Le théorème de Čebotarev

Benoit Jacob - Sujet proposé par David Harari

Exposé présenté le 12 Juin 2002

Table des matières

En ce qui concerne les "pré-requis", le cours d'Algèbre 1 suffit. La première section n'est destinée qu'aux non-spécialistes. Le lecteur connaissant déjà le début de la théorie pourra avec profit passer directement à la section 2. Dans ce mémoire, "anneau" signifiera toujours "anneau commutatif unitaire".

1 Introduction à la théorie algébrique des nombres

Commençons par une petite définition :

Définition 1.0.1 *Un* corps de nombres *est une extension finie*[1] *de* $\mathbb{Q}$. *Un* nombre algébrique *est un élément d'un corps de nombres.*

La théorie algébrique des nombres consiste d'abord à associer à tout corps de nombres K un sous-anneau de K, noté $\mathcal{O}_K$ et appelé *l'anneau des entiers* de K. Ce sera fait en 1.2. Pour commencer, nous allons tenter de justifier l'introduction de cette notion.

1.1 L'unique factorisation

Pourquoi peut-on penser que la compréhension d'un corps de nombres K passe par la construction et l'étude d'un certain sous-anneau de K ? Considérons le théorème suivant, connu depuis l'Antiquité :

Théorème 1.1.1 *Pour tout* $x \in \mathbb{Q}^*$, *il existe une unique manière d'écrire*

$$x = \varepsilon p_1^{e_1} \dots p_r^{e_r},$$

où $\varepsilon = \pm 1$, *les* p_i *sont des nombres premiers et les* e_i *sont dans* $\mathbb{Z}$.

Corollaire 1.1.2 *Le groupe multiplicatif de* $\mathbb{Q}$ *est isomorphe à* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^{(\mathbb{N})}$.

Corollaire 1.1.3 *Soient* x *et* n *deux entiers* $\geqslant 1$. *Si* $\sqrt[n]{x}$ *n'est pas entier, alors* $\sqrt[n]{x}$ *est irrationnel. En particulier,* $\sqrt{2}$ *est irrationnel.*

Démonstration. Supposons que $\sqrt[n]{x}$ soit rationnel. Par le théorème, on peut écrire de façon unique $\sqrt[n]{x} = p_1^{e_1} \dots p_r^{e_r}$. Donc, en élevant ceci à la puissance n, nous obtenons $x = p_1^{ne_1} \dots p_r^{ne_r}$. Or x est entier. Donc il peut se factoriser avec des exposants positifs. Mais la factorisation est unique. Donc les ne_i sont tous positifs. Donc les e_i aussi. Donc $\sqrt[n]{x}$ est entier. $\diamondsuit$

On peut se demander comment généraliser ce théorème, et donc ses corollaires, à tout corps de nombres K. Visiblement, la première chose à faire est de généraliser la notion de nombre premier à K. Pour fixer le vocabulaire, rappelons les définitions suivantes :

Définition 1.1.1 *Soit* A *un anneau. Une* unité *de* A *est un élément inversible de* A. *Deux éléments de* A *sont dits* associés *si l'un est le produit de l'autre par une unité. Donc les unités sont exactement les éléments associés à 1. Un élément de* A *est dit* irréductible *s'il n'est pas une unité et si chacun de ses diviseurs est associé soit à lui, soit à 1.*

[1] Une extension K d'un corps k est dite finie si $[K : k] < \infty$.

On peut reformuler dans ce langage la définition d'un nombre premier : *un élément $x \in \mathbb{Q}$ est dit premier si c'est un élément irréductible (positif) de l'anneau* $\mathbb{Z}$. Selon cette définition, pour pouvoir généraliser la notion de nombre premier, et donc le théorème 1.1.1, nous devons trouver une généralisation de l'anneau $\mathbb{Z}$. Autrement dit, nous cherchons un anneau, que nous noterons $\mathcal{O}_K$, qui doit jouer vis-à-vis de K un rôle analogue à celui de $\mathbb{Z}$ vis-à-vis de $\mathbb{Q}$. Nous appellerons $\mathcal{O}_K$ l'*anneau des entiers algébriques de* K . Une fois que nous aurons un tel anneau sous la main, nous serons peut-être en mesure d'écrire pour K un énoncé similaire au théorème 1.1.1.

1.2 Définition de l'anneau des entiers

Dans cette sous-section, nous n'allons donner que des résultats sans preuves. Pour les calculs, recommandons en particulier le premier chapitre de [Neukirch 1], qui est très riche et bien organisé.

Définition 1.2.1 *Un nombre algébrique x est appelé un* entier algébrique *si l'anneau $\mathbb{Z}[x]$ est de type fini comme $\mathbb{Z}$-module.*

Proposition 1.2.1 *Un nombre algébrique x est un entier algébrique ssi son polynôme minimal sur $\mathbb{Q}$ (qui, par convention, est unitaire) est à coefficients entiers.*

Exemple 1.2.1 *$\sqrt[3]{7}$ est un entier algébrique car son polynôme minimal est $X^3 - 7$. $\frac{1+\sqrt{5}}{2}$ est un entier algébrique car son polynôme minimal est $X^2 - X - 1$. Mais $\frac{1+\sqrt{3}}{2}$ n'est pas un entier algébrique car son polynôme minimal est $X^2 - X - \frac{1}{2}$.*

On montre que les entiers algébriques appartenant à un corps de nombres K forment un sous-anneau de K, d'où la définition suivante :

Définition 1.2.2 *Soit K un corps de nombres algébriques. On appelle* l'anneau des entiers *de K, et on note $\mathcal{O}_K$ le sous-anneau de K formé des entiers algébriques appartenant à K.*

La proposition suivante montre que $\mathcal{O}_K$ se comporte exactement comme nous pourrions l'attendre de sa part :

Proposition 1.2.2 *Pour tout corps de nombres K, $\mathcal{O}_K$ est de type fini comme $\mathbb{Z}$-module. De plus, on a :*

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

et

$$\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}.$$

Exemple 1.2.2 *On a bien entendu $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. Avec un peu de calculs, on peut aussi calculer $\mathcal{O}_K$ pour $K = \mathbb{Q}(\sqrt{D})$, où $D \in \mathbb{Z}$ est sans facteur carré. Voici le résultat :*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{si } D \equiv 2 \text{ ou } 3 \mod (4), \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & \text{si } D \equiv 1 \mod (4). \end{cases}$$

Enfin, soit $K = \mathbb{Q}(\zeta)$, où ζ est une racine de l'unité. On a $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

1.3 La norme

Maintenant, pour généraliser le théorème 1.1.1, il *suffirait* de voir que $\mathcal{O}_K$ est factoriel[2]. En effet, la définition de la factorialité donne immédiatement :

[2] Un anneau A est dit *factoriel* si tout élément non nul de A se factorise de façon unique en un produit $\varepsilon p_1^{e_1} \dots p_r^{e_r}$, où ε est une unité de A, les p_i sont des irréductibles de A et les $e_i \geqslant 0$. La factorisation est unique à la multiplication près des facteurs par des unités de A.

Proposition 1.3.1 *Soit K un corps de nombres. Si $\mathcal{O}_K$ est factoriel, alors pour tout $x \in K^*$, il existe une factorisation*

$$x = \varepsilon p_1^{e_1} \dots p_r^{e_r},$$

où ε est une unité de $\mathcal{O}_K$, les p_i sont des irréductibles de $\mathcal{O}_K$, et les e_i sont dans $\mathbb{Z}$. La factorisation est unique à la multiplication près des facteurs par des unités de $\mathcal{O}_K$.

Par exemple, les seules unités de $\mathbb{Z}$ sont ± 1, donc, pour $K = \mathbb{Q}$, nous retrouvons bien le théorème 1.1.1. Malheureusement, $\mathcal{O}_K$ n'est pas toujours factoriel ! Prenons l'exemple de $K = \mathbb{Q}(\sqrt{-5})$. La règle donnée à l'exemple précédent nous donne $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Mais, dans $\mathbb{Z}[\sqrt{-5}]$, on a l'identité :

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Un bref calcul[3] montre que 2, 3, $1+\sqrt{-5}$ et $1-\sqrt{-5}$ sont irréductibles. Pour autant, ceci contredit-t-il la factorialité de $\mathcal{O}_K$? Si $\mathcal{O}_K$ était factoriel, alors 6 n'aurait qu'une factorisation, à la multiplication des facteurs par des unités près. Ainsi, $1 + \sqrt{-5}$ serait associé soit à 2, soit à 3. Pour montrer que ce n'est pas le cas, introduisons un objet qui joue un rôle très important en théorie algébrique des nombres :

Définition 1.3.1 *Soit K/k une extension galoisienne de corps de nombres. Pour $x \in K$, on définit la* norme de x *ainsi :*

$$\mathrm{N}_k^K(x) = \prod_{\sigma \in \mathrm{Gal}(K/k)} \sigma(x).$$

Il est clair que $\mathrm{N}_k^K(x) \in k$ (puisqu'il est fixé par les $\sigma \in \mathrm{Gal}(K/k)$). On prend parfois une autre définition, qui a l'avantage de s'appliquer à toutes les extensions finies : pour $x \in K$, la multiplication par x est un endomorphisme linéaire de K, vu comme k-espace vectoriel. La norme de x est alors le déterminant de cet endomorphisme.

Exemple 1.3.1 *Reprenons l'exemple de $k = \mathbb{Q}$ et $K = \mathbb{Q}(\sqrt{D})$ ($D \in \mathbb{Z}$, sans facteur carré). Le groupe de Galois* $\mathrm{Gal}(K/k)$ *possède deux éléments : l'identité sur K, et un autre automorphisme σ tel que $\forall x, y \in \mathbb{Q}$, $\sigma(x + y\sqrt{D}) = x - y\sqrt{D}$. Donc la norme est donnée par : $\mathrm{N}_{\mathbb{Q}}^K(x + y\sqrt{D}) = x^2 - Dy^2$.*

Proposition 1.3.2 *La norme est multiplicative : pour tous $x, y \in K$, on a :*

$$\mathrm{N}_k^K(xy) = \mathrm{N}_k^K(x)\mathrm{N}_k^K(y).$$

De plus, la norme d'un entier de K est un entier de k, et la norme d'une unité de $\mathcal{O}_K$ est une unité de $\mathcal{O}_k$.

Démonstration. On a, pour tous $x, y \in K$:

$$\mathrm{N}_k^K(xy) = \prod_{\sigma \in \mathrm{Gal}(K/k)} \sigma(xy) = \prod_{\sigma \in \mathrm{Gal}(K/k)} \sigma(x)\sigma(y) = \mathrm{N}_k^K(x)\,\mathrm{N}_k^K(y)$$

Soit x un entier de K. Soit $P \in \mathbb{Z}[X]$ son polynôme minimal. Alors, $\forall \sigma \in \mathrm{Gal}(K/k)$, $P(\sigma(x)) = \sigma(P(x)) = 0$. Donc $\sigma(x)$ est un entier de K. Or $\mathcal{O}_K$ est stable par multiplication. Donc $\mathrm{N}_k^K(x) = \prod_\sigma \sigma(x) \in \mathcal{O}_K$. Or $\mathrm{N}_k^K(x) \in k$. Donc $\mathrm{N}_k^K(x) \in \mathcal{O}_k$.
Soit x une unité de $\mathcal{O}_K$. Alors $x^{-1} \in \mathcal{O}_K$. Mais $\mathrm{N}_k^K(x \cdot x^{-1}) = \mathrm{N}_k^K(1) = 1$ et donc, par multiplicativité, $\mathrm{N}_k^K(x)\mathrm{N}_k^K(x^{-1}) = 1$. Donc $\mathrm{N}_k^K(x)$ est une unité. $\diamondsuit$

[3] En fait, ce calcul est trivialisé par la notion de *norme* que nous introduisons dans cette sous-section. Par exemple, montrons que $1 + \sqrt{-5}$ est irréductible. Sa norme vaut 6. Donc si $1 + \sqrt{-5}$ avait un diviseur non-trivial, sa norme serait un diviseur non-trivial de 6 : donc sa norme serait 2 ou 3. Mais aucun élément de $\mathcal{O}_K$ n'est de norme 2 ou 3. Donc $1 + \sqrt{-5}$ est irréductible.

Corollaire 1.3.3 *Soit K/k une extension de corps de nombres. Deux entiers x et y de K sont associés (dans $\mathcal{O}_K$) si, et seulement si leurs normes sont associées (dans $\mathcal{O}_k$).*

Démonstration. Si x et y sont associés dans $\mathcal{O}_K$, alors il existe une unité ε de $\mathcal{O}_K$ telle que $x = \varepsilon y$. On a donc $\mathrm{N}_k^K(x) = \mathrm{N}_k^K(\varepsilon)\mathrm{N}_k^K(y)$. Mais $\mathrm{N}_k^K(\varepsilon)$ est une unité de $\mathcal{O}_k$. Donc $\mathrm{N}_k^K(x)$ et $\mathrm{N}_k^K(y)$ sont associées.
Réciproquement, si $\mathrm{N}_k^K(x)$ et $\mathrm{N}_k^K(y)$ sont associées, alors, en posant $\varepsilon = \frac{x}{y}$, on obtient que $\mathrm{N}_{\mathbb{Q}}^K\varepsilon$ est une unité de $\mathcal{O}_k$. Donc c'est une unité de $\mathcal{O}_K$. En revenant à la définition de la norme, on voit alors que l'inverse de ε est $(\mathrm{N}_{\mathbb{Q}}^K\varepsilon)^{-1}\prod_{\sigma\neq 1}\sigma(\varepsilon) \in \mathcal{O}_K$. Donc $\varepsilon = \frac{x}{y}$ est une unité, donc x et y sont associés. $\diamondsuit$

Nous sommes maintenant en mesure de prouver que $1+\sqrt{-5}$ n'est associé ni à 2, ni à 3. En effet, $K = \mathbb{Q}(\sqrt{-5})$ est une extension galoisienne de $\mathbb{Q}$. La norme y est donnée par : $\mathrm{N}_{\mathbb{Q}}^K(x+y\sqrt{-5}) = x^2+5y^2$. Ainsi, on a $\mathrm{N}_{\mathbb{Q}}^K 2 = 4$, $\mathrm{N}_{\mathbb{Q}}^K 3 = 9$, $\mathrm{N}_{\mathbb{Q}}^K(1+\sqrt{-5}) = 6$. Ceci montre que $1+\sqrt{-5}$ n'est associé ni à 2, ni à 3. Donc $\mathcal{O}_K$ n'est pas factoriel. La proposition 1.3.1 ne s'applique donc pas à K. Ce n'est donc pas la bonne façon de généraliser le théorème 1.1.1. Nous allons maintenant voir la vraie généralisation.

1.4 Anneaux de Dedekind et idéaux fractionnaires

Le contexte historique dans lequel sont apparus les idéaux est très brièvement décrit en annexe A. Rappelons que le produit des idéaux $\mathfrak{i}$ et $\mathfrak{j}$ est l'idéal $\mathfrak{ij}$ engendré par les produits ij, où $i \in \mathfrak{i}$ et $j \in \mathfrak{j}$. Pour les idéaux, *diviser, c'est contenir*. Nous voudrions montrer que les idéaux de $\mathcal{O}_K$ se factorisent de façon unique en produits d'idéaux premiers. Nous allons commencer par définir une classe d'anneaux dont on peut montrer (théorème ci-dessous) que leurs idéaux se factorisent de façon unique :

Définition 1.4.1 *Un anneau intègre A est dit* de Dedekind *s'il est nœthérien*[4]*, si tous ses idéaux premiers non nuls sont maximaux, et s'il est intégralement clos (ce qui signifie que tout élément de $Frac(A)$ qui est annulé par un polynôme unitaire $P \in \mathbb{Z}[X]$ appartient à A).*

Théorème 1.4.1 *Soit A un anneau de Dedekind. Soit $\mathfrak{i}$ un idéal non nul de A. Il existe une unique manière d'écrire*

$$\mathfrak{i} = \mathfrak{p}_1^{e_1}\dots\mathfrak{p}_r^{e_r},$$

où les $\mathfrak{p}_i$ sont des idéaux premiers de A et les e_i sont dans $\mathbb{N}^*$.

Démonstration. C'est long à démontrer. La preuve figure dans [Lang 1] et [Neukirch 1], entre autres. $\diamondsuit$

Maintenant, bien entendu, il nous faut montrer que $\mathcal{O}_K$ est de Dedekind :

Proposition 1.4.2 *Pour tout corps de nombres K, $\mathcal{O}_K$ est de Dedekind.*

Démonstration. $\mathcal{O}_K$ est bien intégralement clos (proposition 1.2.1).

Montrons que $\mathcal{O}_K$ est nœthérien. A la proposition 1.2.2, nous avons vu que, comme $\mathbb{Z}$-module, $\mathcal{O}_K$ était de type fini. Puisque $\mathbb{Z}$ est principal et $\mathcal{O}_K$ est sans torsion, ceci implique que $\mathcal{O}_K$ est libre de type fini sur $\mathbb{Z}$. Donc tout idéal de $\mathcal{O}_K$, étant un sous-module de $\mathcal{O}_K$, est libre de type fini sur $\mathbb{Z}$. Donc les idéaux de $\mathcal{O}_K$

[4]Ceci signifie que les idéaux de A sont de type fini comme A-modules. Pour cela, il suffit (mais il n'est pas nécessaire) qu'ils soient de type fini comme $\mathbb{Z}$-modules.

sont de type fini. Donc $\mathcal{O}_K$ est nœthérien.

Montrons que les idéaux premiers non nuls de $\mathcal{O}_K$ sont maximaux. Soit $\mathfrak{P}$ un idéal premier non nul de $\mathcal{O}_K$. $\mathfrak{P} \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$, donc il existe un nombre premier p tel que $\mathfrak{P} \cap \mathbb{Z} = (p)$. Alors $\mathcal{O}_K/\mathfrak{P}$ est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel. Sa dimension est finie car, par la proposition 1.2.2, $\mathcal{O}_K$ est de type fini comme $\mathbb{Z}$-module. Soit $x \in \mathcal{O}_K/\mathfrak{P}$ non nul. La famille $(1, x, x^2, \ldots)$ est liée car on est en dimension finie. Donc il existe des $a_0, \ldots, a_n \in \mathbb{Z}/p\mathbb{Z}$, $a_0 \neq 0$, tels que :

$$a_n x^n + \cdots + a_1 x + a_0 = 0.$$

Donc

$$-a_0^{-1}(a_n x^{n-1} + \cdots + a_1)x = 1.$$

Donc x est inversible, donc $\mathcal{O}_K/\mathfrak{P}$ est un corps, donc $\mathfrak{P}$ est maximal. $\diamondsuit$

Jusqu'à présent, étant donné un idéal premier $\mathfrak{p}$ et un nombre négatif e, nous n'avons pas donné de sens au symbole $\mathfrak{p}^e$. Pour y remédier, introduisons la notion suivante :

Définition 1.4.2 *Soit K un corps de nombres. Un* idéal fractionnaire *de K est un sous-$\mathcal{O}_K$-module $\mathfrak{a}$ de K tel qu'il existe un élément non nul $c \in K$ tel que $c\mathfrak{a} \subset \mathcal{O}_K$.*

Exemple 1.4.1 *Les idéaux fractionnaires de $\mathbb{Q}$ sont les $q\mathbb{Z}$, avec $q \in \mathbb{Q}$.*

Notons que les idéaux sont des idéaux fractionnaires : il suffit de prendre $c = 1$ dans la définition. On définit le produit de deux idéaux fractionnaires comme on le fait pour les idéaux (voir plus haut). $\mathcal{O}_K$ est le neutre pour cette multiplication. La notion de divisibilité n'existe que pour les idéaux non fractionnaires. Toutefois, on dit formellement qu'un idéal premier $\mathfrak{p}$ divise un idéal fractionnaire $\mathfrak{a}$ s'il apparaît dans sa factorisation (voir le théorème ci-dessous). Sinon on dit que $\mathfrak{a}$ est premier avec $\mathfrak{p}$. Tout idéal fractionnaire non nul $\mathfrak{a}$ possède un inverse $\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subset \mathcal{O}_K\}$. Donc les idéaux fractionnaires non nuls de K forment un groupe, appelé le *groupe d'idéaux* de K, que nous noterons I_K. Le théorème 1.4.1 donne alors :

Théorème 1.4.3 *Soit K un corps de nombres. Soit $\mathfrak{a} \in I_K$. Il existe une unique manière d'écrire*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r},$$

où les $\mathfrak{p}_i$ sont des idéaux premiers de $\mathcal{O}_K$ et les e_i sont dans $\mathbb{Z}$.

1.5 Le groupe de classes d'idéaux

Au départ, c'est l'unique factorisation sur K^* que nous recherchions. Dans quelle mesure ce résultat sur I_K est-il une réponse satisfaisante ?

Proposition 1.5.1 *On a un morphisme $K^* \to I_K$ donné par : $x \mapsto x\mathcal{O}_K$.*

Définition 1.5.1 *L'image de ce morphisme, notée P_K, est appelée* le groupe des idéaux (fractionnaires) principaux. *Pour $x \in K$, l'idéal (fractionnaire) principal $x\mathcal{O}_K$ est simplement noté (x).*

Ainsi, K^* a pour image un sous-groupe P_K de I_K. Pour $x \in K^*$, nous obtenons donc une factorisation de x non pas comme produit d'éléments de K^*, comme nous l'avions initialement espéré, mais comme produit d'idéaux fractionnaires. Toutefois, le théorème suivant (admis) montre que cela revient presque au même :

Théorème 1.5.2 *Soit K un corps de nombres. P_K est d'indice fini dans I_K.*

Ce que ce théorème nous dit de très intéressant, c'est que I_K est à peine plus gros que l'image de K^*. Ainsi, pour récupérer l'unique factorisation sur K^*, nous n'avons eu besoin de rajouter que *peu de choses* à K^*. Tout ceci appelle une petite définition.

Définition 1.5.2 *Soit K un corps de nombres. On note $C_K = I_K/P_K$. C_K est appelé le* groupe de classes (d'idéaux) *de K. On note $h_K = |C_K|$. On appelle h_K le* nombre de classes (d'idéaux) *de K.*

On a :

$$h_K = 1 \iff \mathcal{O}_K \text{ est principal} \iff \mathcal{O}_K \text{ est factoriel.}$$

Dans le cas contraire, h_K mesure la quantité de choses qu'il faut rajouter pour récupérer l'unique factorisation.

1.6 Décomposition des idéaux premiers dans les extensions

Renvoyons le lecteur à l'annexe B pour un exemple simple de mise en œuvre des notions exposées ici. Soit K/k une extension de corps de nombres et soit $\mathfrak{p}$ un idéal premier non nul de k (c'est-à-dire, bien entendu, un idéal premier non nul de $\mathcal{O}_k$). Il est naturel[5] de lui associer l'idéal $\mathfrak{p}\mathcal{O}_K$ de K. Le théorème 1.4.3 donne alors une factorisation :

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}, \tag{1}$$

où les $\mathfrak{P}_i$ sont des idéaux premiers de K.

Définition 1.6.1 *Soit $\mathfrak{p}$, resp. $\mathfrak{P}$, un idéal premier non nul de k, resp. de K. On dit que $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$ si $\mathfrak{P} \cap \mathcal{O}_k = \mathfrak{p}$. On note alors : $\mathfrak{P} \mid \mathfrak{p}$.*

Proposition 1.6.1 *$\mathfrak{P}$ est* au-dessus de $\mathfrak{p}$ *ssi $\mathfrak{P}$ divise $\mathfrak{p}\mathcal{O}_K$, ssi $\mathfrak{P}$ est l'un des $\mathfrak{P}_i$ dans* (1).

Démonstration. Pour les idéaux, *diviser, c'est contenir*. Si $\mathfrak{P} \cap \mathcal{O}_k = \mathfrak{p}$, alors $\mathfrak{p} \subset \mathfrak{P}$, donc $\mathfrak{p}\mathcal{O}_K \subset \mathfrak{P}\mathcal{O}_K = \mathfrak{P}$. Réciproquement, si $\mathfrak{p}\mathcal{O}_K \subset \mathfrak{P}$, on a $\mathfrak{P} \cap \mathcal{O}_k \supset \mathfrak{p}\mathcal{O}_K \cap \mathcal{O}_k = \mathfrak{p}$, or $\mathfrak{p}$ est maximal car $\mathcal{O}_k$ est de Dedekind. $\diamondsuit$

Définition 1.6.2 *On note alors $e_{\mathfrak{P}|\mathfrak{p}}$ le plus grand entier e tel que $\mathfrak{P}^e \mid \mathfrak{p}$. Si $\mathfrak{P}$ est égal à $\mathfrak{P}_i$ dans* (1)*, alors $e_{\mathfrak{P}|\mathfrak{p}} = e_i$; $e_{\mathfrak{P}|\mathfrak{p}}$ est appelé* l'indice de ramification de $\mathfrak{P}$.

Définition 1.6.3 *$\mathcal{O}_K/\mathfrak{P}$ est une extension de $\mathcal{O}_k/\mathfrak{p}$, dont le degré est appelée le* degré résiduel de $\mathfrak{P}$*, et noté $f_{\mathfrak{P}|\mathfrak{p}}$.*

Soit $\mathfrak{p}$ un idéal premier de k, et notons $\mathfrak{P}_i$, $i = 1 \dots r$, les idéaux premiers de K au-dessus de $\mathfrak{p}$. Notons e_i leurs indices de ramification et f_i leurs degrés résiduels, de sorte que la factorisation (1) a lieu. Nous distinguons trois cas :
· Premier cas : $r = 1$ et $e_1 = 1$. Alors la factorisation s'écrit : $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1$. Donc $\mathfrak{p}\mathcal{O}_K$ est un idéal premier de K. Dans ce cas, on dit que $\mathfrak{p}$ *reste premier dans K* .
· Deuxième cas : $r > 1$ et $\forall i, e_i = 1$. Alors $\mathfrak{p}\mathcal{O}_K$ se factorise comme produit d'idéaux premiers *distincts* de K. Dans ce cas on dit que $\mathfrak{p}$ *se décompose dans K*. Si de plus tous les f_i sont égaux à 1, on dit que $\mathfrak{p}$ *se décompose totalement.*
· Troisième cas : $\exists i, e_i > 1$. Alors on dit que $\mathfrak{p}$ *se ramifie dans K.*

Proposition 1.6.2 *Seul un nombre fini de $\mathfrak{p}$ se ramifient.*

[5] Ceci par analogie avec le cas des idéaux principaux : à l'idéal $p\mathcal{O}_k$ de $\mathcal{O}_k$ on associe l'idéal $p\mathcal{O}_K$ de $\mathcal{O}_K$.

Démonstration. Par la proposition 1.2.2, nous pouvons écrire $\mathcal{O}_K = \mathcal{O}_k[\alpha_1, \ldots, \alpha_m]$. Par récurrence sur m, on se ramène au cas où $m = 1$. On a alors $\mathcal{O}_K = \mathcal{O}_k[\alpha]$. Soit u le polynôme minimal de α sur $\mathcal{O}_k$ et soit $\widetilde{u}$ sa réduction $\mod \mathfrak{p}$. Notons $d \in \mathcal{O}_k$ le discriminant de u et $\widetilde{d} \in \mathcal{O}_k/\mathfrak{p}$ celui de $\widetilde{u}$. Si $\mathfrak{p}$ se ramifie, alors, par la proposition B.1, $\widetilde{u}$ possède un facteur multiple, donc, dans une clôture algébrique de $\mathcal{O}_k/\mathfrak{p}$, $\widetilde{u}$ possède une racine multiple. Donc $\widetilde{d} = 0$. Or $\widetilde{d} = d \mod \mathfrak{p}$. Donc $\mathfrak{p}$ divise (d). Donc cela n'arrive que pour un nombre fini de $\mathfrak{p}$. $\diamondsuit$

Le théorème suivant est parfois appelé l'*identité fondamentale* :

Théorème 1.6.3 *Soit $n = [K : k]$ le degré de l'extension. On a :*

$$n = e_1 f_1 + \ldots + e_r f_r.$$

Démonstration. Partant de la décomposition (1) page 7, il "suffit" de montrer que, comme $\mathcal{O}_k/\mathfrak{p}$-espaces vectoriels, $\dim \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K = n$ et $\dim \mathcal{O}_K/\mathfrak{P}_i^{e_i} = e_i f_i$. Ensuite, on peut utiliser le théorème chinois pour écrire : $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K = \bigoplus \mathcal{O}_K/\mathfrak{P}_i^{e_i}$. $\diamondsuit$

1.7 Extensions galoisiennes et normes d'idéaux

Dans toute cette sous-section, K/k est une extension galoisienne de corps de nombres de degré n.

Définition 1.7.1 *Deux idéaux $\mathfrak{P}$ et $\mathfrak{Q}$ de K sont dits conjugués si*

$$\exists \sigma \in \mathrm{Gal}(K/k),\ \mathfrak{Q} = \sigma\mathfrak{P}.$$

Il est clair que si $\mathfrak{P}$ et $\mathfrak{Q}$ sont conjugués, alors ils sont au-dessus du même idéal de $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_k = \mathfrak{Q} \cap \mathcal{O}_k$. La réciproque est vraie :

Proposition 1.7.1 *Soit $\mathfrak{p}$ un idéal premier non nul de k. Soient $\mathfrak{P}$ et $\mathfrak{Q}$ au-dessus de $\mathfrak{p}$. $\mathfrak{P}$ et $\mathfrak{Q}$ sont conjugués.*

Démonstration. Si ce n'était pas le cas, par le théorème chinois, il existerait $x \in \mathcal{O}_K$ tel que : $\begin{cases} x \equiv 0 \mod \mathfrak{P} \\ x \equiv 1 \mod \sigma\mathfrak{Q} \quad \forall \sigma \in \mathrm{Gal}(K/k). \end{cases}$
Ainsi, $x \in \mathfrak{P}$, donc $\mathrm{N}_k^K x = x \prod_{\sigma \neq 1} \sigma x \in \mathfrak{P}$. Mais (proposition 1.3.2) $\mathrm{N}_k^K x \in \mathcal{O}_k$. Donc $\mathrm{N}_k^K x \in \mathfrak{p}$. Donc $\mathrm{N}_k^K x \in \mathfrak{Q}$. Mais, par construction, $\forall \sigma, \sigma^{-1} x \notin \mathfrak{Q}$. Ceci contredit la primalité de $\mathfrak{Q}$. $\diamondsuit$

En d'autres termes, $\mathrm{Gal}(K/k)$ agit transitivement[6] sur l'ensemble des idéaux $\mathfrak{P}$ au-dessus de $\mathfrak{p}$. Ceci a la conséquence suivante, typique des extensions galoisiennes :

Corollaire 1.7.2 *Soit $\mathfrak{p}$ un idéal premier non nul de k et $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r}$ sa décomposition de produit d'idéaux premiers de $\mathcal{O}_K$. Alors les indices de ramification e_i sont tous égaux à un même entier e, et les degrés résiduels f_i sont tous égaux à un même entier f.*

Démonstration. Par la proposition 1.7.1, pour $i, j \in \{1, \ldots, r\}$, il existe un $\sigma \in \mathrm{Gal}(K/k)$ tel que $\sigma\mathfrak{P}_j = \mathfrak{P}_i$. Montrons que $f_i = f_j$. σ induit un isomorphisme

$$\mathcal{O}_K/\mathfrak{P}_j \to \mathcal{O}_K/\mathfrak{P}_i.$$

[6] Notons l'analogie avec la topologie algébrique, où le groupe fondamental agit transitivement sur la fibre au-dessus d'un point.

Donc ces extensions de $\mathcal{O}_k/\mathfrak{p}$ ont même degré. Donc les degrés résiduels coïncident. Montrons que $e_i = e_j$. σ induit une permutation $\widetilde{\sigma}$ de $\{1,\dots,r\}$, caractérisée par : $\sigma\mathfrak{P}_x = \mathfrak{P}_{\widetilde{\sigma}(x)}$. On a : $\widetilde{\sigma}(j) = i$. Mais σ fixe k, donc $\sigma\mathfrak{p} = \mathfrak{p}$. Donc $\mathfrak{P}_{\widetilde{\sigma}(1)}^{e_1} \dots \mathfrak{P}_{\widetilde{\sigma}(r)}^{e_r} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$. Donc, pour tout x, $e_{\widetilde{\sigma}^{-1}(x)} = e_x$. Donc, en appliquant ceci à $x = i$, on obtient : $e_j = e_i$. Donc les indices de ramification coïncident. $\diamondsuit$

Ce corollaire nous apprend que, dans une extension galoisienne, les nombres $e_{\mathfrak{P}|\mathfrak{p}}$ et $f_{\mathfrak{P}|\mathfrak{p}}$ ne dépendent que de $\mathfrak{p}$, et pas de $\mathfrak{P}$ au-dessus de $\mathfrak{p}$. Il est donc logique de les appeler respectivement l'*indice de ramification de* $\mathfrak{p}$ et le *degré résiduel de* $\mathfrak{p}$, et de les noter respectivement $e_\mathfrak{p}$ et $f_\mathfrak{p}$, ou e et f. L'identité fondamentale (théorème 1.6.3) se reformule alors ainsi :

$$efr = n.$$

Nous allons maintenant définir la norme d'un idéal. Le lecteur pourra trouver une définition plus conceptuelle dans [Serre 1].

Définition 1.7.2 *Soit $\mathfrak{P}$ un idéal premier non nul de K et $\mathfrak{p} = \mathfrak{P} \cap k$ l'idéal premier de k en-dessous de $\mathfrak{P}$. On définit la* norme *de $\mathfrak{P}$ par :*

$$\mathrm{N}_k^K(\mathfrak{P}) = \mathfrak{p}^{f_\mathfrak{p}}.$$

On étend N_k^K à tout I_K par multiplicativité.

Ainsi, la norme est un morphisme

$$\mathrm{N}_k^K \ : \ I_K \to I_k.$$

Notons que, pour les idéaux principaux, cette définition est bien consistante avec la définition 1.3.1 : pour $x \in K^*$, on a $\mathrm{N}_k^K(x)\mathcal{O}_k = \mathrm{N}_k^K(x\mathcal{O}_K)$.

Définition 1.7.3 *Soit $\mathfrak{a}$ un idéal de K. La* norme absolue *de $\mathfrak{a}$ est l'unique $\mathbf{N}\mathfrak{a} \geqslant 0$ tel que $\mathrm{N}_\mathbb{Q}^K(\mathfrak{a}) = (\mathbf{N}\mathfrak{a})$.*

Définition 1.7.4 *Soit $\mathfrak{p}$ un idéal premier de K. Son* degré absolu $\mathbf{f}_\mathfrak{p}$ *est la dimension de $\mathcal{O}_K/\mathfrak{p}$ sur $\mathbb{Z}/p\mathbb{Z}$, où p est l'unique nombre premier dans $\mathfrak{p}$.*

Ainsi, on a $\mathbf{N}\mathfrak{p} = p^{\mathbf{f}_\mathfrak{p}}$. Plus généralement, $\mathbf{N}\mathfrak{a}$ est égal au cardinal de l'anneau $\mathcal{O}_K/\mathfrak{a}$.

1.8 Groupes de décomposition

Dans toute cette sous-section, K/k est une extension galoisienne de corps de nombres de degré n. Soit $\mathfrak{p}$ un idéal premier de k et $\mathfrak{P}$ au-dessus de $\mathfrak{p}$. Notons $\mathbf{F}_\mathfrak{p} = \mathcal{O}_k/\mathfrak{p}$, $\mathbf{F}_\mathfrak{P} = \mathcal{O}_K/\mathfrak{P}$.

Proposition 1.8.1 *$\mathbf{F}_\mathfrak{P}/\mathbf{F}_\mathfrak{p}$ est une extension galoisienne de degré $f_\mathfrak{p}$.*

Démonstration. Il est immédiat à partir de la proposition 1.2.2 que $\mathbf{F}_\mathfrak{p}$ et $\mathbf{F}_\mathfrak{P}$ sont finis. Or toute extension de corps finis est galoisienne. Et par définition de $f_\mathfrak{p}$, $\mathbf{F}_\mathfrak{P}/\mathbf{F}_\mathfrak{p}$ est de degré $f_\mathfrak{p}$. $\diamondsuit$

Définition 1.8.1 *Le* groupe de décomposition *de $\mathfrak{P}$ est le sous-groupe $G_\mathfrak{P}$ de* $\mathrm{Gal}(K/k)$ *formé des éléments σ tels que $\sigma\mathfrak{P} = \mathfrak{P}$.*

Quel est l'intérêt de cette définition ? Si $\sigma\mathfrak{P} = \mathfrak{P}$, alors σ induit par réduction mod $\mathfrak{P}$ un $\widetilde{\sigma} \in \mathrm{Gal}(\mathbf{F}_\mathfrak{P}/\mathbf{F}_\mathfrak{p})$. Ainsi, l'application $\sigma \mapsto \widetilde{\sigma}$ donne un morphisme

$$G_\mathfrak{P} \to \mathrm{Gal}(\mathbf{F}_\mathfrak{P}/\mathbf{F}_\mathfrak{p}).$$

Notre but (proposition 1.8.4) est désormais de montrer que, lorsque $\mathfrak{p}$ ne se ramifie pas dans K, ce morphisme est en fait un isomorphisme.

Définition 1.8.2 *Le* corps de décomposition $D_\mathfrak{P}$ *de* $\mathfrak{P}$ *est le corps fixe de* $G_\mathfrak{P}$.

C'est donc le sous-corps de K que la théorie de Galois associe au sous-groupe $G_\mathfrak{P}$ de $\mathrm{Gal}(K/k)$. Notons $\mathfrak{Q} = \mathfrak{P} \cap \mathcal{O}_{D_\mathfrak{P}}$ et $\mathbf{F}_\mathfrak{Q} = \mathcal{O}_{D_\mathfrak{P}}/\mathfrak{Q}$.

Proposition 1.8.2 *L'injection* $\mathcal{O}_k/\mathfrak{p} \to \mathcal{O}_{D_\mathfrak{P}}/\mathfrak{Q}$ *est un isomorphisme.*

Démonstration. Soit Γ le complémentaire de $G_\mathfrak{P}$ dans G. Pour $\sigma \in \Gamma$, notons $\mathfrak{Q}_\sigma = \sigma^{-1}\mathfrak{P} \cap \mathcal{O}_{D_\mathfrak{P}}$. Soit $x \in \mathcal{O}_{D_\mathfrak{P}}$. Nous voulons montrer que x est congru à un élément de $\mathcal{O}_k \mod \mathfrak{Q}$. Le théorème chinois dit qu'il existe $y \in \mathcal{O}_{D_\mathfrak{P}}$ tel que : $y \equiv x \mod \mathfrak{Q}$ et $\forall \sigma \in \Gamma,\ y \equiv 1 \mod \mathfrak{Q}_\sigma$. Mais, modulo $\mathfrak{P}$, ces congruences donnent : $y \equiv x \mod \mathfrak{P}$ et $\forall \sigma \in \Gamma,\ \sigma y \equiv 1 \mod \mathfrak{P}$. Donc :

$$\mathrm{N}_k^{D_\mathfrak{P}}(y) \equiv x \mod \mathfrak{P}.$$

Mais, par la proposition 1.3.2, $\mathrm{N}_k^{D_\mathfrak{P}}(y) \in \mathcal{O}_k$. Comme x et $\mathrm{N}_k^{D_\mathfrak{P}}(y)$ sont dans $\mathcal{O}_{D_\mathfrak{P}}$, on a :

$$\mathrm{N}_k^{D_\mathfrak{P}}(y) \equiv x \mod \mathfrak{Q}.$$

C'est la congruence que nous recherchions. $\diamondsuit$

Théorème 1.8.3 *Le morphisme* $G_\mathfrak{P} \to \mathrm{Gal}(\mathbf{F}_\mathfrak{P}/\mathbf{F}_\mathfrak{p})$, $\sigma \mapsto \widetilde{\sigma}$, *est toujours surjectif.*

Démonstration. Par la proposition, on a : $\mathrm{Gal}(\mathbf{F}_\mathfrak{P}/\mathbf{F}_\mathfrak{p}) = \mathrm{Gal}(\mathbf{F}_\mathfrak{P}/\mathbf{F}_\mathfrak{Q})$. Et, par définition de $D_\mathfrak{P}$, $G_\mathfrak{P} = \mathrm{Gal}(K/D_\mathfrak{P})$. Donc il suffit de montrer que la réduction mod $\mathfrak{P}$

$$\mathrm{Gal}(K/D_\mathfrak{P}) \to \mathrm{Gal}(\mathbf{F}_\mathfrak{P}/\mathbf{F}_\mathfrak{Q}),\ \sigma \mapsto \widetilde{\sigma}$$

est surjective. $\mathbf{F}_\mathfrak{P}/\mathbf{F}_\mathfrak{Q}$ est séparable, donc, par le théorème de l'élément primitif, il existe $x_1 \in \mathcal{O}_K$ tel que $\mathbf{F}_\mathfrak{P} = \mathbf{F}_\mathfrak{Q}(\widetilde{x}_1)$. Soit u le polynôme minimal de x_1 sur $\mathcal{O}_{D_\mathfrak{P}}$, et $x_1, \ldots, x_m$ ses racines. Alors $\widetilde{\sigma} \in \mathrm{Gal}(\mathbf{F}_\mathfrak{P}/\mathbf{F}_\mathfrak{Q})$ est déterminé par $\widetilde{\sigma}(\widetilde{x}_1)$, qui est l'un des $\widetilde{x}_1, \ldots, \widetilde{x}_m$. Mais $\mathrm{Gal}(K/D_\mathfrak{P})$ permute transitivement les racines de u, donc $\forall i, \exists \sigma, \sigma(x_1) = x_i$. On a alors : $\widetilde{\sigma}(\widetilde{x}_1) = \widetilde{x}_i$. Donc $\sigma \mapsto \widetilde{\sigma}$ est surjective. $\diamondsuit$

Définition 1.8.3 *Le noyau* $I_\mathfrak{P}$ *de* $G_\mathfrak{P} \to \mathrm{Gal}(\mathbf{F}_\mathfrak{P}/\mathbf{F}_\mathfrak{p})$ *est appelé le* groupe d'inertie *de* $\mathfrak{P}$.

Proposition 1.8.4 *On a :* $|I_\mathfrak{P}| = e_\mathfrak{p}$. *Donc* $G_\mathfrak{P} \to \mathrm{Gal}(\mathbf{F}_\mathfrak{P}/\mathbf{F}_\mathfrak{p})$ *est un isomorphisme si, et seulement si* $\mathfrak{p}$ *ne se ramifie pas dans* K.

Démonstration. Comme $|\mathrm{Gal}(\mathbf{F}_\mathfrak{P}/\mathbf{F}_\mathfrak{p})| = f_\mathfrak{p}$, il suffit de montrer que $|G_\mathfrak{P}| = e_\mathfrak{p} f_\mathfrak{p}$. Ecrivons la factorisation :

$$\mathfrak{p}\mathcal{O}_K = (\mathfrak{P}_1 \ldots \mathfrak{P}_r)^{e_\mathfrak{p}}.$$

Soit $G = \mathrm{Gal}(K/k)$. On a $|G| = n$, et, par la proposition 1.7.1, G agit transitivement sur un ensemble à r éléments. Donc la théorie des actions de groupes donne : $|G_\mathfrak{P}| = n/r$. Mais l'identité fondamentale nous dit que c'est égal à $e_\mathfrak{p} f_\mathfrak{p}$. $\diamondsuit$

Pour $\mathfrak{p}$ non ramifié et $\mathfrak{P} \mid \mathfrak{p}$, nous avons donc un isomorphisme

$$G_{\mathfrak{P}} \to \mathrm{Gal}(\mathbf{F}_{\mathfrak{P}}/\mathbf{F}_{\mathfrak{p}}).$$

Mais $G_{\mathfrak{P}} \subset \mathrm{Gal}(K/k)$. Nous sommes donc en mesure, partant d'un élément de $\mathrm{Gal}(\mathbf{F}_{\mathfrak{P}}/\mathbf{F}_{\mathfrak{p}})$, de lui associer un élément de $\mathrm{Gal}(K/k)$. Or, parmi les éléments de $\mathrm{Gal}(\mathbf{F}_{\mathfrak{P}}/\mathbf{F}_{\mathfrak{p}})$, il en est un d'une importance particulière, car il s'exprime simplement et est un générateur de $\mathrm{Gal}(\mathbf{F}_{\mathfrak{P}}/\mathbf{F}_{\mathfrak{p}})$. On l'appelle le *Frobenius* de $\mathbf{F}_{\mathfrak{P}}/\mathbf{F}_{\mathfrak{p}}$.

1.9 Le Frobenius

Définition 1.9.1 *L'application* $\mathrm{Fr}_{\mathfrak{P}} : \mathbf{F}_{\mathfrak{P}} \to \mathbf{F}_{\mathfrak{P}}$, $x \mapsto x^{\mathbf{N}\mathfrak{p}}$ *est appelé le* Frobenius *de* $\mathbf{F}_{\mathfrak{P}}/\mathbf{F}_{\mathfrak{p}}$. *C'est un générateur de* $\mathrm{Gal}(\mathbf{F}_{\mathfrak{P}}/\mathbf{F}_{\mathfrak{p}})$.

Définition 1.9.2 *Supposons* $\mathfrak{p}$ *non ramifié. L'élément* $(\mathfrak{P}, K/k)$ *de* $G_{\mathfrak{P}} \subset \mathrm{Gal}(K/k)$ *qui correspond à* $\mathrm{Fr}_{\mathfrak{P}}$ *est encore appelé le* Frobenius associé à $\mathfrak{P}$. *Il est uniquement déterminé par la propriéte :*

$$\forall x \in \mathcal{O}_K,\ (\mathfrak{P},\ K/k)(\alpha) \equiv \alpha^{\mathbf{N}\mathfrak{p}} \mod \mathfrak{P}. \tag{2}$$

Notons que $(\mathfrak{P},\ K/k)$ n'est pas uniquement déterminé par $\mathfrak{p}$, mais dépend aussi de $\mathfrak{P} \mid \mathfrak{p}$. Cependant, nous avons la proposition suivante :

Proposition 1.9.1 *La classe de conjugaison de* $(\mathfrak{P},\ K/k)$ *dans* $\mathrm{Gal}(K/k)$ *est uniquement déterminée par* $\mathfrak{p}$.

Démonstration. Soient $\mathfrak{P}$ et $\mathfrak{Q}$ au-dessus de $\mathfrak{p}$. Par la proposition 1.7.1, il existe $\tau \in \mathrm{Gal}(K/k)$ tel que $\tau\mathfrak{P} = \mathfrak{Q}$. Il est alors immédiat à partir de l'équation (2) que $\tau(\mathfrak{P},\ K/k)\tau^{-1} = (\mathfrak{Q},\ K/k)$. $\diamondsuit$

Définition 1.9.3 *Une extension galoisienne* K/k *est dite* abélienne *si* $\mathrm{Gal}(K/k)$ *est abélien.*

Corollaire 1.9.2 *Si* K/k *est une extension abélienne, alors* $(\mathfrak{P},\ K/k)$ *est uniquement déterminé par* $\mathfrak{p}$ *et ne dépend pas de* $\mathfrak{P} \mid \mathfrak{p}$.

Définition 1.9.4 *Si* K/k *est une extension abélienne, et* $\mathfrak{p}$ *un idéal premier non nul de* k *ne se ramifiant pas dans* K, *on appelle le* Frobenius de $\mathfrak{p}$, *et on note* $(\mathfrak{p},\ K/k)$ *le Frobenius* $(\mathfrak{P},\ K/k)$ *de* $\mathfrak{P}$, *pour n'importe quel* $\mathfrak{P} \mid \mathfrak{p}$.

Exemple 1.9.1 Traitons l'exemple de $K = k(\zeta)$, où ζ est une racine primitive m-ième de l'unité. Montrons les deux faits suivants :

$$\text{Si } \mathfrak{p} \text{ se ramifie dans } K, \text{ alors } \mathfrak{p} \text{ divise } (m).$$

Le raisonnement que nous avons utilisé à la proposition 1.6.2 nous dit que si $\mathfrak{p}$ se ramifie, $\mathfrak{p}$ divise (d), où d est le discriminant du polynôme minimal P de ζ sur k. Mais $X^m - 1$ annule ζ, donc P divise $X^m - 1$. Or, au signe près, le discriminant de $X^m - 1$ est m^m. Donc, si $\mathfrak{p}$ se ramifie, alors $\mathfrak{p}$ divise (m^m), donc $\mathfrak{p}$ divise (m).

Si $\mathfrak{p}$ ne divise pas (m), alors le Frobenius est donné par : $(\mathfrak{p},\ K/k)(\zeta) = \zeta^{\mathbf{N}\mathfrak{p}}$.

En effet, comme $\mathfrak{p}$ ne divise pas (m), $\mathbf{N}\mathfrak{p}$ est premier avec m, donc ζ et $\zeta^{\mathbf{N}\mathfrak{p}}$ ont le même polynôme minimal sur k. Donc il existe un morphisme $\sigma : K \to K$ fixant k et vérifiant $\sigma(\zeta) = \zeta^{\mathbf{N}\mathfrak{p}}$. Or σ est injectif, comme tout morphisme de corps. Or on est en dimension finie, donc $\sigma \in \mathrm{Gal}(K/k)$. Et σ satisfait l'équation (2) page 11. Or, parmi les éléments de $\mathrm{Gal}(K/k)$, $(\mathfrak{p},\ K/k)$ est uniquement déterminé par cette propriété, donc $(\mathfrak{p},\ K/k) = \sigma$.

2 Les théorèmes de densité

2.1 Enoncé du théorème de Čebotarev

Nous allons maintenant énoncer le théorème principal de cet exposé. Nous parlerons de la *densité* de certaines parties de l'ensemble des idéaux premiers d'un corps de nombres k. Commençons par introduire deux notions de densité : une première, très intuitive, et une seconde, très pratique dans les calculs.

Définition 2.1.1 *Soit k un corps de nombres. Soit M une partie de l'ensemble des idéaux premiers de k. La* densité naturelle $\delta(M)$ *de M est la limite suivante, quand elle existe :*

$$\delta(M) = \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \in M \mid \mathbf{N}\mathfrak{p} \leqslant x\}}{\#\{\mathfrak{p} \mid \mathbf{N}\mathfrak{p} \leqslant x\}}.$$

La densité de Dirichlet $d(M)$ *de M est la limite suivante, quand elle existe :*

$$d(M) = \lim_{s\to 1+} \frac{\sum_{\mathfrak{p}\in M} \mathbf{N}\mathfrak{p}^{-s}}{\sum_{\mathfrak{p}} \mathbf{N}\mathfrak{p}^{-s}}.$$

$\mathfrak{p}$ *varie parmi tous les idéaux premiers non nuls de k.*

Si $\delta(M)$ existe, alors on montre que $d(M)$ aussi, et qu'on a :

$$d(M) = \delta(M).$$

Dans un premier temps, nous allons introduire beaucoup de vocabulaire : application et noyau d'Artin, fonction ζ de Dedekind, séries L. Nous montrerons que les séries L ne s'annulent pas en 1, ce qui nous donnera, grâce à la théorie du corps de classes, une preuve du théorème de Čebotarev.

Définition 2.1.2 *Soit K/k une extension galoisienne de corps de nombres et $\sigma \in \mathrm{Gal}(K/k)$. On note $P_{K/k}(\sigma)$ l'ensemble des idéaux premiers $\mathfrak{p}$ de k ne se ramifiant pas et tels qu'il existe $\mathfrak{P}$ au-dessus de $\mathfrak{p}$ tel que $(\mathfrak{P}, K/k) = \sigma$ (voir la définition 1.9.2).*

Donc, dans le cas où K/k est abélienne, $P_{K/k}(\sigma)$ est l'ensemble des $\mathfrak{p}$ de k ne ramifiant pas et tels que $(\mathfrak{p}, K/k) = \sigma$ (voir la définition 1.9.4).

Théorème 2.1.1 (Čebotarev) *Soit K/k une extension galoisienne de corps de nombres de degré n, $\sigma \in \mathrm{Gal}(K/k)$, et c le cardinal de la classe de conjugaison de σ dans $\mathrm{Gal}(K/k)$. Alors $d(P_{K/k}(\sigma))$ existe, et vaut c/n.*

Nous allons maintenant énoncer (théorème 2.1.3) une conséquence du théorème de Čebotarev, que nous prouverons à la fin de ce mémoire.

Proposition 2.1.2 *Soit K/k une extension galoisienne de corps de nombres. L'ensemble $P_{K/k}(1)$ est l'ensemble des $\mathfrak{p}$ de k qui se décomposent totalement dans K.*

Démonstration. Dans une extension galoisienne, par le corollaire 1.7.2, $\mathfrak{p}$ se décompose totalement ssi $f_{\mathfrak{p}} = 1$. Si $\mathfrak{p} \in P_{K/k}(1)$, alors il existe $\mathfrak{P}$ au-dessus de $\mathfrak{p}$ tel que $\mathrm{Fr}_{\mathfrak{P}} = 1$. Mais $\mathrm{Fr}_{\mathfrak{P}}$ engendre $\mathrm{Gal}(\mathbf{F}_{\mathfrak{P}}/\mathbf{F}_{\mathfrak{p}})$. Donc $\mathbf{F}_{\mathfrak{P}} = \mathbf{F}_{\mathfrak{p}}$, donc $f_{\mathfrak{p}} = 1$. Réciproquement, si $\mathfrak{p}$ se décompose totalement, $f_{\mathfrak{p}} = 1$ donc, pour tout $\mathfrak{P}$ au-dessus de $\mathfrak{p}$, $\mathbf{F}_{\mathfrak{P}} = \mathbf{F}_{\mathfrak{p}}$, d'où $\mathrm{Fr}_{\mathfrak{P}} = 1$, donc $\mathfrak{p} \in P_{K/k}(1)$. $\diamondsuit$

Définition 2.1.3 *Pour deux ensembles A et B d'idéaux premiers de k, notons $A \succ B$ pour dire que B est inclus dans A, sauf pour un ensemble de densité de Dirichlet 0. Notons $A \approx B$ si $A \succ B$ et $B \succ A$.*

Théorème 2.1.3 *Soient K et L deux extensions galoisiennes de k, incluses dans une même clôture algébrique de k. On a :*

$$P_{K/k}(1) \succ P_{L/k}(1) \Longleftrightarrow K \subset L.$$

Donc, en particulier,

$$P_{K/k}(1) \approx P_{L/k}(1) \Longleftrightarrow K = L.$$

Ainsi, une extension galoisienne de k est uniquement déterminée par l'ensemble des $\mathfrak{p}$ de k qui s'y décomposent totalement. C'est un début de réponse à la question, posée par KRONECKER, de savoir comment caractériser les extensions de k seulement en termes de parties de $\mathrm{Spec}\,^7\mathcal{O}_k$, *"de la même façon que le théorème de Cauchy détermine une fonction par ses valeurs sur le bord"*.

2.2 Le symbole d'Artin

Soit K/k une extension *abélienne* de corps de nombres. Nous avons déjà vu (proposition 1.6.2) que les $\mathfrak{p}$ de k se ramifiant dans K sont en nombre fini. On peut donc considérer un idéal $\mathfrak{c}$ de $\mathcal{O}_k$ divisible par tous les $\mathfrak{p}$ se ramifiant dans K.

Définition 2.2.1 *On note $I(\mathfrak{c})$ l'ensemble des $\mathfrak{i} \in I_k$ premiers avec $\mathfrak{c}$.*

Définition 2.2.2 *Soit $\mathfrak{a} \in I(\mathfrak{c})$. Ecrivons sa factorisation : $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$. Pour chaque i, nous avons défini $(\mathfrak{p}_i,\ K/k)$ en 1.9.4. On définit le* symbole d'Artin *$(\mathfrak{a},\ K/k)$ ainsi :*

$$(\mathfrak{a},\ K/k) := (\mathfrak{p}_1,\ K/k)^{e_1} \dots (\mathfrak{p}_r,\ K/k)^{e_r}.$$

On a donc un morphisme, appelé l'application d'Artin :

$$I(\mathfrak{c}) \longrightarrow \mathrm{Gal}(K/k),\ \mathfrak{a} \mapsto (\mathfrak{a},\ K/k).$$

Dans la section 2.4, nous montrerons que l'application d'Artin est toujours surjective. Son noyau est appelé le *noyau d'Artin*. Notons-le $\mathcal{A}_\mathfrak{c}$. Ainsi, l'application d'Artin induit un isomorphisme

$$I(\mathfrak{c})/\mathcal{A}_\mathfrak{c} \longrightarrow \mathrm{Gal}(K/k).$$

On peut voir $I(\mathfrak{c})/\mathcal{A}_\mathfrak{c}$ comme une généralisation du groupe de classes d'idéaux C_k, et ses éléments comme des *classes d'idéaux généralisées*. Il se pose alors la question de savoir à quoi ressemble $\mathcal{A}_\mathfrak{c}$. La réponse, dans le cas général, est donnée par la loi de réciprocité d'Artin.

Définition 2.2.3 *On note $\mathfrak{N}(\mathfrak{c},\ K/k)$ le sous-groupe de $I(\mathfrak{c})$ formé des éléments de la forme $\mathrm{N}_k^K(\mathfrak{i})$, où $\mathfrak{i} \in I_K$.*

Proposition 2.2.1 *On a $\mathfrak{N}(\mathfrak{c},\ K/k) \subset \mathcal{A}_\mathfrak{c}$.*

Démonstration. On a à montrer que, pour $\mathfrak{a} \in I_K$ tel que $\mathrm{N}_k^K(\mathfrak{a}) \in I(\mathfrak{c})$, $(\mathrm{N}_k^K(\mathfrak{a}), K/k) = 1$. Par multiplicativité, il suffit de le montrer pour $\mathfrak{a} = \mathfrak{P}$ premier. Soit $\mathfrak{p}$ l'idéal premier de k en-dessous de $\mathfrak{P}$. On a $\mathrm{N}_k^K(\mathfrak{P}) = \mathfrak{p}^{f_\mathfrak{p}}$. Donc, pour $x \in \mathcal{O}_K$, en notant $\sigma = (\mathrm{N}_k^K(\mathfrak{P}),\ K/k)$, on a : $\sigma(x) \equiv x^{\mathbf{N}\mathfrak{p}^{f_\mathfrak{p}}} \mod \mathfrak{P}$. Mais $\mathbf{N}\mathfrak{p}^{f_\mathfrak{p}} = \mathbf{N}\mathfrak{P}$, et $x^{\mathbf{N}\mathfrak{P}} \equiv x \mod \mathfrak{P}$, d'où le résultat. $\diamondsuit$

Ainsi, nous connaissons déjà une partie du noyau d'Artin. Dans la sous-section suivante, nous allons introduire un autre sous-groupe de $I(\mathfrak{c})$, noté $P_\mathfrak{c}$, et plus loin on verra (loi de réciprocité d'Artin) que $\mathcal{A}_\mathfrak{c} = P_\mathfrak{c}\mathfrak{N}(\mathfrak{c},\ K/k)$.

[7] Le spectre d'un anneau est l'ensemble de ses idéaux premiers.

2.3 Classes d'idéaux généralisées

Jusqu'ici, nous avons considéré un *idéal* $\mathfrak{c}$ de $\mathcal{O}_k$. En fait, nous allons avoir besoin d'un objet un peu plus général, que Lang appelle un *cycle* et qui est aussi souvent appelé un *module*. L'idée est la suivante : considérer un idéal $\mathfrak{c}$ revient à considérer, pour tout $\mathfrak{p}$, un entier $v_\mathfrak{p}(\mathfrak{c}) \geqslant 0$. La correspondance est donnée par :

$$\mathfrak{c} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{c})}.$$

Nous allons maintenant considérer les morphismes injectifs $\lambda : k \longrightarrow \mathbb{R}$ (appelés les *plongements réels*) comme des *idéaux premiers infinis* (on ignore les plongements complexes non réels). On dit que λ se *ramifie* dans une extension K/k s'il existe un plongement complexe non réel de K coïncidant avec λ sur k. Les idéaux premiers traditionnels sont dits *finis*. Un *cycle* de k est alors par définition un produit formel

$$\mathfrak{c} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{c})},$$

où $\mathfrak{p}$ parcourt tous les idéaux premiers, finis et infinis, $v_\mathfrak{p}(\mathfrak{c}) \geqslant 0$, et $v_\mathfrak{p}(\mathfrak{c}) = 0$ sauf pour un nombre fini de $\mathfrak{p}$. Le produit restreint aux $\mathfrak{p}$ finis s'appelle la *partie finie* de $\mathfrak{c}$. On la note $\mathfrak{c}_0$. Ainsi, $\mathfrak{c}_0$ est un idéal de $\mathcal{O}_k$.

Dans la suite, $\mathfrak{c}$ désigne un cycle, et non plus un simple idéal. Bien sûr, les notations que nous avons introduites auparavant restent valides. Par exemple, $I(\mathfrak{c})$ désignera en fait $I(\mathfrak{c}_0)$. Ainsi, $I(\mathfrak{c})$ ne dépend pas de la partie infinie de $\mathfrak{c}$.

Introduisons maintenant $P_\mathfrak{c}$. Pour tout $x \in k^*$, on note $v_\mathfrak{p}(x)$ l'exposant de $\mathfrak{p}$ dans la factorisation de (x) donnée par le théorème 1.4.3.

Définition 2.3.1 *On dit que* $x \equiv 1 \mod \mathfrak{c}$ *soit si* $x = 1$, *soit si* $x \neq 1$ *et :*
1) pour tout $\mathfrak{p}$ *fini tel que* $v_\mathfrak{p}(\mathfrak{c}) > 0$, *on a* $v_\mathfrak{p}(x) = 0$ *et* $v_\mathfrak{p}(x-1) \geqslant v_\mathfrak{p}(\mathfrak{c})$
2) pour tout λ *infini tel que* $v_\lambda(\mathfrak{c}) > 0$, *on a* $\lambda(x) > 0$.

Définition 2.3.2 $P_\mathfrak{c}$ *est le sous-groupe de* I_k *formé des idéaux principaux* (x), *avec* $x \equiv 1 \mod \mathfrak{c}$.

Le point 1) dans la définition ci-dessus implique que $P_\mathfrak{c} \subset I(\mathfrak{c})$. Il est aussi clair que $P_\mathfrak{c}$ est un groupe. Le groupe quotient $I(\mathfrak{c})/P_\mathfrak{c}$ est appelé le *groupe des* $\mathfrak{c}$*-classes d'idéaux*. Quand $\mathfrak{c} = 1$, on retrouve C_k. De façon générale, ayant admis la finitude de C_k, il est aisé (grâce au théorème chinois) de voir que $I(\mathfrak{c})/P_\mathfrak{c}$ est fini.

Exemple 2.3.1 *Prenons* $k = \mathbb{Q}$. *Soit* $m \in \mathbb{N}$ *et soit* λ_∞ *l'unique plongement* $\mathbb{Q} \to \mathbb{R}$. *Soit* $\mathfrak{c} = (m)\lambda_\infty$. *Les idéaux premiers* $\mathfrak{p} \in P_\mathfrak{c}$ *sont les* (p), *avec* p *un nombre premier (donc,* > 0*) tel que* $p \equiv 1 \mod m$. *Soit* $K = \mathbb{Q}(\zeta)$, *avec* ζ *une racine primitive* m*-ième de l'unité. L'exemple 1.9.1 montre alors que* K/k *est non ramifiée en dehors de* $\mathfrak{c}$ *(attention,* λ_∞ *se ramifie) et que* $\mathfrak{p} \in P_\mathfrak{c} \Rightarrow (\mathfrak{p}, K/k) = 1$.

2.4 Fonction ζ de Dedekind

Le lecteur a certainement déjà rencontré la fonction ζ de Riemann :

$$\zeta(s) := \prod_{p \text{ premier}} \frac{1}{1-p^{-s}}.$$

Ce produit converge si $\Re s > 1$ et on a alors :

$$\zeta(s) = \sum_{a \geqslant 1} \frac{1}{a^s}.$$

Soit maintenant k un corps de nombres. On pose :

$$\zeta_k(s) := \prod_{\mathfrak{p}} \frac{1}{1-\mathbf{N}\mathfrak{p}^{-s}} = \sum_{\mathfrak{a}} \frac{1}{\mathbf{N}\mathfrak{a}^s}.$$

ζ_k est appelée la *fonction ζ de Dedekind*. Dans le cas $k = \mathbb{Q}$, on retrouve bien la fonction ζ de Riemann. Poursuivons les définitions. Soit $\mathfrak{A}$ un ensemble d'idéaux. On pose :

$$\zeta_k(s, \mathfrak{A}) := \sum_{\mathfrak{a}\in\mathfrak{A}} \frac{1}{\mathbf{N}\mathfrak{a}^s}.$$

Attention ! la somme n'est prise que sur les idéaux entiers (non fractionnaires) dans $\mathfrak{A}$. Soit maintenant $\mathfrak{c}$ un cycle de k. On pose :

$$\zeta_k(s, \mathfrak{c}) := \prod_{\mathfrak{p}\nmid\mathfrak{c}} \frac{1}{1-\mathbf{N}\mathfrak{p}^{-s}} = \sum_{\mathfrak{a}\in I(\mathfrak{c})} \frac{1}{\mathbf{N}\mathfrak{a}^s} = \zeta_k(s, I(\mathfrak{c})).$$

Il est alors immédiat que

$$\zeta_k(s, \mathfrak{c}) = \sum_{\mathfrak{A}\in I(\mathfrak{c})/P_{\mathfrak{c}}} \zeta_k(s, \mathfrak{A}).$$

En ce qui concerne la convergence, nous n'aurons pas besoin du plan tout entier. En fait, nous n'étudierons ces fonctions qu'au voisinage de 1. Il suffit donc de voir que ces fonctions se prolongent sur un ouvert contenant 1. Admettons le théorème suivant :

Théorème 2.4.1 *Soit k un corps de nombres de degré n sur $\mathbb{Q}$, $\mathfrak{c}$ un cycle de k, et $\mathfrak{A} \in I(\mathfrak{c})/P_{\mathfrak{c}}$. Alors les fonctions $\zeta_k(s)$, $\zeta_k(s, \mathfrak{c})$ et $\zeta_k(s, \mathfrak{A})$ se prolongent en des fonctions méromorphes sur le demi-plan $\Re s > 1 - 1/n$, et leur seul pôle est $s = 1$. C'est un pôle simple, de résidu un réel > 0.*

Définition 2.4.1 *Soit U un voisinage de 1 dans $\mathbb{C}$ et soient f et g deux fonctions holomorphes sur $U \setminus \{1\}$. Attention, on ne les suppose même pas méromorphes sur U. On note $f(x) \sim g(x)$ si $f - g$ est holomorphe sur un voisinage de 1. On note $f \gtrsim g$ s'il existe $\varepsilon > 0$ et $\Delta \in \mathbb{R}$ tels que, sur $]1; 1+\varepsilon[$, f et g sont à valeurs réelles et $f \geqslant g + \Delta$.*

Définition 2.4.2 *Nous allons prendre la détermination du logarithme induite par $\log(1-s) = -s - s^2/2 - s^3/3 - \ldots$ et prolongée analytiquement à $\mathbb{C} \setminus \mathbb{R}^-$.*

Proposition 2.4.2

$$\log \frac{1}{s-1} \sim \log \zeta_k(s) \sim \sum_{\mathfrak{p}} \frac{1}{\mathbf{N}\mathfrak{p}^s} \sim \sum_{\mathbf{f}_{\mathfrak{p}}=1} \frac{1}{\mathbf{N}\mathfrak{p}^s}.$$

Démonstration. Par le théorème 2.4.1, en notant r le résidu de ζ_k en 1, il existe une fonction h analytique dans un voisinage de 1 telle que : $\zeta_k(s) = \frac{r}{s-1} + h(s)$. D'où $\zeta_k(s) = \frac{1}{s-1}(r + (s-1)h(s))$, d'où $\log \zeta_k(s) = \log \frac{1}{s-1} + \log(r + (s-1)h(s))$. Mais $r \neq 0$, donc $\log \zeta_k(s) \sim \log \frac{1}{s-1}$.

D'autre part, on a $\zeta_k(s) = \prod_{\mathfrak{p}} \frac{1}{1-\mathbf{N}\mathfrak{p}^{-s}}$, donc $\log \zeta_k(s) = \sum_{\mathfrak{p}} -\log(1-\mathbf{N}\mathfrak{p}^{-s})$, donc :

$$\log \zeta_k(s) = \sum_{\mathfrak{p}, m\geqslant 1} \frac{1}{m\mathbf{N}\mathfrak{p}^{ms}}.$$

Mais la somme pour $m \geqslant 2$ converge quand $s = 1$, donc : $\log \zeta_k(s) \sim \sum_{\mathfrak{p}} \frac{1}{\mathbf{N}\mathfrak{p}^s}$. Enfin, $\mathbf{N}\mathfrak{p} = p^{\mathbf{f}_{\mathfrak{p}}}$, où p est l'unique nombre premier dans $\mathfrak{p}$. Donc la somme sur les

$\mathfrak{p}$ tels que $\mathbf{f}_\mathfrak{p} \geqslant 2$ converge, d'où le résultat. $\diamondsuit$

Ce résultat analytique suffit déjà à la preuve de la surjectivité de l'application d'Artin, annoncée en 2.2.

Théorème 2.4.3 *Soit K/k une extension abélienne de corps de nombres, non ramifiée en dehors d'un certain cycle $\mathfrak{c}$ de k. L'application d'Artin*

$$I(\mathfrak{c}) \to \mathrm{Gal}(K/k)\,,\ \mathfrak{a} \mapsto (\mathfrak{a},\ K/k)$$

est surjective.

Lemme 2.4.4 *Si l'application d'Artin est constante, alors $K = k$.*

Démonstration du lemme 2.4.4. Par la proposition 2.4.2, on a

$$\log \frac{1}{s-1} \sim \log \zeta_K(s) \sim \sum_{\mathfrak{P}} \frac{1}{\mathbf{N}\mathfrak{P}^s} \sim \sum_{\mathfrak{p}} \sum_{\mathfrak{P}|\mathfrak{p}} \frac{1}{\mathbf{N}\mathfrak{P}^s}.$$

Mais l'application d'Artin est constante, donc, par la proposition 2.1.2, tous les $\mathfrak{p} \in I(\mathfrak{c})$ se décomposent totalement dans K. Donc, au-dessus de chaque $\mathfrak{p} \in I(\mathfrak{c})$, il y a n $\mathfrak{P}$, où $n = [K : k]$, et on a $\mathbf{N}\mathfrak{P} = \mathbf{N}\mathfrak{p}$. Donc, pour tout $\mathfrak{p} \in I(\mathfrak{c})$,

$$\sum_{\mathfrak{P}|\mathfrak{p}} \frac{1}{\mathbf{N}\mathfrak{P}^s} = \sum_{\mathfrak{P}|\mathfrak{p}} \frac{1}{\mathbf{N}\mathfrak{p}^s} = n\frac{1}{\mathbf{N}\mathfrak{p}^s}.$$

Donc

$$\log \frac{1}{s-1} \sim n \sum_{\mathfrak{p}} \frac{1}{\mathbf{N}\mathfrak{p}^s} \sim n \log \zeta_k(s) \sim n \log \frac{1}{s-1},$$

donc $n = 1$, donc $K = k$. $\diamondsuit$

Démonstration du théorème 2.4.3. Soit H l'image de l'application d'Artin. Remarquons que H est distingué dans $\mathrm{Gal}(K/k)$. Soit F le corps fixe de H (donc, $k \subset F \subset K$). Grâce à la théorie de Galois, il suffit de montrer que $F = k$. Tout $\mathfrak{p}$ de k qui se ramifie dans F se ramifie dans K. Donc on peut définir l'application d'Artin

$$I(\mathfrak{c}) \longrightarrow \mathrm{Gal}(F/k),\ \mathfrak{a} \mapsto (\mathfrak{a},\ F/k).$$

Mais, pour $\mathfrak{p}$ premier dans $I(\mathfrak{c})$, $(\mathfrak{p},\ F/k)$ est la restriction de $(\mathfrak{p},\ K/k)$ à F. Donc, par définition de F, $(\mathfrak{p},\ F/k) = 1$. Donc, par le lemme 2.4.4, $F = k$. $\diamondsuit$

2.5 Séries L

Définition 2.5.1 *Soit G un groupe abélien fini. Un* caractère *de G est un morphisme $\chi : G \longrightarrow \mathbb{C}^*$. Les caractères de G forment un groupe pour la multiplication, noté $\hat{G}$.*

On montre[8] que $\hat{G}$ est isomorphe à G. Pour nos calculs, nous allons utiliser la formule dite "d'orthogonalité" :

Proposition 2.5.1 *Pour tout $x \in G$, on a :*

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} 0 & \text{si } x \neq 0, \\ |G| & \text{si } x = 0. \end{cases}$$

[8] C'est évident à partir du théorème de structure des groupes abéliens finis, sachant que les caractères d'un groupe cyclique sont très faciles à étudier.

Démonstration. Si $x = 0$, c'est clair. Si $x \neq 0$, alors $\exists \chi_x \in \hat{G}$ tel que $\chi_x(x) \neq 1$. On a alors : $\sum_{\chi \in \hat{G}} \chi(x) = \sum_{\chi \in \hat{G}} \chi_x \chi(x) = \chi_x(x) \sum_{\chi \in \hat{G}} \chi(x)$, d'où le résultat. $\diamondsuit$

Définition 2.5.2 *Soit k un corps de nombres, $\mathfrak{c}$ un cycle de k, et χ un caractère de $I(\mathfrak{c})/P_{\mathfrak{c}}$. On définit la* série L *ainsi :*

$$L_{\mathfrak{c}}(s, \chi) := \prod_{\mathfrak{p} \nmid \mathfrak{c}} \frac{1}{1 - \chi(\mathfrak{p}) \mathbf{N}\mathfrak{p}^{-s}}.$$

Ainsi, dans le cas où $\chi = 1$, on a : $L_{\mathfrak{c}}(s, \chi) = \zeta_k(s, \mathfrak{c})$. Revenons au cas général. Comme pour les fonctions ζ, on a une expression additive :

$$L_{\mathfrak{c}}(s, \chi) = \sum_{\mathfrak{a} \in I(\mathfrak{c})} \frac{\chi(\mathfrak{a})}{\mathbf{N}\mathfrak{a}^s}$$

Rappelons que ces sommes sont toujours prises sur les idéaux entiers (pas fractionnaires) $\mathfrak{a}$. On en déduit :

$$L_{\mathfrak{c}}(s, \chi) = \sum_{\mathfrak{A} \in I(\mathfrak{c})/P_{\mathfrak{c}}} \chi(\mathfrak{A})\, \zeta_k(s, \mathfrak{A}).$$

En reprenant la démonstration de la proposition 2.4.2, on obtient :

$$\log L_{\mathfrak{c}}(s, \chi) \sim \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{\mathbf{N}\mathfrak{p}^s} \sim \sum_{\mathbf{f}_{\mathfrak{p}} = 1} \frac{\chi(\mathfrak{p})}{\mathbf{N}\mathfrak{p}^s} \tag{3}$$

C'est au niveau de la convergence en 1 que le comportement des séries L diffère fondamentalement de celui des fonctions ζ :

Proposition 2.5.2 *Soit $n = [k : \mathbb{Q}]$. Si $\chi \neq 1$, la série L converge pour tout s avec $\Re s > 1 - 1/n$, et définit ainsi une fonction holomorphe sur ce demi-plan.*

Ainsi, les fonctions L n'ont pas de pôle en 1. Le théorème suivant est d'une grande importance pour la théorie du corps de classes. Nous avons reporté en annexe C un énoncé plus général ; celui-ci suffit à la preuve du théorème de Čebotarev.

Théorème 2.5.3 *Soit K/k une extension galoisienne de corps de nombres, de degré n. Soit $\mathfrak{c}$ un cycle de k divisible par tous les $\mathfrak{p}$ qui se ramifient dans K. Soit $H = P_{\mathfrak{c}}\mathfrak{N}(\mathfrak{c}, K/k)$. Pour tout caractère $\chi \neq 1$ de $I(\mathfrak{c})/H$, en considérant χ comme un caractère de $I(\mathfrak{c})/P_{\mathfrak{c}}$, on a :*

$$L_{\mathfrak{c}}(1, \chi) \neq 0.$$

De plus, $|I(\mathfrak{c})/H| \leqslant n$.

Démonstration. Notons $h = |I(\mathfrak{c})/H|$. Soit $\chi \neq 1$ un caractère de $I(\mathfrak{c})/H$. Soit $m(\chi) \geqslant 0$ l'ordre du zéro de $L_{\mathfrak{c}}(s, \chi)$ en 1. Montrons que $m(\chi) = 0$. On a :

$$\log L_{\mathfrak{c}}(s, \chi) \sim m(\chi) \log(s - 1) = -m(\chi) \log \frac{1}{s - 1}. \tag{4}$$

Réutilisons l'équation (3) page 17. Par définition de χ, $\chi(\mathfrak{p})$ ne dépend que de la classe de $\mathfrak{p} \mod H$, donc

$$\log L_{\mathfrak{c}}(s, \chi) \sim \sum_{\mathfrak{A} \in I(\mathfrak{c})/H} \chi(\mathfrak{A}) \sum_{\mathfrak{p} \in \mathfrak{A}} \frac{1}{\mathbf{N}\mathfrak{p}^s}.$$

En sommant sur tous les χ, on obtient : $\sum_\chi \log L_\mathfrak{c}(s,\chi) \sim \sum_\chi \sum_\mathfrak{A} \chi(\mathfrak{A}) \sum_{\mathfrak{p}\in\mathfrak{A}} \frac{1}{\mathbf{N}\mathfrak{p}^s}$. Pour $\chi \neq 1$, on peut réutiliser (4). Pour $\chi = 1$, on a $\log L_\mathfrak{c}(s,\chi) = \log \zeta_k(s,\mathfrak{c}) \sim \log \zeta_k(s)$, et on réutilise la proposition 2.4.2. Il vient :

$$(1 - \sum_{\chi\neq 1} m(\chi)) \log \frac{1}{s-1} \sim \sum_\chi \sum_{\mathfrak{A}\in I(\mathfrak{c})/H} \chi(\mathfrak{A}) \sum_{\mathfrak{p}\in\mathfrak{A}} \frac{1}{\mathbf{N}\mathfrak{p}^s}.$$

Occupons-nous maintenant du terme de droite. Nous pouvons intervertir les sommes sur χ et sur $\mathfrak{A}$, et appliquer la proposition 2.5.1. Cela donne :

$$(1 - \sum_{\chi\neq 1} m(\chi)) \log \frac{1}{s-1} \sim h \sum_{\mathfrak{p}\in H} \frac{1}{\mathbf{N}\mathfrak{p}^s}.$$

Remarquons que la définition de la norme, $\mathrm{N}_k^K \mathfrak{P} = \mathfrak{p}^{f_\mathfrak{p}}$, nous dit que : $\mathfrak{p} \in \mathfrak{N}(\mathfrak{c},\, K/k)$ ssi $\mathfrak{p} \in I(\mathfrak{c})$ et $f_\mathfrak{p} = 1$. Donc, vu notre choix de $\mathfrak{c}$, $\mathfrak{p} \in \mathfrak{N}(\mathfrak{c},\, K/k) \Leftrightarrow \mathfrak{p}$ est premier avec $\mathfrak{c}$ et se décompose totalement dans K. Or $\mathfrak{N}(\mathfrak{c},\, K/k) \subset H$. Donc :

$$\sum_{\mathfrak{p}\in H} \frac{1}{\mathbf{N}\mathfrak{p}^s} \gtrsim \sum_{\mathfrak{p}\in P_{K/k}(1)} \frac{1}{\mathbf{N}\mathfrak{p}^s} \gtrsim \frac{1}{n} \sum_{f_\mathfrak{P}=1} \frac{1}{\mathbf{N}\mathfrak{P}^s},$$

puisqu'au-dessus de chaque $\mathfrak{p}$ se décomposant totalement, il y a n $\mathfrak{P}$. Donc :

$$(1 - \sum_{\chi\neq 1} m(\chi)) \log \frac{1}{s-1} \gtrsim \frac{h}{n} \log \frac{1}{s-1}.$$

Donc $1 - \sum_{\chi\neq 1} m(\chi) \geqslant h/n$. Donc $h/n \leqslant 1$, et pour tout $\chi \neq 1$, on a $m(\chi) = 0$. C'est exactement ce que nous devions prouver. $\diamondsuit$

2.6 Enoncés de la théorie du corps de classes

Nous en savons maintenant suffisament pour énoncer les principaux théorèmes du corps de classes. Commençons par le théorème principal : la loi de réciprocité d'Artin (théorème 2.6.2).

Soit k un corps de nombres , $\mathfrak{c}$ un cycle de k, et K/k une extension abélienne de degré n non ramifiée en dehors de $\mathfrak{c}$, ce qui signifie que $\mathfrak{c}$ est divisible par tous les $\mathfrak{p}$ de k (finis et infinis) qui se ramifient dans K. Nous avons montré en 2.4 que l'application d'Artin était une surjection de $I(\mathfrak{c})$ sur $\mathrm{Gal}(K/k)$. Il s'agit de déterminer son noyau $\mathcal{A}_\mathfrak{c}$. Commençons par une petite conséquence de l'étude des fonctions L faite ci-dessus :

Proposition 2.6.1 *Si $P_\mathfrak{c} \subset \mathcal{A}_\mathfrak{c}$, alors $\mathcal{A}_\mathfrak{c} = P_\mathfrak{c}\mathfrak{N}(\mathfrak{c},\, K/k)$.*

Démonstration. Notons $H = P_\mathfrak{c}\mathfrak{N}(\mathfrak{c},\, K/k)$. Par définition de $\mathcal{A}_\mathfrak{c}$, l'application d'Artin est un isomorphisme : $I(\mathfrak{c})/\mathcal{A}_\mathfrak{c} \to \mathrm{Gal}(K/k)$. Donc $|I(\mathfrak{c})/\mathcal{A}_\mathfrak{c}| = n$. On sait (proposition 2.2.1) que $\mathfrak{N}(\mathfrak{c},\, K/k) \subset \mathcal{A}_\mathfrak{c}$. Donc, si $P_\mathfrak{c} \subset \mathcal{A}_\mathfrak{c}$, alors $H \subset \mathcal{A}_\mathfrak{c}$. Supposons que l'inclusion soit stricte. Alors $|I(\mathfrak{c})/H| > n$. Ceci contredit le théorème 2.5.3. Donc $H = \mathcal{A}_\mathfrak{c}$. $\diamondsuit$

Voici maintenant la loi de réciprocité d'Artin :

Théorème 2.6.2 *Pour tout cycle $\mathfrak{c}$ de k et pour toute extension abélienne finie K/k non ramifiée en dehors de $\mathfrak{c}$, l'application d'Artin est un isomorphisme :*

$$I(\mathfrak{c})/P_\mathfrak{c}\mathfrak{N}(\mathfrak{c},\, K/k) \longrightarrow \mathrm{Gal}(K/k).$$

Démonstration. La surjectivité a été démontrée en 2.4. Il s'agit donc de montrer que $\mathcal{A}_\mathfrak{c} = P_\mathfrak{c}\mathfrak{N}(\mathfrak{c},\, K/k)$. Par la proposition 2.6.1, il "suffit" de montrer que $P_\mathfrak{c} \subset \mathcal{A}_\mathfrak{c}$. C'est fait dans [Lang 1], pp. 200-206. Dans le cas particulier où $k = \mathbb{Q}$, $K = k(\zeta)$, avec ζ une racine primitive m-ième de l'unité, et $\mathfrak{c} = (m)\lambda_\infty$, l'exemple 2.3.1 montre que K/k est non ramifiée en dehors de $\mathfrak{c}$ et que $\mathfrak{p} \in P_\mathfrak{c} \Rightarrow (\mathfrak{p},\, K/k) = 1$. On en déduit aisément que $P_\mathfrak{c} \subset \mathcal{A}_\mathfrak{c}$, ce qui prouve donc la loi dans ce cas particulier. $\diamondsuit$

Ainsi, la loi de réciprocité d'Artin fait correspondre à une extension abélienne K/k non ramifiée en dehors de $\mathfrak{c}$ un groupe $H = P_\mathfrak{c}\mathfrak{N}(\mathfrak{c},\, K/k)$. Le théorème suivant (admis) est appelé le théorème d'existence du corps de classes. Il fait la construction inverse :

Théorème 2.6.3 *Soit $\mathfrak{c}$ un cycle de k. Soit H un groupe tel que $P_\mathfrak{c} \subset H \subset I(\mathfrak{c})$. Alors il existe une extension abélienne K/k, non ramifiée en dehors de $\mathfrak{c}$, telle que $H = P_\mathfrak{c}\mathfrak{N}(\mathfrak{c},\, K/k)$. K est appelé le* corps de classes *associé à H.*

Nous n'aurons pas besoin de ce théorème pour prouver le théorème de Čebotarev. Il nous servira en annexe C à obtenir un résultat général sur les fonctions L.

Etant donné un cycle $\mathfrak{c}$ de k, la théorie du corps de classes donne donc une correspondance entre, d'une part, les extensions abéliennes K/k non ramifiées en dehors de $\mathfrak{c}$ (les "corps de classes"), et d'autre part les groupes H tels que $P_\mathfrak{c} \subset H \subset I(\mathfrak{c})$ (les "groupes de classes").

2.7 Cas abélien du théorème de Čebotarev

Commençons par prouver le résultat suivant :

Théorème 2.7.1 *Soient k un corps de nombres, $\mathfrak{c}$ un cycle de k, et H un groupe tel que $P_\mathfrak{c} \subset H \subset I(\mathfrak{c})$. Soient $h = |I(\mathfrak{c})/H|$ et $\mathfrak{A}_0 \in I(\mathfrak{c})/H$. Si, pour tout caractère $\chi \neq 1$ de $I(\mathfrak{c})/H$, on a $L_\mathfrak{c}(1,\chi) \neq 0$, alors*

$$\sum_\mathfrak{p} \frac{1}{\mathbf{N}\mathfrak{p}^s} \sim h \sum_{\mathfrak{p}\in\mathfrak{A}_0} \frac{1}{\mathbf{N}\mathfrak{p}^s}.$$

Démonstration. Nous allons exprimer $\sum_\chi \chi(\mathfrak{A}_0^{-1}) \log L_\mathfrak{c}(s,\chi)$, où χ parcourt les caractères de $I(\mathfrak{c})/H$, de deux façons différentes au voisinage de 1. D'abord, on a :

$$\sum_\chi \chi(\mathfrak{A}_0^{-1}) \log L_\mathfrak{c}(s,\chi) = \log \zeta_k(s,\mathfrak{c}) + \sum_{\chi\neq 1} \chi(\mathfrak{A}_0)^{-1} \log L_\mathfrak{c}(s,\chi),$$

or $\log \zeta_k(s,\mathfrak{c}) \sim \sum_\mathfrak{p} \frac{1}{\mathbf{N}\mathfrak{p}^s}$ par la proposition 2.4.2 ($\zeta_k(s,\mathfrak{c})$ et $\zeta_k(s)$ ne diffèrent que par un nombre fini de termes) et $\sum_{\chi\neq 1} \chi(\mathfrak{A}_0)^{-1} \log L_\mathfrak{c}(s,\chi) \sim 0$ puisque $L_\mathfrak{c}(1,\chi) \neq 0$. Donc :

$$\sum_\chi \chi(\mathfrak{A}_0^{-1}) \log L_\mathfrak{c}(s,\chi) \sim \sum_\mathfrak{p} \frac{1}{\mathbf{N}\mathfrak{p}^s}.$$

Mais, d'autre part, en utilisant l'équation (3) page 17, on obtient :

$$\sum_\chi \chi(\mathfrak{A}_0^{-1}) \log L_\mathfrak{c}(s,\chi) \sim \sum_\chi \sum_\mathfrak{p} \frac{\chi(\mathfrak{A}_0^{-1})\chi(\mathfrak{p})}{\mathbf{N}\mathfrak{p}^s}.$$

Or $\chi(\mathfrak{p})$ ne dépend que de la classe $\mathfrak{A} \in I(\mathfrak{c})/P_\mathfrak{c}$ de $\mathfrak{p}$, donc

$$\sum_\chi \sum_\mathfrak{p} \frac{\chi(\mathfrak{A}_0^{-1})\chi(\mathfrak{p})}{\mathbf{N}\mathfrak{p}^s} = \sum_\chi \sum_\mathfrak{A} \chi(\mathfrak{A}_0^{-1}\mathfrak{A}) \sum_{\mathfrak{p}\in\mathfrak{A}} \frac{1}{\mathbf{N}\mathfrak{p}^s}.$$

On peut alors intervertir les sommes sur $\mathfrak{A}$ et sur χ, et appliquer la formule d'orthogonalité 2.5.1, ce qui donne immédiatement le résultat. $\diamondsuit$

A la lumière de la loi de réciprocité d'Artin, nous pouvons déjà en déduire la partie essentielle du théorème de Čebotarev :

Théorème 2.7.2 (Cas abélien du théorème de Čebotarev) *Soit K/k une extension abélienne de degré n. Pour tout $\sigma \in \mathrm{Gal}(K/k)$, on a :*

$$d(P_{K/k}(\sigma)) = \frac{1}{n}\cdot$$

Démonstration. Soient $\mathfrak{c}$ un cycle en dehors duquel K/k est non ramifiée, $H = P_{\mathfrak{c}}\mathfrak{N}(\mathfrak{c},\, K/k)$ et $h = |I(\mathfrak{c})/H|$. La loi de réciprocité d'Artin donne un isomorphisme

$$I(\mathfrak{c})/H \longrightarrow \mathrm{Gal}(K/k).$$

Donc $h = n$ et $P_{K/k}(\sigma) \in I(\mathfrak{c})/H$. Notons $\mathfrak{A}_0 = P_{K/k}(\sigma)$. Par le théorème 2.5.3, pour tout caractère $\chi \neq 1$ de $I(\mathfrak{c})/H$, $L_{\mathfrak{c}}(1,\chi) \neq 0$. Donc le théorème 2.7.1 s'applique et nous donne :

$$\sum_{\mathfrak{p}} \frac{1}{\mathbf{N}\mathfrak{p}^s} \sim n \sum_{\mathfrak{p}\in\mathfrak{A}_0} \frac{1}{\mathbf{N}\mathfrak{p}^s}\cdot$$

Il en découle que $d(\mathfrak{A}_0) = 1/n$. $\diamondsuit$

Exemple 2.7.1 (Théorème de la progression arithmétique) Appliquons ceci à $k = \mathbb{Q}$, $\mathfrak{c} = (m)\lambda_\infty$, et $K = \mathbb{Q}(\zeta)$, où ζ est une racine primitive m-ième de l'unité. K/k est abélienne et on a vu qu'elle était non ramifiée en dehors de $\mathfrak{c}$ et que pour tout nombre premier p ne divisant pas m, $(p,\, K/k)(\zeta) = \zeta^p$. Donc, pour tout entier positif a premier avec m, $(a,\, K/k)(\zeta) = \zeta^a$. Donc $p \equiv a \mod m \Leftrightarrow (p,\, K/k) = (a,\, K/k) \Leftrightarrow p \in P_{K/k}(a,\, K/k)$. Par le théorème 2.7.2, $d(P_{K/k}(a,\, K/k)) > 0$, donc $P_{K/k}(a,\, K/k)$ contient une infinité de p, donc il existe une infinité de p tels que $p \equiv a \mod m$.

2.8 Théorème de Čebotarev

Nous allons maintenant prouver le résultat central de ce mémoire. Nous avons déjà fait la partie difficile en 2.7.2.

Théorème 2.8.1 (Čebotarev) *Soit K/k une extension galoisienne de corps de nombres de degré n, $\sigma \in \mathrm{Gal}(K/k)$, et c le cardinal de la classe de conjugaison de σ dans $\mathrm{Gal}(K/k)$. Alors*

$$d(P_{K/k}(\sigma)) = \frac{c}{n}\cdot$$

Démonstration. Soit f l'ordre de σ dans $\mathrm{Gal}(K/k)$ et soit Z le corps fixe de $\langle\sigma\rangle$ (le sous-groupe cyclique de $\mathrm{Gal}(K/k)$ engendré par σ). Alors $\mathrm{Gal}(K/Z) = \langle\sigma\rangle$. En particulier, $\mathrm{Gal}(K/Z)$ est abélien, donc, par le théorème 2.7.2, $d(P_{K/Z}(\sigma)) = 1/f$. Soit $P(\sigma)$ l'ensemble des $\mathfrak{P}$ de K tels que $(\mathfrak{P},\, K/k) = \sigma$. Alors $P(\sigma)$ correspond[9] à l'ensemble $P'_{K/Z}(\sigma)$ des $\mathfrak{q} \in P_{K/Z}(\sigma)$ tels que $\mathfrak{q}\cap k$ se décompose totalement dans Z.

[9] Explicitons cette correspondance, que nous noterons $\cong$. Dans un sens, elle est donnée par : $\mathfrak{P} \mapsto \mathfrak{q} := \mathfrak{P} \cap \mathcal{O}_Z$. On a $\mathfrak{q} \in P_{K/Z}(\sigma)$. En effet, $\mathfrak{P}$ est au-dessus de $\mathfrak{q}$, et $(\mathfrak{P},\, K/Z) = \sigma$ car Z est fixé par σ. Montrons que $\mathfrak{p} := \mathfrak{q} \cap \mathcal{O}_k$ se décompose totalement dans Z. On a $(\mathfrak{P},\, K/Z) = \sigma = (\mathfrak{P},\, K/k)$, donc, en revenant à l'équation (2) page 11, on voit que $\mathbf{N}\mathfrak{q} = \mathbf{N}\mathfrak{p}$. Donc $f_{\mathfrak{q}|\mathfrak{p}} = 1$. Donc $\mathfrak{p}$ se décompose totalement dans Z. Dans l'autre sens, la correspondance est donnée par : $\mathfrak{q} \mapsto \mathfrak{P} := \mathfrak{q}\mathcal{O}_K$. En effet, $\mathfrak{q}$ reste premier dans K.

Comme les idéaux premiers restants sont soit ramifiés, soit de degré absolu > 1, nous pouvons les omettre et obtenir $d(P'_{K/Z}(\sigma)) = d(P_{K/Z}(\sigma)) = 1/f$. Nous avons une application surjective $\rho : P'_{K/Z}(\sigma) \to P_{K/k}(\sigma)$, $\mathfrak{q} \mapsto \mathfrak{q} \cap k$. Comme $P'_{K/Z}(\sigma) \cong P(\sigma)$, nous obtenons, pour tout $\mathfrak{p} \in P_{K/k}(\sigma)$,

$$\rho^{-1}(\{\mathfrak{p}\}) \cong \{\mathfrak{P} \in P(\sigma) \text{ tels que } \mathfrak{P} \mid \mathfrak{p}\} \cong G_\sigma/\langle\sigma\rangle,$$

où G_σ est le sous-groupe de $\mathrm{Gal}(K/k)$ formé des éléments commutant avec σ. Donc :

$$d(P_{K/k}(\sigma)) = \frac{1}{|G_\sigma/\langle\sigma\rangle|} d(P'_{K/Z}(\sigma)) = \frac{1}{|G_\sigma|},$$

or l'indice de G_σ dans $\mathrm{Gal}(K/k)$ est c, d'où le résultat. $\diamondsuit$

Corollaire 2.8.2 *Soit K une extension galoisienne de k. On a :*

$$d(P_{K/k}(1)) = \frac{1}{[K:k]}.$$

Corollaire 2.8.3 *Soient K et L deux extensions galoisiennes[10] de k, incluses dans une même clôture algébrique de k. On a :*

$$P_{K/k}(1) \succ P_{L/k}(1) \Longleftrightarrow K \subset L.$$

Démonstration. Si $K \subset L$, alors $P_{K/k}(1) \succ P_{L/k}(1)$. Réciproquement, si $P_{K/k}(1) \succ P_{L/k}(1)$, alors, comme

$$P_{KL/k}(1) = P_{K/k}(1) \cap P_{L/k}(1),$$

on a :

$$P_{KL/k}(1) \succ P_{L/k}(1).$$

Donc $d(P_{KL/k}(1)) \geqslant d(P_{L/k}(1))$, d'où, par le corollaire précédent, $[KL:k] \leqslant [L:k]$, donc $KL = L$, donc $K \subset L$. $\diamondsuit$

[10] Il est possible de supprimer l'hypothèse "L galoisienne".

A Les nombres idéaux

Au début du 19ième siècle, Sophie Germain prouva le dernier théorème de Fermat pour toute une classe d'exposants[11] , dont 5, 11, 23... A peu près à la même époque, Gabriel Lamé vint à bout de l'exposant 7. Après cela, l'Académie des sciences instaura un prix de 3000 francs et une médaille d'or pour la personne qui prouverait le grand théorème de Fermat. Les plus âpres compétiteurs étaient Lamé et Cauchy. Lors de la séance du 1er mars 1847, ils annoncèrent chacun avoir découvert une preuve. Voici, en simplifiant, quel était leur raisonnement : supposons que nous ayons $x^p + y^p = z^p$ avec p premier impair et x, y, et z dans $\mathbb{Z}$. Alors, en posant $\zeta = e^{\frac{2i\pi}{p}}$, on a : $y^p = z^p - x^p = (z-x)(z-\zeta x)\dots(z-\zeta^{p-1}x)$. On obtient donc une nouvelle factorisation de y^p, qui se factorisait déjà en $y^p = y \dots y$. Ceci contredit effectivement la factorialité de $\mathbb{Z}[\zeta]$. Or, par analogie avec $\mathbb{Z}$, les deux Français croyaient, chacun de leur côté, qu'ils pourraient facilement montrer que $\mathbb{Z}[\zeta]$ est toujours factoriel, et ainsi prouver le grand théorème de Fermat. Finalement, le 24 mai 1847, l'Académie reçut un courrier signé par Ernst Eduard Kummer, qui expliquait que $\mathbb{Z}[\zeta]$ n'était pas toujours factoriel, ruinant ainsi les espoirs de Lamé et Cauchy. Mais Kummer avait fait une autre découverte : il avait compris que, même si les nombres ordinaires se factorisaient mal, il était possible de considérer des *nombres idéaux* plus généraux qui, eux, se factorisent bien. Comment définir de tels nombres idéaux ? Clairement, un nombre idéal doit être uniquement déterminé par l'ensemble de ses multiples dans $\mathcal{O}_K$. On doit donc pouvoir identifier un nombre idéal $\mathfrak{i}$ à une certaine partie I de $\mathcal{O}_K$, de cette façon :

$$\forall x \in \mathcal{O}_K, \quad \mathfrak{i} \mid x \Longleftrightarrow x \in I$$

Maintenant, on peut supposer que certaines règles arithmétiques ordinaires doivent rester vraies pour les nombres idéaux. Nous allons en déduire les propriétés que doit vérifier $I \subset \mathcal{O}_K$. Pour commencer, on a la règle :

$$\forall x, y \in \mathcal{O}_K, \quad \mathfrak{i} \mid x \text{ et } \mathfrak{i} \mid y \Longrightarrow \mathfrak{i} \mid x - y.$$

Ceci se traduit par :

$$\forall x, y \in \mathcal{O}_K, \quad x \in I \text{ et } y \in I \Longrightarrow x - y \in I.$$

Ainsi, I est un sous-groupe additif de $\mathcal{O}_K$. Mais nous avons aussi la règle :

$$\forall x, y \in \mathcal{O}_K, \quad \mathfrak{i} \mid x \Longrightarrow \mathfrak{i} \mid xy.$$

Ceci se traduit par :

$$\forall x, y \in \mathcal{O}_K, \quad x \in I \Longrightarrow xy \in I.$$

Donc I est un idéal de $\mathcal{O}_K$, au sens moderne du terme. L'introduction des nombres idéaux a permis à Kummer de combler certaines lacunes dans les calculs de Lamé et Cauchy, et ainsi de démontrer le théorème de Fermat pour tous les exposants premiers[12] inférieurs à 100, sauf 37, 59 et 67. Le lecteur intéressé par ce sujet trouvera de plus amples informations dans [Neukirch 1] et [Koch 1].

[11] En fait pour tout exposant premier p tel que $2p+1$ est aussi premier. Un tel nombre premier p est depuis appelé un "nombre de Sophie Germain".

[12] Kummer a prouvé le théorème de Fermat pour tout exposant p "régulier". p est dit régulier ssi p ne divise pas le nombre de classes d'idéaux de $\mathbb{Q}(e^{2i\pi/p})$. Kummer a montré que p est régulier ssi p ne divise aucun des numérateurs des nombres de Bernoulli $B_2, B_4, \dots, B_{p-3}$.

B Factorisation explicite d'un idéal premier

Le lecteur a peut-être déjà entendu parler de la célèbre question suivante :

Question B.1 *Quels sont les nombres premiers p qui peuvent s'écrire $p = a^2 + b^2$, avec a et b entiers ?*

On peut remarquer que $a^2 + b^2 = (a + b\sqrt{-1})(a - b\sqrt{-1})$. Ainsi, p s'écrit $a^2 + b^2$ si, et seulement si p n'est pas irréductible dans $\mathbb{Z}[\sqrt{-1}]$. Or p est irréductible dans $\mathbb{Z}[\sqrt{-1}]$ si, et seulement si l'idéal $p\mathbb{Z}$ reste premier dans $\mathbb{Z}[\sqrt{-1}]$. Mais rappelons (exemple 1.2.2) que $\mathbb{Z}[\sqrt{-1}]$ est l'anneau des entiers de $\mathbb{Q}(\sqrt{-1})$. La question B.1 est donc équivalente à la suivante :

Question B.2 *Quels sont les idéaux premiers $\mathfrak{p}$ de $\mathbb{Q}$ qui ne restent pas premiers dans $\mathbb{Q}(\sqrt{-1})$?*

Afin de réprondre à cette question, prouvons la proposition suivante :

Proposition B.1 *Soit K/k une extension de corps de nombres telle que : $\exists \alpha \in \mathcal{O}_K$, $\mathcal{O}_K = \mathcal{O}_k[\alpha]$. Soit $u \in \mathcal{O}_k[X]$ le polynôme minimal de α sur k. Soit $\mathfrak{p}$ un idéal premier non nul de k, et $\widetilde{u} \in (\mathcal{O}_k/\mathfrak{p})[X]$ la réduction de $u \mod \mathfrak{p}$. Alors :*

$$\mathfrak{p} \text{ reste premier dans } K \iff \widetilde{u} \text{ est irréductible dans } (\mathcal{O}_k/\mathfrak{p})[X]. \tag{5}$$

$$\mathfrak{p} \text{ se ramifie dans } K \iff \widetilde{u} \text{ a un facteur multiple dans } (\mathcal{O}_k/\mathfrak{p})[X]. \tag{6}$$

Démonstration. L'application $X \mapsto \alpha$ donne un isomorphisme

$$\mathcal{O}_k[X]/(u) \longrightarrow \mathcal{O}_K.$$

Donc $\mathcal{O}_K/\mathfrak{p} = \mathcal{O}_k[X]/(u)/\mathfrak{p} = \mathcal{O}_k[X]/\mathfrak{p}/(\widetilde{u}) = (\mathcal{O}_k/\mathfrak{p})[X]/(\widetilde{u})$. Or, par définition, $\mathfrak{p}$ reste premier dans K $\iff \mathcal{O}_K/\mathfrak{p}$ est intègre. Donc c'est le cas ssi $(\mathcal{O}_k/\mathfrak{p})[X]/(\widetilde{u})$ est intègre, ssi $\widetilde{u}$ est irréductible. Donc (5) est déjà prouvée. Quant à (6), on peut remarquer que $\mathfrak{p}$ se ramifie dans K ssi $\mathcal{O}_K/\mathfrak{p}$ possède un nilpotent, ssi $(\mathcal{O}_k/\mathfrak{p})[X]/(\widetilde{u})$ possède un nilpotent. Donc c'est le cas ssi $\widetilde{u}$ a un facteur multiple dans $(\mathcal{O}_k/\mathfrak{p})[X]$. $\diamondsuit$

Appliquons ceci à $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{-1})$. A l'exemple 1.2.2 on a vu que : $\mathcal{O}_k = \mathbb{Z}$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$. Prenons $\alpha = \sqrt{-1}$. On a $u = X^2 + 1$. Donc la proposition nous dit que : pour tout nombre premier p, p peut s'écrire $a^2 + b^2$ ssi $X^2 + 1$ a une racine dans $\mathbb{Z}/p\mathbb{Z}$. C'est le cas ssi -1 est un carré dans $(\mathbb{Z}/p\mathbb{Z})^*$ ssi (exercice facile de théorie des groupes) $p = 2$ ou $p \equiv 1 \mod 4$. Voici donc la réponse à la question B.1 !

La généralisation suivante de la proposition B.1 permet d'écrire explicitement la factorisation de $\mathfrak{p}$:

Proposition B.2 *Avec les notations de la proposition B.1, écrivons $\widetilde{u} = \widetilde{u}_1^{e_1} \dots \widetilde{u}_r^{e_r}$ la décomposition de $\widetilde{u}$ en produit d'irréductibles. Pour tout i, soit $u_i \in \mathcal{O}_k[x]$ un polynôme unitaire tel que $u_i \mod \mathfrak{p} = \widetilde{u}_i$. Alors, dans K, $\mathfrak{p}$ admet la décomposition*

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r},$$

où $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_K + u_i(\alpha)\mathcal{O}_K$. De plus, le degré (résiduel) de $\mathfrak{P}_i$ est égal à $\deg u_i$.

Démonstration. C'est un calcul d'une bonne page dont nous avons déjà fait une partie. Le reste est dans [Neukirch 1], entre autres. $\diamondsuit$

C Théorème de Dirichlet généralisé

Comme d'habitude, k désigne un corps de nombres. Soit $\mathfrak{c}$ un cycle de k et H un groupe tel que $P_{\mathfrak{c}} \subset H \subset I(\mathfrak{c})$.

Théorème C.1 *Soit $\chi \neq 1$ un caractère de $I(\mathfrak{c})/H$. Alors :*

$$L_{\mathfrak{c}}(1, \chi) \neq 0.$$

Démonstration. Appliquons le théorème d'existence 2.6.3. On obtient une extension abélienne K/k, non ramifiée en dehors de $\mathfrak{c}$, telle que $H = P_{\mathfrak{c}}\mathfrak{N}(\mathfrak{c},\, K/k)$. Donc χ est un caractère de $I(\mathfrak{c})/P_{\mathfrak{c}}\mathfrak{N}(\mathfrak{c},\, K/k)$. Par le théorème 2.5.3, $L_{\mathfrak{c}}(1, \chi) \neq 0$. $\diamondsuit$

Corollaire C.2 (théorème de Dirichlet généralisé) *Soit $h = |I(\mathfrak{c})/H|$. Pour tout $\mathfrak{A} \in I(\mathfrak{c})/H$, on a :*

$$d(\mathfrak{A}) = \frac{1}{h}\cdot$$

Démonstration. Grâce au théorème C.1, nous pouvons appliquer le théorème 2.7.1, qui donne immédiatement le résultat. $\diamondsuit$

D Références

Par ordre décroissant d'utilisation pour la rédaction de ce mémoire :

[Lang 1]
S. Lang, *Algebraic number theory*, Springer

[Neukirch 1]
J. Neukirch, *Algebraic number theory*, Springer

[Milne]
www.jmilne.org

[Lang 2]
S. Lang, *Algebra*, Addison-Wesley

[Silverman 1]
J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer (pour les rappels de théorie du corps de classes).

[Serre 1]
J.-P. Serre, *Corps locaux*, Hermann

[Koch 1]
H. Koch, *Algebraic number theory*, Springer