \in A$, mais le cas de $x \in K^*$ général suit. Que $x \mapsto n$ soit un morphisme est une conséquence formelle de l'unicité de n.

Tout idéal fractionnaire dans un anneau principal est principal, ce qui montre (ii) connaissant (i). □

Définition 1.3.24. *Le morphisme de groupe*

$$v : K^* \to \mathbb{Z}, \epsilon\varpi^n \mapsto n$$

est appelé la valuation. On note $v(x)$ la valuation de x.

La valuation est caractérisée par la formule

$$\forall x \in K^*, (x) = \mathfrak{m}^{v(x)}.$$

Remarquons ce qui suit – de démonstration immédiate.

Proposition 1.3.25. *Soit A un anneau de valuation discrète de corps des fractions K, et soit v la valuation de K^*. Alors, pour tout $x \in K^*$,*

$$x \in A \iff v(x) \geq 0.$$

Plus généralement, pour tout $n \in \mathbb{Z}$,

$$x \in \mathfrak{m}^n \iff v(x) \geq n.$$

Notons ici comment calculer avec les valuations :

Proposition 1.3.26. *Soit A un anneau de valuation discrète de corps des fractions K, et soit v la valuation de K^*. Alors*

$$\forall x, y \in K^*, v(xy) = v(x) + v(y) \text{ et } v(x) + v(y) \geq \min(v(x), v(y)),$$

avec égalité dès que $v(x) \neq v(y)$.

On note souvent $v(0) = \infty$, de sorte que les formules des propositions précédentes valent pour tout $x, y \in K$.

Démonstration. La première égalité traduit simplement le fait que v est un morphisme de groupes. Montrons la seconde. Quitte à multiplier par une puissance adéquate de l'uniformisante et à intervertir x et y, on peut supposer $x = 1$ et $y \in A$, soit $v(y) \geq 0$. Alors $1 + y \in A$ et $v(1 + y) \geq 0$ par la proposition précédente.

Si $v(y) > 0$, alors $y \in \mathfrak{m}$ et $1+y$ est inversible – car $1+y \notin \mathfrak{m}$ – et $v(1+y) = 0$. □

Ce qui suit est facile, mais important.

Théorème 1.3.27. *Soit A un anneau de Dedekind local. Alors A est un anneau de valuation discrète.*

En particulier, les localisés des anneaux de Dedekind en des idéaux premiers non-nuls sont des anneaux de valuation discrète.

Démonstration. Soit $\mathfrak{m}$ l'idéal maximal de A. Le théorème 1.3.8 montre que les idéaux non-nuls de A sont exactement les $\mathfrak{m}^n$, $n \geq 0$. Soit ϖ un élément de $\mathfrak{m} \setminus \mathfrak{m}^2$. Alors

$$\mathfrak{m}^2 \subsetneq (\varpi) \subset \mathfrak{m},$$

donc $(\varpi) = \mathfrak{m}$. On a ensuite $\mathfrak{m}^n = (\varpi)^n$, ce qui prouve que A est principal. □

Voici comment les idéaux des anneaux de Dedekind se comportent par localisation.

Proposition 1.3.28. *Soit $\mathcal{O}$ un anneau de Dedekind, et $\mathfrak{p}$ un idéal premier non-nul de $\mathcal{O}$. Soit $I = \mathfrak{p}^n J$ un idéal de $\mathcal{O}$, où J est premier à $\mathfrak{p}$. Alors*

$$I\mathcal{O}_{\mathfrak{p}} = \mathfrak{p}^n \mathcal{O}_{\mathfrak{p}}.$$

Démonstration. Il suffit de montrer que $J\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}$, ce qui est clair puisque J est premier à $\mathfrak{p}$, donc contient un élément inversible dans $\mathcal{O}_{\mathfrak{p}}$. □

1.3.3 Extensions d'anneaux de Dedekind

On va maintenant examiner comment les structures précédentes se comportent par extensions. On se donne donc $\mathcal{O} = \mathcal{O}_K$ un anneau de Dedekind de corps de fractions K, L une extension finie de K, et $\mathcal{O}_L$ l'anneau des entiers de L. On suppose K de caractéristique nulle – ou au moins l'extension L/K séparable. Soit $n = [L : K]$.

Proposition 1.3.29. *Avec les notations précédentes, $\mathcal{O}_L$ est un anneau de Dedekind, qui est un $\mathcal{O}_K$-module de type fini.*

Démonstration. Nous ne traitons que le cas où l'extension L/K est séparable, ce qui suffit à nos besoins puisqu'on ne travaille qu'en caractéristique nulle. Montrons d'abord que $\mathcal{O}_K$ est bien un $\mathcal{O}_K$-module de type fini. Soit $e_1, \ldots, e_n$ une base de L comme K-espace vectoriel, dans laquelle les e_i sont dans $\mathcal{O}_L$. On adapte la preuve de la proposition 1.2.4.

L'application $\mathcal{O}_K$-bilinéaire

$$\mathcal{O}_L \times \mathcal{O}_L \to \mathcal{O}_K, (x, y) \mapsto Tr_{L/K}(xy)$$

est non-dégénérée car L/K est séparable. Soit M le $\mathcal{O}_K$-module libre engendré par les e_i. Soit M^* le $\mathcal{O}_K$-module des $x \in L$ tels que

$$\forall y \in M, Tr_{L/K}(xy) \in \mathcal{O}_K.$$

Alors

$$M \subset \mathcal{O}_L \subset M^*,$$

et M^* est le $\mathcal{O}_K$-module libre de base la base duale de (e_i), donc $\mathcal{O}_L$ est de type fini sur $\mathcal{O}_K$.

Le $\mathcal{O}_K$-module $\mathcal{O}_L$ est de type fini, donc noethérien. L'anneau $\mathcal{O}_L$ est donc noethérien. Il reste à montrer que tout idéal premier non-nul de $\mathcal{O}_L$ est maximal. Soit $\mathfrak{P}$ un idéal premier non-nul de $\mathcal{O}_L$. Alors $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K$ – l'image réciproque de $\mathfrak{P}$ dans $\mathcal{O}_K$ est un idéal premier de $\mathcal{O}_K$, non-nul car il contient la norme de tout élément de $\mathfrak{P}$. C'est donc un idéal maximal. L'anneau $\mathcal{O}_L/\mathfrak{P}$ est intègre, de dimension finie sur le corps $\mathcal{O}_K/\mathfrak{p}$, c'est donc un corps, ce qui prouve que $\mathfrak{P}$ est maximal. □

Remarque 1.3.30. *Voici une reformulation de la preuve du caractère noethérien de $\mathcal{O}_L$. Soit M un $\mathcal{O}_K$-module muni d'une application bilinéaire non-dégénérée $<.,.>$. On dispose par construction d'un morphisme injectif de M vers son dual. Soit C son conoyau : c'est un $\mathcal{O}_K$-module fini. Son discriminant D est défini comme suit : localement en $\mathfrak{p}$, on écrit*

$$C_{\mathfrak{p}} = \Pi_i \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}^{n_i}.$$

Alors D est le produit des $\mathfrak{p}^{\sum_i n_i}$.

Si M est libre de base les e_i, alors D est l'idéal engendré par le déterminant des $< e_i, e_j >$ – travailler par exemple localement pour le montrer.

Si $N \subset M$ sont localement libres de même rang, alors le discriminant de M divise le discriminant de M, et il le divise strictement si $M \neq N$. Dans ce qui précède, on prend M un sous-module de $\mathcal{O}_L$ de type fini, de discriminant maximal. Alors $M = \mathcal{O}_L$.

Considérons l'aspect schématique des choses : on dispose dans la situation précédente d'un morphisme

$$\pi : \operatorname{Spec} \mathcal{O}_L \to \operatorname{Spec} \mathcal{O}_K.$$

Il envoie un idéal premier $\mathfrak{P}$ de $\mathcal{O}_L$ sur $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K$. Ce morphisme est fini, car $\mathcal{O}_L$ est un $\mathcal{O}_K$-module de type fini. Par ailleurs, le point générique de $\operatorname{Spec} \mathcal{O}_L$ – qui correspond à l'idéal nul de $\mathcal{O}_L$ – s'envoie sur le point générique de $\operatorname{Spec} \mathcal{O}_K$.

Définition 1.3.31. *Avec les notations précédentes, on dit que $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$, ou que $\mathfrak{P}$ divise $\mathfrak{p}$, si $\pi(\mathfrak{P}) = \mathfrak{p}$, i.e., si $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. On note $\mathfrak{P}|\mathfrak{p}$.*

On sait par ailleurs – c'est dans le cours de théorie des schémas – que les morphismes finis sont fermés. On en tire deux conclusions, qui sont par ailleurs faciles à vérifier directement (on a déjà prouvé la première), et que l'on résume dans la proposition qui suit.

Proposition 1.3.32. *Avec les notations précédentes,*

(i) l'image d'un point fermé de $\operatorname{Spec} \mathcal{O}_L$ dans $\operatorname{Spec} \mathcal{O}_K$ est fermée : autrement dit, si $\mathfrak{P}$ est un idéal premier non nul de $\mathcal{O}_L$, alors $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K$ est un idéal premier non nul de $\mathcal{O}_K$;

(ii) le morphisme $\operatorname{Spec} \mathcal{O}_L \to \operatorname{Spec} \mathcal{O}_K$ est surjectif. Autrement dit, si $\mathfrak{p}$ est un idéal premier non nul de $\mathcal{O}_K$, il existe un idéal premier non nul $\mathfrak{P}$ de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}$, i.e., tel que $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.

Démonstration. Le premier énoncé est évident. Pour le second, il suffit de remarquer que l'image de π contient le point générique de $\operatorname{Spec} \mathcal{O}_K$, donc son adhérence, qui est $\operatorname{Spec} \mathcal{O}_K$ tout entier. □

On examine maintenant les fibres de π. Il s'agit de comprendre, étant donné $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$, quels sont les $\mathfrak{P} \in \operatorname{Spec} \mathcal{O}_L$ au-dessus de $\mathfrak{p}$. Ces idéaux sont les points

de la fibre schématique $\pi^{-1}(\operatorname{Spec}\kappa(\mathfrak{p})) = \operatorname{Spec}\mathcal{O}_L \times_{\operatorname{Spec}\mathcal{O}_K} \operatorname{Spec}\kappa(\mathfrak{p})$. Concrètement, cette fibre est le schéma affine associé à l'anneau

$$\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_K/\mathfrak{p} = \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L.$$

Comprendre les fibres de π, c'est donc comprendre la factorisation dans $\mathcal{O}_L$ de l'idéal $\mathfrak{p}\mathcal{O}_L$.

Factorisons $\mathfrak{p}\mathcal{O}_L$:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r},$$

où les e_i sont strictement positifs et les $\mathfrak{P}_k$ sont des idéaux premiers deux à deux distincts – dans la suite, on écrira souvent $\mathfrak{p}$ pour $\mathfrak{p}\mathcal{O}_L$.

Lemme 1.3.33. *Les $\mathfrak{P}_i$ sont exactement les idéaux premiers de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}$.*

Démonstration. L'intersection de $\mathfrak{P}_i$ avec $\mathcal{O}_K$ est un idéal premier de $\mathcal{O}_K$ qui contient $\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K$, donc qui contient $\mathfrak{p}$. Comme $\mathfrak{p}$ est maximal, on a bien $\mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p}$.

Réciproquement, si $\mathfrak{P}$ contient $\mathfrak{p}$, alors $\mathfrak{P}$ contient $\mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$, donc $\mathfrak{P}$ est égal à l'un des $\mathfrak{P}_i$. □

Définition 1.3.34. *Avec les notations précédentes, e_i est l'indice de ramification de $\mathfrak{P}_i$.*

On note f_i le degré de l'extension de corps $(\mathcal{O}_L/\mathfrak{P}_i)/(\mathcal{O}_K/\mathfrak{p})$. On dit que f_i est le degré résiduel.

Un peu de vocabulaire sur les types de décomposition. On garde les mêmes notations.

Définition 1.3.35. *On dit que $\mathfrak{P}_i$ est ramifié si $e_i > 1$ ou si l'extension résiduelle $(\mathcal{O}_L/\mathfrak{P}_i)/(\mathcal{O}_K/\mathfrak{p})$ n'est pas séparable. On dit que $\mathfrak{p}$ est non ramifié si tous les $\mathfrak{P}_i$ au-dessus de $\mathfrak{p}$ sont non ramifiés.*

On dit que $\mathfrak{p}$ est totalement décomposé si tous les f_i et les e_i valent 1*. On dit que $\mathfrak{p}$ est totalement ramifié – ou que l'extension L/K est totalement ramifiée en $\mathfrak{p}$ – si la factorisation de $\mathfrak{p}$ dans $\mathcal{O}_L$ est*

$$\mathfrak{p} = \mathfrak{P}^e$$

pour un certain premier $\mathfrak{P}$ de degré résiduel 1*.*

On notera $e_{\mathfrak{P}}$, ou $e_{\mathfrak{P}/\mathfrak{p}}$, et de même pour f, suivant les besoins du contexte.

Remarque 1.3.36. *La factorisation de l'idéal $\mathfrak{p}$, ainsi que les degrés résiduels et de ramification, sont inchangés après localisation en $\mathfrak{p}$, comme il suit par exemple de la discussion schématique.*

La proposition suivante résume les propriétés de base des structures que l'on vient d'introduire.

Proposition 1.3.37. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$, dont la factorisation dans $\mathcal{O}_L$ est*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}.$$

Alors l'anneau $\mathcal{O}_L/\mathfrak{p}$ est une $\mathcal{O}_K/\mathfrak{p}$-algèbre de degré $n = [L : K]$, isomorphe au produit

$$\mathcal{O}_L/\mathfrak{P}_1^{e_1} \times \ldots \times \mathcal{O}_L/\mathfrak{P}^{e_r}.$$

On a

$$n = e_1 f_1 + \ldots + e_r f_r.$$

Démonstration. La remarque ci-dessus permet de localiser en $\mathfrak{p}$, puis de supposer que $\mathcal{O}_K$ est local, d idéal maximal $\mathfrak{p}$ – il faut pour cela remarquer que si $S = \mathcal{O}_K \setminus \mathfrak{p}$, alors $S^{-1}\mathcal{O}_L$ est bien la clôture intégrale de $S^{-1}\mathcal{O}_K$ dans L comme la proposition 1.3.20, (i) le montre.

L'anneau $\mathcal{O}_K$ est principal puisque c'est un anneau de Dedekind local. L'anneau $\mathcal{O}_L$ est donc un $\mathcal{O}_K$-module libre de rang n. Ainsi, après réduction modulo $\mathfrak{p}$, il apparaît que $\mathcal{O}_L/\mathfrak{p}$ est un $\mathcal{O}_K/\mathfrak{p}$-espace vectoriel de dimension n.

Le théorème chinois nous montre que l'application naturelle

$$\mathcal{O}_L/\mathfrak{p} \to \mathcal{O}_L/\mathfrak{P}_1^{e_1} \dots \mathcal{O}_L/\mathfrak{P}^{e_r}$$

est un isomorphisme. Comparant les degrés, on trouve

$$n = n_{\mathfrak{P}_1} + \ldots + n_{\mathfrak{P}_r},$$

où $n_{\mathfrak{P}}$ est la dimension de $\mathcal{O}_L/\mathfrak{P}^{e_{\mathfrak{P}}}$ comme $\mathcal{O}_L/\mathfrak{p}$-espace vectoriel. L'espace vectoriel $\mathcal{O}_L/\mathfrak{P}^{e_{\mathfrak{P}}}$ est muni d'une filtration par ses sous-espaces $\mathfrak{P}^i/\mathfrak{P}^{e_{\mathfrak{P}}}$, $i < e_{\mathfrak{P}}$, d'où la formule

$$n_{\mathfrak{P}} = \sum_{i=0}^{e_{\mathfrak{P}}-1} \dim_{\mathcal{O}_K/\mathfrak{p}}(\mathfrak{P}^i/\mathfrak{P}^{i+1}).$$

Soit $\varpi_{\mathfrak{P}}$ un élément de $\mathfrak{P} \setminus \mathfrak{P}^2$. La multiplication par $\varpi_{\mathfrak{P}}^i$ induit un isomorphisme de $\mathcal{O}_K/\mathfrak{p}$-espace vectoriel

$$\mathcal{O}_K/\mathfrak{P} \to \mathfrak{P}^i/\mathfrak{P}^{i+1},$$

ce qui achève la preuve. □

Corollaire 1.3.38. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. Le nombre d'idéaux premiers de $\mathcal{O}_L$ qui divisent $\mathfrak{p}$ est compris entre 1 et n. Il vaut n si et seulement si $\mathfrak{p}$ est totalement décomposé.*

Si $\mathcal{O}_K$ n'a qu'un nombre fini d'idéaux premiers, alors $\mathcal{O}_L$ n'a qu'un nombre fini d'idéaux premiers.

Remarque 1.3.39. *Il n'est pas difficile de montrer en utilisant le théorème chinois qu'un anneau de Dedekind qui n'a qu'un nombre fini d'idéaux premiers (on dit qu'il est semilocal) est principal.*

Corollaire 1.3.40. *Avec les notations de la proposition, soit $S = \mathcal{O}_K \setminus \mathfrak{p}$. Alors $S^{-1}\mathcal{O}_L$ est semilocal, d'idéaux premiers les $\mathfrak{P}_i$.*

Corollaire 1.3.41. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$, et soit k une clôture algébrique de $\mathcal{O}_K/\mathfrak{p}$. Alors $\mathfrak{p}$ est non-ramifié si et seulement si l'anneau*

$$\mathcal{O}_L/\mathfrak{P} \otimes_{\mathcal{O}_K/\mathfrak{p}} k$$

est réduit.

Si $\mathfrak{p}$ est non ramifié, cet anneau est produit de n copies de k. Réciproquement, si $\mathcal{O}_L/\mathfrak{p} \otimes_{\mathcal{O}_K/\mathfrak{p}} k$ a au moins n idéaux premiers, alors $\mathfrak{p}$ est non ramifié.

Le corollaire est plus clair formulé de manière schématique : $\mathfrak{p}$ est non ramifié si et seulement si la fibre géométrique de $\pi : \operatorname{Spec} \mathcal{O}_L \to \operatorname{Spec} \mathcal{O}_K$ est réduite. Dans ce cas, il s'agit d'une union disjointe de n copies de $\operatorname{Spec} \mathcal{O}_K$.

Remarque 1.3.42. *Si les corps résiduels sont finis, les questions de séparabilité disparaissent, et dans ce qui précède on peut prouver que $\mathfrak{p}$ est non ramifié si et seulement si $\mathcal{O}_L/\mathfrak{p}$ est réduit.*

Pour conclure, on étend la définition de la norme aux idéaux.

Définition 1.3.43. *Soit $I = \Pi_i \mathfrak{P}_i^{r_i}$ un idéal fractionnaire de $\mathcal{O}_L$, où les $\mathfrak{P}_i$ sont premiers et les r_i entiers relatifs. On définit la norme de I, notée $N_{L/K}(I)$, par la formule*

$$N_{L/K}(I) = \Pi_i \mathfrak{p}_i^{f_i r_i},$$

où les $\mathfrak{P}_i$ sont premiers, $\mathfrak{p}_i = \mathfrak{P}_i \cap \mathcal{O}_K$ et $f_i = f_{\mathfrak{P}_i}$. Il s'agit d'un idéal fractionnaire de $\mathcal{O}_K$.

Proposition 1.3.44. *On garde les notations précédentes.*

(i) La norme définit un morphisme de groupes

$$N_{L/K} : J_L \to J_K;$$

(ii) si L'/L est une extension finie séparable, on a $N_{L'/K} = N_{L/K} \circ N_{L'/L}$;

(iii) si I est un idéal fractionnaire de $\mathcal{O}_K$, alors $N_{L/K}(I\mathcal{O}_L) = I^n$.

(iv) la construction de la norme est compatible à la localisation ;

(v) si x est un élément de $\mathcal{O}_L$, alors $N_{L/K}(x\mathcal{O}_L) = N_{L/K}(x)\mathcal{O}_K$;

(vi) La norme induit un morphisme de groupes

$$N_{L/K} : Cl(L) \to Cl(K),$$

dont le conoyau est tué par n.

Démonstration. Les points $(i), (ii)$ et (iv) sont formels. Pour prouver (iii), on peut supposer $I = \mathfrak{p}$ premier, auquel cas il suffit d'appliquer la dernière formule de la proposition 1.3.37. Pour prouver (v), l'énoncé (ii) nous permet de nous ramener au cas d'une extension galoisienne, et nous traiterons ce cas plus bas.

Le point (vi) suit de $(i), (iii)$ et (v). □

1.3.4 Calculs explicites

On reprend les notations de la partie précédente. Comme l'extension L/K est séparable, elle est monogène. Soit donc α un élément de L tel que $L = K[\alpha]$. On peut supposer α entier, soit $P \in \mathcal{O}_K[X]$ son polynôme minimal. Il est unitaire de degré n.

Comme α est entier sur $\mathcal{O}_K$, on a bien sûr $\mathcal{O}_K[\alpha] \subset \mathcal{O}_L$. On a déjà démontré les deux résultats suivants de manière schématique, réécrivons-les de manière élémentaire. Pour fixer les idées, on suppose que K (et donc L) est un corps de nombres.

Lemme 1.3.45. *Le groupe quotient $\mathcal{O}_L/\mathcal{O}_K[\alpha]$ est un groupe fini.*

Démonstration. Le groupe en question est de torsion. Il est par ailleurs de type fini car $\mathcal{O}_L$ est un $\mathcal{O}_K$-module de type fini. □

Proposition 1.3.46. *Il n'existe qu'un nombre fini d'idéaux premiers $\mathfrak{p}$ de $\mathcal{O}_K$ tels que*

$$\mathcal{O}_{L,\mathfrak{p}} \neq \mathcal{O}_{K,\mathfrak{p}}[\alpha].$$

Dans l'énoncé ci-dessus, on a noté $\mathcal{O}_{L,\mathfrak{p}} = S^{-1}\mathcal{O}_L$, avec $S = \mathcal{O}_K \setminus \mathfrak{p}$. Il s'agit de la clôture intégrale de $\mathcal{O}_{K,\mathfrak{p}}$ dans L.

Démonstration. Supposons que $\mathfrak{p}$ soit premier à l'ordre N du groupe fini $\mathcal{O}_{L,\mathfrak{p}}/\mathcal{O}_{K,\mathfrak{p}}[\alpha]$. Alors N est inversible dans $\mathcal{O}_{L,\mathfrak{p}}$, donc la multiplication par N est inversible dans le quotient $\mathcal{O}_{L,\mathfrak{p}}/\mathcal{O}_{K,\mathfrak{p}}[\alpha]$. Soit donc x un élément de $\mathcal{O}_{L,\mathfrak{p}}$. On peut trouver un élément d de $\mathcal{O}_K$, premier à $\mathfrak{p}$, tel que $dx \in \mathcal{O}_L$. Ainsi, $Ndx \in \mathcal{O}_K[\alpha]$. Comme Nd est premier à p, on trouve

$$x \in \mathcal{O}_{K,\mathfrak{p}}[\alpha].$$

Les idéaux premiers à N satisfont ainsi la conclusion de la proposition. □

La proposition précédente signifie que même si $\mathcal{O}_K[\alpha]$ n'est pas l'anneau des entiers de $\mathcal{O}_L$, c'est le cas partout sauf un nombre fini de points de $\operatorname{Spec} \mathcal{O}_L$. On peut comparer la factorisation des idéaux premiers comme dans le lemme avec celle de P.

Proposition 1.3.47. *Soit $\mathfrak{p}$ un idéal premier qui satisfait les conclusions de la proposition précédente. Soit $k = \mathcal{O}_K/\mathfrak{p}$, et soit $\overline{P}$ la réduction de P modulo $\mathfrak{p}$. Soit*

$$\overline{P} = \Pi_i \overline{P_i}^{e_i}$$

la décomposition en facteurs irréductibles du polynôme $\overline{P}$ dans $k[X]$, où les P_i sont dans $\mathcal{O}_K[X]$, unitaires. Alors, notant

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + P_i(\alpha)\mathcal{O}_L,$$

les $\mathfrak{P}_i$ sont les idéaux premiers distincts de $\mathcal{O}_L$ divisant $\mathfrak{p}$, et l'on a

$$\mathfrak{p}\mathcal{O}_L = \Pi_i \mathfrak{P}_i^{e_i}.$$

Démonstration. On a

$$\mathcal{O}_L/\mathfrak{p} = \mathcal{O}_K[\alpha]/\mathfrak{p} = \mathcal{O}_K[X]/(\mathfrak{p}, P) = k[X]/(\overline{P}) = \Pi_i k[X]/(\overline{P_i}^{e_i}).$$

Les idéaux premiers de $\Pi_i k[X]/(\overline{P_i}^{e_i})$ sont exactement les $\Pi_i(\overline{P_i})/(\overline{P_i}^{e_i})$. Cela montre, en prenant l'image réciproque dans $\mathcal{O}_L$, que les idéaux premiers de $\mathcal{O}_L$ contenant $\mathfrak{p}$ sont exactement les $\mathfrak{p}\mathcal{O}_L + P_i(\alpha)\mathcal{O}_L$. On a par ailleurs

$$\mathfrak{p}\mathcal{O}_L \subset \Pi_i \mathfrak{P}_i^{e_i}$$

car le produit des $\overline{P_i}^{e_i}$ s'envoie sur 0 dans $k[X]/(\overline{P})$, et

$$\mathfrak{p} \subset\neq \Pi_i \overline{P_i}^{e_i'}$$

si l'un des e_i' est strictement inférieur à e_i, par le même calcul. On a donc bien la factorisation annoncée de $\mathfrak{p}$. □

Corollaire 1.3.48. *Il n'existe qu'un nombre fini d'idéaux premiers $\mathfrak{p}$ de $\mathcal{O}_K$ qui sont ramifiés dans $\mathcal{O}_L$.*

Démonstration. On peut ne considérer que les idéaux au-dessus des $\mathfrak{p}$ comme dans la proposition précédente. Pour un tel $\mathfrak{p}$, la proposition précédente – dont on reprend les notations – garantit que $\mathfrak{p}$ est non-ramifié si et seulement si la réduction de P modulo $\mathfrak{p}$ n'a pas de racines multiples dans $\overline{k}$ la clôture algébrique de $\mathcal{O}_K/\mathfrak{p}$. C'est le cas dès que la réduction modulo $\mathfrak{p}$ du discriminant de P – qui est un élément non-nul de $\mathcal{O}_K$ – est non nulle modulo $\mathfrak{p}$, ce qui est vrai pour presque tout $\mathfrak{p}$. □

La discussion précédente n'a pas beaucoup d'intérêt pratique tant que l'on ne spécifie pas quels $\mathfrak{p}$ satisfont la condition de la proposition. Donnons deux exemples dans lesquels on sait garantir l'égalité $\mathcal{O}_{L,\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}[\alpha]$. Puisque tout nos énoncés sont compatibles à la localisation, supposons que $\mathcal{O}_K$ est un anneau de valuation discrète, d'idéal maximal $\mathfrak{p}$.

Lemme 1.3.49. *Soit A un anneau local, intègre noethérien, d'idéal maximal $\mathfrak{m}$. Alors A est un anneau de valuation discrète si et seulement si $\mathfrak{m}$ est principal.*

Démonstration. Il faut seulement montrer que si $\mathfrak{m}$ est principal, A est un anneau de valuation discrète.

Soit ϖ un élément de A tel que $(\varpi) = \mathfrak{m}$. On commence par montrer que l'intersection des $\mathfrak{m}^n$ est réduite à 0. Soit x un élément de $\bigcap_{n\geq 0} \mathfrak{m}^n$. Pour tout $n \geq 0$, on peut écrire

$$x = x_n \varpi^n$$

pour un certain $x_n \in A$. Alors on a $x_{n+1}\varpi = x_n$ pour tout $n \geq 0$. Si $x \neq 0$, la suite des idéaux (x_n) est donc strictement croissante, ce qui est une contradiction.

Soit maintenant I un idéal non nul de A. Soit n maximal tel que $I \subset \mathfrak{m}^n$. Un tel n existe grâce à ce que l'on vient de démontrer. Alors $\varpi^{-n} I$ est un idéal de A, qui n'est pas inclus dans $\mathfrak{m}$. C'est donc A, et $I = (\varpi^n)$, ce qui montre que A est principal. □

Proposition 1.3.50. *Avec les notations précédentes, si la réduction $\overline{P}$ de P modulo $\mathfrak{p}$ est irréductible, alors $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. C'est un anneau de valuation discrète. Si $\mathfrak{P}$ est l'unique idéal maximal de $\mathcal{O}_L$, on a $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}$, et $f_{\mathfrak{P}} = n$.*

Démonstration. Il s'agit simplement au vu de ce qui précède de montrer l'égalité $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Il est équivalent de montrer que $\mathcal{O}_K[\alpha]$ est intégralement clos, et il suffit de montrer que $A := \mathcal{O}_K[\alpha]$ est un anneau de valuation discrète.

Soit $\mathfrak{P}$ un idéal maximal de A. Supposons que $\mathfrak{P}$ ne contienne pas $\mathfrak{p}A$. Alors on a $\mathfrak{p}A + \mathfrak{P} = A$. Le lemme de Nakayama – puisque A est un $\mathcal{O}_K$-module de type fini –montre que $\mathfrak{P} = A$, contradiction. Ainsi, tout idéal maximal de A contient $\mathfrak{p}$. Par ailleurs, le quotient $A/\mathfrak{p}$ est isomorphe à $k[X]/(\overline{P})$, où k est le corps résiduel de $\mathfrak{p}$. L'hypothèse sur P garantit que ce quotient est un corps, ce qui montre que $\mathfrak{p}$ est l'unique idéal maximal de $\mathcal{O}_K$.

Comme $\mathcal{O}_K$ est un anneau de valuation discrète, $\mathfrak{p}$ est principal, donc $\mathfrak{p}A$ est principal. Le lemme précédent permet de conclure. □

Remarque 1.3.51. *On peut formuler une réciproque à la proposition précédente qui garantit l'existence d'un tel P dans la situation où $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}$.*

Voici un autre cas, qui correspond lui à la situation totalement ramifiée.

Proposition 1.3.52. *Avec les notations précédentes, supposons que P soit de la forme*

$$P = X^n + a_{n-1}X^{n-1} + \ldots + a_0,$$

où les a_i sont tous dans $\mathfrak{p}$, et $a_0 \notin \mathfrak{p}^2$. Alors $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. C'est un anneau de valuation discrète. Si $\mathfrak{P}$ est l'unique idéal maximal de $\mathcal{O}_L$, on a $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^n$, et $f_{\mathfrak{P}} = 1$.

Démonstration. Le critère d'Eiseinstein garantit qu'un tel P est toujours irréductible. La réduction $\overline{P}$ de P modulo $\mathfrak{p}$ est X^n. Soit $\mathfrak{P}$ un idéal maximal de $A = \mathcal{O}_K[\alpha]$. L'argument de la proposition précédente montre que $\mathfrak{P}$ contient $\mathfrak{p}A$. En particulier, $\mathfrak{P}$ contient α^n, donc α. Le quotient de A par $\mathfrak{p}A+(\alpha)$ est isomorphe à $\mathcal{O}_K[X]/(\mathfrak{p}, X) = k$, où k est le corps résiduel de $\mathfrak{p}$. C'est un corps, donc $\mathfrak{p}A+(\alpha)$ est l'unique idéal maximal de A.

Par hypothèse, a_0 est une uniformisante de $\mathfrak{p}$. Par ailleurs, a_0 est divisible par α dans A. On a donc $\mathfrak{p}A + (\alpha) = (\alpha)$, ce qui montre que l'idéal maximal de A est principal. Le lemme 1.3.49 permet de conclure. □

Remarque 1.3.53. *Voici l'analogie géométrique : soient $a_0, \ldots, a_{n-1}$ des fonctions $\mathcal{C}^\infty$ d'une variable t, qui s'annulent en $t = 0$, et considérons la sous-variété V de $\mathbb{R} \times \mathbb{R}$ définie localement au voisinage de $(0, 0)$ par l'équation*

$$f(X, t) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0.$$

On a $\partial f/\partial t(0, 0) = a_0'(0)dt$, donc si a_0 ne s'annule pas au second ordre en 0, alors V est lisse. On a par ailleurs $\partial f/\partial X(0, 0) = a_1(0) = 0$, donc c'est une condition nécessaire.

Remarque 1.3.54. *On peut là encore formuler et prouver une réciproque à la proposition précédente.*

1.3.5 Extensions galoisiennes

Reprenons encore les notations de 1.3.3. On suppose en outre que l'extension L/K est galoisienne de groupe G.

Proposition 1.3.55. *L'action du groupe G sur L laisse $\mathcal{O}_L$ globalement invariant.*

Démonstration. Soit α un élément de $\mathcal{O}_L$. Alors il existe un polynôme unitaire P à coefficients dans $\mathcal{O}_K$ qui annule α. Tout conjugué de α par G est annulé par P, donc est entier sur $\mathcal{O}_K$: il appartient à $\mathcal{O}_L$. □

Ce qui précède est facile mais fondamental : cela signifie que le groupe G agit sur le schéma affine $\operatorname{Spec} \mathcal{O}_L$. Par ailleurs, le fait que l'action laisse $\mathcal{O}_K$ invariant signifie précisément que G agit par automorphismes du $\operatorname{Spec} \mathcal{O}_K$-schéma $\operatorname{Spec} \mathcal{O}_L$. Autrement dit, si π est le morphisme fini $\operatorname{Spec} \mathcal{O}_L \to \operatorname{Spec} \mathcal{O}_K$, on a $\pi = \pi \circ g$ pour tout $g \in G$.

La proposition suivante montre que la condition galoisienne est la même, que l'on considère G comme agissant sur L ou sur $\operatorname{Spec} \mathcal{O}_L$.

Proposition 1.3.56. *Soit $\mathfrak{p}$ un idéal de $\mathcal{O}_K$.*

(i) Si $\mathfrak{P}$ est un diviseur premier de $\mathfrak{p}$ dans $\mathcal{O}_L$, et si σ est un élément de G, alors $\sigma(\mathfrak{P})$ est un diviseur premier de $\mathfrak{p}$ dans $\mathcal{O}_L$.

(ii) Le groupe G agit transitivement sur l'ensemble des diviseurs premiers de $\mathfrak{p}$.

Démonstration. Prouvons (i) (qui est évident : l'image inverse d'un idéal premier par un automorphisme d'anneaux est encore un idéal premier). La proposition précédente garantit que l'image d'un idéal de $\mathcal{O}_L$ par un élément de G est encore un idéal de $\mathcal{O}_L$. On a en outre un isomorphisme d'anneaux

$$\mathcal{O}_L/I \to \mathcal{O}_L/\sigma(I), x \mapsto \sigma(x)$$

qui garantit que I est premier si et seulement si $\sigma(I)$ est premier. Enfin, on a

$$I \cap \mathcal{O}_K = \sigma(I \cap \mathcal{O}_K) = \sigma(I) \cap \mathcal{O}_K,$$

ce qui montre que G agit bien sur l'ensemble des diviseurs premiers de $\mathfrak{p}$.

Raisonnons par l'absurde pour prouver (ii), et supposons qu'il existe deux diviseurs premiers $\mathfrak{P}$ et $\mathfrak{P}'$ tels que pour tout $\sigma \in G$, $\sigma(\mathfrak{P}) \neq \mathfrak{P}'$. Le théorème des restes chinois nous permet de trouver un élément x de $\mathcal{O}_L$ qui appartient à $\mathfrak{P}'$ mais à aucun des $\sigma(\mathfrak{P})$. On a

$$N_{L/K}(x) = \Pi_{\sigma \in G}\sigma(x) \in \mathfrak{P}' \cap \mathcal{O}_L = \mathfrak{p}.$$

En particulier, le produit des $\sigma(x)$ est dans $\mathfrak{P}$, mais, par hypothèse, aucun des $\sigma(x)$ n'est dans $\mathfrak{P}$, contradiction. □

La transitivité de l'action de Galois a la conséquence immédiate suivante.

Proposition 1.3.57. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. Si $\mathfrak{P}$ et $\mathfrak{P}'$ sont deux idéaux de $\mathcal{O}_L$ divisant $\mathfrak{p}$, on a*

$$e_{\mathfrak{P}} = e_{\mathfrak{P}'}$$

et

$$f_{\mathfrak{P}} = f'_{\mathfrak{P}}.$$

En particulier, si $g_{\mathfrak{p}}$ est le nombre d'idéaux premiers de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}$, on a

$$n = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}.$$

La proposition précédente nous permet de noter $e_{\mathfrak{p}}$ et $f_{\mathfrak{p}}$ pour les indices de ramification et les degrés d'inertie de tout premier divisant $\mathfrak{p}$.

On peut finir la preuve de la proposition 1.3.44.

Preuve de 1.3.44, (v). On peut supposer que $\mathcal{O}_K$ est un anneau de valuation discrète d'idéal maximal $\mathfrak{p}$, et que L/K est une extension galoisienne. Dans ce cas, $\mathcal{O}_L$ est principal, et on peut supposer que x est l'uniformisante d'un idéal premier $\mathfrak{P}$ au-dessus de $\mathfrak{p}$. La norme de x est

$$N_{L/K}(x) = \Pi_{\sigma \in G}\sigma(x),$$

donc, par transitivité,

$$N_{L/K}(x)\mathcal{O}_L = \Pi_{\sigma\in G}\sigma(\mathfrak{P}) = \Pi_{\mathfrak{P}'|\mathfrak{p}}\mathfrak{P}'^r,$$

où r est le quotient de $n = |G|$ par le nombre de $\mathfrak{P}$ au-dessus de $\mathfrak{p}$, i.e. $r = e_\mathfrak{p} f_\mathfrak{p}$. Cela montre

$$N_{L/K}(x)\mathcal{O}_K = \Pi_{\mathfrak{P}'|\mathfrak{p}}\mathfrak{P}'^{e_\mathfrak{p} f_\mathfrak{p}} = (\mathfrak{p}\mathcal{O}_L)^{f_\mathfrak{p}}.$$

On a par ailleurs

$$N_{L/K}(x\mathcal{O}_L) = N_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f_\mathfrak{p}}$$

par définition, ce qui conclut via le lemme ci-dessous. □

Lemme 1.3.58. *Soient $\mathcal{O}_K$ un anneau de Dedekind de corps des fractions K, et L/K une extension finie séparable. Soient I et J deux idéaux fractionnaires de $\mathcal{O}_K$ tels que $I\mathcal{O}_L = J\mathcal{O}_L$. Alors $I = J$.*

Démonstration. On a, n dénotant le degré de L sur K,

$$I^n = N_{L/K}(I\mathcal{O}_L) = N_{L/K}(J\mathcal{O}_L) = J^n,$$

donc $I = J$ – factoriser en produit d'idéaux premiers. □

Définition 1.3.59. *Soit $\mathfrak{P}$ un idéal de $\mathcal{O}_L$. Le sous-groupe de G qui laisse $\mathfrak{P}$ globalement stable est le groupe de décomposition de $\mathfrak{P}$. On note $Z_\mathfrak{P}$ le sous-corps de L sur lequel $D_\mathfrak{P}$ agit trivialement : c'est le corps de décomposition de $\mathfrak{P}$.*

La transitivité de l'action de G sur les diviseurs d'un $\mathfrak{p}$ donné et les bases sur les actions de groupes et la théorie de Galois nous donnent le résultat suivant.

Proposition 1.3.60. *Gardons les notations précédentes. Soit $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$.*

(i) Si $\mathfrak{P}'$ est un diviseur premier de $\mathfrak{p}$, les groupes de décomposition $D_\mathfrak{P}$ et $D_{\mathfrak{P}'}$ sont conjugués.

(ii) L'indice de $D_\mathfrak{P}$ dans G est égal au nombre $g_\mathfrak{p}$ de diviseurs premiers de $\mathfrak{p}$.

(iii) On a

$$[Z_\mathfrak{P} : K] = g_\mathfrak{p}, [L : Z_\mathfrak{P}] = e_\mathfrak{p} f_\mathfrak{p},$$

et l'extension $L/Z_\mathfrak{P}$ est galoisienne de groupe $D_\mathfrak{P}$.

(iv) $\mathfrak{p}$ est totalement décomposé si et seulement si $D_\mathfrak{P} = \{1\}$.

(v) $\mathcal{O}_{L,\mathfrak{p}}$ est un anneau de valuation discrète si et seulement si $D_\mathfrak{P} = G$.

Proposition 1.3.61. *Notons $\mathcal{O}_Z$ l'anneau des entiers de $Z_\mathfrak{P}$, et $\mathfrak{P}_Z$ l'idéal $\mathfrak{P} \cap \mathcal{O}_Z$. Alors*

(i) $\mathfrak{P}$ *est l'unique diviseur premier de* $\mathfrak{P}_Z$*, son indice de ramification est* $e_{\mathfrak{P}}$ *et son degré résiduel* $f_{\mathfrak{P}}$ *(au-dessus de* $\mathcal{O}_Z$*) ;*

(ii) l'indice de ramification et le degré de $\mathfrak{P}_Z$ *au-dessus de* $\mathfrak{p}$ *sont tous les deux égaux à* 1*.*

Démonstration. Les idéaux de $\mathcal{O}_L$ au-dessus de $\mathfrak{P}_Z$ sont les $\sigma(\mathfrak{P})$, $\sigma \in D_{\mathfrak{P}}$, ils sont donc tous égaux à $\mathfrak{P}$. En particulier, les différents $\mathfrak{P}_Z$ sont deux à deux distincts.

Écrivons

$$\mathfrak{P}_Z \mathcal{O}_L = \mathfrak{P}^{e'_{\mathfrak{P}}}.$$

Alors, si $f'_{\mathfrak{P}}$ est le degré résiduel de $\mathfrak{P}$ sur $\mathcal{O}_Z$, on a

$$e'_{\mathfrak{P}} f'_{\mathfrak{P}} = [L : Z_{\mathfrak{P}}] = e_{\mathfrak{P}} f_{\mathfrak{P}}.$$

Comme par ailleurs $e'_{\mathfrak{P}}$ et $f'_{\mathfrak{P}}$ divisent $e_{\mathfrak{P}}$ et $f_{\mathfrak{P}}$ respectivement, on bien l'égalité de (i). L'égalité de (ii) suit. □

Notons $\kappa(\mathfrak{p})$ et $\kappa(\mathfrak{P})$ les corps résiduels de $\mathfrak{p}$ et $\mathfrak{P}$ respectivement. Supposons l'extension résiduelle séparable (c'est le cas automatiquement si $\kappa(\mathfrak{p})$ est fini).

Proposition 1.3.62. *L'extension résiduelle* $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ *est galoisienne. Le morphisme naturel*

$$D_{\mathfrak{P}} \to Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$$

est surjectif.

Démonstration. Explicitons le morphisme naturel. Soit $\sigma \in D_{\mathfrak{P}}$. Par définition, σ laisse invariant $\mathfrak{P}$, donc passe à la réduction modulo $\mathfrak{P}$ pour induire un automorphisme de $\kappa(\mathfrak{P})$. Cet automorphisme laisse $\kappa(\mathfrak{p})$ invariant car σ laisse K invariant.

Pour montrer le résultat, on peut remplacer K par $Z_{\mathfrak{P}}$ au vu de l'énoncé (ii) de la proposition précédente. On peut aussi localiser et supposer pour fixer les idées que $\mathcal{O}_K$ est un anneau de valuation discrète d'idéal maximal $\mathfrak{p}$. Comme $\mathfrak{P}$ est l'unique diviseur premier de $\mathfrak{p}$ dans $\mathcal{O}_L$, $\mathcal{O}_L$ est lui aussi un anneau de valuation discrète. On a dans ce cas $D_{\mathfrak{P}} = G$.

Par hypothèse, l'extension résiduelle est séparable. Soit donc α un élément de $\mathcal{O}_L$ dont la réduction $\overline{\alpha}$ modulo $\mathfrak{P}$ engendre $\kappa(\mathfrak{P})$ sur $\kappa(\mathfrak{p})$. Soit P le polynôme minimal de α. Alors la réduction $\overline{P}$ de P modulo $\mathfrak{p}$ annule $\overline{\alpha}$. Comme L/K est galoisienne, P est scindé sur L, donc $\overline{P}$ est scindé sur $\kappa(\mathfrak{P})$, et l'extension résiduelle est bien galoisienne.

Enfin, comme L/K est galoisienne, G agit transitivement sur les racines de P dans L, dont les réductions modulo $\mathfrak{P}$ sont d'après ce qui précède les racines de $\overline{P}$ dans $\kappa(\mathfrak{P})$. On a donc bien la surjection cherchée. □

Définition 1.3.63. *Le noyau $I_{\mathfrak{P}}$ du morphisme*

$$D_{\mathfrak{P}} \to Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$$

est le groupe d'inertie de $\mathfrak{P}$ sur K. On note $T_{\mathfrak{P}}$ le sous-corps de L fixé par $I_{\mathfrak{P}}$.

À la suite exacte

$$1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \to Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) \to 1$$

correspond la tour d'extensions

$$K \subset Z_{\mathfrak{P}} \subset T_{\mathfrak{P}} \subset L.$$

Proposition 1.3.64. *Avec les notations précédentes, notons $\mathfrak{P}_T = \mathfrak{P} \cap T$:*

(i) l'indice de ramification de $\mathfrak{P}$ sur $\mathfrak{P}_T$ est e, et le degré résiduel est 1 ;

(ii) l'indice de ramification de $\mathfrak{P}_T$ sur $\mathfrak{P}_Z$ est 1, et le degré résiduel est f.

Démonstration. Par construction, on a $\kappa(\mathfrak{P}_T) = \kappa(\mathfrak{P})$. Cela montre que le degré résiduel de $\mathfrak{P}$ sur $\mathfrak{P}_T$ est 1. Les autres inégalités s'en déduisent. □

1.3.6 Discriminant, différente

Une référence ardue mais complète pour comprendre le lien entre les différentielles de Kähler et le module dualisant dans le cas qui nous occupe (et plus généralement le cas de dimension relative nulle) est le chapitre 47 du Stacks Projects.

On commence par du calcul différentiel.

Définition 1.3.65. *Soit A un anneau, et soit B une A-algèbre. Soit M un B-module. Une A-dérivation de B est un morphisme de A-modules*

$$d : B \to M$$

qui satisfait la règle de Leibniz :

$$\forall x, y \in B, d(xy) = xd(y) + yd(x).$$

Il n'est pas difficile de montrer le théorème suivant.

Théorème 1.3.66. *Soit A un anneau, et soit B une A-algèbre. Il existe un B-module $\Omega^1_{B/A}$, et une dérivation*

$$d : B \to \Omega^1_{B/A},$$

universels au sens suivant : pour toute dérivation $d_M : B \to M$, il existe un unique morphisme B-modules $\Omega^1_{B/A} \to M$ qui fait commuter le diagramme

$$\begin{array}{ccc} B & \xrightarrow{d} & \Omega^1_{B/A} \\ & \searrow^{d_M} & \downarrow \\ & & M. \end{array}$$

Définition 1.3.67. *Avec les notations précédentes, $\Omega^1_{B/A}$ est le module des différentielles relatives de B sur A.*

On peut donner une description explicite de $\Omega^1_{B/A}$: c'est le B-module engendré par les symboles dx, $x \in B$, avec les relations $d(x+y) = dx + dy$ et $d(xy) = xd(y) + yd(x)$ pour $x, y \in B$, et $da = 0$ pour $a \in A$. Bien entendu, la propriété universelle qui les caractérise montre que $\Omega^1_{B/A}$ et la dérivation universelle sont uniques à unique isomorphisme près.

Voici quelques propriétés du module des différentielles qui sont garanties par la propriété universelle et la description ci-dessus.

Proposition 1.3.68. *Soit B une algèbre sur un anneau A.*

(i) Si B est une algèbre de type fini sur A, engendrée par les x_i, alors $\Omega^1_{B/A}$ est un B-module de type fini, engendré par les dx_i.

(ii) Soit A' une A-algèbre. Alors $\Omega^1_{(B\otimes_A A')/A'} = \Omega^1_{B/A} \otimes_A A'$.

(iii) Soit C une B-algèbre. On dispose d'une suite exacte de C-modules

$$\Omega^1_{B/A} \otimes_B C \to \Omega^1_{C/A} \to \Omega^1_{C/B} \to 0.$$

(iv) Soit S un sous-ensemble multiplicatif de B. Alors

$$\Omega^1_{S^{-1}B/A} = S^{-1}\Omega^1_{B/A}.$$

Démonstration. Le premier point est une conséquence de la description de $\Omega^1_{B/A}$ par générateurs et relations ci-dessus.

Avec les notations du deuxième énoncé, notons $B' = B \otimes_A A'$. Si M est un B-module, toute dérivation $B \to M$ donne lieu par produit tensoriel à une dérivation $B' \to M' := M \otimes_B B'$. Appliquant cela à la dérivation universelle, on trouve une flèche

$$\Omega^1_{B'/A'} \to \Omega^1_{B/A},$$

qui envoie $d(b \otimes a')$ sur $a'd(b)$. Par ailleurs, la dérivation universelle $B' \to \Omega^1_{B'/A'}$ donne, par précomposition avec $B \to B'$, une A-dérivation $B \to \Omega^1_{B'/A'}$, d'où un morphisme de B-modules

$$\Omega^1_{B/A} \to \Omega^1_{B'/A'}$$

qui envoie $d(b)$ sur $d(b\otimes 1)$. On en déduit un morphisme $\Omega^1_{B/A} \otimes_B B' \to \Omega^1_{B'/A'}$, inverse du précédent.

Prouvons le troisième point. Si M est un C-module, notons $Der_A(C, M)$ le C-module des A-dérivations de C dans M. On a une suite exacte (exercice)

$$0 \to Der_B(C, M) \to Der_A(C, M) \to Der_A(B, M) \otimes_B C.$$

La propriété universelle des modules de différentielles permet de conclure.

Le dernier point est laissé en exercice. □

Considérons l'exemple fondamental d'une extension monogène.

Proposition 1.3.69. *Soit A un anneau, et soit $P \in A[X]$. Soit $B = A[X]/(P)$. Alors*

$$\Omega^1_{B/A} = B/(P'(X))dX = A[X]/(P, P')dX$$

comme B-module.

Démonstration. La proposition 1.3.68 montre que le B-module $\Omega^1_{B/A}$ est engendré par dX. On a $P(X) = 0$ dans B, donc en dérivant, $P'(X)dX = 0$ dans $\Omega^1_{B/A}$. Enfin, la flèche

$$B \to B/(P'(X))dX, Q(X) \mapsto Q'(X)dX$$

est bien définie, et c'est une dérivation, d'où une flèche $\Omega^1_{B/A} \to B/(P'(X))dX$, qui est surjective car elle envoie dX sur dX, et injective d'après ce qui précède. □

Proposition 1.3.70. *Soit k un corps, P un polynôme à coefficients dans k, $K = k[X]/(P)$. Alors $\Omega^1_{K/k}$ est nul si et seulement si le polynôme P est séparable.*

Démonstration. On applique la proposition ci-dessus et le fait que P et P' sont premiers entre eux si et seulement si P est séparable. □

Remarque 1.3.71. *Avec les notations de la preuve, remarquons que dans le cas $P = (X - \alpha)^n$, la dimension de $\Omega^1_{K/k}$ comme k-espace vectoriel est $n - 1$ si n est premier à la caractéristique de k, et n sinon.*

Proposition 1.3.72. *Soit k un corps, et soit K une K-algèbre finie. Soit $\overline{k}$ une clôture algébrique de k. Alors $\Omega^1_{K/k}$ est nul si et seulement si $K \otimes_k \overline{k}$ est réduit.*

En particulier, si K est un corps, alors $\Omega^1_{K/k}$ est nul si et seulement si K/k est séparable.

Démonstration. Le second énoncé est une conséquence immédiate du premier.

Pour montrer le premier, on peut supposer k algébriquement clos. Dans ce cas, on sait que K est un produit direct de k-algèbres locales A dont l'idéal maximal $\mathfrak{m}$ vérifie $\mathfrak{m}^n = 0$ pour un certain entier n. On peut remplacer K par A, et il faut montrer que si $\mathfrak{m} \neq 0$, alors $\Omega^1_{A/k} \neq 0$.

Si $\mathfrak{m} \neq 0$, alors le lemme de Nakayama montre que $\mathfrak{m} \neq \mathfrak{m}^2$. Notons que $A/\mathfrak{m}$ est un corps, qui est une extension finie de k. C'est donc k lui-même. On obtient ainsi un morphisme de k-algèbres $A \to k$ de noyau $\mathfrak{m}$, ce qui nous permet, via l'inclusion naturelle $k \to A$, d'identifier A à $k \oplus \mathfrak{m}$.

Soit $\phi : \mathfrak{m}/\mathfrak{m}^2 \to k$ une application k-linéaire non-nulle. On définit une dérivation d de A par la formule

$$d(c + m) = \phi(\overline{m}),$$

où c est un élément de k, m un élément de $\mathfrak{m}$, et $\overline{m}$ l'image de m dans $\mathfrak{m}/\mathfrak{m}^2$. On vérifie immédiatement que d est une dérivation non-nulle. Cela prouve que $\Omega^1_{A/k}$ est non-nul. □

Nous allons maintenant considérer le cas particulier des anneaux de Dedekind.

Donnons-nous $\mathcal{O}_K$ un anneau de Dedekind de corps des fractions K, L une extension finie séparable de K, et $\mathcal{O}_L$ l'anneau des entiers de L. On sait donc que $\mathcal{O}_L$ est un anneau de Dedekind fini sur $\mathcal{O}_K$. On peut considérer le $\mathcal{O}_L$-module $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$.

Proposition 1.3.73. *Le $\mathcal{O}_L$-module $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$ est de torsion. Son support est l'ensemble des $\mathfrak{P} \in \mathrm{Spec}\,(\mathcal{O}_L)$ qui sont ramifiés.*

Démonstration. Rappelons que le support d'un A-module M est l'ensemble des $\mathfrak{p} \in \mathrm{Spec}\,(A)$ tels que $M \otimes_A A/\mathfrak{p} \neq 0$. Si A est intègre, alors M est de torsion si et seulement si $M \otimes_A \mathrm{Frac}(A) = 0$, i.e. si et seulement si son support ne contient pas le point générique de $\mathrm{Spec}\,(A)$. L'idéal nul de $\mathcal{O}_L$ n'étant pas ramifié, il suffit de prouver le second énoncé.

On va appliquer une variante du corollaire 1.3.41. Soit $\mathfrak{P}$ un idéal premier de $\mathcal{O}_L$, divisant l'idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$. Considérons la $\kappa(\mathfrak{p})$-algèbre $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. Le théorème chinois garantit un isomorphisme canonique

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L/\mathfrak{P}^e \times A,$$

où A est un quotient de $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ dans lequel $\mathfrak{P}$ devient l'idéal A. La compatibilité de la formation de Ω^1 au produit tensoriel – donc au passage au quotient – montre que l'on a

$$\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} \otimes_{\mathcal{O}_L} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = \Omega^1_{\mathcal{O}_L/\mathcal{O}_K} \otimes_{\mathcal{O}_K} \kappa(\mathfrak{p}) = \Omega^1_{\mathcal{O}_L/\mathfrak{p}/\kappa(\mathfrak{p})}.$$

Localisant en $\mathfrak{P}$, il vient

$$\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} \otimes_{\mathcal{O}_L} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = \Omega^1_{(\mathcal{O}_L/\mathfrak{P}^e)/\kappa(\mathfrak{p})}$$

et enfin, en réduisant modulo $\mathfrak{P}$,

$$\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} \otimes_{\mathcal{O}_L} \kappa(\mathfrak{P}) = \Omega^1_{(\mathcal{O}_L/\mathfrak{P}^e)/\kappa(\mathfrak{p})} \otimes \kappa(\mathfrak{P}),$$

de sorte que $\mathfrak{P}$ appartient au support de $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$ si et seulement si le $\mathcal{O}_L/\mathfrak{P}^e$-module $\Omega^1_{(\mathcal{O}_L/\mathfrak{P}^e)/\kappa(\mathfrak{p})}$ est non-nul, i.e., via la proposition ci-dessus, si et seulement si $(\mathcal{O}_L/\mathfrak{P}^e)/\kappa(\mathfrak{p})$ est géométriquement réduit. Le calcul du corollaire 1.3.41 montre que c'est le cas si et seulement si $\mathfrak{P}$ est ramifié. □

Remarque 1.3.74. *On retrouve la finitude du nombre de premiers ramifiés.*

La discussion précédente ne permet pas facilement de calculer le module des différentielles relatives d'une extension d'anneaux d'entiers de corps de nombres quand celle-ci n'est pas donnée par une présentation explicite. Dans ce qui suit, on va remédier à ce problème.

Définition 1.3.75. *Le module dualisant de L/K, noté $\omega_{L/K}$, est l'idéal fractionnaire*

$$\omega_{L/K} = \{x \in L | \mathrm{Tr}_{L/K}(x\mathcal{O}_L) \subset \mathcal{O}_K\}.$$

La différente de L/K, notée $\mathfrak{D}_{L/K}$, est l'idéal fractionnaire inverse de $\omega_{L/K}$.

Remarque 1.3.76. *Il faudrait noter $\mathcal{O}_L/\mathcal{O}_K$ dans les indices, mais on gardera cet abus de notation. On appelle souvent $\omega_{L/K}$ la codifférente, ou différente inverse.*

La compatibilité manifeste de la formation de $\omega_{L/K}$ à la localisation montre que la formation de la différente est compatible à la localisation.

Remarque 1.3.77. *Si B est un $\mathcal{O}_K$-ordre de L, on peut considérer le module $\omega_{B/\mathcal{O}_K}$ défini comme ci-dessus. La compatibilité à la localisation s'exprime par l'égalité*

$$\omega_{S^{-1}B/S^{-1}\mathcal{O}_K} = S^{-1}\omega_{B/\mathcal{O}_K},$$

où S est un sous-ensemble multiplicatif de $\mathcal{O}_K$.

Proposition 1.3.78. *Soit $K \subset L \subset M$ une tour d'extension finie. Alors*

$$\omega_{M/K} = \omega_{M/L}\omega_{L/K}$$

et

$$\mathfrak{D}_{M/K} = \mathfrak{D}_{M/L}\mathfrak{D}_{L/K}.$$

Démonstration. Il suffit de prouver l'énoncé sur le module dualisant. On a clairement

$$\omega_{M/L}\omega_{L/K} \subset \omega_{M/K}.$$

Pour l'autre sens, on remarque

$$Tr_{M/L}(\omega_{M/K}\mathcal{O}_M) \subset \omega_{L/K}$$

d'où, multipliant par $\omega_{L/K}^{-1}$,

$$Tr_{M/L}(\omega_{L/K}^{-1}\omega_{M/K}\mathcal{O}_M) \subset \mathcal{O}_L$$

ce qui prouve le résultat. □

Proposition 1.3.79. *On a un isomorphisme canonique*

$$\omega_{B/\mathcal{O}_K} \to \mathrm{Hom}_{\mathcal{O}_K}(B, \mathcal{O}_K), x \mapsto (y \mapsto \mathrm{Tr}_{L/K}(xy)).$$

Démonstration. Le morphisme ci-dessus est bien défini par définition du module dualisant. Il est injectif par non-dégénérescence de la trace pour les extensions séparables.

Quant à la surjectivité, elle est formelle : tout K-morphisme de L vers K est de la forme $y \mapsto \mathrm{Tr}_{L/K}(xy))$ pour un certain x de K. Les x qui induisent un morphisme de B dans $\mathcal{O}_K$ sont précisément ceux qui appartiennent au module dualisant, par définition de celui-ci. □

Nous identifierons maintenant $\omega_{L/K}$ et $\mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K)$. On dispose d'un morphisme injectif naturel (l'inclusion !)

$$\mathcal{O}_L \to \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{O}_L, \mathcal{O}_K) = \omega_{L/K}.$$

Plus généralement, on a une injection

$$B \to \omega_{B/\mathcal{O}_K}.$$

On va montrer que le quotient est le module des différentielles relatives – au moins dans le cas monogène, on traitera le cas général plus tard.

Proposition 1.3.80. *Soit $B = \mathcal{O}_K[\alpha]$. Alors on a une suite exacte*

$$0 \to B \to \omega_{B/\mathcal{O}_K} \to \Omega^1_{B/\mathcal{O}_K} \to 0.$$

Démonstration. Commençons par calculer $\omega_{B/\mathcal{O}_K}$. Soit P le polynôme minimal de α, soit

$$P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0.$$

On a la formule

$$Tr_{L/K}\Big(\frac{P(X)}{X-\alpha}\frac{\alpha^r}{P'(\alpha)}\Big) = X^r$$

pour tout r entre 0 et $n-1$. Pour la montrer, soit M une clôture galoisienne de L/K, et α_i les racines de P dans M. Il s'agit de prouver

$$\sum_{i=1}^{n} \frac{P(X)}{X-\alpha_i}\frac{\alpha_i^r}{P'(\alpha_i)} = X^r.$$

C'est clair : les deux membres sont des polynômes de degré $\leq n-1$, qui prennent les mêmes valeurs en les α_i.

La formule signifie que la base duale de $(1, \alpha, \ldots, \alpha^{n-1})$ par rapport à la forme bilinéaire donnée par la trace est donnée par $\frac{1}{P'(\alpha)}(b_0, \ldots, 1)$, où

$$\frac{P(X)}{X-\alpha} = X^{n-1} + \ldots + b_0.$$

On vérifie par ailleurs sans difficulté que $\mathcal{O}_K b_0 + \ldots + \mathcal{O}_K b_{n-1}$ est l'anneau $B = \mathcal{O}_K[\alpha]$. En particulier, on trouve enfin

$$\omega_{B/\mathcal{O}_K} = \frac{1}{P'(\alpha)}B.$$

On conclut directement via la proposition 1.3.69. □

Corollaire 1.3.81. *Supposons $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Alors la différente $\mathfrak{D}_{L/K}$ est l'annulateur de $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$.*

Démonstration. Écrivons $\omega_{L/K} = \Pi_i \mathfrak{P}_i^{-e_i}$. Alors $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} \simeq \Pi_i \mathcal{O}_L/\mathfrak{P}_i^{e_i}$ et $\mathfrak{D}_{L/K} = \Pi_i \mathfrak{P}_i^{e_i}$. □

Les deux résultats précédents sont vrais pour $\mathcal{O}_L$ sans supposer qu'il est monogène. Montrons que c'est le cas pour le second. Pour cela, commençons par un résultat de structure, qui contient une réciproque à la proposition 1.3.52.

Proposition 1.3.82. *Soit A un anneau de valuation discrète, d'idéal maximal $\mathfrak{p}$ et de corps des fractions K, et soit L une extension finie séparable de degré n de K. Soit B la clôture intégrale de B dans A, et soit $\mathfrak{P}$ un idéal premier de B. On suppose l'extension résiduelle $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ séparable. Alors il existe un élément x de B tel que les localisés de $A[x]$ en un idéal premier et de B en $\mathfrak{P}$ coïncident.*

Démonstration. Soit ϖ un générateur de $\mathfrak{P}B_{\mathfrak{P}}$ qui est dans B, et soit x un élément de B dont la réduction modulo $\mathfrak{P}$ engendre l'extension résiduelle (qui est séparable donc monogène). Alors si $B' = A[x, \varpi]$, le localisé de B' en (ϖ) coïncide avec $B_{\mathfrak{P}}$. D'après le lemme de Nakayama, il suffit pour cela de montrer que la flèche naturelle $B'_{\varpi}/(\varpi) \to B_{\varpi}/(\varpi)$ est un isomorphisme, ce qui est clair.

Pour conclure à la première partie de l'énoncé, il suffit donc de trouver x comme ci-dessus de telle sorte qu'un certain polynôme $R(x)$ en x soit un générateur de $\mathfrak{P}$. On choisit d'abord x quelconque. Soit R le relevé dans A d'un polynôme annulateur de la réduction de x modulo $\mathfrak{P}$. Alors ϖ divise $R(X)$ dans le localisé B_{ϖ}. On considère les valuations dans B_{ϖ}. Si $R(x)$ a valuation 1, on a trouvé un x adéquat. Sinon, $R(x)$ a valuation au moins 2 et l'on écrit.

$$R(x + \varpi) = R(x) + \varpi R'(x) + \varpi^2 y,$$

$y \in B$. Comme la réduction de R modulo $\mathfrak{P}$ est séparable, $R'(x)$ a valuation 0, donc $R(x + \varpi)$ a valuation 1. □

Remarque 1.3.83. *On peut bien entendu appliquer le lemme en partant d'un anneau de Dedekind quelconque A, et en le localisant en $\mathfrak{p}$.*

Proposition 1.3.84. *On a une suite exacte*

$$0 \to \mathcal{O}_L \to \omega_{L/K} \to \Omega^1_{\mathcal{O}_L/\mathcal{O}_K} \to 0.$$

La différente $\mathfrak{D}_{L/K}$ est l'annulateur de $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$.

Démonstration. La suite exacte signifie que le quotient de $\omega_{L/K}$ par $\mathcal{O}_L$ est isomorphe à $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$.

Les deux propriétés sont locales, on peut donc supposer que $\mathcal{O}_K = A$ est un anneau de valuation discrète. Soit $\mathfrak{p}$ l'idéal maximal de A. Soit $\mathfrak{P}$ un idéal de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}$.

On utilise le lemme précédent pour trouver une extension monogène B de A dans L qui coïncide avec $\mathcal{O}_L$ après localisation en $\mathfrak{P}$. Appliquant la proposition 1.3.80 et la compatibilité des modules dualisants à la localisation, on conclut. □

Remarque 1.3.85. *La suite exacte ci-dessus est l'analogue de la suite exacte de Riemann-Hurwitz pour des morphismes de courbes sur un corps.*

Les invariants que l'on a défini vivent sur $\mathcal{O}_L$. On peut prendre leur norme.

Définition 1.3.86. *Le discriminant $\mathfrak{d}_{L/K}$ est l'idéal de $\mathcal{O}_K$ défini par*

$$\mathfrak{d}_{L/K} = N_{L/K}(\mathfrak{D}_{L/K}).$$

On peut calculer le discriminant explicitement. Si $\alpha_1, \ldots, \alpha_n$ sont n éléments d'un module sur un anneau A, muni d'une forme bilinéaire $< ., . >$, on note $d(\alpha_1, \ldots, \alpha_n)$ le déterminant de la matrice $< \alpha_i, \alpha_j >$. C'est le *discriminant* des α_i. Dans le cas qui nous occupe, L est muni d'une K-forme bilinéaire donnée par

$$< x, y >= Tr_{L/K}(xy).$$

Lemme 1.3.87. *Supposons L/K de degré n. Soit L' une clôture galoisienne de L/K, et $\sigma_1, \ldots, \sigma_n$ les K-plongements de L dans L'. Soient $\alpha_1, \ldots, \alpha_n$ des éléments de L. Alors $d(\alpha_1, \ldots, \alpha_n)$ est le carré du déterminant de la matrice $(\sigma_i(\alpha_j))$.*

Démonstration. La trace de $\alpha_i\alpha_j$ est la somme sur k des $\sigma_k(\alpha_i)\sigma_k(\alpha_j)$. Ainsi, la matrice

$$(Tr_{L/K}(\alpha_i\alpha_j))_{i,j}$$

est le produit de la matrice $(\sigma_i(\alpha_j))$ et de sa transposée. □

Proposition 1.3.88. *Supposons L de degré n sur K. Le discriminant $\mathfrak{d}_{L/K}$ est l'idéal de $\mathcal{O}_K$ engendré par tous les discriminants $d(\alpha_1, \ldots, \alpha_n)$, où $(\alpha_1, \ldots, \alpha_n)$ parcourt les bases de L sur K contenues dans $\mathcal{O}_L$.*

Démonstration. La question est locale, on peut donc supposer que $A = \mathcal{O}_K$ est un anneau de valuation discrète. Dans ce cas, A est un anneau principal. Soit $\alpha_1, \ldots, \alpha_n$ une base de $B = \mathcal{O}_L$ comme A-module. Le discriminant de toute base $\beta_1, \ldots, \beta_n$ de L sur K, contenue dans $\mathcal{O}_L$, est divisible par $d(\alpha_1, \ldots, \alpha_n)$. Il s'agit donc de montrer l'égalité

$$\mathfrak{d}_{L/K} = d(\alpha_1, \ldots, \alpha_n).$$

Soit $\alpha'_1, \ldots, \alpha'_n$ la base duale de $\alpha_1, \ldots, \alpha_n$ dans L. Par définition, on a

$$\omega_{L/K} = \mathcal{O}_K\alpha'_1 + \ldots \mathcal{O}_K\alpha'_n.$$

Comme B est principal, on peut écrire

$$\omega_{L/K} = (x) = \mathcal{O}_K x\alpha_1 + \ldots + \mathcal{O}_K x\alpha_n$$

et

$$\mathfrak{d}_{L/K} = N_{L/K}(x)^{-1}.$$

Calculons enfin le discriminant du B-module $\omega_{L/K}$ – cf la remarque 1.3.30 pour la définition. Ce discriminant vaut

$$d(\alpha_1', \ldots, \alpha_n') = d(x\alpha_1, \ldots, x\alpha_n).$$

Le lemme précédent montre directement que le membre de droite vaut

$$d(x\alpha_1, \ldots, x\alpha_n) = N_{L/K}(x)^2 d(\alpha_1, \ldots, \alpha_n).$$

Par ailleurs, notant $M(\alpha_1, \ldots, \alpha_n)$ la matrice des $\sigma_i(\alpha_j)$ (notations du lemme ci-dessus), on a

$$M(\alpha_1, \ldots, \alpha_n)^t M(\alpha_1', \ldots, \alpha_n') = \mathrm{Id}$$

par définition de la base duale. Ainsi, grâce au lemme précédent

$$d(\alpha_1, \ldots, \alpha_n) d(\alpha_1', \ldots, \alpha_n') = 1.$$

On a donc

$$d(\alpha_1, \ldots, \alpha_n)^{-1} = d(\alpha_1, \ldots, \alpha_n) N_{L/K}(x)^2$$

et

$$d(\alpha_1, \ldots, \alpha_n)^2 = N_{L/K}(x)^{-2},$$

ce qui conclut. □

Un cas particulièrement intéressant est le suivant, que l'on a démontré en passant.

Proposition 1.3.89. *Avec les notations précédentes, si $\mathcal{O}_K$ est principal, et si $\alpha_1, \ldots, \alpha_n$ est une base de $\mathcal{O}_L$ comme $\mathcal{O}_K$-module, alors*

$$\mathfrak{d}_{L/K} = d(\alpha_1, \ldots, \alpha_n).$$

Le cas où $K = \mathbb{Q}$ est très important : il nous permet de faire le lien entre la théorie que l'on a développée, essentiellement locale, et des propriétés archimédiennes.

Définition 1.3.90. *Soit K un corps de nombres. Le discriminant de K, noté d_K, est l'entier*

$$d_K = d(\alpha_1, \ldots, \alpha_n),$$

où $\alpha_1, \ldots, \alpha_n$ est une base de $\mathcal{O}_K$ comme $\mathbb{Z}$-module.

Remarque 1.3.91. *L'idéal $\mathfrak{d}_{K/\mathbb{Q}} = (d_K)$ ne détermine le discriminant qu'au signe près.*

1.3.7 Géométrie des nombres, suite

On va reprendre les résultats que l'on a obtenu par géométrie de nombres dans un contexte où l'on peut préciser les covolumes des réseaux considérés.

On se donne un corps de nombres K, de degré n sur $\mathbb{Q}$. Soient $\sigma_1, \dots, \sigma_{r_1}$ les plongements de K dans $\mathbb{R}$. Soient $\tau_1, \dots, \tau_{r_2}$ et leurs conjugués les plongements complexes. On considère l'injection

$$i : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, x \mapsto (\sigma_1(x), \dots, \sigma_{r_1}(x), \tau_1(x), \dots, \tau_{r_2}(x)).$$

La proposition 1.2.22 et sa démonstration garantit que $K \otimes_{\mathbb{Q}} \mathbb{R}$ s'identifie à $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ de manière induite par i. En particulier, i identifie l'anneau des entiers $\mathcal{O}_K$ – et, plus généralement, tout sous $\mathcal{O}_K$-module de type fini dans K, et donc tout idéal fractionnaire – à un réseau dans le $\mathbb{R}$-espace vectoriel $V = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, de dimension n sur $\mathbb{R}$. On identifiera souvent K à son image dans V.

Commençons par établir quelques propriétés de la norme. En particulier, on a en vue l'explicitation de la proposition 1.2.37 dans notre contexte.

Proposition 1.3.92. *Soit $x \in K$, et notons $(t_1, \dots, t_{r_1}, x_1, y_1, \dots, x_{r_2}, y_{r_2}) = i(x) \in V = \mathbb{R}^n$. Alors*

$$|N_{K/\mathbb{Q}}(x)| = |t_1| \dots |t_{r_1}| \Pi_{i=1}^{r_2} (x_i^2 + y_i^2).$$

En particulier, on a

$$|N_{K/\mathbb{Q}}(x)| \leq n^{-n/2} \Big(\sqrt{t_1^2 + \dots + t_{r_1}^2 + 2(x_1^2 + y_1^2) + \dots + 2(x_{r_2}^2 + y_{r_2}^2)} \Big)^n.$$

Démonstration. La première égalité est claire par définition de i. La seconde est l'inégalité entre moyenne géométrique et moyenne L^2. □

La proposition ci-dessus justifie la définition de la norme euclidienne $||.||$ sur V définie par

$$||(t_1, \dots, t_{r_1}, x_1, y_1, \dots, x_{r_2}, y_{r_2})||^2 = t_1^2 + \dots + t_{r_1}^2 + 2(x_1^2 + y_1^2) + \dots + 2(x_{r_2}^2 + y_{r_2}^2).$$

On munit V de la mesure correspondante.

La proposition précédente devient donc :

Proposition 1.3.93. *Soit $x \in K$. Alors*

$$|N_{K/\mathbb{Q}}(x)| \leq n^{-n/2} ||i(x)||^n.$$

Lemme 1.3.94. *Soit I un idéal de $\mathcal{O}_K$. Alors*

$$N_{K/\mathbb{Q}}(I) = \big(|\mathcal{O}_K / I| \big).$$

Démonstration. Factorisant I en produit d'idéaux premiers et utilisant le théorème chinois, on peut supposer que I est de la forme $\mathfrak{p}^r$, où $\mathfrak{p}$ est premier dans $\mathcal{O}_K$ et $r > 0$. Filtrant $\mathcal{O}_K/\mathfrak{p}^r$ par les $\mathfrak{p}^i/\mathfrak{p}^r$, on se ramène au cas où $r = 1$, auquel cas on a par définition

$$N_{K/\mathbb{Q}}(\mathfrak{p}) = (p)^{f_\mathfrak{p}},$$

où p est le nombre premier de $\mathbb{Z}$ divisible par $\mathfrak{p}$. On a par ailleurs

$$\left|\mathcal{O}_K/\mathfrak{p}\right| = \left|\mathbb{Z}/p\mathbb{Z}\right|^{f_\mathfrak{p}} = p^{f_\mathfrak{p}},$$

ce qui conclut. □

Proposition 1.3.95. *Soit I un idéal fractionnaire de K. Alors*

$$\mathrm{covol}(I) = \sqrt{|d_K|} N_{K/\mathbb{Q}}(I).$$

Démonstration. La proposition 1.2.4 nous permet de remplacer I par xI, pour $x \in K^*$. On peut donc supposer que I est un idéal de $\mathcal{O}_K$. Le lemme précédent et l'exemple 1.2.3.1 nous permettent de ne traiter que le cas où $I = \mathcal{O}_K$.

Soit $\alpha_1, \ldots, \alpha_n$ une base de $\mathcal{O}_K$ comme $\mathbb{Z}$-module. Alors le covolume de $\mathcal{O}_K$ dans V est, au signe près, 2^{r_2} fois le déterminant de la matrice de colonnes $i(\alpha_1), \ldots, i(\alpha_n)$, i.e., au signe près, 2^{r_2} fois celui de la matrice dont la i-ème colonne est

$$\sigma_1(\alpha_i), \ldots, \sigma_{r_1}(\alpha_i), \Re(\tau_1(\alpha_i)), \Im(\tau_1(\alpha_i)), \ldots, \Re(\tau_{r_2}(\alpha_i)), \Im(\tau_{r_2}(\alpha_i)).$$

Une manipulation élémentaire sur les lignes et les colonnes nous montre que ce déterminant est, au signe près, le déterminant de la matrice des $\sigma_j(\alpha_i)$, ce qui conclut. □

Remarque 1.3.96. *Il serait plutôt naturel de considérer le sous-espace vectoriel réel V' de $\mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$ consistant des $(x_1, \ldots, x_{r_1}, z_1, \overline{z_1}, \ldots, z_{r_2}, \overline{z_{r_2}})$ muni de sa mesure naturelle, ainsi que l'injection naturelle de K dans V au moyen de tous les plongements, réels ou non, de K dans $\mathbb{C}$. Cela éliminerait les puissances de 2 dans la preuve.*

Pour combiner les résultats ci-dessus, il faut connaître enfin le volume de la boule unité associé à la norme euclidienne $||.||$ dans V. C'est bien connu, on ne donne pas de preuve.

Proposition 1.3.97. *Le volume de la boule unité dans l'espace euclidien de dimension n est*

$$V_n = \frac{\pi^{n/2}}{\Gamma(1 + n/2)}.$$

Rappelons que la fonction Γ vérifie :

(i)

$$\Gamma(1) = 1;$$

(ii)
$$\Gamma(1/2) = \sqrt{\pi};$$

(iii)
$$\forall x > 0, \Gamma(x+1) = x\Gamma(x).$$

Théorème 1.3.98 (Minkowski)**.** *Soit I un idéal fractionnaire de K. Alors I contient un élément non nul de norme au plus (en valeur absolue)*

$$\frac{\Gamma(1+n/2)}{n^{n/2}}\Big(\frac{4}{\pi}\Big)^{n/2}\sqrt{|d_K|}N_{K/\mathbb{Q}}(I).$$

Démonstration. On applique le théorème de Minkowski : soit $r > 0$ tel que

$$r^n V_n \leq 2^n \mathrm{covol}(I).$$

Alors I contient un élément x non nul tel que $||x|| \leq r$. Concrètement, soit r tel que

$$r^n \frac{\pi^{n/2}}{\Gamma(1+n/2)} = 2^n\sqrt{|d_K|}N_{K/\mathbb{Q}}(I),$$

i.e.

$$r^n = 2^n \frac{\Gamma(1+n/2)}{\pi^{n/2}}\sqrt{|d_K|}N_{K/\mathbb{Q}}(I).$$

Alors le théorème de Minkowski et la proposition 1.3.93 nous permettent de trouver un élément non nul x de I tel que

$$|N_{K/\mathbb{Q}}(x)| \leq \frac{\Gamma(1+n/2)}{n^{n/2}}\Big(\frac{4}{\pi}\Big)^{n/2}\sqrt{|d_K|}N_{K/\mathbb{Q}}(I).$$

□

Remarque 1.3.99. *On peut être un peu plus précis dans la borne de Minkowski en considérant au lieu de la boule de rayon r la boule L^1 et remplacer le facteur*

$$\frac{\Gamma(1+n/2)}{n^{n/2}}\Big(\frac{4}{\pi}\Big)^{n/2}$$

par

$$\frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^{r_2}.$$

Cela s'applique bien sûr dans tous les corollaires qui suivent.

Corollaire 1.3.100. *Soit α un élément du groupe de classe de K. On peut trouver un idéal I de $\mathcal{O}_K$ dont la classe est α et tel que*

$$N_{K/\mathbb{Q}}(I) \leq \frac{\Gamma(1+n/2)}{n^{n/2}}\Big(\frac{4}{\pi}\Big)^{n/2}\sqrt{|d_K|}.$$

Démonstration. Soit I un idéal de classe β pour un $\beta \in Cl(\mathcal{O}_K)$. Trouvons x comme dans le théorème précédent. Alors l'idéal fractionnaire $(x)I^{-1}$ est un idéal, de norme au plus $\frac{\Gamma(1+n/2)}{n^{n/2}}\left(\frac{4}{\pi}\right)^{n/2}\sqrt{|d_K|}$ et de classe β^{-1}. On conclut en prenant $\beta = \alpha^{-1}$. □

Corollaire 1.3.101. *Si*

$$\frac{\Gamma(1+n/2)}{n^{n/2}}\left(\frac{4}{\pi}\right)^{n/2}\sqrt{|d_K|} < 2,$$

alors $\mathcal{O}_K$ est principal.

Démonstration. Il suffit de remarquer que le seul idéal de norme 1 est $\mathcal{O}_K$ lui-même. □

Exemple 1.3.7.1. *Prenons $n = 2$. L'inégalité précédente devient*

$$|d_K| < \pi^2,$$

soit

$$|d_K| \leq 9.$$

La norme d'un élément non nul de $\mathcal{O}_K$ est toujours supérieure ou égale à 1 en valeur absolue. Prenant $I = \mathcal{O}_K$ dans le théorème précédent, il vient

Proposition 1.3.102. *On a*

$$\sqrt{|d_K|} \geq \frac{n^{n/2}}{\Gamma(1+n/2)}\left(\frac{\pi}{4}\right)^{n/2}.$$

On en déduit :

Théorème 1.3.103 (Minkowski)**.** *Si K est une extension de $\mathbb{Q}$ de degré au moins 1, alors $|d_K| > 1$.*

Démonstration. Il suffit de montrer l'inégalité

$$\frac{n^{n/2}}{\Gamma(1+n/2)}\left(\frac{\pi}{4}\right)^{n/2} = V_n n^{n/2} 2^{-n} > 1$$

pour tout $n > 1$.

Si $n > 1$, la boule unité de $\mathbb{R}^n$ contient strictement l'ensemble $[-\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n}}]^n$, ce qui implique

$$V_n > 2^n n^{-n/2}$$

et montre le résultat.

□

Le théorème de Minkowski signifie que toute extension de $\mathbb{Q}$ est ramifiée en au moins un nombre premier – autrement dit, le schéma Spec $(\mathbb{Z})$ est simplement connexe. Il a une variante plus générale, mais moins précise.

On commence par quelques résultats sur la ramification – ce sont des résultats loin d'être optimaux, on les raffinera plus tard quand on saura compléter.

Proposition 1.3.104. *Soit $\mathcal{O}_K$ un anneau de Dedekind de corps de fractions K, soit L/K une extension finie séparable de degré d, d'anneau des entiers $\mathcal{O}_L$. Soit $\mathfrak{P}$ un idéal premier non nul de $\mathcal{O}_L$. Supposons $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_L$ totalement ramifié dans L. Soit r le plus grand entier tel que $\mathfrak{P}^r | \mathfrak{D}_{L/K}$. Soit p la caractéristique résiduelle de $\mathfrak{p}$. Alors*

(i) si d est premier à p, $r = d - 1$;

(ii) sinon, on a $d - 1 \leq r \leq d - 1 + v_{\mathfrak{P}}(d) \leq d - 1 + d \log_p(d)$.

Démonstration. On peut supposer que $A = \mathcal{O}_K$ est un anneau de valuation discrète, et donc que $B = \mathcal{O}_L$ est un anneau de valuation discrète. La proposition 1.3.82 nous montre que B est de la forme

$$B = A[\alpha],$$

où α est une uniformisante de $\mathfrak{P}$, et son polynôme annulateur P est un polynôme d'Eisenstein. Écrivons

$$P(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_0.$$

Alors $\mathfrak{D}_{L/K}$ est l'idéal engendré par $P'(\alpha)$. L'entier r est donc $v_{\mathfrak{P}}(P'(\alpha))$. On a

$$P'(\alpha) = d\alpha^{d-1} + \ldots + a_1.$$

La valuation $v_{\mathfrak{P}}(a)$ d'un élément a de $\mathcal{O}_K$ est égale à $dv_{\mathfrak{p}}(a)$, donc la valuation $\mathfrak{P}$-adique de

$$(d-i)a_{d-i}\alpha^{d-i-1}$$

est congrue à $-i-1$ modulo d. En particulier, ces valuations sont deux à deux distinctes quand i varie, et la valuation $\mathfrak{P}$-adique de $P'(\alpha)$ est le plus petit des

$$v_{\mathfrak{P}}((d-i)a_{d-i}\alpha^{d-i-1}).$$

Elle vaut donc au plus

$$v_{\mathfrak{P}}(d\alpha^{d-1}) = v_{\mathfrak{P}}(d) + d - 1.$$

Par ailleurs, comme les a_i, $i \neq d$ sont tous dans $\mathfrak{p}$, on a, pour $i \neq d$,

$$v_{\mathfrak{P}}((d-i)a_{d-i}\alpha^{d-i-1}) \geq e,$$

ce qui conclut. □

Corollaire 1.3.105. *Soit $\mathcal{O}_K$ un anneau de Dedekind de corps de fractions K, soit L/K une extension finie séparable de degré d, d'anneau des entiers $\mathcal{O}_L$. Soit $\mathfrak{P}$ un idéal premier non nul de $\mathcal{O}_L$, de caractéristique résiduelle p. La plus grande puissance de $\mathfrak{P}$ qui divise la différente $\mathfrak{D}_{L/K}$ divise*

$$\mathfrak{P}^{d!-1+d!\log_p(d!)}.$$

Démonstration. La proposition 1.3.78 nous ramène à montrer que si L/K est galoisienne, alors la plus grande puissance de $\mathfrak{P}$ qui divise la différente $\mathfrak{D}_{L/K}$ divise $\mathfrak{P}^{d-1+d\log_p(d)}$.

Les propositions 1.3.61 et 1.3.61 nous permettent de supposer que l'idéal $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ est totalement ramifié dans L. La proposition précédente permet de conclure. □

Corollaire 1.3.106. *Soit L/K une extension de degré d de corps de nombres. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Alors la plus grande puissance de $\mathfrak{p}$ qui divise $\mathfrak{d}_{L/K}$ est au plus*

$$\mathfrak{p}^{d(d!-1+d!\log_p(d!))}.$$

Démonstration. La différente s'écrit

$$\mathfrak{D}_{L/K} = \Pi_{\mathfrak{P}|\mathfrak{p}}\mathfrak{P}^{r_\mathfrak{P}} I,$$

avec I premier à $\mathfrak{P}$ et $r_\mathfrak{P} \leq d! - 1 + d!\log_p(d!)$, donc

$$\mathfrak{d}_{L/K} = \Pi_{\mathfrak{P}|\mathfrak{p}}\mathfrak{p}^{f_\mathfrak{P} r_\mathfrak{P}} J,$$

avec J premier à $\mathfrak{p}$. Comme

$$\mathfrak{p}^d = \Pi_{\mathfrak{P}|\mathfrak{p}}\mathfrak{p}^{f_\mathfrak{P}},$$

on trouve

$$\Pi_{\mathfrak{P}|\mathfrak{p}}\mathfrak{p}^{f_\mathfrak{P} r_\mathfrak{P}} | \mathfrak{p}^{d(d!-1+d!\log_p(d!))}.$$

□

Théorème 1.3.107 (Hermite)**.** *(i) Soit S un ensemble fini de nombre premiers. Il existe un nombre fini d'extensions de $\mathbb{Q}$ non-ramifiées en dehors de S, de degré borné ;*

(ii) Il n'existe qu'un nombre fini de corps de nombres de discriminant borné.

Démonstration. Le corollaire précédent montre que le discriminant d'une extension de degré n de $\mathbb{Q}$ non ramifiée en dehors de S est borné par une fonction de n. D'autre part, la proposition 1.3.102 montre qu'une borne sur le discriminant d'une extension finie de $\mathbb{Q}$ implique une borne sur son degré. Les deux énoncés du théorème se ramènent donc à montrer qu'étant donnés n et d, il n'existe qu'un nombre fini d'extensions de $\mathbb{Q}$ de degré n et discriminant d.

Soit K une telle extension. On reprend les notations précédentes. Supposons pour fixer les idées que $r_1 \neq 0$ – le cas où $r_1 = 0$ est similaire. On peut trouver une constante C ne dépendant que de n et d telle que l'on puisse trouver $\alpha \in \mathcal{O}_K$ satisfaisant $|\sigma_i(\alpha)| < 1, |\tau_j(\alpha)| < 1$ pour tout $i \neq 1$, $1 \leq j \leq r_2$, et $|\sigma_1(\alpha)| \leq C$. Comme la norme de α est un entier non-nul, elle vaut au moins 1, donc $\sigma_1(\alpha) > 1$. Cela implique que $\sigma_1(\alpha)$ n'est égal à $\sigma(\alpha)$ pour aucun plongement $\sigma : K \to \mathbb{C}$ distinct de σ_1, donc en particulier que $K = \mathbb{Q}[\alpha]$. Les coefficients du polynôme de α sont des entiers bornés en fonction de C et n. Ce dernier ne peut donc prendre qu'un nombre fini de valeurs possibles dans $\mathbb{Z}[X]$, ce qui conclut. □

Chapitre 2

Corps locaux

Ce chapitre est consacré à la théorie locale des corps de nombres. Plutôt que de s'intéresser à un corps de nombre K (théorie globale), on va considérer la complétion de K pour la topologie induite par une valuation de K associée à un idéal premier non nul.

Du point de vue de la géométrie algébrique, cette construction est très naturelle. Les anneaux locaux que l'on a étudié pour le moment sont définis via la topologie de Zariski, qui est souvent trop grossière pour les applications. L'analogue géométrique de ce que l'on a en tête est la chose suivante : soit X une courbe lisse sur $\mathbb{C}$, et soit x un point complexe de X. Alors, pour la topologie usuelle, X est isomorphe au voisinage de x à la droite complexe $\mathbb{C}$. Autrement dit, on peut trouver une coordonnée locale z en x. Toute fonction holomorphe au voisinage de x est une série entière en z.

Dans la situation des corps de nombres, c'est p qui joue le rôle de coordonnée locale de $\mathbb{Z}$ en p : il s'agit bien d'un générateur de l'idéal maximal engendré par x. L'analogue de l'anneau des séries formelles est l'anneau $\mathbb{Z}_p$ des entiers p-adiques.

Une façon conceptuelle de procéder (et qui s'appliquerait à des schémas plus généraux que $\operatorname{Spec} \mathcal{O}_K$) serait d'introduire une topologie adaptée sur le schéma considéré, plus fine que la topologie de Zariski, et d'en considérer les anneaux locaux. Dans notre cas, ce serait la topologie de Nisnevich (un peu plus grossière que la topologie étale). Le sens de cette construction se reflète dans le fait que les extensions des corps locaux viennent, en un sens, soit d'extensions totalement ramifiée, soit d'extensions du corps résiduel. On ne poursuivera pas dans cette direction, puisque tout peut se formuler de manière élémentaire à l'aide de valuations.

2.1 Propriétés génerales

2.1.1 Valuations, topologie

Voici une définition que l'on a essentiellement déjà vue en 1.3.2.

Définition 2.1.1. *Soit K un corps. Une valuation discrète sur K est un morphisme de groupes surjectif*

$$v : K^* \to \mathbb{Z}$$

tel que, posant $v(0) = \infty$, on a

$$\forall x, y \in K, v(x+y) \geq \min(v(x), v(y)).$$

Si A est un anneau de valuation discrète (i.e. intègre, local, principal), la valuation de A est bien une valuation discrète. La réciproque est vraie.

Proposition 2.1.2. *Soit K un corps muni d'une valuation discrète v, l'ensemble*

$$A = \{x \in K, v(x) \geq 0\}$$

est un sous-anneau de K, de corps des fractions K. C'est un anneau de valuation discrète de valuation $v_{|A}$. L'unique idéal maximal de A est $\{x \in A, v(x) \geq 1\}$.

Démonstration. Laissé au lecteur. □

Définition 2.1.3. *Si K est un corps muni d'une valuation discrète v, l'anneau de valuation de K est*

$$A = \{x \in K, v(x) \geq 0\}.$$

Voici quelques exemples fondamentaux :

1. Soit k un corps, $x \in k$, $K = k(T)$. Alors la valuation v qui envoie un élément de la forme $T^n P/Q$ sur n, où P et Q sont deux polynômes en T premiers à T, est une valuation discrète, d'anneau de valuation

   $$A_K = k[T]_{(T)} = \{P/Q, P, Q \in k[T], P \wedge T = 1\}.$$

   L'élément T est une uniformisante.

2. Si k est encore un corps, soit $L = k((T))$ le corps des séries de Laurent :

   $$A_L = k((T)) = \{\sum_{i=m}^{\infty} a_i T^i, m \in \mathbb{Z}, a_i \in k\}.$$

   Alors la valuation qui envoie $\sum_{i=m}^{\infty} a_i T^i$ sur m quand m est choisi de telle sorte que $a_m \neq 0$, est une valuation discrète. Son anneau de valuation est

l'anneau $k[[T]]$ des séries formelles, et T est une uniformisante. Un argument de développement en série entières montre que l'on a une inclusion naturelle de K dans L, telle que la valuation de L prolonge celle de k. Cette inclusion induit, pour tout n, un isomorphisme $A_K/\mathfrak{m}_K^n \to A_L/\mathfrak{m}_L^n$, où $\mathfrak{m}_K$ et $\mathfrak{m}_L$ sont les idéaux maximaux de L et K respectivement.

3. Soit K un corps de nombres, d'anneaux des entiers $\mathcal{O}_K$, et soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Alors le localisé $\mathcal{O}_{K,\mathfrak{p}}$ est un anneau de valuation discrète.

Le pendant "exponentiel" de la notion de valuation est celui de valeur absolue.

Définition 2.1.4. *Soit K un corps. Une valeur absolue sur K est une application*

$$|.| : K \to \mathbb{R}_+$$

vérifiant les propriétés suivantes :

(i) $\forall x \in K, |x| = 0 \iff x = 0$;

(ii) $\forall x, y \in K, |xy| = |x|\,|y|$;

(iii) $\forall x, y \in K, |x + y| \leq |x| + |y|$.

On dit que $|.|$ est non-archimédienne si l'on a

$$\forall x, y \in K, |x + y| \leq \max(|x|, |y|).$$

Sinon, on dit que $|.|$ est archimédienne. La valeur absolue triviale est celle qui est identiquement égale à 1 sur K^*.

Lemme 2.1.5. *Soit K un corps muni d'une valeur absolue $|.|$. Alors $|.|$ est non-archimédienne si et seulement si la suite $(|n|)_{n\geq 0}$ est bornée.*

Démonstration. Si $|.|$ est non-archimédienne, on a toujours $|n| = |1 + \ldots + 1| \leq 1$. Supposons donc qu'il existe une constante C telle que $|n| \leq C$ pour tout entier n. Soient $x, y \in K$. Alors

$$|x + y|^n \leq |(x + y)^n| \leq C \sum_{i=0}^{n} |x|^i |y|^j \leq C(n + 1) \max(|x|, |y|)^n.$$

Prenant la racine n-ième et faisant tendre n vers ∞, on trouve bien que $|.|$ est non-archimédienne. □

Si $|.|$ est une valeur absolue sur K, et si s est un réel strictement supérieur à 1, alors $|.|^s$ est encore une valeur absolue.

Définition 2.1.6. *Soit K un corps. Deux valeurs absolues $|.|_1$ et $|.|_2$ sur K sont équivalentes s'il existe $s \in \mathbb{R}$ tel que $|.|_2 = |.|_1^s$.*

L'équivalence des valeurs absolues est bien entendu une relation d'équivalence.

Une valeur absolue sur K définit une distance d sur K par la formule

$$d(x,y) = |x-y|.$$

La condition (iii) de la définition est équivalente à l'inégalité triangulaire. En particulier, K est muni naturellement de sa topologie d'espace métrique.

Proposition 2.1.7. *Soit K un corps muni de valeurs absolues $|.|_1$ et $|.|_2$. Les topologies sur K induites par $|.|_1$ et $|.|_2$ sont égales si et seulement si $|.|_1$ et $|.|_2$ sont équivalentes.*

Démonstration. Si $|.|_1$ et $|.|_2$ sont équivalentes, alors toute boule ouverte pour $|.|_1$ est une boule ouverte pour $|.|_2$, donc les topologies induites sont les mêmes.

Réciproquement, supposons que $|.|_1$ et $|.|_2$ induisent la même topologie sur K. En particulier, si $x \in K$, alors la suite (x^n) tend vers 0 pour la première topologie si et seulement si elle tend vers 0 pour la seconde. Autrement dit,

$$|x|_1^n \to 0 \iff |x|_2^n \to 0,$$

i.e.

$$|x|_1 < 1 \iff |x|_2 < 1.$$

Appliquant ce résultat à x^{-1}, on trouve $|x|_1 \neq 1 \iff |x|_2 \neq 1$ et

$$|x_1| = 1 \iff |x|_2 = 1.$$

Si pour tout $x \neq 0$, $|x|_1 = 1$, alors ce qui précède montre que les deux valeurs absolues sont égales. Supposons donc donné x tel que $|x|_1 \neq 0, 1$. Soit s l'unique réel tel que

$$|x|_2 = |x|_1^s.$$

Soit $y \in K$. D'après ce qui précède, pour tout entiers relatifs m et n, on a

$$|x^m y^n|_1 < 1 \iff |x^m y^n|_2 < 1,$$

soit $|y|_1 < |x|_1^{-m/n} \iff |y|_2 < |x|_1^{-sm/n}$ et

$$|y|_1^s < |x|_1^{-sm/n} \iff |y|_2 < |x|_1^{-sm/n},$$

ce qui implique $|y|_2 = |y|_1^s$ et conclut. □

Définition 2.1.8. *Soit k un corps. Une place de k est une classe d'équivalence de valeurs absolues sur k. On dit que la place est archimédienne ou non suivant que la valeur absolue l'est.*

Les valeurs absolues non-archimédiennes correspondent aux valuations.

Proposition 2.1.9. *Soit K un corps, et soit v une valuation discrète sur K. Soit $q > 0$ un nombre réel. L'application*

$$|.| : x \mapsto q^{-v(x)}$$

est une valeur absolue non-archimédienne sur K, dont la classe d'équivalence ne dépend pas du choix de q.

Démonstration. Laissé au lecteur. □

Remarque 2.1.10. *Réciproquement, si $|.|$ est une valeur absolue sur K, alors $-\log|.|$ est une valuation sur K (au sens de la définition 2.1.1, en choisissant $\mathbb{R}$ comme groupe dans lequel v prend ses valeurs.*

La proposition précédente montre en particulier qu'une valuation discrète sur K définit une topologie naturelle d'espace métrique sur K, dont une base d'ouverts est donné par les

$$\{x \in K, v(x-y) \geq n\} = \{x \in K, x \in y + \mathfrak{m}^n\}$$

où y parcourt K et n parcourt $\mathbb{Z}$. Autrement dit, une base de voisinage ouverts de 0 est donnée par les $\mathfrak{m}^n, n \in \mathbb{Z}$. C'est bien entendu une topologie compatible à la structure d'anneau : addition et multiplication sont continues. Notons aussi que A est à la fois ouvert et fermé dans K.

Voici une conséquence directe.

Proposition 2.1.11. *Soit K un corps muni d'une valuation v, soit A l'anneau de valuation, et soit $n \geq 0$. L'application quotient*

$$A \to A/\mathfrak{m}^n$$

est continue, où $A/\mathfrak{m}^n$ est muni de la topologie discrète.

Démonstration. Il faut montrer que les préimages de singleton sont ouvertes, ce qui est donné par la remarque ci-dessus. □

Si $n \geq m$, on dispose de l'application quotient

$$A/\mathfrak{m}^n \to A/\mathfrak{m}^n.$$

Cela nous permet de considérer la limite (projective)

$$\widehat{A} = \lim_n A/\mathfrak{m}^n \subset \prod_n A/\mathfrak{m}^n,$$

définie comme l'ensemble des $(x_n) \in \prod_n A/\mathfrak{m}^n$ tels que pour tous $n \geq m$, l'image de x_n dans $A/\mathfrak{m}^m$ est x_m. L'ensemble $\widehat{A}$ est muni d'une topologie naturelle, induite par la topologie produit sur $\prod_n A/\mathfrak{m}^n$, dont une base d'ouverts est donnée par les préimages d'éléments de $A/\mathfrak{m}^n$. Cette topologie est compatible à la structure d'anneau.

Proposition 2.1.12. *L'application naturelle*

$$A \to \widehat{A}$$

est continue, injective. Son image est dense dans $\widehat{A}$, et la topologie de A est la topologie induite par celle de $\widehat{A}$.

Démonstration. L'injectivité vient de ce que l'intersection des $\mathfrak{m}^n, n \geq 0$, est vide. Pour montrer la continuité, il suffit de montrer que les images inverses des éléments d'une base d'ouverts de $\widehat{A}$ sont des ouverts de A, i.e., que les préimages dans A d'éléments de $A/\mathfrak{m}^n$ sont ouverts, ce qui est prouvé dans la proposition précédente. Si $x = (x_n)$ in $\widehat{A}$, et si (y_n) est une suite d'éléments de A tels que la réduction de y_n modulo $\mathfrak{m}^n$ est x_n, alors la suite y_n converge vers x dans $\widehat{A}$, ce qui montre que A est dense dans $\widehat{A}$. Le dernier énoncé est laissé au lecteur. □

Des valeurs absolues qui ne sont pas équivalentes sont indépendentes – au sens où l'on peut formuler une généralisation du théorème des restes chinois.

Proposition 2.1.13 (Théorème d'approximation faible)**.** *Soit $|.|_1, \ldots, |.|_n$ des valeurs absolues sur K, deux à deux non-équivalentes. Soit $\varepsilon > 0$, et soient $a_1, \ldots, a_n \in K$. Alors on peut trouver $x \in K$ tel que*

$$\forall i \in \{1, \ldots, n\}, |x - a_i|_i < \varepsilon.$$

Démonstration. Il suffit de trouver des éléments α_i tels que $|\alpha_i| > 1$ et $|\alpha_i|_j < 1$ pour $i \neq j$ pour $1 \leq i \leq n$. En effet, si r est suffisamment grand, alors

$$x = \sum_{i=1}^{n} \frac{\alpha_i^r}{1 + \alpha_i^r} a_i$$

satisfait la conclusion de la proposition. Il suffit de trouver α tel que $|\alpha|_1 > 1$ et $|\alpha|_i < 1$ pour $i \neq 1$. On raisonne par récurrence sur n.

Si $n = 2$, on trouve ϕ, ψ tels que $|\phi|_1 < 1$ et $|\phi|_2 \geq 1$, $|\psi|_1 \geq 1$ et $|\psi|_2 < 1$ (utiliser l'argument de la proposition 2.1.7). Alors on peut prendre $\alpha = \phi/\psi$.

Supposons $n \geq 3$. Par hypothèse de récurrence, on peut trouver $\phi \in k$ tel que $|\phi|_1 > 1$ et $|\phi|_i < 1$ pour $2 \leq i \leq n-1$. Si $|\phi|_n < 1$, on prend $\alpha = \phi$.

On peut trouver par ailleurs, grâce à l'argument précédent, $\psi \in k$ tel que $|\psi|_1 > 1$ et $|\psi|_n < 1$. Si $|\phi|_n = 1$, on prend $\alpha = \phi^r \psi$ pour r suffisamment grand. Si $|\phi|_n > 1$, on prend $\alpha = \frac{\phi^r}{1+\phi^r}\psi$ pour r suffisamment grand. □

Remarque 2.1.14. *La proposition ci-dessus peut se reformuler comme suit : soit K_i l'espace topologique d'ensemble sous-jacent K, muni de la topologie induite par $|.|_i$. Alors l'application diagonale*

$$K \hookrightarrow \prod_i K_i$$

est d'image dense.

Remarque 2.1.15. *Il existe un théorème d'approximation forte, qui ne vaut pas pour des corps arbitraires. Sur un corps de nombre, il demande un x satisfaisant une condition d'approximation à* toutes *les valeurs absolues sauf au plus une.*

Concluons par le théorème suivant, qui décrit les valeurs absolues sur le corps $\mathbb{Q}$. On en déduira plus bas les valeurs absolues sur les corps de nombres.

Théorème 2.1.16 (Ostrowski)**.** *Toute valeur absolue non triviale sur $\mathbb{Q}$ est équivalente soit à la valeur absolue non-archimédienne associée à un nombre premier, soit à la valeur absolue usuelle.*

Démonstration. Soit $|.|$ une valeur absolue sur $\mathbb{Q}$. Supposons d'abord $|.|$ non-archimédienne. Alors, pour tout $n \in \mathbb{Z}$, $|n| \leq 1$. Si tout nombre premier p satisfait $|p| = 1$, alors la valeur absolue est triviale. On peut donc trouver p premier tel que $|p| < 1$. Soit I l'idéal de $\mathbb{Z}$ constitué des n tels que $|n| < 1$. Alors $p \in I$, et $I \neq \mathbb{Z}$, donc $I = (p)$. En particulier, si a est premier à p, alors $|a| = 1$. On en déduit l'équivalence de $|.|$ et de la valeur absolue associée à la valuation p-adique.

Supposons $|.|$ archimédienne. Soient $a, b \in \mathbb{Z}$, avec $a, b > 1$. On écrit en base b

$$a = a_0 + a_1 b + \ldots + a_n b^n,$$

où les a_i sont compris entre 0 et $b-1$, et $n \leq \frac{\log a}{\log b}$. On en déduit

$$|a| \leq C(1 + \frac{\log a}{\log b}) \max(1, |b|^{\log a / \log b}),$$

où C est la plus grande valeur de $|c|$ pour $0 \leq c \leq b-1$. Appliquant cette inégalité à a^n, faisant tendre n vers ∞ et prenant la racine n-ième, il vient

$$|a| \leq \max(1, |b|^{\log a / \log b}).$$

En particulier, choisissant grâce au lemme 2.1.5 un a tel que $|a| > 1$, on trouver que $|b| > 1$ pour tout $b > 1$ et

$$|a|^{1/\log a} \leq |b|^{1/\log b}.$$

Par symétrie, on a égalité ci-dessus, ce qui montre que $|.|$ est équivalente à la valeur absolue usuelle. □

On dit que la classe d'équivalence de la valeur absolue archimédienne sur $\mathbb{Z}$ est la place à l'infini. Les autres places sont les places finies.

2.1.2 Nombres p-adiques

Avant d'aller plus loin dans la théorie générale, décrivons un exemple important. Soit p un nombre premier.

Définition 2.1.17. *Un nombre p-adique est une série formelle*

$$\sum_{i \geq n} a_i p^i,$$

où $n \in \mathbb{Z}$ et les a_i sont des entiers compris entre 0 et $p-1$. Un entier p-adique est un nombre p-adique de la forme

$$\sum_{i \geq 0} a_i p^i.$$

On note $\mathbb{Q}_p$ l'ensemble des nombres p-adiques, et $\mathbb{Z}_p$ l'ensemble des entiers p-adiques.

Cette définition n'est pas très praticable, même si elle a l'avantage de la simplicité ! Il n'est même pas clair que $\mathbb{Q}_p$ ou $\mathbb{Z}_p$ soient des groupes. Le lemme suivant permet de mieux la comprendre.

Lemme 2.1.18. *Soit $n \geq 1$. Tout élément a de $\mathbb{Z}/p^n\mathbb{Z}$ s'écrit de manière unique comme somme*

$$a = a_0 + a_1 p + \ldots + a_{n-1} p^{n-1},$$

où les a_i sont des entiers strictement compris entre 0 et $p-1$.

Démonstration. Laissé au lecteur. □

La définition même de $\mathbb{Z}_p$ nous fournit, pour tout $n \geq 1$, une application $\pi_n : \mathbb{Z}_\mathfrak{p} \to \mathbb{Z}/p^n\mathbb{Z}$ qui à

$$\sum_{i \geq 0} a_i p^i$$

associe l'image de $\sum_{i=0}^{n-1} a_i p^i$ dans $\mathbb{Z}/p^n\mathbb{Z}$. Les π_n sont compatibles aux applications quotients $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$, $n \geq m$, d'où une flèche naturelle $\mathbb{Z}_p \to \lim_n \mathbb{Z}/p^n\mathbb{Z}$.

Proposition 2.1.19. *L'application $\mathbb{Z}_p \to \lim_n \mathbb{Z}/p^n\mathbb{Z}$ est une bijection.*

Démonstration. Laissé au lecteur. □

La proposition précédente munit $\mathbb{Z}_p$ d'une structure d'anneau topologique naturelle venant de celle de $\lim_n \mathbb{Z}/p^n\mathbb{Z}$.

Proposition 2.1.20. *Soit $v : \mathbb{Q}_p \to \mathbb{Z}$ la fonction qui à $\sum_{i \geq n} a_i p^i$, avec $a_n \neq 0$, associe n. Alors $v_{|\mathbb{Z}_p}$ est une valuation discrète sur $\mathbb{Z}_p$.*

On dit que v est la valuation p-adique.

Démonstration. On vérifie sans difficulté que $\lim_n \mathbb{Z}/p^n\mathbb{Z}$ est un anneau de valuation discrète, d'idéal maximal engendré par p, et que v est la valuation associée à cet anneau. □

Corollaire 2.1.21. *L'ensemble $\mathbb{Q}_p$ des nombres p-adiques s'identifie au corps des fractions de $\mathbb{Z}_p$, et l'on a $\mathbb{Q}_p = \bigcup_n p^{-n}\mathbb{Z}_p$.*

Démonstration. On a certainement $\mathbb{Q}_p = \bigcup_n p^{-n}\mathbb{Z}_p$. Comme $\mathbb{Z}_p$ est un anneau de valuation discrète d'idéal maximal (p), son corps des fractions est bien $\bigcup_n p^{-n}\mathbb{Z}_p$. □

Exemple 2.1.2.1. *Exemples de calculs donnés en cours.*

Voici un premier témoignage de l'importance des nombres p-adiques en arithmétique.

Proposition 2.1.22. *Soit $P \in \mathbb{Z}_p[X_1, \ldots, X_n]$. Alors l'équation*

$$P(x_1, \ldots, x_n) = 0$$

a une solution dans $\mathbb{Z}_p^n$ si et seulement si elle a une solution dans $(\mathbb{Z}/p^k\mathbb{Z})^n$ pour tout entier positif k.

Démonstration. Preuve vue en cours. □

Finissons cette section par une propriété topologique basique.

Proposition 2.1.23. *L'anneau topologique $\mathbb{Z}_p$ est compact, et $\mathbb{Q}_p$ est localement compact.*

Démonstration. On a $\mathbb{Q}_p = \bigcup_n p^{-n}\mathbb{Z}_p$, donc le second énoncé suit du premier. On a vu en cours l'argument diagonal permettant de prouver la compacité. □

Puisque $\mathbb{Z}_p$ est un espace métrique compact, il est complet.

2.1.3 Complétions

Rappelons qu'un espace métrique est dit complet si toute suite de Cauchy converge. Si K est un corps muni d'une valeur absolue $|.|$, la complétude de K ne dépend que de la classe d'équivalence de $|.|$.

Le théorème suivant, que l'on démontre comme dans le cas de la construction de $\mathbb{R}$, résume les propriétés de base de la complétion.

Théorème 2.1.24. *Soit K un corps muni d'une valeur absolue $|.|$. Il existe un corps $\overline{K}$ contenant K, muni d'une valeur absolue prolongeant $|.|$ pour laquelle il est complet et pour laquelle K est dense dans $\overline{K}$. Notant encore $|.|$ pour le prolongement de la valeur absolue à $\overline{K}$, la paire $(K \subset \overline{K}, |.|)$ vérifie la propriété suivante : tout plongement de K dans un corps L complet pour une valeur absolue prolongeant celle de L s'étend en un plongement $\overline{K} \to L$.*

On dit que $\overline{K}$ est le complété de K pour la valeur absolue $|.|$. Il ne dépend manifestement que de la classe d'équivalence de $|.|$.

Soit maintenant K un corps muni d'une valuation discrète v, d'anneau de valuation A et d'idéal maximal $\mathfrak{m}$.

Proposition 2.1.25. *Soit $\overline{K}$ le complété de K pour la valuation v. Alors v s'étend en une valuation discrète sur $\overline{K}$, qui définit la topologie de $\overline{K}$. Si $\overline{A}$ est l'anneau de valuation de $\overline{K}$, et $\overline{\mathfrak{m}}$ l'idéal maximal de $\overline{A}$, alors on a*

$$\overline{\mathfrak{m}} = \mathfrak{m}\overline{A}$$

et

$$\overline{\mathfrak{m}} \cap A = \overline{\mathfrak{m}}.$$

L'application naturelle

$$A/\mathfrak{m}^n \to \overline{A}/\overline{\mathfrak{m}}^n$$

est un isomorphisme pour tout $n \geq 0$.

Démonstration. Soit $|.|$ la valeur absolue sur K définie par $x \mapsto q^{-v(x)}$. Nous laissons au lecteur le soin de vérifier que l'extension de $|.|$ à $\overline{K}$ prend les mêmes valeurs que $|.|$, et que, prenant le log en base q, on obtient une extension de v à $\overline{K}$ qui est bien une valuation discrète.

Soit ϖ une uniformisante de R. Alors $v(\varpi) = 1$, donc ϖ est une uniformisante de $\overline{R}$, et $\overline{\mathfrak{m}} = (\varpi) = \mathfrak{m}\overline{R}$. L'intersection $\overline{\mathfrak{m}} \cap R$ est un idéal non trivial de R contenant l'idéal maximal $\mathfrak{m}$, c'est donc $\mathfrak{m}$.

Soit $n \geq 0$. L'application $A/\mathfrak{m}^n \to \overline{A}/\overline{\mathfrak{m}}^n$ est injective. Soit $x \in \overline{A}$. Comme K est dense dans $\overline{K}$, A est dense dans $\overline{A}$ (tout élément de K suffisamment proche d'un élément de $\overline{A}$ a valuation positive donc est dans A), et l'on peut trouver $y \in A$ tel que $x - y \in m^n$. Alors l'image de y dans $A/\mathfrak{m}^n$ s'envoie sur celle de y dans $\overline{A}/\overline{\mathfrak{m}}^n$, d'où la surjectivité. □

On peut prendre un autre point de vue sur la complétion.

Proposition 2.1.26. *Soit A un anneau muni d'une valuation discrète v, d'idéal maximal $\mathfrak{m}$, et soit K son corps des fractions. Alors l'anneau*

$$\widehat{A} = \lim_n A/\mathfrak{m}^n$$

est complet pour sa topologie naturelle. Cette topologie est induite par une valuation prolongeant celle de A, et le corps des fractions de $\widehat{A}$ est le complété de K pour la valuation v.

Démonstration. Commençons par décrire la valuation qui induit la topologie sur $\widehat{A}$. Soit $x \in \widehat{A}$. Alors il existe un plus petit entier positif n tel que l'image de x par la projection naturelle $\widehat{A} \to A/\mathfrak{m}^n$ soit non nul. On pose $v(x) = n$. Il est clair que v est une valuation discrète. En particulier, l'idéal maximal de $\widehat{A}$ est le noyau de $\widehat{A} \to A/\mathfrak{m}$, qui est égal à $\mathfrak{m}\widehat{A}$ (rappelons que $\widehat{A}$ contient A).

La description en 2.1.1 de la topologie sur $\widehat{A}$ montre qu'une base de voisinages de 0 dans $\widehat{A}$ est donné par les noyaux des $\widehat{A} \to A/\mathfrak{m}^n$, ce qui montre bien que la valuation v induit la topologie naturelle de A.

On pourrait directement vérifier que $\widehat{A}$ est complet, mais donnons un autre argument. Soit $\overline{K}$ la complétion de K, $\overline{A}$ son anneau de valuation, $\overline{\mathfrak{m}}$ son idéal maximal. La proposition précédente permet d'identifier $\overline{A}/\overline{\mathfrak{m}}^n$ à $A/\mathfrak{m}^n$. On peut donc identifier $\widehat{A}$ à $\widehat{\overline{A}}$.

Par ailleurs, $\overline{A}$ est complet, et dense dans $\widehat{\overline{A}}$, donc égal à $\widehat{\overline{A}}$. Cela prouve bien que $\widehat{A}$ est complet.

Soit ϖ une uniformisante de A, que l'on voit comme un élément de $\widehat{A}$. Alors le corps des fractions de A est $\bigcup_n \varpi^{-n}A$, et le corps des fractions de $\widehat{A}$ est $\bigcup_n \varpi^{-n}\widehat{A}$. La densité de A dans $\widehat{A}$ se transmet donc au corps des fractions, tout comme la complétude de $\widehat{A}$ à son corps des fractions, ce qui conclut. □

On se concentre maintenant dans le cas d'un corps résiduel fini.

Proposition 2.1.27. *Soit K un corps complet pour une valuation discrète. Soit A son anneau de valuation. Si le corps des fractions de A est fini, alors A est compact et K est localement compact.*

Démonstration. L'argument est le même que celui de la proposition 2.1.23. □

Dans le cas d'un corps résiduel fini, il y a une valeur absolue distinguée dans sa classe d'équivalence : c'est celle telle que

$$|x| = q^{-v(x)},$$

où q est le cardinal du corps résiduel. On dit que c'est la *valeur absolue normalisée*. La proposition suivante en donne deux propriétés basiques.

Proposition 2.1.28. *Soit K un corps complet pour une valuation discrète de corps résiduel fini. Soit $|.|$ la valeur absolue normalisée.*

(i) Soit $x \in A$. Alors $|x| = |A/(x)|$;

(ii) Soit μ la mesure de Haar sur le groupe compact $(A, +)$. Alors, pour $x \in A$, on a $\mu(xA) = |x|$.

Démonstration. Les deux énoncés se ramènent au cas où $x = \varpi^n$, où ϖ est une uniformisante de A. Alors $|x| = q^{-n}$, et $\mathbb{A}/\mathfrak{m}^n$ est de cardinal q^n (filtrer par les $\mathfrak{m}^i/\mathfrak{m}^n$). Le premier énoncé suit, et le second suit de l'invariance par translation de la mesure de Haar qui garantit que si les y_i sont un système de représentants de $A/\mathfrak{m}^n$, alors les $y_i + \mathfrak{m}^n$ sont deux à deux disjoints, de même mesure, et recouvrent A, ce qui montre qu'ils ont tous mersure q^{-n}. □

Concluons par la définition clé de ce chapitre.

Définition 2.1.29. *Un corps local est un corps complet pour une valuation discrète de corps résiduel fini.*

Remarque 2.1.30. *Cette définition est un peu restrictive : on rajoute parfois* $\mathbb{R}$ *et* $\mathbb{C}$ *aux corps locaux.*

Notons bien sûr :

Proposition 2.1.31. *Soit K un corps de nombres, et soit $\mathfrak{p}$ un idéal premier non-nul de K. Le complété de $\mathcal{O}_K$ pour la valuation discrète correspondant à $\mathfrak{p}$ est un corps local.*

Remarque 2.1.32. *On peut montrer que les corps locaux de caractéristique nulle sont tous donnés par des complétions de corps de nombres comme ci-dessus.*

La proposition 2.1.22 s'étend au cas de corps locaux arbitraires, avec la même preuve.

Proposition 2.1.33. *Soit K un corps local, d'anneau des entiers $\mathcal{O}_K$, et d'idéal maximal $\mathfrak{p}$. Soit $P \in \mathcal{O}_K[X_1, \ldots, X_n]$. Alors l'équation*

$$P(x_1, \ldots, x_n) = 0$$

a une solution dans $\mathcal{O}_K^n$ si et seulement si elle a une solution dans $(\mathcal{O}_K/\mathfrak{p}^k)^n$ pour tout entier positif k.

2.1.4 Extensions

On discute brièvement du comportement des valeurs absolues et des complétions par extension de corps. On se concentre sur le cas non-archimédien. Dans ce qui suit, les hypothèses de séparabilité ne sont pas nécessaires, mais on les garde par simplicité, ce qui ne nous gênera pas par la suite.

Théorème 2.1.34. *Soit K un corps muni d'une valuation discrète v, et soit A son anneau de valuation. Soit $|.|$ une valeur absolue associée. Soit L une extension finie séparable de K, et soit B son anneau des entiers. Alors*

(i) Il existe au moins une valeur absolue sur L qui étend $|.|$. Elle est nécessairement associée à une valuation discrète et son anneau de valuation contient B ;

(ii) le nombre d'extensions de v à L est égal au nombre d'idéaux premiers non nuls de B ;

(iii) si K est complet, l'extension de v à L est unique, et L est complet.

Démonstration. L'anneau A est un anneau de valuation discrète, soit $\mathfrak{p}$ son idéal maximal. La théorie générale des extensions d'anneaux de Dedekind nous montre que B est principal, et a un nombre fini d'idéaux premiers non nuls – qui sont tous au-dessus de $\mathfrak{p}$ – notés $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$.

À un idéal premier $\mathfrak{p}_i$, on associe le localisé B_i de B en $\mathfrak{P}_i$. Alors B_i est un anneau de valuation discrète. Soit ϖ une uniformisante de B_i, et soit n_i l'entier tel que $\mathfrak{P}_i^{n_i} = (\varpi^{n_i}) = \mathfrak{p}B$. Alors la valuation discrète v_i sur B_i vérifie

$$(v_i)_{|A} = n_i v,$$

donc si q est tel que $|x| = q^{-v(x)}$, la valeur absolue sur B_i $x \mapsto q^{-1/n_i v_i(x)}$ étend $|.|$ à L. On dispose donc d'au moins r extensions de $|.|$ à L. Le critère 2.1.5 nous garantit que toute telle extension est non-archimédienne, d'où une valuation $w : L \to \mathbb{R}$ qui étend v. Soit G l'image de W. C'est un sous-groupe de $\mathbb{R}$ contenant $\mathbb{Z}$. Il est donc soit dense dans $\mathbb{R}$, soit de la forme $\frac{1}{d}\mathbb{Z}$. Soit x un élément de L de valuation strictement positive. Supposons $w(x) < 1/n$, où $n = [L : K]$. On écrit

$$a_n x^n + \ldots + a_0 = 0.$$

Alors les $w(a_i x^i)$ sont deux à deux distinctes, donc

$$w(a_n x^n + \ldots + a_0) = \min_i(w(a_i x^i)) \neq \infty,$$

contradiction. Finalement, $w(L)$ est bien de la forme $\frac{1}{d}\mathbb{Z}$, et dw est une valuation discrète.

Enfin, si $x \in L$ est entier sur A, on écrit

$$x^n = a_{n-1}x^{n-1} + \ldots + a_0,$$

où les a_i sont dans A, donc de valuation positive. Si la valuation de x est négative, la valuation de x^n est strictement inférieure à celle de $a_{n-1}x^{n-1} + \ldots + a_0$, contradiction.

Nous avons donc montré (i) et une inégalité dans (ii). Pour montrer (ii), il faut montrer que les $q^{-1/n_i v_i}$ sont les seules extensions de $|.|$ à L. Soit $|.|_L$ une telle extension, et soit w la valuation discrète sur B associée, B_w l'anneau de valuation, et $\mathfrak{p}_w$ son idéal maximal. Alors B_w contient B, et $\mathfrak{p}_w$ contient $\mathfrak{p}$, donc $\mathfrak{p}_w \cap A = \mathfrak{p}$. En particulier, $\mathfrak{p}_w \cap B$ est un idéal premier $\mathfrak{P}_i$ de B. Soit $x \in B_i$. Alors on peut trouver $y \in B \setminus \mathfrak{P}_i$ tel que $yx \in B$, donc $w(xy) \geq 0$. Comme $y \notin \mathfrak{p}_w$, on a $w(y) = 0$ et finalement $w(x) \geq 0$,

soit $x \in B_w$. Autrement dit, B_w contient l'anneau de valuation discrète B_i. Soit ϖ une uniformisante de B_i, et soit ϖ' une uniformisante de B_w. Écrivant $\varpi' = \varpi^n \varepsilon$ avec $\varepsilon \in B_I^* \subset B_w^*$, on voit que $n = 1$, donc que ϖ est une uniformisante de B_w, ce qui montre que $B_w = B_i$, et que $w = v_i$, ce qui conclut la preuve de (ii).

Supposons enfin que K soit complet. Alors L est un espace vectoriel de dimension finie sur K, donc toutes les normes d'espace vectoriel sur L sont équivalentes et complètes. Si $|.|_i$ est un prolongement de $|.|$ à L, alors $|.|_i$ est en particulier une norme de K-espace vectoriel sur L. Les valeurs absolues $|.|_i$ définissent toutes la même topologie, ce qui montre qu'elles sont toutes équivalentes, donc égales puisque leur restriction à K est fixée. □

Remarque 2.1.35. *On peut reformuler le point (ii) du théorème comme suit – c'est un exercice de théorie des corps. Si $\overline{K}$ est le complété de K pour $|.|$, alors $L \otimes_K \overline{K}$ est le produit des complétés de K pour les valeurs absolues associée aux différents premiers de $\mathcal{O}_L$. Un énoncé similaire vaut pour les anneaux d'entiers.*

Du point de vue schématique, c'est plus clair : le spectre de l'anneau des entiers de $\overline{K}$ s'interprète comme un voisinage de l'idéal maximal suffisamment petit pour que la fibre de $\operatorname{Spec} \mathcal{O}_L \to \operatorname{Spec} \mathcal{O}_K$ soit union disjointe de voisinages des préimages de $\mathfrak{p}$.

Dans le cas (iii) du théorème, on peut donner une forme explicite pour l'extension de la valeur absolue de K à L.

Proposition 2.1.36. *Soit K un corps complet pour une valeur absolue $|.|$, associée à une valuation discrète, et soit L une extension finie séparable de degré n de K. Alors l'unique extension de $|.|$ à L est donnée par*

$$x \mapsto \left|N_{L/K}(x)\right|^{1/n}.$$

Démonstration. La compatibilité de la norme aux extensions successives et l'unicité de l'extension des valeurs absolues nous permet de remplacer L par sa clôture galoisienne.

Soit $|.|_L$ l'extension de $|.|$ à L. Si $\sigma \in Gal(L/K)$, alors

$$x \mapsto |\sigma(x)|_L$$

est une valeur absolue de L qui étend $|.|$, donc c'est $|.|_L$. Ainsi,

$$|\sigma(x)|_L = |x|_L$$

pour tout $x \in L$. Prenant le produit sur tous les σ, il vient

$$|x|_L^n = |N_{L/K}(x)|,$$

ce que l'on souhaitait montrer. □

Corollaire 2.1.37. *Soit K un corps complet pour une valuation discrète. Soit L une extension finie séparable de K. Alors l'anneau des entiers de L est un anneau de valuation discrète.*

Démonstration. C'est la conséquence des énoncés (ii) et (iii) du théorème précédent, et du fait qu'un anneau de Dedekind local est un anneau de valuation discrète. □

Corollaire 2.1.38. *Soit K un corps local, et soit L une extension finie séparable de K. Alors L est un corps local.*

Démonstration. On a vu ci-dessus que L est muni d'une valuation discrète naturelle qui le rend complet. La théorie générale des anneaux de Dedekind garantit que le corps résiduel de L est une extension finie du corps résiduel de K. Il est donc en particulier fini, ce qui montre que L est local. □

La théorie générale des anneaux de Dedekind nous garantit que si $\mathfrak{p}$ et $\mathfrak{P}$ sont les idéaux maximaux des anneaux d'entiers $\mathcal{O}_K$ et $\mathcal{O}_L$ respectivement, alors on a

$$\mathfrak{P}^n = \mathfrak{p}\mathcal{O}_L,$$

où n est un entier tel que

$$n[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] = [L : K].$$

Proposition 2.1.39. *Soit K un corps complet pour une valuation discrète, et soit $\mathcal{O}_K$ son anneau d'entiers. Soit L une extension finie séparable de K. Alors l'anneau des entiers de L est de la forme $\mathcal{O}_K[\alpha]$ pour un certain $\alpha \in L$.*

Démonstration. Soit $\mathfrak{P}$ l'idéal maximal de l'anneau des entiers $\mathcal{O}_L$, dont on a montré qu'il est local. La proposition 1.3.82 montre que le localisé de $\mathcal{O}_L$ en $\mathfrak{P}$, i.e., $\mathcal{O}_L$ lui-même, est le localisé d'un anneau de la forme $\mathcal{O}_K[\alpha]$, ce qui conclut. □

Proposition 2.1.40. *Soit K un corps muni d'une valuation discrète v, $|.|$ la valeur absolue associée, $\mathfrak{p}$ l'idéal premier correspondant. Soit $|L|$ une extension finie galoisienne de K, $|.|$ une valeur absolue de L qui étend celle de K, $\mathfrak{P}$ l'idéal premier correspondant. Soient $\overline{K}$ et $\overline{L}$ les complétés de K et L respectivement par rapport à $|.|$. Soit $D_{\mathfrak{P}}$ le groupe de décomposition en $\mathfrak{P}$. Alors le degré de $\overline{L}$ sur $\overline{K}$ est ef, où e est tel que $\mathfrak{P}^e = \mathfrak{p}$, et f est le degré de l'extension résiduelle.*

On a un isomorphisme canonique

$$D_{\mathfrak{P}} \simeq Gal(\overline{L}/\overline{K}).$$

Démonstration. La première formule est évidente.

Soit σ un élément de $D_{\mathfrak{P}}$. Alors $\sigma : L \to L$ préserve l'idéal $\mathfrak{P}$, donc envoie uniformisante sur uniformisante, et unité sur unité. En particulier, σ est une isométrie

pour la valeur absolue de L, et s'étend en un automorphisme de corps de $\overline{L}$, qui laisse fixe K, donc son adhérence $\overline{K}$. On dispose ainsi d'une injection

$$D_{\mathfrak{P}} \to Gal(\overline{L}/\overline{K}),$$

qui est une bijection par égalité des cardinaux. □

2.1.5 Le lemme de Hensel

Le lemme de Hensel, sous ses diverses formes, relie factorisation de polynômes sur le corps résiduel d'un corps complet pour une valuation discrète, et factorisation sur le corps lui-même.

Fixons dans tout ce qui suit un corps local K complet pour une valuation discrète v. On note $\mathcal{O}_K$ l'anneau des entiers de K, et $\mathfrak{p}$ l'idéal maximal. Soit k le corps résiduel de K.

Lemme 2.1.41. *Soit P un polynôme unitaire irréductible à coefficients dans $\mathcal{O}_K$. Alors la réduction de P modulo $\mathfrak{p}$ est une puissance d'un polynôme irréductible.*

Démonstration. Soit $p \geq 0$ la caractéristique de K. On peut trouver un entier positif n tel que $P(X) = Q(X^{p^n})$ et Q est irréductible et séparable. Soient $\overline{P}$ et $\overline{Q}$ les réductions de P et Q modulo $\mathfrak{p}$ respectivement. Supposons que $\overline{Q}$ soit une puissance d'un polynôme irréductible R. Comme le corps résiduel de $\mathcal{O}_K$ est parfait, on peut écrire

$$R(X^{p^n}) = S(X)^{p^n},$$

pour un certain polynôme S dans $k[X]$. Si $S = S_1 S_2$, alors

$$R(X^{p^n}) = S_1(X)^{p^n} S_2(X)^{p^n} = T_1(X^{p^n}) T_2(X^{p^n}),$$

où T_1 et T_2 ont même degrés que S_1 et S_2 respectivement. Comme R est irréductible, S est ainsi irréductible, et, finalement, $\overline{P}$ est une puissance du polynôme irréductible S.

La discussion précédente nous permet de supposer P séparable. Soit $L = K[X]/(P)$. Alors L est une extension finie séparable de K. C'est donc un corps local. Considérons les inclusions

$$\mathcal{O}_K \subset \mathcal{O}_K[X]/(P) \subset \mathcal{O}_L.$$

Comme $\mathcal{O}_L$ est fini sur $\mathcal{O}_K$, $\mathcal{O}_L$ est fini sur $\mathcal{O}_K[X]/(P)$. On sait que $\mathcal{O}_L$ est local, donc $\mathcal{O}_K[X]/(P)$ est local. Considérons le morphisme surjectif

$$\mathcal{O}_K[X]/(P) \to k[X]/(P).$$

Si (P) n'est pas puissance d'un irréductible, alors $k[X]/(P)$ a au moins deux idéaux maximaux distincts, d'où deux idéaux maximaux distincts dans $\mathcal{O}_K[X]/(P)$, contradiction, ce qui conclut. □

Proposition 2.1.42 (Lemme de Hensel)**.** *Soit P un polynôme unitaire à coefficients dans $\mathcal{O}_K$. Supposons que la réduction $\overline{P}$ de P modulo $\mathfrak{p}$ s'écrit*

$$\overline{P} = \overline{Q}\,\overline{R},$$

où $\overline{Q}$ et $\overline{R}$ sont deux polynômes à coefficients dans k, premiers entre eux. Alors on peut écrire $P = QR$, où Q et R sont deux polynômes à coefficients dans $\mathcal{O}_K$ de réduction $\overline{Q}$ et $\overline{R}$ respectivement.

Démonstration. On peut supposer $\overline{Q}$ et $\overline{R}$ unitaires. Supposons que ni $\overline{Q}$ ni $\overline{R}$ ne soient constants. Le lemme précédent montre que P n'est pas irréductible, ni même une puissance d'un polynôme irréductible. On peut donc écrire $P = ST$, avec S, T unitaires non constants, à coefficients dans $\mathcal{O}_K$. Alors $\overline{S}\,\overline{T} = \overline{Q}\,\overline{R}$, donc on peut écrire

$$\overline{S} = \overline{Q}_1\,\overline{R}_1$$

et

$$\overline{T} = \overline{Q}_2\,\overline{R}_2,$$

où les $\overline{Q}_i$ (resp. $\overline{R}_i$) divisent $\overline{Q}$. On conclut par récurrence sur le degré. □

Remarque 2.1.43. *On pourrait montrer que la proposition vaut même si P n'est pas supposé unitaire, mais seulement non nul modulo $\mathfrak{p}$.*

Corollaire 2.1.44. *Soit P un polynôme unitaire à coefficients dans $\mathcal{O}_K$, et soit $\alpha \in k$ une racine simple de la réduction de P modulo $\mathfrak{p}$. Alors α se relève en une racine simple de P dans $\mathcal{O}_K$.*

Démonstration. L'hypothèse est que l'on peut écrire $\overline{P} = (X - \alpha)\overline{Q}$, où $\overline{Q}$, où $\overline{Q}$ est premier à $(x - \alpha)$, ce qui permet d'appliquer la proposition précédente. □

On peut adopter un point de vue plus algorithmique sur le corollaire 2.1.44, ce qui permet d'en prouver des raffinements. En voici un, que l'on ne démontre pas – il s'agit essentiellement d'appliquer la méthode de Newton.

Proposition 2.1.45. *Soit P un polynôme à coefficients dans $\mathcal{O}_K$, et soit α_0 un élément de $\mathcal{O}_K$ tel que $|P(\alpha_0)| < |P'(\alpha_0)|^2$, où $|.|$ est une valeur absolue associée à la valuation de K. Alors il existe une unique racine α de P dans K telle que*

$$|\alpha - \alpha_0| \leq |P(\alpha_0)|/|P'(\alpha_0)|^2.$$

Exemple 2.1.5.1. *Soit K un corps local de corps résiduel $\mathbb{F}_q$. Alors K contient les racines $(q-1)$-èmes de l'unité. En effet, le polynôme $X^{q-1} -$ est scindé à racines simples dans $\mathbb{F}_q$, donc dans K.*

2.1.6 Ramification

Soit K un corps local complet pour une valuation discrète v, $\mathcal{O}_K$ son anneau des entiers, $\mathfrak{p}$ l'idéal maximal, k le corps résiduel.

Extensions non ramifiées

Si L est une extension finie de K, d'anneaux des entiers $\mathcal{O}_L$ et d'idéal maximal $\mathfrak{P}$, rappelons que L/K est dite non-ramifiée si $\mathfrak{P} = \mathfrak{p}\mathcal{O}_L$. Cette propriété est équivalente à $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = 0$.

Dans ce cas, la valuation discrète v s'étend de manière unique à L, et toute uniformisante de K est une uniformisante de L.

Proposition 2.1.46. *Les propriétés suivantes sont vérifiées.*

(i) Si L est une extension non-ramifiée de K, et si L' est une extension non-ramifiée de L, alors L' est une extension non-ramifiée de K.

(ii) Si L est une extension non-ramifiée de K, et si $K \subset L' \subset L$ est une extension intermédiaire, alors L/K et L'/L sont non ramifiées.

(iii) Si L est une extension non-ramifiée de K, et si L' est une extension finie arbitraire de K, alors LL'/L' est non-ramifiée.

Démonstration. Ces énoncés suivent des propriétés générales de la ramification et sont laissés au lecteur. □

Remarquons que la proposition précédente implique que si L et L' sont deux extensions non-ramifiées de K, alors LL' est une extension non-ramifiée de K.

Si L/K est une extension non-ramifiée de degré d, alors l'extension résiduelle associée est de degré d. Ce qui suit est une conséquence du théorème de Hensel.

Théorème 2.1.47. *L'application qui à une extension non-ramifiée de K associe l'extension résiduelle de k induit une bijection entre les classes d'isomorphismes d'extension non-ramifiées de K et les extensions finies de k. Si L/K est une extension non-ramifiée, alors elle est galoisienne et le groupe de Galois $Gal(L/K)$ s'identifie canoniquement au groupe de Galois de l'extension résiduelle.*

Démonstration. Soit l une extension finie de degré d de k. Comme k est fini, l/k est galoisienne, donc de la forme $k[X]/(P)$ pour un certain polynôme P irréductible de degré d dans $k[X]$, scindé à racines simples dans l. Soit Q un relèvement de P de degré d, et soit $L = K[X]/(P)$. D'après la proposition 1.3.50, L est une extension de degré d non-ramifiée de K, de corps résiduel l. Comme P est scindé à racines simples, le lemme de Hensel montre que Q est scindé à racines simples, donc que L/K est une extension galoisienne. La théorie générale de la ramification montre bien que le morphisme naturel $Gal(L/K) \to Gal(l/k)$ est un isomorphisme.

Pour conclure, il reste à montrer que la construction de L est indépendante du choix d'un relèvement de P. Soit donc R un relèvement de P de degré d, M le corps $K[X]/(R)$. Alors la réduction de R modulo l'idéal maximal de $\mathcal{O}_L$ est égale à P, donc elle est scindée à racines simples. Le lemme de Hensel garantit que R est scindé dans L, ce qui montre que L et L' sont isomorphes. □

Remarque 2.1.48. *L'énoncé précédent pourrait être précisé en une équivalence de catégories entre la catégorie des extensions finies de k et celle des extensions finies non ramifiée de K.*

On déduit immédiatement du théorème les deux énoncés suivants.

Corollaire 2.1.49. *Toute extension non-ramifiée de K est cyclique, de groupe de Galois engendré par un relèvement du Frobenius.*

Corollaire 2.1.50. *Soit L une extension finie de K. Il existe une extension intermédiaire $K \subset T \subset L$, non-ramifiée sur K et contenant toute sous-extension de L non-ramifiée sur K. L'extension L/T est totalement ramifiée. On l'appelle l'extension maximale non-ramifiée de L dans K. Elle est galoisienne de groupe de Galois $Gal(l/k)$, où l est le corps résiduel de L.*

Corollaire 2.1.51. *Extension maximale non ramifiée.*

Extensions modérément ramifiées

Définition 2.1.52. *Soit L une extension finie de K, T l'extension maximale non-ramifiée de L dans K. On dit que L/K est modérément ramifiée si le degré $[L : T]$ est premier à la caractéristique résiduelle de K.*

Ce qui suit est évident.

Proposition 2.1.53. *Les propriétés suivantes sont vérifiées.*

(i) Si L est une extension modérément ramifiée de K, et si L' est une extension modérément ramifiée de L, alors L' est une extension modérément ramifiée de K.

(ii) Si L est une extension modérément ramifiée de K, et si $K \subset L' \subset L$ est une extension intermédiaire, alors L/K et L'/L sont non ramifiées.

(iii) Si L est une extension modérément ramifiée de K, et si L' est une extension finie arbitraire de K, alors LL'/L' est modérément ramifiée.

Corollaire 2.1.54. *Soit L une extension finie de K. Il existe une extension intermédiaire $K \subset L' \subset L$, modérément ramifiée sur K et contenant toute sous-extension de L modérément ramifiée sur K. L'extension L/L' est totalement ramifiée, et a pour degré une puissance de la caractéristique résiduelle de K.*

Voici le théorème de structure des extensions modérément ramifiées.

Théorème 2.1.55. *Soit L une extension totalement et modérément ramifiée de K, de degré d. Alors il existe une uniformisante ϖ de K telle que $L = K(\varpi^{1/d})$.*

Réciproquement, si d est un entier premier à la caractéristique résiduelle de K, et si ϖ est une uniformisante de K, alors $K(\varpi^{1/d})$ est une extension de K totalement et modérément ramifiée.

Démonstration. Si π est une uniformisante de K, le polynôme $X^d - \varpi$ est un polynôme d'Eisenstein, donc $K(\varpi^{1/d})$ est une extension totalement ramifiée de K, qui est bien modérément ramifiée.

Soit L une extension totalement et modérément ramifiée de K, de degré d. Soit ϖ' une uniformisante de L. Comme L/K est totalement ramifiée, l'idéal (ϖ^d) est $\mathfrak{p}\mathcal{O}_L$, ce qui signifie que l'on peut écrire $\varpi'^d = u\varpi$, où u est une unité de $\mathcal{O}_L$ et ϖ une uniformisante de K. Comme l'extension résiduelle de L/K est triviale, on peut trouver une unité v de $\mathcal{O}_K$ telle que $uv^{-1} \in 1 + \mathfrak{P}$, où $\mathfrak{P}$ est l'idéal maximal de $\mathcal{O}_L$. Quitte à remplacer ϖ par $v\varpi$, on peut donc supposer que u est congru à 1 modulo $\mathfrak{P}$.

Le lemme de Hensel garantit que le polynôme $X^d - u$ à une racine puisque sa réduction modulo $\mathfrak{P}$ $X^d - 1$ est scindé à racines simples. Écrivons $u = x^d$. Alors x est une unité de $\mathcal{O}_L$ et

$$(x^{-1}\varpi')^d = \varpi.$$

Le corps $K(x^{-1}\varpi')$ est de degré d sur K. En effet, si r est son degré, et si w est la valuation discrète sur $K(x^{-1}\varpi')$, alors on a $v = \alpha w_{|K}$ avec α divisant r. La formule précédente montre que α est divisible par d, donc $r = d$. Ainsi $K(x^{-1}\varpi') = L$, ce qui conclut. □

2.2 Théorie du corps de classes local

Les deux résultats principaux de cette section sont la détermination du groupe de Brauer d'un corps local, et la détermination des extensions abéliennes d'un corps local. Un point clé sera pour nous la construction d'extensions abéliennes par une méthode qui généralise les extensions cyclotomiques – il s'agira de la théorie de Lubin-Tate.

2.2.1 Le groupe de Brauer d'un corps local

Soit K un corps local. On note v sa valuation discrète, $\mathcal{O}_K$ l'anneau des entiers de K, $\mathfrak{p} = (\varpi)$ son idéal maximal, et k son corps résiduel, qui est fini. On va calculer le groupe de Brauer de K.

Commençons par quelques préliminaires topologiques. Soit D une algèbre à division centrale de dimension n^2 sur K. Si $x \in D^*$, posons

$$v'(x) = v(Nrd_{D/K}(x)),$$

où $Nrd_{D/K}$ est la norme réduite de D, et posons $v'(0) = \infty$. Alors $v' : D^* \to \mathbb{Z}$ est un morphisme de groupes. Si n^2 est la dimension de D sur K, alors

$$\forall x \in K, v'(x) = nv(x).$$

Soit r le pgcd des $v'(x), x \in D^*$. Alors r divise n. On note $w = \frac{1}{r}v'$, de sorte que

$$w : D^* \to \mathbb{Z}$$

est un morphisme de groupes surjectif. On a

$$\forall x \in K, w(x) = ev(x),$$

avec $e = n/r$.

Soit L un sous-corps de D contenant K. Soit x un élément de L. Alors

$$Nrd_{D/K}(x)^n = N_{D/K}(x)$$

par la proposition 1.1.34, où $N_{D/K}$ est la norme d'algèbre de D, et par ailleurs, considérant D comme un L-espace vectoriel de dimension $n^2/[L : K]$, on trouve

$$N_{D/K}(x) = N_{L/K}(x)^{n^2/[L:K]},$$

d'où [1]

$$Nrd_{D/K}(x)^{n[L:K]} = N_{L/K}(x)^{n^2}.$$

Il suit en particulier que la restriction de w à L est un multiple de la valuation discrète normalisée de L, puisque celle-ci est un multiple de $v \circ N_{L/K}$ par la proposition 2.1.36. En particulier, prenant pour L un corps de la forme $K(xy^{-1})$, on trouve

$$\forall x, y \in D^*, w(1 + xy^{-1}) \geq \min(0, w(xy^{-1}))$$

puis

$$\forall x, y \in D, w(x + y) \geq \min(w(x), w(y)).$$

Comme dans le cas commutatif, on montre que l'ensemble $\mathcal{O}_D$ des éléments x de D tels que $w(x) \geq 0$ est une sous-$\mathcal{O}_K$-algèbre de D, et que c'est l'ensemble des x qui sont entiers sur $\mathcal{O}_K$.

L'ensemble des $x \in D$ tels que $w(x) > 0$ est un idéal bilatère $\mathfrak{P}$ de $\mathcal{O}_D$. Le quotient $\mathcal{O}_D/\mathfrak{P}$ est manifestement une k-algèbre à division, c'est donc une extension finie de k puisque k est fini.

1. On pourrait montrer en fait $Nrd_{D/K}(x)^{[L:K]} = N_{L/K}(x)^n$.

Lemme 2.2.1. *Pour tout entier $i \geq 0$, on a*

$$\mathfrak{P}^i = \{x \in D, w(x) \geq i\}.$$

Démonstration. On a certainement

$$\mathfrak{P}^i \subset \{x \in D, w(x) \geq i\}.$$

Par définition de w, il existe un $x \in \mathfrak{P}$ tel que $w(x) = 1$. Alors x est non nul, donc inversible dans D. Soit y un élément de D avec $w(D) \geq i$. Alors $w(x^{-i}y) \geq 0$, donc $y \in x^i\mathcal{O}_D$, et $y \in \mathfrak{P}^i$, ce qui montre l'inclusion inverse. □

On a par ailleurs

$$\mathfrak{p}\mathcal{O}_D = \{\varpi x, x \in \mathcal{O}_D\} = \{x \in D, w(x) \geq e\}.$$

d'où

$$\mathfrak{p}\mathcal{O}_D = \mathfrak{P}^e.$$

Définition 2.2.2. *Avec les notations précédentes, le corps résiduel de D est le corps $\mathcal{O}_D/\mathfrak{P}$.*

Soit f est le degré du corps résiduel de D sur k. Comme k est fini, l'extension résiduelle est séparable, et engendrée par la réduction d'un élément x de $\mathcal{O}_D$. Soit $L = K[x]$. Par construction, L est une extension de K de degré au moins f, et L/K est non ramifiée donc galoisienne. La proposition 1.1.62 ci-dessus implique $f \leq n$.

Par ailleurs, comme dans le cas commutatif, on a

$$ef = \dim_K(D) = n^2.$$

Comme $e, f \leq n$, cela implique $e = f = n$.

La discussion précédente a la conséquence suivante.

Proposition 2.2.3. *Soit A une algèbre simple centrale de dimension finie n^2 sur K. Alors il existe une extension non ramifiée L de K, de degré n, incluse dans D.*

Démonstration. Si A est une algèbre à division, c'est ce que montre la discussion précédente. Dans le cas général, écrivons $A = M_r(D')$, avec D' une algèbre à division centrale sur K. Alors $n^2 = r^2d'^2$, où d'^2 est la dimension de D' sur K.

D'après ce qui précède, on peut trouver une extension non ramifiée L' de K de degré d', incluse dans D'. Le degré de L' sur K est donc n/r.

Rappelons qu'il existe une unique extension non ramifiée de K de degré fixé. Soit donc L l'extension non ramifiée de degré n de K. Comme $[L' : K]$ divise n, on peut inclure L' dans L de telle sorte que L est une extension de degré r de L', séparable donc engendrée par un élément x de polynôme minimal P. Soit $M \subset M_r(D')$ la matrice compagnon de polynôme caractéristique P. Alors le sous-corps de $M_r(D')$ engendré par M et $L' \subset D'$ est isomorphe à L, ce qui conclut. □

Avec ces préliminaires, on peut enfin déterminer le groupe de Brauer d'un corps local. Le corps K est maintenant le corps local du début de la section.

Commençons par un lemme.

Lemme 2.2.4. *Soit L une extension finie non ramifiée de K. Alors*

$$N_{L/K}(\mathcal{O}_L^*) = \mathcal{O}_K^*.$$

Démonstration. Commençons par remarquer que si k'/k est une extension de corps finis, alors les applications norme et trace sont surjectives. Pour la norme, c'est par exemple une application du théorème de Wedderburn qui assure que toutes les algèbres cycliques sont déployées (mais on peut le démontrer de manière élémentaire). Pour la trace, c'est bien sûr une propriété générale des extensions séparables.

La surjectivité de la norme au niveau des extensions résiduelles garantit que pour tout $x \in \mathcal{O}_L^*$, on peut trouver $y \in \mathcal{O}_L^*$ tel que x et y sont congrus modulo $\mathfrak{p}$. On peut donc se restreindre à montrer que le groupe $N_{L/K}(\mathcal{O}_L^*)$ contient $1 + \varpi\mathcal{O}_K$.

Soit $x = 1 + \varpi x_1 \in 1 + \varpi\mathcal{O}_K$. Soit $\alpha_1 \in \mathcal{O}_L$ de trace égale à x_1 modulo $\mathfrak{p}$. Alors $N_{L/K}(1 + \varpi\alpha_1) = 1 + \varpi x_1$ modulo ϖ^2, et

$$xN_{L/K}(1 + \varpi\alpha_1)^{-1} = 1 + \varpi^2 x_2$$

pour un certain $x_2 \in \mathcal{O}_K$. Par récurrence, on trouve une suite α_i telle que pour tout $n \geq 1$, on ait

$$xN_{L/K}((1 + \varpi\alpha_1)\dots(1 + \varpi^n\alpha_n))^{-1} = 1 + \varpi^{n+1}x_{n+1}$$

pour un certain $x_{n+1} \in \mathcal{O}_K$. Cela montre que x est adhérent au groupe $N_{L/K}(1 + \varpi\mathcal{O}_K)$, qui est compact comme image d'un compact, donc $x \in N_{L/K}(1 + \varpi\mathcal{O}_K)$. □

Théorème 2.2.5. *Soit L l'extension non ramifiée de degré n de K, et soit σ un générateur du groupe de Galois de L/K. Notons $Br(L/K)$ le sous-groupe de $Br(K)$ constitué des classes d'algèbres simples centrales déployées par L.*

(i) On a un diagramme commutatif

$$\begin{array}{ccc} K^*/N_{L/K}(L^*) & \xrightarrow{a\mapsto[(\sigma,a)]} & Br(L/K) \\ & \searrow^{a\mapsto 1/nv(a)} \quad \swarrow & \\ & (1/n\mathbb{Z})/\mathbb{Z} & \end{array}$$

dans lequel toutes les flèches sont des isomorphismes.

(ii) Notons $inv_{L,K} : Br(L/K) \to (1/n\mathbb{Z})/\mathbb{Z}$ l'isomorphisme ci-dessus obtenu en choisissant pour σ le Frobenius. Si L' est une extension finie non ramifiée de L, de degré mn, alors on a un diagramme commutatif

$$\begin{array}{ccc} Br(L/K) & \hookrightarrow & Br(L'/K) \\ \downarrow{\scriptstyle inv_{L,K}} & & \downarrow{\scriptstyle inv_{L',K}} \\ (1/n\mathbb{Z})/\mathbb{Z} & \hookrightarrow & (1/mn\mathbb{Z})/\mathbb{Z} \end{array}$$

(iii) Les isomorphismes $inv_{L,K}$ ci-dessus induisent un isomorphisme canonique

$$inv_K : Br(K) \to \mathbb{Q}/\mathbb{Z}.$$

Démonstration. Considérons d'abord l'application

$$K^*/N_{L/K}(L^*) \to Br(L/K), a \mapsto [(\sigma, a)].$$

La proposition 1.1.66 montre qu'il s'agit d'un morphisme de groupes, bien défini et injectif par la proposition 1.1.68.

Si x est un élément de L, alors $v(N_{L/K}(x))$ est divisible par n – utiliser la proposition 2.1.36 et le fait que la valuation de K s'étend à L car L est non ramifié sur K. L'application

$$K^*/N_{L/K}(L^*) \to (1/n\mathbb{Z})/\mathbb{Z}, a \mapsto 1/nv(a)$$

est donc bien définie. Elle est manifestement surjective.

Notons pour le moment $inv_{L,K} : B_L \to (1/n\mathbb{Z})/\mathbb{Z}$ le morphisme ainsi obtenu, et montrons qu'il s'agit d'une injection – donc d'un isomorphisme. On raisonne par l'absurde et l'on se donne $a \in K^*$ tel que (σ, a) n'est pas déployée mais $v(a)$ est divisible par n.

Quitte à multiplier à par une puissance de $N_{L/K}(\varpi) = \varpi^n$, on peut supposer $a \in \mathcal{O}_K^*$. Il faut montrer que $a \in N_{L/K}(\mathcal{O}_L^*)$, ce que l'on a vu dans le Lemme 2.2.4.

Dans le diagramme commutatif

$$\begin{array}{ccc} K^*/N_{L/K}(L^*) & \xrightarrow{a\mapsto[(\sigma,a)]} & B_L \\ & \searrow^{a\mapsto 1/nv(a)} \quad \swarrow & \\ & (1/n\mathbb{Z})/\mathbb{Z} & \end{array}$$

les trois flèches sont donc bien des isomorphismes.

La discussion précédente nous fournit, avec les notations de (ii), des inclusions naturelles $B_L \subset B_{L'}$, et des diagrammes commutatifs

$$\begin{array}{ccc} B_L & \hookrightarrow & B'_L \\ \downarrow{\scriptstyle inv_{L,K}} & & \downarrow{\scriptstyle inv_{L',K}} \\ (1/n\mathbb{Z})/\mathbb{Z} & \hookrightarrow & (1/mn\mathbb{Z})/\mathbb{Z} \end{array}$$

où σ est le Frobenius.

En particulier, la réunion des B_L, où L parcourt les extensions non-ramifiées de K, est un sous-groupe B' de $Br(K)$, et les applications $inv_{L,K}$ fournissent un isomorphisme canonique

$$inv : B' \to \mathbb{Q}/\mathbb{Z}.$$

Par définition, le groupe B' est le groupe des classes d'algèbres cycliques sur K associées à des extensions non ramifiées. Les propositions 2.2.3 et 1.1.63 montrent que l'on a $B' = Br(K)$, d'où le dernier énoncé.

Pour conclure la preuve du théorème, il faut montrer que l'on a $B_L = Br(L/K)$ pour toute extension non ramifiée L de K. C'est une conséquence de la proposition suivante. □

Définition 2.2.6. *L'isomorphisme inv_K construit dans le théorème précédent est appelé l'invariant de Hasse.*

Voici la propriété de fonctorialité de l'invariant de Hasse.

Proposition 2.2.7. *Soit L une extension finie de K, de degré d. Alors le diagramme suivant commute :*

$$\begin{array}{ccc} Br(K) & \xrightarrow{inv_K} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \otimes_K L} & & \downarrow{\scriptstyle d} \\ Br(L) & \xrightarrow{inv_L} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Démonstration. Soit $n > 0$. Soit L' l'extension non ramifiée de degré n de K, σ le Frobenius dans $Gal(L'/K)$. Soit a un élément de K^*, et $A = (\sigma, a)$. Alors $inv_K(A)$ est $\frac{1}{n}v(a)$. On veut montrer

$$inv_L(A \otimes_K L) = n\, inv_K(A) = \frac{d}{n}v(a) \in \mathbb{Q}/\mathbb{Z}.$$

Commençons par supposer que $L \subset L'$. Alors d divise n. Le Frobenius de L'/L est σ^d. Il faut montrer que

$$inv_L(A \otimes_K L) = inv_L(\sigma^d, a),$$

soit

$$A \otimes_K L \simeq M_{r/d}(L) \otimes_L (\sigma^d, a).$$

C'est un calcul semblable à celui qui montre que (σ, a) est déployée par L, que nous laissons au lecteur.

Le calcul précédent nous permet de supposer que l'extension L est disjointe de L'. Alors $L' \otimes_K L$ est un corps, extension non-ramifiée de L de degré n, et l'on a manifestement

$$A \otimes_K L \simeq (\sigma', a),$$

où σ' est le L-automorphisme de $L' \otimes_K L$ induit par σ. Soient e et f l'indice de ramification et le degré résiduel de l'extension L/K. Alors le Frobenius de $L' \otimes_K L$ est $(\sigma')^f$, et, si w est la valuation de L, on a $w_{|K} = ev$.

Nous laissons en exercice au lecteur l'isomorphisme

$$(\sigma', a) = (\sigma'^f, a^f)$$

(utiliser que f est inversible modulo n). On en déduit

$$inv_L(\sigma', a) = inv_L((\sigma')^f, a^f) = \frac{f}{n} w(a) = \frac{ef}{n} v(a) = d\, inv_K(A).$$

□

Le corollaire suivant finit la preuve du théorème.

Corollaire 2.2.8. *Dans le Théorème 2.2.5, on a $B_L = Br(L/K)$.*

Démonstration. La proposition précédente montre que le noyau $Br(L/K)$ de $Br(K) \to Br(L)$ est de cardinal d, qui est aussi le cardinal de B_L, ce qui conclut. □

2.2.2 L'application de réciprocité d'Artin

Soit K un corps local de clôture algébrique $\overline{K}$, et soit $G_K = Gal(\overline{K}/K)$ le groupe de Galois absolu de K. Rappelons les résultats et les constructions de 1.1.9.

Soit comme précédemment

$$X(K) = \mathrm{Hom}(G_K, \mathbb{Q}/\mathbb{Z})$$

le groupe des morphismes continus du groupe de Galois absolu G_k vers $\mathbb{Q}/\mathbb{Z}$ (muni de sa topologie usuelle ou discrète). Le groupe $X(K)$ est un groupe abélien de torsion. On le munit de la topologie discrète – on peut montrer que c'est sa topologie naturelle en tant que dual de G (la topologie compact-ouverte).

Soit χ un élément de $X(K)$. Son image est de la forme $1/n\mathbb{Z}/\mathbb{Z}$ pour un certain $n \geq 1$. À χ sont associés une extension cyclique L – le sous-corps de $\overline{K}$ fixé par le noyau de χ – et un générateur σ distingué de $Gal(L/K)$ tel que $\chi(\sigma) = 1$.

Si a est un élément de k^*, on note $(\chi, a) \in Br(K)$ la classe de l'algèbre cyclique (σ, a). On a vu dans le théorème 1.1.90 que l'application

$$X(K) \times K^* \longrightarrow Br(K)$$

est bilinéaire. Si χ est un élément de $X(K)$ associé à une extension cyclique L/K, alors le morphisme de groupes

$$K^* \longrightarrow Br(K), a \mapsto (\chi, a)$$

induit un isomorphisme

$$K^*/N_{L/K}(K^*) \longrightarrow Br(L/K).$$

Enfin, si L est une extension finie de K, l'application de restriction naturelle $X(K) \to X(L)$, l'inclusion $K^* \subset L^*$ et l'extension des scalaires $Br(K) \to Br(L)$ induisent un diagramme commutatif

$$\begin{array}{ccc} X(K) \times K^* & \longrightarrow & Br(K) \\ \downarrow & & \downarrow \\ X(L) \times L^* & \longrightarrow & Br(L) \end{array}$$

Remarque 2.2.9. *Dans le théorème 1.1.90, on n'a pas montré la surjectivité de*

$$K^*/N_{L/K}(K^*) \longrightarrow Br(L/K)$$

si L est une extension cyclique de K. Dans le cas qui nous occupe, elle suit du théorème 2.2.5 sur la structure du groupe de Brauer d'un corps local.

Soit $a \in K^*$. On peut considérer l'application

$$X(K) \longrightarrow \mathbb{Q}/\mathbb{Z},\ \chi \mapsto (\chi, a).$$

Elle est continue car $X(K)$ est discret.

L'accouplement

$$X(K) \times K^* \longrightarrow \mathbb{Q}/\mathbb{Z}$$

ci-dessus induit donc un morphisme

$$K^* \to \mathrm{Hom}(X(K), \mathbb{Q}/\mathbb{Z})$$

de K^* vers le groupe des morphismes continus de $X(K)$ vers $\mathbb{Q}/\mathbb{Z}$.

Pour aller plus loin, on a besoin d'un important théorème de Pontryagin. Soit G_K^{ab} l'abélianisé de G_K. Ce groupe est à la fois – on en laisse la vérification au lecteur – le groupe de Galois de l'extension abélienne maximale de K, et le groupe profini limite des $Gal(L/K)$, où L parcourt les extensions abéliennes de K contenues dans une clôture séparable de K fixée.

Bien sûr, tout caractère

$$\chi : G_K \longrightarrow \mathbb{Q}/\mathbb{Z}$$

de G_K se factorise par G_K^{ab}. On obtient ainsi un morphisme naturel de bidualité

$$\phi : G_K^{\mathrm{ab}} \longrightarrow \mathrm{Hom}(X(K), \mathbb{Q}/\mathbb{Z})$$

qui à l'image d'un élément g de G_K dans G_K^{ab} associe

$$\chi \mapsto \chi(g).$$

Le membre de gauche est muni de sa topologie profinie – limite des topologies discrètes sur ses quotients finis, et le membre de droite de sa topologie compact-ouverte, dont une base d'ouverts est donnée par les ensembles

$$\{\alpha \in X(K) | \alpha(F) \subset U\}$$

où U est un ouvert de $\mathbb{Q}/\mathbb{Z}$ et F un ensemble fini.

Théorème 2.2.10. *L'application de bidualité ϕ est un isomorphisme de groupes topologiques.*

Remarque 2.2.11. *Ce théorème s'applique plus généralement à des groupes abéliens localement compacts.*

Suivant les constructions précédentes, on obtient un morphisme

$$\rho_K : K^* \longrightarrow G_K^{ab}$$

C'est *l'application de réciprocité d'Artin*, un objet fondamental de la théorie des corps locaux, qui relie deux objets de natures a priori différentes. Elle est caractérisée par la propriété suivante :

$$\forall \chi \in X(K), \forall a \in K^*, inv_K(\chi, a) = \chi(\rho_K(a)) \in \mathbb{Q}/\mathbb{Z}.$$

Voici le théorème principal de la théorie du corps de classe local.

Théorème 2.2.12. *Soit K un corps local.*

1. *L'application de réciprocité ρ_K est l'unique morphisme continu de K^* dans G_K^{ab} tel que*
   (i) Si L est une extension abélienne finie de K, ρ_K induit un isomorphisme
   $$K^*/N_{L/K}(L^*) \to Gal(L/K);$$
   (ii) Si K a pour corps résiduel $\mathbb{F}_q$ et v et sa valuation, on a un diagramme commutatif
   $$\begin{array}{ccc} K^* & \xrightarrow{\rho_K} & G_K^{ab} \\ \downarrow{\scriptstyle v} & & \downarrow \\ \mathbb{Z} & \longrightarrow & Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q) \end{array}$$
   où $G_K^{ab} \to Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ est la composition
   $$G_K^{ab} \to Gal(K^{nr}/K) \to Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$$
   et $\mathbb{Z} \to Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ envoie 1 sur le Frobenius.

2. *$U \mapsto \rho_K^{-1}(U)$ est une bijection de l'ensemble des sous-groupes ouverts de G_K^{ab} vers l'ensemble des sous-groupes (ouverts) d'indice fini de K^*.*

Il y a beaucoup de choses à prouver dans ce théorème important. Heureusement, la section précédente nous fournit une partie des résultats sans qu'il soit nécessaire de travailler beaucoup.

Avant de continuer, rajoutons un résultat sur la fonctorialité de l'application de réciprocité.

Proposition 2.2.13. *L'application de réciprocité ρ_K vérifie la propriété suivante : soit L une extension finie de K. Alors le diagramme*

$$\begin{array}{ccc} L^* & \xrightarrow{\rho_L} & G_L^{ab} \\ \downarrow{\scriptstyle N_{L/K}} & & \downarrow \\ K^* & \xrightarrow{\rho_K} & G_K^{ab} \end{array}$$

commute, où la flèche $G_L^{ab} \to G_K^{ab}$ est induite par la restriction $G_L \to G_K$.

Remarque 2.2.14. *Manque ici la fin de la partie p-adique : preuves du corps de classe local et application à Kronecker-Weber local et global.*

Chapitre 3

Méthodes analytiques

3.1 Fonction ζ de Dedekind

Soit K un corps de nombres de degré n sur $\mathbb{Q}$, et soit $\mathcal{O}_K$ son anneau des entiers. Si I est un idéal de K, on note $N(I)$ l'entier positif tel que

$$(N(I)) = N_{K/\mathbb{Q}}(I).$$

Définition 3.1.1. *La fonction ζ de Dedekind de K, notée ζ_K, et la fonction d'une variable complexe*

$$s \mapsto \sum_I \frac{1}{N(I)^s},$$

où la somme porte sur tous les idéaux non nuls de $\mathcal{O}_K$.

Exemple 3.1.0.1. *Si $K = \mathbb{Q}$, on a par définition*

$$\zeta_{\mathbb{Q}}(s) = \sum_{n \geq 1} \frac{1}{n^s}.$$

On retrouve la fonction ζ de Riemann.

On sait bien que la série qui définit la fonction ζ de Riemann converge absolument pour $\Re s > 1$, et que dans ce domaine on a l'égalité

$$\zeta(s) = \prod_p \left(1 - p^{-s}\right)^{-1},$$

où le produit est pris sur l'ensemble des nombres premiers. La proposition suivante généralise ce fait.

Proposition 3.1.2. *La série qui définit ζ_K est absolument convergente dans le domaine $\Re s > 1$ et définit une fonction holomorphe. On a l'égalité*

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - N(\mathfrak{p})^{-s}\right)^{-1},$$

où le produit est pris sur l'ensemble des idéaux premiers non nuls de $\mathcal{O}_K$.

Démonstration. Partons du produit infini $\prod_{\mathfrak{p}} \left(1-N(\mathfrak{p})^{-s}\right)^{-1}$. On commence par montrer qu'il est convergent dans le domaine $\Re s > 1$. Il s'agit de montrer que la série

$$\sum_{\mathfrak{p}} \log\left(1 - N(\mathfrak{p})^{-s}\right)$$

converge absolument dans ce domaine, donc, par une majoration facile, que la série

$$\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}$$

converge absolument

Si $\mathfrak{p}$ est un idéal premier non nul de $\mathcal{O}_K$, au-dessus du premier p de $\mathbb{Z}$, alors la norme de $\mathfrak{p}$ vaut au moins p. Par ailleurs, il y a au plus n idéaux premiers distincts de $\mathcal{O}_K$ au-dessus de p. Ces deux remarques nous montrent

$$\sum_{\mathfrak{p}} \left|N(\mathfrak{p})^{-s}\right| \leq n \sum_{p} p^{-\Re s}.$$

La remarque ci-dessus garantit la convergence de cette somme pour $\Re s > 1$. Le produit $\prod_{\mathfrak{p}} \left(1 - N(\mathfrak{p})^{-s}\right)^{-1}$ est donc bien convergent dans ce domaine.

Pour $\Re s > 1$, la même manipulation que celle utilisée pour la fonction ζ de Riemann garantit l'égalité

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - N(\mathfrak{p})^{-s}\right)^{-1},$$

et la convergence de la somme qui définit la fonction ζ de Dedekind. □

Hecke a prouvé que la fonction ζ de Dedekind s'étend en une fonction méromorphe de s sur $\mathbb{C}$ tout entier, avec un unique pôle simple en $s = 1$, et qu'elle satisfait une équation fonctionnelle semblable à celle que satisfait la fonction ζ de Riemann. Ces résultats sont sensiblement plus difficiles à prouver que ceux qui concernent la fonction ζ de Riemann.

Dans cette section, on va se contenter de montrer le prolongement analytique de ζ_K en une fonction méromorphe dans le domaine $\Re s > 1 - \frac{1}{[K:\mathbb{Q}]}$, avec un pôle simple en $s = 1$, et de calculer le résidu en 1. Ce dernier résultat est la *formule analytique du nombre de classe*. Avant de l'énoncer, on va discuter plus précisément de quelques problèmes de comptage.

Pour comprendre ce que l'on veut montrer, voici un lemme analytique.

Lemme 3.1.3. *Soit $(a_n)_{n\geq 1}$ une suite de nombre complexes. On suppose*

$$\sum_{n=1}^{r} a_n = \rho r + O(r^\sigma)$$

pour un certain $\rho \neq 0$, et $0 < \sigma < 1$. Alors la série

$$\sum_{n\geq 1} a_n n^{-s}$$

converge absolument pour $\Re s > 1$, et s'étend en une fonction méromorphe sur le domaine $\Re s > \sigma$, qui est holomorphe hors de $s = 1$, où elle a un pôle simple de résidu ρ.

Démonstration. Si les a_n sont constant, égaux à ρ, le résultat est une conséquence du cas, connu, de la fonction ζ de Riemann. Remplaçant a_n par $a_n - \rho$, on peut supposer $\rho = 0$ et $a_n = O(n^\sigma)$. On va montrer que la série $\sum_{n\geq 1} a_n n^{-s}$ converge absolument pour $\Re s > \sigma$. On peut pour cela supposer les a_n réels positifs.

Soit $A(r) = \sum_{1\leq n\leq r} a_n$. Alors

$$\sum_{n=1}^{N} a_n n^{-s} = \sum_{n=1}^{N} (A(n) - A(n-1))n^{-s} = A(N)(N+1)^{-s} + \sum_{n=1}^{N} A(n)(n^{-s} - (n+1)^{-s}).$$

Supposons $\Re s > \sigma$. Alors

$$A(N)(N+1)^{-s} = O(N^{\sigma - s}) = o(1)$$

et

$$n^{-s} - (n+1)^{-s} = O(n^{-s-1}),$$

donc

$$A(n)(n^{-s} - (n+1)^{-s}) = O(N^{\sigma - s - 1}),$$

ce qui conclut à la convergence désirée. □

On peut réécrire la fonction ζ de Dedekind comme

$$\zeta_K(s) = \sum_{n\geq 1} a_n n^{-s},$$

où a_n est le nombre d'idéaux non-nuls de $\mathcal{O}_K$ de norme n. Le lemme précédent nous incite donc à étudier la quantité

$$A(r) = \big|\{I \subset \mathcal{O}_K, N(I) \leq r\}\big|,$$

où par I on désigne un idéal non-nul de $\mathcal{O}_K$.

On va étudier $A(r)$ en séparant leurs idéaux suivant leur classe dans $Cl(\mathcal{O}_K)$. On va donc commencer par l'étude du nombre

$$X(r) = \left|\{x \in \mathcal{O}_K, x \neq 0, |N(x)| \leq r\}/\mathcal{O}_K^*\right|$$

des idéaux principaux non nuls de $\mathcal{O}_K$ de norme au plus n. On va faire cette estimation en plusieurs temps.

On reprend les notations de 1.3.7 : en particulier, V est la $\mathbb{R}$-algèbre $K \otimes_{\mathbb{Q}} \mathbb{R}$, isomorphe à $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. On note $(\underline{t}, \underline{z})$ les coordonnée d'un élément de V.

On note N la norme sur V, qui envoie $(t_1, \ldots, t_{r_1}, z_1, \ldots, z_{r_2})$ sur le produit

$$t_1 \ldots t_{r_1} |z_1|^2 \ldots |z_{r_2}|^2.$$

On note V^* le groupe des éléments inversibles de V pour la multiplication. Il s'agit des éléments de norme non nulle. On note V^1 l'ensemble des éléments de norme ± 1.

Le théorème des unités de Dirichlet nous permet d'écrire

$$\mathcal{O}_K^* = F \times W,$$

où W est un groupe fini – le sous-groupe de torsion de $\mathcal{O}_K^*$, et F est un groupe abélien libre de type fini (et de rang $r_1 + r_2 - 1$). La décomposition n'est pas canonique, mais on peut en choisir une. Soit

$$Y(r) = \left|\{x \in \mathcal{O}_K, x \neq 0, |N(x)| \leq n\}/F.\right|$$

Le groupe W agit sans point fixe sur $Y(n)$, d'où

$$Y(r) = \frac{1}{w} X(r), \tag{3.1.1}$$

où w est le cardinal de W.

Considérons le diagramme suivant, déjà considéré en 1.2.2 :

$$\begin{array}{ccccc} V^* & \longrightarrow & \mathbb{R}^{r_1+r_2} \times \{\pm 1\}^{r_1} \times \mathbb{S}^{r_2} & & \\ \uparrow & & \downarrow & & \\ V^1 & \longrightarrow & H & \hookrightarrow & \mathbb{R}^{r_1+r_2} \end{array}$$

dans lequel la flèche horizontale supérieure est un isomorphisme, et la composée

$$V^* \to \mathbb{R}^{r_1+r_2}$$

est la flèche

$$(\underline{t}, \underline{z}) \mapsto (\log|\underline{t}|, 2\log|\underline{z}|).$$

Ici H est l'hyperplan de $\mathbb{R}^{r_1+r_2}$ donné par le noyau de la trace

$$T : (\underline{x}) \mapsto \sum_i x_i.$$

Le groupe abélien libre F s'envoie de manière injective dans H. Le théorème des unités de Dirichlet montre que F s'identifie à un réseau de H.

Notons

$$\sigma : V^* \to V^1, x \mapsto |N(x)|^{1/n} x.$$

C'est une section de l'inclusion $V^1 \subset V^*$.

Soit Δ' un domaine fondamental pour l'action de F sur H. Soit Δ l'image réciproque de Δ' par la composée

$$V^* \xrightarrow{\sigma} V^1 \longrightarrow H.$$

Lemme 3.1.4. *L'ensemble Δ est un domaine fondamental pour l'action de F sur V^*. Si $\Delta_{\leq r} = \{x \in \Delta, |N(x)| \leq r\}$, alors $\Delta_{\leq r}$ est un domaine fondamental de $\{x \in V^*, |N(x)| \leq r\}$ pour l'action de F.*

Démonstration. La flèche composée $\phi : V^* \to H$ est équivariante pour l'action de F :

$$\forall (x, f) \in V^* \times F, \phi(xf) = \phi(x) + \phi(f).$$

La conclusion est formelle, et le même argument prouve le second énoncé. □

Faire intervenir Δ permet de ne pas passer au quotient dans l'étude de la quantité $Y(n)$. On a en effet, grâce au lemme ci-dessus :

$$Y(r) = \big|\{x \in \mathcal{O}_K \cap \Delta_{\leq r}\}\big|. \tag{3.1.2}$$

Remarquons l'égalité

$$\Delta_{\leq r} = r^{1/n} \Delta_{\leq 1}.$$

.

Supposons maintenant que Δ' est un domaine fondamental standard, de la forme

$$\Delta' = \sum_i [0, 1[\alpha_i.$$

où $\alpha_1, \ldots, \alpha_{r_1+r_2}$ est une base de l'image de F dans H.

Soit μ la mesure de Lebesgue sur V correspondant au produit scalaire normalisé considéré en 1.3.7 – donc avec des facteurs 2 aux facteurs complexes.

Proposition 3.1.5. *Quand r tend vers ∞, on a*

$$Y(r) = \frac{\mu(\Delta_{\leq r})}{\mathrm{covol}(\mathcal{O}_K)} + O(r^{1-1/n}) = \frac{\mu(\Delta_{\leq 1})}{\sqrt{|d_K|}} r + O(r^{1-1/n}).$$

Cette proposition est un cas particulier d'un résultat plus général sur le nombre de points d'un réseau dans des domaines de taille croissante. On le prouvera plus tard – finissons d'abord notre calcul. Il s'agit de calculer la mesure de $\Delta_{\leq 1}$. On va utiliser l'isomorphisme naturel

$$i : V^* \to \mathbb{R}^{r_1+r_2} \times \{\pm 1\}^{r_1} \times \mathbb{S}^{r_2}.$$

Alors l'image de Δ par i est par construction

$$i(\Delta) = \big(\mathbb{R}(1,\dots,1) + \Delta'\big) \times \{\pm 1\}^{r_1} \times \mathbb{S}^{r_2},$$

où H s'identifie au sous-espace des éléments de trace nulle, et par conséquent

$$i(\Delta_{\leq 1}) = \big(\mathbb{R}_-(1,\dots,1) + \Delta'\big) \times \{\pm 1\}^{r_1} \times \mathbb{S}^{r_2},$$

où $\mathbb{R}_-$ est l'ensemble des réels négatifs ou nuls.

Calculons la mesure image de μ par i. On travaille séparément sur chacun des facteurs réels ou complexes de V. Considérons d'abord

$$\mathbb{R}^* \to \mathbb{R} \times \{\pm 1\}, x \mapsto (\log|x|, \mathrm{sgn}(x)).$$

La flèche inverse est

$$(\alpha, \varepsilon) \mapsto \varepsilon e^{\alpha}.$$

Il suit directement que la mesure image sur $\mathbb{R} \times \{\pm 1\}$ est le produit de la mesure de comptage sur $\{\pm 1\}$ et de la mesure $e^{\alpha} d\alpha$.

Regardons

$$\mathbb{C}^* \to \mathbb{R} \times \mathbb{S}, z \mapsto (2\log|z|, \arg(z)), .$$

L'application inverse est

$$(\alpha, \theta) \mapsto e^{\alpha/2+\theta},$$

où l'on a identifié $\mathbb{S}$ avec le cercle unité complexe. La mesure image de la mesure $2dxdy = 2rdrd\theta$ (en coordonnées polaires) sur $\mathbb{R} \times \mathbb{C}$ est donc la mesure

$$2e^{\alpha/2} d(e^{\alpha/2}) d(\theta/i) = e^{\alpha} d\alpha d(\theta/i).$$

Ces deux calculs montrent que la mesure image de μ par i est la mesure

$$e^T \mu_{st}$$

où μ_{st} est le produit des mesures usuelles sur $\mathbb{R}$, $\{\pm 1\}$ et $\mathbb{S}$.

Considérons le changement de coordonnées

$$\mathbb{R}^{r_1+r_2} \to \mathbb{R}^{r_1+r_2}, \underline{x} \mapsto (x_1, \dots, x_{r_1+r_2-1}, T(\underline{x})).$$

Ce changement de coordonnées préserve les volumes. On trouve finalement

$$\mu(\delta_{\leq 1}) = 2^{r_1}(2\pi)^{r_2}\mathrm{covol}(F)\int_{-\infty}^{0} e^t dt = 2^{r_1}(2\pi)^{r_2}\mathrm{covol}(F), \tag{3.1.3}$$

où F est considéré comme un réseau dans $\mathbb{R}^{r_1+r_2-1}$ via la projection sur les r_1+r_2-1 premières coordonnées.

Définition 3.1.6. *Considérons l'application*

$$\mathcal{O}_K \to V \to \mathbb{R}^{r_1+r_2}$$

définie ci-dessus. Le régulateur de K est le covolume de l'image de $\mathcal{O}_K^*$ dans $\mathbb{R}^{r_1+r_2-1}$ via la projection sur les r_1+r_2-1 premières coordonnées.

Nous avons donc montré, à l'aide de (3.1.3), la proposition 3.1.5 et (3.1.1), l'estimation

$$\big|\{x \in \mathcal{O}_K, x \neq 0, |N(x)| \leq r\}/\mathcal{O}_K^*\big| = \frac{2^{r_1}(2\pi)^{r_2}R_K}{w\sqrt{|d_K|}}r + O(r^{1-1/n}).$$

Soit plus généralement h un élément du groupe de classes de $\mathcal{O}_K$. On estime le nombre

$$X_h(r) = \big|\{I \subset \mathcal{O}_K, [I] = h, N(I) \leq r\}$$

des idéaux de $\mathcal{O}_K$ dont la classe est h et la norme est au plus r. Soit I_0 un idéal fixé de classe $-h$. La multiplication par I induit une bijection entre les idéaux de $\mathcal{O}_K$ de classe h et les idéaux principaux de $\mathcal{O}_K$ inclus dans I_0, qui multiplie la norme par $N(I_0)$. On a donc

$$X_h(r) = \big|\{x \in I_0, x \neq 0, |N(x)| \leq rN(I_0)\}/\mathcal{O}_K^*\big|.$$

L'analogue de la proposition 3.1.5, qui est aussi une conséquence de la proposition 3.1.12 – dont il nous faut encore donner la preuve – s'énonce

$$X_h(r) = \frac{\mu(\Delta_{\leq rN(I_0)})}{w\mathrm{covol}(I_0)} + O(r^{1-1/n}) = \frac{\mu(\Delta_{\leq 1})}{w\sqrt{|d_K|}N(I_0)}rN(I_0) + O(r^{1-1/n}) = \frac{\mu(\Delta_{\leq 1})}{w\sqrt{|d_K|}}r + O(r^{1-1/n}),$$

où par rapport à la proposition on a divisé par w car on estime le quotient par $\mathcal{O}_K^*$ et non F. On a donc obtenu le théorème suivant :

Théorème 3.1.7 (Formule analytique du nombre de classe)**.** *La fonction ζ de Dedekind de K s'étend en une fonction méromorphe sur la bande*

$$\Re s > 1 - \frac{1}{[K:\mathbb{Q}]}.$$

Elle est holomorphe en dehors de $s = 1$, et elle admet un pôle simple en 1, de résidu

$$\mathrm{Res}_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}h_K R_K}{w\sqrt{|d_K|}},$$

où h_K est le nombre de classes de $\mathcal{O}_K$, R_K le régulateur, d_K le discriminant, w le cardinal du sous-groupe de torsion de $\mathcal{O}_K^*$, et r_1 (resp. r_2) est le nombre de plongements réels (resp. complexes à conjugaison près) de K.

Le corollaire suivant est très utile.

Corollaire 3.1.8. *La fonction ζ_K a un pôle simple en 1.*

Remarque 3.1.9. *Si X est un schéma de type fini sur $\mathbb{Z}$, on peut définir sa fonction ζ par le produit eulérien*

$$\zeta_X(s) = \prod_x (1 - |\kappa(x)|^{-s})^{-1},$$

où x parcourt les points fermés de X, et $\kappa(x)$ est le corps résiduel de x.

Si $X = \mathrm{Spec}\,\mathcal{O}_K$, on retrouve la fonction ζ de Dedekind. Si X définie sur un corps fini, les conjectures de Weil (prouvées par Grothendieck et Deligne) montrent que ζ_X se prolonge en une fraction rationnelle et satisfait une équation fonctionnelle. Elles déterminent les zéros et les pôles de ζ_X. Dans le cas général, prolongement analytique et équations fonctionnelles sont connues (grâce à Hecke pour $\mathrm{Spec}\,\mathcal{O}_K$). La détermination des zéros pour $X = \mathrm{Spec}\,\mathcal{O}_K$ constitue l'hypothèse de Riemann.

La fonction ζ_X a un pôle en $s = \dim(X)$. Dès que $\dim(X) > 1$, la détermination du résidu en ce pôle n'est connue que dans des cas très particuliers et fait l'objet de conjectures difficiles (sur les corps finis, c'est la conjecture de Tate).

Pour conclure cette partie, il faut encore prouver la proposition 3.1.5. On a besoin d'une définition pour l'énoncer dans une généralité convenable.

Définition 3.1.10. *Soit X un sous-ensemble de $\mathbb{R}^n$, et soit d un entier positif. On dit que X admet un d-paramétrage lipschitzien s'il existe un ensemble fini de fonctions lipschitziennes $f : [0,1]^d \to X$ dont l'union des images contient X.*

La proposition 3.1.12 généralise la proposition 3.1.5 – on en laisse l'application au lecteur. On commence par un résultat préliminaire.

Lemme 3.1.11. *Soit D un sous-ensemble mesurable de $\mathbb{R}^n$, image d'une fonction lipschitzienne*

$$f : [0,1]^{n-1} \longrightarrow \mathbb{R}^n.$$

Soit $r > 0$. Alors, quand t tend vers $+\infty$, on a

$$\mu(tD + B(0,r)) = O(t^{n-1}).$$

Démonstration. Comme la fonction $t \mapsto \mu(tD + B(0, \sqrt{n}))$ est croissante, on peut supposer $t = N$ entier. Alors il existe une constante $C > 0$ tel que tout point de $ND + B(0, r)$ soit à une distance au plus C d'un point de $Nf\big(\frac{1}{N}\mathbb{Z}^n \cap [0,1]^{n-1}\big)$. Ce dernier ensemble ayant $(N+1)^{n-1}$ points, on a le résultat. □

Proposition 3.1.12. *Soit B un sous-ensemble mesurable de $\mathbb{R}^n$. On suppose que le bord de B admet un $(n-1)$-paramétrage lipschitzien. Alors, quand t tend vers ∞, on a*

$$\big|tB \cap \mathbb{Z}^n\big| = t^n \mu(B) + O(t^{n-1}),$$

où μ est la mesure de Lebesgue usuelle sur $\mathbb{R}^n$.

Démonstration. Soit C le cube

$$C = \{(x_1, \dots, x_n), \forall i, 0 \leq x_i < 1\}.$$

Alors on a

$$\big|\{x \in \mathbb{Z}^n, x + C \subset tB\}\big| \leq \big|tB \cap \mathbb{Z}^n\big| \leq \big|\{x \in \mathbb{Z}^n, x + C \cap tB \neq 0\}\big|$$

et

$$\big|\{x \in \mathbb{Z}^n, x + C \subset tB\}\big| \leq t^n \mu(B) = \mu(tB) \leq \big|\{x \in \mathbb{Z}^n, x + C \cap tB \neq 0\}\big|.$$

Il faut donc montrer que l'ensemble

$$D(t) = \{x \in \mathbb{Z}^n, x + C \not\subset tB, x + C \cap tB \neq 0\}$$

est de cardinal $O(t^{n-1})$. Tout élément de $D(t)$ est à une distance au plus $\sqrt{n}$ du bord $\partial(tB)$ de tB. Il faut montrer que $\mu(\partial(tB) + B(0, \sqrt{n})) = O(t^{n-1})$. C'est une conséquence du lemme 3.1.11. □

Exemple 3.1.0.2. *Pour $K = \mathbb{Q}$, on a $r_1 = 1, r_2 = 0, h_{\mathbb{Q}} = 1, R_{\mathbb{Q}} = 1, w = 2, d_{\mathbb{Q}} = 1$, et le résidu de la fonction ζ en 1 est bien $\frac{2}{2} = 1$.*

La seule quantité que l'on n'a pas encore discuté en détail est le régulateur. Voici une formule.

Définition 3.1.13. *Un système fondamental d'unités dans $\mathcal{O}_K$ est la donnée d'éléments de $\mathcal{O}_K^*$ $(\varepsilon_i)_{1 \leq i \leq r_1 + r_2 - 1}$ dont l'image dans le quotient de $\mathcal{O}_K^*$ par son sous-groupe de torsion forme une base.*

Proposition 3.1.14. *Soit $(\varepsilon_i)_{1 \leq i \leq r_1 + r_2 - 1}$ un système fondamental d'unités dans $\mathcal{O}_K$. Le régulateur R_K est égal à la valeur absolue d'un mineur arbitraire de taille $(r_1 + r_2 - 1) \times (r_1 + r_2 - 1)$ de la matrice*

$$\begin{pmatrix} \log|\sigma_1(\varepsilon_1)| & \dots & \log|\sigma_1(\varepsilon_{r_1+r_2-1})| \\ \vdots & & \vdots \\ 2\log|\tau_{r_2}(\varepsilon_1)| & \dots & 2\log|\tau_{r_2}(\varepsilon_{r_1+r_2-1})| \end{pmatrix}$$

Démonstration. Par définition, le régulateur est égal à la valeur absolue du mineur de la matrice de taille $(r_1+r_2-1)\times(r_1+r_2-1)$ obtenue en enlevant la dernière ligne. Un calcul élémentaire nous montre qu'il s'agit de $\frac{1}{\sqrt{r_1+r_2}}$ fois le covolume de F (le quotient de $\mathcal{O}_K^*$ par son sous-groupe de torsion) dans l'hyperplan de $\mathbb{R}^{r_1+r_2-1}$ des éléments dont la somme des coordonnées est nulle. On en déduit le résultat d'indépendence souhaité. □

3.1.1 Corps quadratiques

On étudie brièvement les conséquences de la formule du nombre de classes pour les corps quadratiques. On recommande

`http://gaetan.chenevier.perso.math.cnrs.fr/MAT552/cours9.pdf`

pour des compléments.

On commence par calculer les invariants basiques des corps quadratiques. On traite séparément le cas imaginaire et le cas réel.

Soit d un entier différent de 0 et de 1, sans facteur carré. Soit $K = \mathbb{Q}[\sqrt{d}]$, et $\mathcal{O}_K$ son anneau des entiers. Calculons les invariants de K qui interviennent dans la formule du nombre de classes.

Proposition 3.1.15. *L'anneau des entiers de $K = \mathbb{Q}[\sqrt{d}]$ est*

(i) $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ *si d est congru à 2 ou 3 modulo 4 ;*

(ii) $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ *si d est congru à 1 modulo 4.*

Démonstration. Un élément $a+b\sqrt{d}$ de $\mathbb{Q}[\sqrt{d}]$, avec $a, b \in \mathbb{Q}$, est entier si et seulement si sa norme et sa trace sont dans $\mathbb{Z}$, i.e. si et seulement si $a^2 - db^2$ et $2a$ sont dans $\mathbb{Z}$. Supposons que ce soit le cas.

Si a est entier, alors db^2 est entier, et b est entier car d est sans facteur carré. Si a est de la forme $a'/2$, où a' est entier impair, alors $a^2 - db^2$ est entier si et seulement si $a'^2 - d(2b)^2$ est un entier divisible par 4, i.e. si et seulement si $d(2b)^2$ est un entier congru à 1 modulo 4. C'est le cas si et seulement si $2b$ est en entier impair et d est congru à 1 modulo 4. □

Remarque 3.1.16. *On a*

(i) $\mathcal{O}_K = \mathbb{Z}[X]/(X^2 - d)$ *si d est congru à 2 ou 3 modulo 4 ;*

(ii) $\mathcal{O}_K = \mathbb{Z}[X]/(X^2 - X + \frac{1-d}{2})$ *si d est congru à 1 modulo 4.*

Par ailleurs, on a toujours

$$\mathcal{O}_K[1/2] = \mathbb{Z}[1/2, X]/(X^2 - d).$$

Corollaire 3.1.17. *Le discriminant de K est*

(i) $4d$ *si* d *est congru à* 2 *ou* 3 *modulo* 4 *;*

(ii) d *si* d *est congru à* 1 *modulo* 4.

Démonstration. D'après le lemme 1.3.87, d_K est le carré du déterminant de la matrice

$$\begin{pmatrix} 1 & \omega \\ 1 & \overline{\omega} \end{pmatrix}$$

où $\omega = \sqrt{d}$ ou $\omega = \frac{1+\sqrt{d}}{2}$ suivant la classe de d modulo 4, i.e.

$$d_K = (\omega - \overline{\omega})^2,$$

ce qui prouve le résultat. □

Corps quadratiques réels. Supposons $d > 0$. Alors $r_1 = 2, r_2 = 0$. Comme par ailleurs les seules racines de l'unité réelles sont ± 1, le groupe des unités est le produit de $\{\pm 1\}$ par un groupe libre. On considère K comme inclus dans $\mathbb{R}$ par le plongement qui envoie $\sqrt{d}$ sur la racine positive de d.

Définition 3.1.18. *Supposons* $d > 0$. *Une unité fondamentale de* $K = \mathbb{Q}[\sqrt{d}]$ *est un élément* ε *de* $\mathcal{O}_K^*$ *tel que*

$$\mathcal{O}_K^* = \{\pm 1\} \times \varepsilon^{\mathbb{Z}}.$$

Il existe exactement 4 unités fondamentales dans $\mathcal{O}_K$, à savoir $\pm\varepsilon^{\pm 1}$. La définition du régulateur et la proposition 3.1.14 donnent le résultat suivant.

Proposition 3.1.19. *Soit* ε *une unité fondamentale de* K. *Alors le régulateur de* K *est*

$$R_K = |\log(|\varepsilon|)|.$$

La formule du nombre de classes s'exprime donc :

Proposition 3.1.20. *Soit* $K = \mathbb{Q}[\sqrt{d}]$, *avec* $d > 0$ *comme plus haut. Soit* ε *une unité fondamentale de* $\mathcal{O}_K$. *Alors le résidu de* ζ_K *en* 1 *est*

$$\frac{|\log(|\varepsilon|)|}{\sqrt{d}} h_K$$

si d *est congru à* 2 *ou* 3 *modulo* 4, *et*

$$\frac{2|\log(|\varepsilon|)|}{\sqrt{d}} h_K$$

sinon.

Corps quadratiques imaginaires. On étudie maintenant le corps $K = \mathbb{Q}[\sqrt{-d}]$, avec $d > 0$, sans facteur carré. Dans ce cas $r_1 = 0$ et $r_2 = 1$. En particulier, le groupe des unités est de torsion, et le régulateur vaut 1.

Proposition 3.1.21. *Le groupe des unités de $\mathcal{O}_K$ est*

(i) $\{\pm 1, \pm i\}$ *si* $K = \mathbb{Q}[i]$;

(ii) $\{\pm 1, \pm e^{2i\pi/3}\}$ *si* $K = \mathbb{Q}[e^{2i\pi/3}]$;

(iii) $\{\pm 1\}$ *si* $d \neq 1, 3$.

Démonstration. Seul le troisième énoncé demande une preuve. On pourrait invoquer l'irréductibilité des polynômes cyclotomiques pour montrer que les seules racines de l'unité de degré 2 sur $\mathbb{Q}$ sont i et $e^{2i\pi/3}$, mais le résultat est plus élémentaire. Le cas où $d = 2$ étant trivial, supposons $d \geq 5$. Un élément de $\mathcal{O}_K$ est toujours de la forme $x = a + b\sqrt{-d}$, où a et b sont entiers ou demi-entiers. La norme de x est $a^2 + db^2$. Si b est non nul, la norme de x vaut au moins $\frac{d}{4} > 1$, ce qui conclut. □

La formule du nombre de classes s'écrit donc :

Proposition 3.1.22. *Soit $K = \mathbb{Q}[\sqrt{-d}]$, avec $d > 0$, sans facteur carré. On suppose $d \neq 1, 3$. Alors le résidu de ζ_K en 1 est*

$$\frac{\pi}{2\sqrt{d}} h_K$$

si d est congru à 1 ou 2 modulo 4, et

$$\frac{\pi}{\sqrt{d}} h_K$$

sinon.

La forme particulièrement simple de la formule ci-dessus la rend propice aux applications. Pour cela, il faut savoir calculer autrement le résidu en 1 de ζ_K. On va utiliser l'expression de ζ_K comme produit eulerien. On a vu l'égalité

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}.$$

Soit p un nombre premier. Considérons les termes du produit eulerien correspondant aux idéaux $\mathfrak{p}$ divisant p. K étant de degré 2 sur $\mathbb{Q}$, on a trois décompositions possibles, suivant que $\mathfrak{p}$ est totalement décomposé, non-ramifié sans être totalement décomposé, ou totalement ramifié (on dit que p est inerte) :

(i) $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1 \neq \mathfrak{p}_2$;

(ii) $p\mathcal{O}_K = \mathfrak{p}$;

(iii) $p\mathcal{O}_K = \mathfrak{p}^2$.

Les degrés résiduels sont respectivement $1, 2$ et 1, donc la norme d'un idéal premier au-dessus de p est respectivement p, p^2 et p. Finalement, on voit que le produit

$$\prod_{\mathfrak{p}|p}(1 - N(\mathfrak{p})^{-s})^{-1}$$

vaut

(i) $(1 - p^{-s})^{-2}$ si p est totalement décomposé ;

(ii) $(1 - p^{-2s})^{-1} = (1 - p^{-s})^{-1}(1 + p^{-s})^{-1}$ si p est inerte ;

(iii) $(1 - p^{-s})^{-1}$ si p est ramifié.

On tire de ce calcul la proposition suivante.

Proposition 3.1.23. *Soit ϕ la fonction de l'ensemble des nombres premiers de $\mathbb{Z}$ vers $\{\pm 1\}$ qui à p associe*

(i) $\phi(p) = 1$ si p est totalement décomposé ;

(ii) $\phi(p) = -1$ si p est inerte ;

(iii) $\phi(p) = 0$ si p est ramifié.

Soit $L(s)$ le produit infini

$$L(s) = \prod_p (1 - \phi(p)p^{-s})^{-1}.$$

Alors $L(s)$ converge absolument pour $\Re s > 1$, et on a l'égalité dans cette bande

$$\zeta_K(s) = \zeta(s)L(s),$$

où $\zeta = \zeta_{\mathbb{Q}}$ est la fonction ζ de Riemann.

Démonstration. La convergence du produit qui définit L se prouve de manière identique à 3.1.2. Les produits convergeant absolument, on peut réordonner leurs termes de telle façon que les calculs précédents montrent l'égalité cherchée. □

La formule du nombre de classe appliquée à ζ et ζ_K nous montre que la fonction L admet comme limite en 1 le résidu de ζ_K en 1, qu'elle calcule. Pour que ce soit utile, il faut comprendre mieux L. C'est un fait très profond qu'on peut le faire simplement.

Proposition 3.1.24. *Soit D le discriminant de K. Il existe un caractère*

$$\chi : (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$$

tel que pour tout p premier non ramifié, on ait

$$\chi(p \bmod D) = \phi(p).$$

On a alors, pour tout s de partie réelle strictement supérieure à 1 :

$$L(s) = \sum_{n \geq 1} \chi(n) n^{-s},$$

où l'on a posé $\chi(n) = 0$ si n n'est pas premier à D.

Démonstration. Le même argument que celui qui permet d'exprimer la fonction ζ de Dedekind comme un produit eulerien montre que le premier énoncé implique le second – remarquant que les termes du produit qui définit L correspondant à des premiers ramifiés valent tous 1.

Pour simplifier l'argument, on suppose $d = \ell$, où ℓ est un nombre premier congru à 1 modulo 4. Alors $D = -4\ell$. Soit p un nombre premier distinct de 2 et de ℓ. Alors p est totalement décomposé dans K si et seulement si $-\ell$ est un carré modulo p – grâce à la remarque 3.1.16 – i.e. si et seulement si le symbole de Legendre

$$\left(\frac{-\ell}{p}\right)$$

vaut 1.

La loi de réciprocité quadratique s'écrit

$$\left(\frac{-\ell}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{\ell}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{\ell}\right)$$

car ℓ est congru à 1 modulo 4. Le caractère

$$(\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}, n \mapsto (-1)^{(n-1)/2}\left(\frac{n}{\ell}\right)$$

convient. □

Le caractère χ construit ci-dessus est le *caractère de Kronecker*. Voici une construction plus générale.

Définition 3.1.25. *Soit N un entier strictement positif, et soit $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}$ un caractère du groupe abélien $(\mathbb{Z}/N\mathbb{Z})^*$. La fonction L de Dirichlet associée à χ est la fonction d'une variable complexe*

$$L(s, \chi) = \sum_{n \geq 1} \chi(n) n^{-s},$$

où l'on a posé $\chi(n) = 0$ si n n'est pas premier à N.

Proposition 3.1.26. *Avec les notations précédentes, si χ n'est pas le caractère trivial, alors la série qui définit L converge absolument sur la bande $\Re s > 0$, et définit une fonction holomorphe.*

Démonstration. Le lemme 3.1.3 nous ramène à montrer

$$\sum_{1\leq n\leq r} \chi(n) = O(1),$$

ce qui suit de la formule

$$\sum_{1\leq n\leq N} \chi(n) = 0$$

et de la N-périodicité de χ. □

Nous avons finalement montré.

Théorème 3.1.27. *Soit D le discriminant de K, et $\chi : (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$ le caractère de Kronecker. Alors on a*

$$L(1,\chi) = \frac{\pi h_K}{\alpha\sqrt{d}},$$

où α vaut 1 si d est congru à 1 ou 2 modulo 4, et 2 sinon. En particulier on a $L(1,\chi) \neq 0$.

3.1.2 Extensions cyclotomiques

Soit $n > 1$ un entier, et soit ζ une racine primitive n-ième de l'unité. On va étudier le *corps cyclotomique* $\mathbb{Q}(\zeta)$. On rassemble ici quelques résultats basiques sur l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ en faisant le moins de calculs possibles.

Proposition 3.1.28. *L'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ est galoisienne de degré $d = \phi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^*\right|$. Les conjugués de ζ sont les ζ^r, $r \in (\mathbb{Z}/n\mathbb{Z})^*$.*

Soit G le groupe de Galois de $\mathbb{Q}(\zeta)/\mathbb{Q}$. Le morphisme qui a un élément σ de G associe l'élément r de $(\mathbb{Z}/n\mathbb{Z})^*$ tel que $\sigma(\zeta) = \zeta^r$ induit un isomorphisme

$$G \to (\mathbb{Z}/n\mathbb{Z})^*.$$

Démonstration. Soit Φ_n le n-ième polynôme cyclotomique, i.e. le produit des $(X-\zeta')$, où ζ' parcourt les racines primitives n-ièmes de l'unité. Il s'agit d'un polynôme unitaire à coefficients dans $\mathbb{Z}$, de degré $\phi(n)$. On sait par ailleurs qu'il s'agit d'un polynôme irréductible. Ses racines étant des puissances de ζ, on en déduit que $\mathbb{Q}(\zeta)/\mathbb{Q}$ est galoisienne de degré $\phi(n)$, et que les conjugués de ζ sont les racines de Φ_n, soit les ζ^r, $r \in (\mathbb{Z}/n\mathbb{Z})^*$.

Le morphisme $G \to (\mathbb{Z}/n\mathbb{Z})^*$ de la proposition est bien défini. Comme G agit transitivement sur les conjugués de ζ, il est surjectif, donc injectif pour des raisons de cardinalité. □

Remarque 3.1.29. *Soit K un corps de nombres arbitraires, et soit ζ une racine primitive n-i'me de l'unité. Il suit de la proposition que l'extension $K(\zeta)/K$ est galoisienne, de groupe de Galois un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$.*

Proposition 3.1.30. *Soit p un nombre premier impair. Alors p est ramifié dans $\mathbb{Q}(\zeta)$ si et seulement si p divise n. Le nombre premier 2 est ramifié dans $\mathbb{Q}(\zeta)$ si et seulement si 4 divise n.*

Démonstration. On commence par montrer que si p (pair ou impair) est premier à n, alors p n'est pas ramifié dans $\mathbb{Q}(\zeta)$. Soit $\mathcal{O}$ l'anneau des entiers de $\mathbb{Q}(\zeta)$. On a certainement $A := \mathbb{Z}[\zeta] \subset \mathcal{O}$. Le polynôme minimal de ζ est Φ_n, et comme n est premier à p, $\Phi_n'(\zeta)$ est premier à p. En effet, Φ_n divise $X^n - 1$, dont la dérivée vaut $n\zeta^{-1}$ en ζ. En particulier, la proposition 1.3.80 montre que le dualisant $\omega_{A_{(p)}/\mathbb{Z}_{(p)}}$ est égal à A. Par définition, on a $\mathcal{O} \subset \omega_{\mathcal{O}/\mathbb{Z}} \subset \omega_{A_{(p)}/\mathbb{Z}_{(p)}}$. On en déduit que le localisé de $\mathcal{O}$ en p est égal au localisé de A en p, et que $\mathcal{O}_{(p)} = \omega_{\mathcal{O}_{(p)}/\mathbb{Z}_{(p)}}$, ce qui signifie que p est non ramifié.

Si $n = 2m$, avec m impair, alors $-\zeta$ est une racine primitive m-ième de l'unité, et $\mathbb{Q}(\zeta) = \mathbb{Q}(-\zeta)$ donc 2 n'est pas ramifié dans $\mathbb{Q}(\zeta)$.

Supposons maintenant $n = p^\alpha, \alpha > 0$. Alors $\mathbb{Q}(\zeta)$ est non ramifié en dehors de p, donc le théorème de Minkowski montre que $\mathbb{Q}(\zeta)$ est ramifié en p si et seulement si $\mathbb{Q}(\zeta) \neq \mathbb{Q}$. C'est toujours le cas si p est impair, et si $p = 2$ c'est le cas si et seulement si $\alpha > 1$. On a donc montré le résultat dans le cas où n est une puissance d'un nombre premier.

Dans le cas général, si p^α divise n, alors $\mathbb{Q}(\zeta)$ contient $\mathbb{Q}(\zeta_{p^\alpha})$, où ζ_{p^α} est une racine primitive p^α-ième de l'unité, donc si p ramifie dans $\mathbb{Q}(\zeta_{p^\alpha})$, il ramifie dans $\mathbb{Q}(\zeta)$, ce qui conclut. □

Remarque 3.1.31. *On peut montrer sans trop de difficultés que $\mathcal{O} = \mathbb{Z}[\zeta]$. Remarquons que la première partie de la preuve s'applique plus généralement à des A tels que $\Omega^1_{A/\mathbb{Z}} = 0$, et vaut au-dessus d'une base arbitraire. En particulier, si $\zeta^n = 1$, et K est un corps de nombres arbitraire d'anneau d'entiers $\mathcal{O}$, alors $K(\zeta)$ est une extension de K non ramifiée en dehors de n, d'anneau des entiers égal à $\mathcal{O}[\zeta]$ en dehors de n.*

Si de plus n est premier au discriminant de K, alors puisque tout premier de $\mathbb{Z}$ divisant n est ramifié dans $K(\zeta)$, et non ramifié dans K, on trouve que les premiers de K qui ramifient dans $K(\zeta)$ sont exactement ceux qui divisent n. Dans ce cas, le théorème de Minkowski garantit que $K \cap \mathbb{Q}(\zeta)$ est trivial, de sorte que le groupe de Galois de $K(\zeta)/K$ est $(\mathbb{Z}/n\mathbb{Z})^*$.

Remarque 3.1.32. *Appliquer le théorème de Minkowski ici est bien entendu bien trop compliqué pour un résultat si élémentaire, mais cela nous permet de ne faire aucun calcul.*

Soit L/K une extension finie galoisienne de corps de nombres, de groupe de Galois G. Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$, $\mathfrak{P}$ un diviseur premier de $\mathfrak{p}$. Soit $D_\mathfrak{P} \subset G$ le groupe de décomposition de $\mathfrak{P}$, i.e., le sous-groupe de G constitué des éléments

laissant $\mathfrak{P}$ globalement invariant. Rappelons que la proposition 1.3.62 nous fournit une suite exacte

$$1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \to Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) \to 0,$$

où par définition $I_{\mathfrak{P}}$ est le groupe d'inertie de $\mathfrak{P}$ sur K. L'idéal $\mathfrak{P}$ est non ramifié si et seulement si $I_{\mathfrak{P}}$ est trivial.

Le corps résiduel de $\mathfrak{p}$ est fini. Soit q son cardinal. L'automorphisme de Frobenius

$$\kappa(\mathfrak{P}) \to \kappa(\mathfrak{P}), x \mapsto x^q$$

est un élément distingué de $Gal(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. Soit $\sigma_{\mathfrak{P}}$ une image inverse du Frobenius dans le groupe $D_{\mathfrak{P}}$. Alors $\sigma_{\mathfrak{P}}$ est bien défini à l'inertie près – en particulier, $\sigma_{\mathfrak{P}}$ est bien défini si $\mathfrak{P}$ est non-ramifié. On dit que $\sigma_{\mathfrak{P}}$ est le *Frobenius en* $\mathfrak{P}$.

Deux idéaux premiers $\mathfrak{P}$ et $\mathfrak{P}'$ au-dessus de $\mathfrak{p}$ sont conjugués par un élément de G. En particulier, $\sigma_{\mathfrak{P}}$ et $\sigma_{\mathfrak{P}'}$ sont conjugués. On peut donc parler du *Frobenius en* $\mathfrak{p}$: c'est une classe de conjugaison dans G. Si G est abélien, on dispose donc d'un élément de Frobenius distingué $\sigma_{\mathfrak{p}} \in G$.

Proposition 3.1.33. *Supposons que n est impair ou divisible par 4. Soit K un corps de nombres, et soit $K(\zeta)$ une extension finie de K, avec ζ une racine primitive n-ième de l'unité. Soit $G \subset (\mathbb{Z}/n\mathbb{Z})^*$ le groupe de Galois de $K(\zeta)/K$.*

Soit $\mathfrak{p}$ un idéal premier non-nul de K, premier à n. Soit $\mathfrak{P}$ un idéal premier de $K(\zeta)$ qui divise $\mathfrak{p}$. Alors la classe de $N_{K/\mathbb{Q}}(\mathfrak{p})$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ appartient à G. C'est le Frobenius en $\mathfrak{p}$.

Remarquons que la proposition précédente nous assure que $\mathfrak{p}$ est non ramifié.

Démonstration. Commençons par supposer que K est le corps $\mathbb{Q}$ des nombres rationnels. On a vu dans la preuve de la proposition précédente que localement en $\mathfrak{p}$, l'anneau des entiers $\mathcal{O}_{\mathbb{Q}(\zeta)}$ de $\mathbb{Q}(\zeta)$ est $\mathbb{Z}[\zeta]$. En particulier, l'extension résiduelle en $\mathfrak{P}$ est engendrée par la réduction de ζ modulo $\mathfrak{P}$.

Soit σ l'élément de G qui envoie ζ sur ζ^p. Le paragraphe précédent montre que σ agit sur l'extension résiduelle en $\mathfrak{P}$ par le Frobenius, ce qui prouve le résultat.

Soit p^f le cardinal du corps résiduel de $\mathfrak{p}$. Alors $N_{K/\mathbb{Q}}(\mathfrak{p}) = (p^f)$. On a vu dans la preuve de la proposition précédente que localement en $\mathfrak{p}$, l'anneau des entiers $\mathcal{O}_{K(\zeta)}$ de $K(\zeta)$ est $\mathcal{O}_K[\zeta]$. En particulier, l'extension résiduelle en $\mathfrak{P}$ est engendrée par la réduction de ζ modulo $\mathfrak{P}$.

Soit σ un élément de G, et soit r l'entier, uniquement déterminé modulo n, tel que $\sigma(\zeta) = \zeta^r$. Supposons que σ stabilise $\mathfrak{P}$ et agisse sur l'extension résiduelle en $\mathfrak{P}$ par le Frobenius $x \mapsto x^{p^f}$, i.e., que σ est l'élément de Frobenius en $\mathfrak{p}$. Alors $\zeta^r - \zeta^{p^f} \in \mathfrak{P}$, ce qui signifie

$$\zeta^{p^f - r} - 1 \in \mathfrak{P}.$$

Le lemme ci-dessous garantit que n divise $p^f - r$, ce qui prouve le résultat. □

Lemme 3.1.34. *Avec les notations précédentes, l'image de ζ dans le corps résiduel $\kappa(\mathfrak{P})$ est une racine primitive n-ième de l'unité.*

Démonstration. Les racines primitives n-ièmes de l'unité dans un corps arbitraire F dans lequel n est inversible sont exactement les racines du polynôme cyclotomique $\Phi_n \in \mathbb{Z}[X]$, ce qui prouve le résultat. □

Voici ce que signifient ces résultats pour les fonctions L (d'Artin) des corps cyclotomiques.

Définition 3.1.35. *Soit K un corps de nombres, et soit L une extension galoisienne de K. Soit n un entier divisible par le discriminant de L/K, et soit G le groupe de Galois de L/K. Soit $\chi : G \to \mathbb{C}^*$ un caractère de G. La* fonction L d'Artin *associée à χ est la fonction*

$$L^{(n)}(K(\zeta)/K, \chi, s) = \prod_{\mathfrak{p} \wedge (n)=1} \left(1 - \chi(\sigma_\mathfrak{p}) N(\mathfrak{p})^{-s}\right)^{-1},$$

où $N = N_{K/\mathbb{Q}}$ et $\mathfrak{p}$ parcourt les idéaux premiers de $\mathcal{O}_K$ premiers à n.

Proposition 3.1.36. *Avec les notations précédentes, le produit qui définit $L^{(n)}(K(\zeta)/K, \chi, s)$ converge absolument si $\Re s > 1$.*

Démonstration. C'est exactement le même argument que pour la fonction ζ de Dedekind, en remarquant que $\chi(\sigma_\mathfrak{p})$ a module 1. □

Exemple 3.1.2.1. *Supposons que $L = K(\zeta)$, où ζ est une racine primitive n-ième de l'unité. Alors*

$$L^{(n)}(K(\zeta)/K, \chi, s) = \prod_{\mathfrak{p} \wedge (n)=1} \left(1 - \chi(N(\mathfrak{p})) N(\mathfrak{p})^{-s}\right)^{-1}.$$

Exemple 3.1.2.2. *Si $\chi = 1$, alors*

$$L^{(n)}(L/K, 1, s) = \prod_{\mathfrak{p} \wedge (n)=1} \left(1 - N(\mathfrak{p})^{-s}\right)^{-1} = \zeta_K(s) \prod_{\mathfrak{p} | (n)} \left(1 - N(\mathfrak{p})^{-s}\right).$$

En particulier, $L^{(n)}(L/K, 1)$ est définie sur le même domaine, a les mêmes zéros et les mêmes pôles que ζ_K.

Proposition 3.1.37. *Supposons G abélien. On a, pour $\Re s > 1$,*

$$\prod_{\chi : G \to \mathbb{C}^*} L^{(n)}(L/K, 1, s) = \zeta_L(s) \prod_{\mathfrak{P} | (n)} \left(1 - N(\mathfrak{P})^{-s}\right)$$

où dans le membre de droite $\mathfrak{P}$ parcourt les idéaux premiers de $\mathcal{O}_L$ qui divisent n.

Démonstration. On regroupe le produit de gauche suivant $\mathfrak{P} \cap \mathcal{O}_K$. Soit donc $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$, premier à (n). Dans le membre de gauche apparaît

$$\prod_{\chi: G \to \mathbb{C}^*} \left(1 - \chi(\sigma_\mathfrak{p}) N(\mathfrak{p})^{-s}\right)^{-1}.$$

On voudrait montrer que ce produit vaut

$$\prod_{\mathfrak{P}|\mathfrak{p}} \left(1 - N(\mathfrak{P})^{-s}\right)^{-1}.$$

Soit d le degré de l'extension $K(\zeta)/K$. Alors G est abélien d'ordre d. Soit f le degré de L/K en $\mathfrak{p}$, g le nombre d'idéaux premiers de L au-dessus de p. Alors $fg = d$. On a de plus

$$N(\mathfrak{P}) = N(\mathfrak{p})^f$$

pour tout $\mathfrak{P}$ au-dessus de $\mathfrak{p}$, de sorte que l'on veut montrer l'égalité

$$\prod_{\chi: G \to \mathbb{C}^*} \left(1 - \chi(\sigma_\mathfrak{p}) N(\mathfrak{p})^{-s}\right) = \left(1 - N(\mathfrak{p})^{-fs}\right)^g.$$

L'ordre de $\sigma_\mathfrak{p}$ dans G est le degré des extensions résiduelles en $\mathfrak{p}$: c'est f. Soit H le sous-groupe de G engendré par $\sigma_\mathfrak{p}$. Alors H est d'ordre f et on a

$$\prod_{\chi: G \to \mathbb{C}^*} \left(1 - \chi(\sigma_\mathfrak{p}) N(\mathfrak{p})^{-s}\right) = \prod_{\psi: H \to \mathbb{C}^*} \left(1 - \psi(\sigma_\mathfrak{p}) N(\mathfrak{p})^{-s}\right)^{|G/H|} = \prod_{\psi: H \to \mathbb{C}^*} \left(1 - \psi(\sigma_\mathfrak{p}) N(\mathfrak{p})^{-s}\right)^g$$

car $fg = |G|$. On veut donc montrer

$$\prod_{\psi: H \to \mathbb{C}^*} \left(1 - \psi(\sigma_\mathfrak{p}) N(\mathfrak{p})^{-s}\right) = 1 - N(\mathfrak{p})^{-fs}.$$

C'est clair en développant le membre de gauche – noter que H est cyclique d'ordre f, engendré par $\sigma_\mathfrak{p}$. □

Théorème 3.1.38. *Soit K un corps de nombres, et soit $K(\zeta)$ une extension finie de K, avec ζ une racine primitive N-ième de l'unité. Soit $G \subset (\mathbb{Z}/N\mathbb{Z})^*$ le groupe de Galois de $K(\zeta)/K$, et soit*

$$\chi : G \to \mathbb{C}^*$$

un caractère de G. Alors la fonction L d'Artin $L(K(\zeta)/K, \chi, s)$ vérifie

$$L^{(N)}(K(\zeta)/K, \chi, s) = \sum_{I \subset \mathcal{O}_K, I \wedge (N) = 1} \chi(N(I)) N(I)^{-s}.$$

Si $\chi \neq 1$, la somme ci-dessus converge pour $\Re s > 1 - \frac{1}{[K:\mathbb{Q}]}$, et l'on a

$$L(K(\zeta)/K, \chi, 1) \neq 0.$$

Remarque 3.1.39. *Ce théorème est important, et son énoncé est typique de résultats plus généraux. Il identifie des objets galoisiens (fonctions L d'Artin définies par leur produit eulerien) et plus analytiques (analogues de fonctions L de Dirichlet, contrôlées par le discriminant de l'extension en question). Cette correspondance fournit, en général comme ici, des informations analytiques sur les fonctions L d'Artin.*

Démonstration. La proposition 3.1.33, jointe au développement habituel du produit eulerien, montre l'égalité

$$L^{(N)}(K(\zeta)/K, \chi, s) = \sum_{I \subset \mathcal{O}_K, I \wedge (N)=1} \chi(N(I))N(I)^{-s}.$$

Supposons démontré que la somme converge pour tout $\chi \neq 1$ et $\Re s > 1 - \frac{1}{[K:\mathbb{Q}]}$. La proposition 3.1.37 montre que l'on a, à multiplication par une fonction entière inversible près,

$$\zeta_{K(\zeta)}(s) = \zeta_K(s) \prod_{\chi \neq 1} L(K(\zeta)/K, \chi, s).$$

Les fonctions $\zeta_{K(\zeta)}$ et ζ_K ont toutes les deux un pôle simple, en $s = 1$, et nous supposons que les fonctions $L(K(\zeta)/K, \chi)$ n'ont pas de pôle en 1. Elles ne peuvent donc pas s'annuler en 1.

Il reste à montrer l'énoncé de convergence. D'après le lemme 3.1.3, il faut montrer l'estimée

$$\sum_{n=1}^{r} \chi(n)a_n = O(r^{1-1/[K:\mathbb{Q}]}),$$

où a_n est le nombre d'idéaux de $\mathcal{O}_K$ de norme n. On voudrait donc estimer la somme des a_n, où n parcourt les entiers $\leq r$ dans une classe donnée modulo N, i.e. l'ensemble des idéaux dont la norme vaut au plus r et est congru à un entier donné modulo N. On va traiter ce problème en remplaçant ce problème par la question de compter des idéaux de classe donnée, en un certain sens.

Soit F_N le groupe multiplicatif des idéaux fractionnaires de K premiers à N, et soit P_N le groupe des idéaux fractionnaires de la forme $x\mathcal{O}_K$, où x est un élément de K congru à 1 modulo N. Soit G_N le groupe quotient F_N/P_N. On ne sait pas a priori que G_N est fini – il se comporte cependant comme un groupe de classes d'idéaux.

On dispose d'un morphisme naturel $G_N \to G \subset (\mathbb{Z}/N\mathbb{Z})^*$ qui à un idéal fractionnaire I dans F_N associe la classe de $N(I)$ modulo N. L'expression

$$L(K(\zeta)/K, \chi, s) = \sum_{I \subset \mathcal{O}_K, I \wedge (N)=1} \chi(N(I))N(I)^{-s}$$

(ou son produit eulerien) montre que la fonction $L(K(\zeta)/K, \chi, s)$ ne dépend que du caractère composé $G_N \to G \to \mathbb{C}^*$.

Soit h un élément de G_N. Les estimées de la formule analytique du nombre de classes montrent, mutantis mutandis, que le nombre d'idéaux dans P_N de classe h et de norme au plus r est

$$Cr + O(r^{1-1/[K:\mathbb{Q}]}),$$

où la constante strictement positive C est indépendante de h. Notons que l'on tire de ce fait la finitude de G_N, puisque le nombre d'idéaux dans P_N de norme au plus r est lui aussi en $O(r)$.

On peut enfin écrire

$$\sum_{n=1}^{r} \chi(n)a_n = \sum_{i\in(\mathbb{Z}/N\mathbb{Z})^*} \chi(i) \sum_{n\leq r,[n]=i} a_n = O(r^{1-1/[K:\mathbb{Q}]})$$

car la somme des $\chi(i)$ est nulle, et que $\sum_{n\leq r,[n]=i} a_n$ est somme d'un nombre fini, indépendant de i, de termes de la forme $Cr + O(r^{1-1/[K:\mathbb{Q}]})$. □

Voici un fait d'intérêt indépendant.

Proposition 3.1.40. *Le morphisme $G_N \to G$ est surjectif.*

Démonstration. Soit r l'indice de l'image de G_N dans G. La fonction

$$\prod_{\chi} L^{(N)}(K(\zeta)/K, \chi, s)$$

est une puissance r-ième. Son ordre d'annulation en 1, et donc celui de

$$\prod_{\chi} L(K(\zeta)/K, \chi, s) = \zeta_{K(\zeta)},$$

est divisible par r. On a donc $r = 1$. □

Nous allons utiliser le théorème précédent dans la section suivante. Donnons cependant une application de sa partie facile à la loi de réciprocité quadratique.

Soit p un nombre premier impair, et soit ζ une racine primitive p-ième de l'unité. Soit $K = \mathbb{Q}(\zeta)$. Le groupe de Galois G de $K/\mathbb{Q}$ est $(\mathbb{Z}/p\mathbb{Z})^*$, qui est cyclique d'ordre $p-1$. Il a en particulier un unique sous-groupe H d'indice 2. Soit L le corps fixé par H. Alors L est une extension quadratique de $\mathbb{Q}$. Comme K est ramifié uniquement en p, il en va de même de L. Le corollaire 3.1.17 montre que $L = \sqrt{p^*}$, avec $p^* = (-1)^{(p-1)/2}p$.

Soit χ l'unique caractère non trivial de $G/H = Gal(L/\mathbb{Q})$. Alors, clairement,

$$L(L/\mathbb{Q}, \chi, s) = L(K/\mathbb{Q}, \chi, s)$$

et le théorème précédent nous fournit un caractère χ' de $(\mathbb{Z}/p\mathbb{Z})^*$ tel que

$$L(L/\mathbb{Q}, \chi, s) = \sum_{n\wedge p=1} \chi'(n)n^{-s}.$$

L'argument de la proposition 3.1.24 nous permet d'en déduire la loi de réciprocité quadratique pour les premiers impairs.

3.1.3 Le théorème de la progression arithmétique de Dirichlet, et le théorème de Cebotarev

Dans cette section, nous appliquons le théorème 3.1.38 à des questions concrètes, qui s'articulent autour du théorème de la progression arithmétique de Dirichlet et de ses variantes.

Définition 3.1.41. *Soit K un corps de nombres, et soit S un ensemble d'idéaux premiers de $\mathcal{O}_K$. On dit que la densité analytique de S est (resp. supérieure ou égale à) ρ si*

$$\lim_{s\to 1} \frac{\sum_{\mathfrak{p}\in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}} = \rho$$

(resp.

$$\liminf_{s\to 1} \frac{\sum_{\mathfrak{p}\in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}} \geq \rho.)$$

Les calculs de la proposition 3.1.2 montrent que le dénominateur de la fraction ci-dessus est équivalent à $\log \zeta_K(s) \sim \log(s-1)$. C'est indépendant de K.

Théorème 3.1.42 (Dirichlet)**.** *Soit N un entier strictement positif. Soit a un élément de $(\mathbb{Z}/N\mathbb{Z})^*$. L'ensemble des nombres premiers qui sont congrus à a modulo N a pour densité analytique $\frac{1}{\phi(N)}$. En particulier, il est infini.*

Démonstration. C'est la proposition 3.1.33 qui est le point de départ de la preuve. Soit donc ζ une racine primitive N-ième de l'unité, et soit K le corps cyclotomique $\mathbb{Q}(\zeta)$. Le groupe de Galois de l'extension $K/\mathbb{Q}$ est $G = (\mathbb{Z}/N\mathbb{Z})^*$. Si χ est un caractère de G, on a vu que

$$L^{nr}(K/\mathbb{Q}, \chi, s) = \prod_p (1 - \chi(p)p^{-s})^{-1}.$$

Prenant le logarithme, et puisque les premiers ramifiés ne contribuent que pour des termes bornés, on trouve, au voisinage de 1,

$$\log L(K/\mathbb{Q}, \chi, s) = \sum_p \chi(p)p^{-s} + O(1).$$

Le théorème 3.1.38 garantit que cette quantité tend vers une limite finie quand s tend vers 1, sauf si $\chi = 1$, auquel cas elle est équivalente à $-\log(s-1)$. Pour exploiter cela, exprimons la fonction indicatrice des p congrus à a modulo n à l'aide des χ – c'est possible a priori car les caractères de G forment une base de l'espace des fonctions $G \to \mathbb{C}$. Les relations d'orthogonalité des caractères impliquent que si n est premier à n, alors $\sum_\chi \chi(n)$ est nul si et seulement si n est congru à 1 modulo N, et vaut $\phi(N)$ sinon. Ainsi, la somme $\sum_\chi \chi(a^{-1})\chi(n)$ est nulle si et seulement si n est congru à a modulo N, et vaut $\phi(N)$ sinon.

On trouve finalement :

$$\sum_{\chi} \chi(a^{-1}) \log L(K/\mathbb{Q}, \chi, s) = \phi(N) \sum_{p=a[N]} p^{-s} + O(1).$$

Par ailleurs, le terme de gauche est équivalent à $-\log(s-1)$ au voisinage de 1, ce qui conclut. □

On vient d'utiliser le théorème 3.1.38 pour les extensions cyclotomiques de $\mathbb{Q}$. Si on l'applique à des extensions de corps de nombres arbitraires, on trouve l'énoncé suivant – on en donnera une version bien plus générale plus loin.

Proposition 3.1.43. *Soit K un corps de nombres, et soit N un entier positif premier au discriminant de K. Soit a un élément de $(\mathbb{Z}/N\mathbb{Z})^*$. L'ensemble des idéaux premiers non nuls de $\mathcal{O}_K$ dont la norme est congrue à a modulo N a pour densité analytique $\frac{1}{\phi(N)}$. En particulier, il est infini.*

Démonstration. La preuve est exactement la même que la précédente. □

Soit maintenant L/K une extension finie galoisienne de corps de nombres, et soit G son groupe de Galois. Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. On notera parfois $\sigma_{\mathfrak{p}}^G$ pour l'élément de Frobenius en $\mathfrak{p}$ quand on voudra insister sur le groupe G, bien défini à conjugaison près.

Théorème 3.1.44 (Cebotarev)**.** *Soit L/K une extension finie galoisienne de corps de nombres, de groupe de Galois G. Soit C une classe de conjugaison dans G. L'ensemble des idéaux premiers $\mathfrak{p}$ non ramifiés de $\mathcal{O}_K$ tels que $\sigma_{\mathfrak{p}}$ a C pour classe de conjugaison a pour densité analytique $\frac{|C|}{|G|}$.*

Avant de donner la preuve, on donne quelques lemmes. Dans la situation précédente, notons $d^-(L/K, C)$ la quantité

$$d^-(L/K, C) = \liminf_{s \to 1} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}},$$

où S est l'ensemble des $\mathfrak{p}$ tels que $\sigma_{\mathfrak{p}}$ a C pour classe de conjugaison. En général, si S est un ensemble de premiers de $\mathcal{O}_K$, on notera

$$d^-(S) = \liminf_{s \to 1} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}}.$$

Lemme 3.1.45. *Soit K un corps de nombres. La densité analytique des premiers $\mathfrak{p}$ de $\mathcal{O}_K$ tels que $f(\mathfrak{p}/(\mathfrak{p} \cap \mathbb{Z})) > 1$ est nulle. Si L/K est une extension finie de corps de nombres, la densité analytique des premiers $\mathfrak{P}$ de $\mathcal{O}_L$ tels que $f(\mathfrak{P}/(\mathfrak{P} \cap \mathcal{O}_K)) > 1$ est nulle.*

Démonstration. Le second point est une conséquence du premier car

$$f(\mathfrak{P}/(\mathfrak{P}\cap\mathbb{Z})) \geq f(\mathfrak{P}/(\mathfrak{P}\cap\mathcal{O}_K)).$$

Soit S l'ensemble des premiers $\mathfrak{p}$ de $\mathcal{O}_K$ tels que $f(\mathfrak{p}/(\mathfrak{p}\cap\mathbb{Z}))>1$. Si $\mathfrak{p}\in S$, et si p est le nombre premier tel que $\mathfrak{p}\cap\mathbb{Z}=(p)$, alors $N(\mathfrak{p})\geq p^2$ car $\kappa(\mathfrak{p})$ est une extension de $\mathbb{Z}/p\mathbb{Z}$ de degré au moins 2. Par ailleurs, étant donné un nombre premier p, le nombre de diviseurs premiers de p dans $\mathcal{O}_K$ est au plus $d:=[K:\mathbb{Q}]$. On a donc, pour $s>1$,

$$\frac{\sum_{\mathfrak{p}\in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}} \leq d\frac{\sum_p p^{-2s}}{\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}} \leq d\frac{\sum_p p^{-2}}{\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}},$$

qui tend vers 0 quand s tend vers 1. □

Lemme 3.1.46. *Soit L/K une extension finie galoisienne de corps de nombres, de groupe de Galois G. Soit σ un élément de G, et soit H le sous-groupe de G engendré par σ. Soit $M=L^H$ le sous-corps de L fixé par H. Soit C la classe de conjugaison de σ dans G.*

Alors

$$\frac{|G|}{|C|}d^-(L/K,C) \geq |H|\, d^-(L/M,\{\sigma\}).$$

Remarque 3.1.47. *A posteriori, les deux membres de l'inégalité valent* 1.

Démonstration. On va compter. Soit S l'ensemble des premiers $\mathfrak{q}$ de $\mathcal{O}_M$, non ramifiés dans $\mathcal{O}_L$ tels que $\sigma_{\mathfrak{q}}^H=\sigma$. Soit S' l'ensemble des $\mathfrak{q}\in S$ tels que $f(\mathfrak{q}/(\mathfrak{q}\cap\mathcal{O}_K))=1$. Le lemme précédent montre l'égalité

$$d^-(L/M,\{\sigma\}) = d^-(M,S) = d^-(M,S').$$

Soit $\mathfrak{q}\in S'$, $\mathfrak{p}=\mathfrak{q}\cap\mathcal{O}_K$. Comme l'extension résiduelle $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ est triviale par définition de S', on a $\sigma_{\mathfrak{p}}^G=\sigma_{\mathfrak{q}}^H$ et $N(\mathfrak{p})=N(\mathfrak{q})$. Soit T l'ensemble des premiers de $\mathcal{O}_K$ de la forme $\mathfrak{q}\cap\mathcal{O}_K$, $\mathfrak{q}\in S'$. On en déduit

$$d^-(L/K,C)\geq d^-(T).$$

Comptons les éléments de S' en les regroupant suivant leur intersection avec $\mathcal{O}_K$, qui est dans T. Comme l'extension M/K n'est pas galoisienne en général, on ne peut pas directement prouver que deux tels éléments sont conjugués par un groupe de Galois.

Néanmoins, si $\mathfrak{q}\in S'$, alors $\mathfrak{q}\mathcal{O}_L$ est premier : en effet, soit $\mathfrak{P}$ dans $\mathcal{O}_L$ au-dessus de $\mathfrak{q}$. Alors $\sigma_{\mathfrak{p}}^H=\sigma$, qui engendre le groupe cyclique H, donc l'extension résiduelle $\kappa(\mathfrak{P})/\kappa(\mathfrak{q})$ est d'ordre $|H|$, et $\mathfrak{P}$ est l'unique idéal de $\mathcal{O}_L$ au-dessus de $\mathfrak{q}$ par la proposition 1.3.57.

Il suit de cette remarque que si $\mathfrak{q}$ et $\mathfrak{q}'$ sont deux éléments de S' tels que $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{q}' \cap \mathcal{O}_K$, alors il existe $\tau \in G$ tel que $\tau(\mathfrak{q}\mathcal{O}_L) = \mathfrak{q}'\mathcal{O}_L$. La réciproque est clairement vraie elle aussi. Bien entendu, on a $\tau(\mathfrak{q}\mathcal{O}_L) = \tau(\mathfrak{q})\mathcal{O}_L$.

Soit maintenant $\mathfrak{q}$ dans S' et $\tau \in G$. A priori, $\tau(\mathfrak{q}\mathcal{O}_L)$ n'est pas de la forme $\mathfrak{q}'\mathcal{O}_L$. Analysons la situation. Bien sûr, $\tau(\mathfrak{q})$ est un idéal de $\tau(\mathcal{O}_M) = (\mathcal{O}_L)^{\tau H \tau^{-1}}$. L'extension $L/L^{\tau H \tau^{-1}}$ a pour groupe de Galois $\tau H \tau^{-1}$ et l'on a

$$\sigma_{\tau(\mathfrak{q})}^{\tau H \tau^{-1}} = \tau \sigma \tau^{-1}$$

donc

$$\sigma_{\tau(\mathfrak{q})\mathcal{O}_L}^{G} = \tau \sigma \tau^{-1}.$$

Si τ commute à σ, alors $\tau(\mathfrak{q})$ est un idéal $\mathfrak{q}'$ de $\mathcal{O}_M$, qui est dans S'. Réciproquement, si $\mathfrak{q}'$ est dans S' avec $\mathfrak{q}'\mathcal{O}_L = \tau(\mathfrak{q})\mathcal{O}_L$, alors

$$\sigma_{\tau(\mathfrak{q})\mathcal{O}_L}^{G} = \sigma_{\mathfrak{q}'\mathcal{O}_L}^{G} = \sigma_{\tau}^{H}(\mathfrak{q}') = \sigma.$$

On déduit de cela que l'ensemble des $\mathfrak{q}' \in S'$ tels que $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{q}' \cap \mathcal{O}_K$ est exactement l'ensemble des $\tau(\mathfrak{q})$, où τ appartient au centralisateur $Z(\sigma)$ de σ.

Soit $\tau \in G$, commutant à σ, tel que $\tau(\mathfrak{q}) = \mathfrak{q}$. Alors $\tau(\mathfrak{q})\mathcal{O}_L = \mathfrak{q}\mathcal{O}_L$: τ appartient au groupe de décomposition de $\mathfrak{q}\mathcal{O}_L$, qui est H par construction.

Enfin, si $\mathfrak{q} \in S'$, alors $N(\mathfrak{q}) = N(\mathfrak{q} \cap \mathcal{O}_K)$ (l'extension résiduelle correspondante à degré 1 par hypothèse). Il suit de ces considérations que l'on a

$$\sum_{\mathfrak{q} \in S'} N(\mathfrak{q})^{-s} = \frac{|Z(\sigma)|}{|H|} \sum_{\mathfrak{p} \in T} N(\mathfrak{p})^{-s} = \frac{|G|}{|H|\,|C|} \sum_{\mathfrak{p} \in T} N(\mathfrak{p})^{-s},$$

ce qui conclut après division par $\log(s-1)$. □

Remarque 3.1.48. *On peut montrer a priori que l'on a en fait égalité dans l'énoncé du lemme.*

On laisse le lemme suivant au lecteur. Il suit formellement de ce qui précède.

Lemme 3.1.49. *Pour prouver le théorème de Cebotarev, il suffit de traiter le cas où G est abélien (et même cyclique).*

Démonstration du Théorème 3.1.44. Si L/K est une extension cyclotomique obtenue par adjonction d'une racine de l'unité d'ordre premier au discriminant de K, le théorème est une conséquence de la proposition 3.1.43 et de la proposition 3.1.33.

Supposons maintenant que L/K est une extension abélienne arbitraire. Dans ce cas, les $\sigma_{\mathfrak{p}}$ sont bien définis comme éléments de G, et $C = \{\sigma\}$ est réduite à un élément de G. Soit d l'ordre de σ.

On va introduire des extensions cyclotomiques auxiliaires. Soit p un nombre premier, et soit ζ une racine primitive p-ième de l'unité. Si p est suffisamment grand, ce que l'on suppose, alors le groupe de Galois de $K(\zeta)/K$ est $G_p = (\mathbb{Z}/p\mathbb{Z})^*$ – car p est premier au discriminant de K – et $L \cap K(\zeta) = K$. Pour cette dernière égalité, remarquons que $L \cap \mathbb{Q}(\zeta) = \mathbb{Q}$ pour des raisons de ramification, donc $L(\zeta)$ est une extension de L de degré $p-1$. Par ailleurs, on a

$$p-1 = [L(\zeta) : L] = [K(\zeta) : L \cap K(\zeta)] \leq [K(\zeta) : K] \leq p-1.$$

On a donc l'égalité $[K(\zeta) : L \cap K(\zeta)] \leq [K(\zeta) : K]$, soit $L \cap K(\zeta) = K$.

Notons $\sigma_{\mathfrak{p}}^G$ pour le Frobenius associé à $\mathfrak{p}$ dans G. Le groupe de Galois de $L(\zeta)/K$ est canoniquement isomorphe à $G \times G_p$. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$, non ramifié dans $L(\zeta)$. Si

$$\sigma_{\mathfrak{p}}^{G \times G_p} = (\sigma, \tau),$$

alors $\sigma_{\mathfrak{p}}^G = \sigma$. Fixons $\rho = (\sigma, \tau) \in G \times G_p$, et soit $M = L(\zeta)^\rho$ le sous-corps de $L(\zeta)$ fixé par ρ. Si d divise l'ordre de τ, alors on a

$$< \rho > \cap (G \times \{1\}) = \{1\}.$$

Dans ce cas, si $\phi \in G \times G_p$ agit trivialement sur $M(\zeta)$, alors ϕ fixe M, donc $\phi \in < \rho >$, et ϕ fixe $K(\zeta)$, donc $\phi \in G \times \{1\}$, ce qui montre que ϕ est trivial, d'où $M(\zeta) = L(\zeta)$: l'extension $L(\zeta)/M$ est une extension cyclotomique.

Le lemme de fonctorialité 3.1.46 et le cas des extensions cyclotomiques nous montre que la densité des $\mathfrak{p}$ dans $\mathcal{O}_K$ tels que $\sigma_{\mathfrak{p}}^G = \sigma$ est au moins égale à $\frac{N_{d,p}}{(p-1)|G|}$, où $N_{d,p}$ est le cardinal de l'ensemble des éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ dont l'ordre est divisible par d. On a bien entendu $0 \leq N_{d,p} \leq p-1$.

Soit $\varepsilon > 0$, et soit k un entier suffisamment grand. Le théorème de la progression arithmétique de Dirichlet nous permet de choisir p congru à 1 modulo d^k, où d est toujours l'ordre de σ. Alors $p-1 = rd^k$ et $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/rd^k\mathbb{Z}$ pour un certain $r \geq 1$.

Considérons la surjection naturelle

$$\phi : \mathbb{Z}/(rd^k)\mathbb{Z} \longrightarrow \mathbb{Z}/d^k\mathbb{Z}.$$

Si d divise l'ordre de $\phi(x)$, alors d divise l'ordre de x, donc

$$N_{d,p} \geq r N_{d^k}$$

où N_{d^k} est le nombre d'éléments dans $\mathbb{Z}/d^k\mathbb{Z}$ dont l'ordre est divisible par d. On laisse en exercice le soin de vérifier que N_{d^k}/d^k tend vers 1 quand k tend vers $+\infty$ (factoriser en produit de nombres premiers).

Ce qui précède montre que la densité des $\mathfrak{p}$ dans $\mathcal{O}_K$ tels que $\sigma_{\mathfrak{p}}^G$ est au moins égale à $\frac{1}{|G|}$. Ceci valant pour tout σ, l'inégalité précédente est une égalité, ce qui termine la preuve du cas abélien. □

Corollaire 3.1.50. *Soit K une extension galoisienne de $\mathbb{Q}$, obtenue comme le corps de décomposition d'un polynôme unitaire irréductible $P \in \mathbb{Z}[X]$. Soit n le degré de P, et soit G le groupe de Galois de $K/\mathbb{Q}$. On considère G comme plongé dans le groupe des permutations $\mathfrak{t}$ des racines de P dans K.*

Soient $n_1 \geq \ldots \geq n_k$ des entiers positifs de somme n. Alors la densité des premiers p tels que la réduction de P modulo p est de la forme $P_1 \ldots P_k$ avec P_i irréductible de degré n_i est la proportion des $\sigma \in G$ dont la décomposition en cycles dans $\mathfrak{t}$ est de type $(n_1, \ldots, n_k)$.

Démonstration. L'ensemble des $\sigma \in G$ dont la décomposition en cycles dans $\mathfrak{t}$ est de type $(n_1, \ldots, n_k)$ est une union X de classes de conjugaisons dans G. L'ensemble des premiers p tels que le Frobenius en p est dans X a donc densité $|X|/|G|$ par le théorème de Cebotarev. Il est bien connu que le Frobenius en p est dans X si et seulement si la réduction de P modulo p est de la forme $P_1 \ldots P_k$ avec P_i irréductible de degré n_i, ce qui conclut. □

Remarque 3.1.51. *En cours, on a discuté le cas des extensions infinies.*