Théorie des nombres – notes du cours de Guy Henniart

François Maillot

1er janvier 2007

Table des matières

Chapitre 1

Rappels sur la théorie des corps et la théorie de Galois

Sauf mention explicite du contraire, les corps considérés sont commutatifs.

1.1 Normes et traces

Une extension d'un corps $\mathbf{F}$ est la donnée d'un corps $\mathbf{E}$ et d'un homomorphisme de corps $\iota : \mathbf{F} \to \mathbf{E}$. L'homomorphisme ι est injectif et en général on identifie $\mathbf{F}$ à son image.

L'extension $\mathbf{E}/\mathbf{F}$ est dite finie si $\mathbf{E}$ et un $\mathbf{F}$-espace vectorielde dimension finie. Sa dimension est notée $[\mathbf{E} : \mathbf{F}] = \dim_{\mathbf{F}} \mathbf{E}$.

Définition 1.1.1. *Soit $\mathbf{E}/\mathbf{F}$ une extension finie de degré d, soit $x \in \mathbf{E}$.*

$m_x : y \mapsto x.y$ est $\mathbf{F}$-linéaire. Son polynôme caractéristique est :
$X^d - Tr_{\mathbf{E}/\mathbf{F}}(x)X^{d-1} + \cdots + (-1)^d N_{\mathbf{E}/\mathbf{F}}(x)$
$Tr_{\mathbf{E}/\mathbf{F}}$ est la trace de $\mathbf{E}$ sur $\mathbf{F}$, $N_{\mathbf{E}/\mathbf{F}}$ la norme de $\mathbf{E}$ sur $\mathbf{F}$.

Proposition 1.1.2. *$Tr_{\mathbf{E}/\mathbf{F}}$ est une forme linéaire sur $\mathbf{E}$.*
$N_{\mathbf{E}/\mathbf{F}}$ est multiplicative : $N_{\mathbf{E}/\mathbf{F}}(x.x') = N_{\mathbf{E}/\mathbf{F}}(x).N_{\mathbf{E}/\mathbf{F}}(x')$
Propriétés de transitivité :
Si $\mathbf{E}'/\mathbf{E}$ est finie,
- $[\mathbf{E}' : \mathbf{F}] = [\mathbf{E}' : \mathbf{E}][\mathbf{E} : \mathbf{F}]$
- $Tr_{\mathbf{E}/\mathbf{F}}\left(Tr_{\mathbf{E}'/\mathbf{E}}\right) = Tr_{\mathbf{E}'/\mathbf{F}}$
- $N_{\mathbf{E}/\mathbf{F}}\left(N_{\mathbf{E}'/\mathbf{E}}\right) = N_{\mathbf{E}'/\mathbf{F}}$

Définition 1.1.3. *Séparabilité :*
Un polynôme $P \in \mathbf{F}[X]$ est dit séparable s'il est premier avec sa dérivée.
Un élément x de $\mathbf{E}/\mathbf{F}$ est séparable si son polynôme minimal sur $\mathbf{F}$ est séparable.
Une extension $\mathbf{E}/\mathbf{F}$ est séparable si tous les éléments de $\mathbf{E}$ sont séparables.

Remarque 1.1.4. *Un polynôme P est non séparable si et seulement si $car(\mathbf{F}) = p > 0$ et P est un polynôme en X^p. L'extension $\mathbf{E}/\mathbf{F}$ est séparable si et seulement si $Tr_{\mathbf{E}/\mathbf{F}} \neq 0$. Un polynôme P est séparable si et seulement si son discriminant est non nul.*

Théorème 1.1.5 (Théorème de l'élément primitif)**.** *Si $\mathbf{E}/\mathbf{F}$ est finie séparable alors il existe $x \in \mathbf{E}$ tel que $E = \mathbf{F}[x]$.*

1.2 Théorie de Galois

Soit $\mathbf{E}/\mathbf{F}$ une extension de corps. On note $Aut(\mathbf{E}/\mathbf{F})$ le groupe des automorphismes $\mathbf{F}$-linéaires du corps $\mathbf{E}$ et $A^B = \{(x \in A)(\forall \sigma \in B)(\sigma(x) = x)\}$.

Théorème 1.2.1. *Les propositions suivantes sont équivalentes :*

1. *Il existe un sous-groupe G de $Aut(\mathbf{E}/\mathbf{F})$ tel que $\mathbf{F} = \mathbf{E}^G$.*
2. *Pour tout $x \in \mathbf{E}$ le polynôme minimal de x sur $\mathbf{F}$ est séparable scindé dans $\mathbf{E}[X]$.*
3. *Le corps $\mathbf{E}$ est engendré sur $\mathbf{F}$ par les racines d'un polynôme séparable.*

Alors $G = Aut(\mathbf{E}/\mathbf{F})$ et $|G| = [\mathbf{E} : \mathbf{F}]$.

Définition 1.2.2. *Une extension qui vérifie ces conditions est dite galoisienne.*

Si G est un sous-groupe de $Aut(\mathbf{E}/\mathbf{F})$ alors $[\mathbf{E} : \mathbf{E}^G] = |G|$ et $G = Aut(\mathbf{E}/\mathbf{E}^G)$.

Si $\mathbf{E}/\mathbf{F}$ est galoisienne alors on écrit $Gal(\mathbf{E}/\mathbf{F})$ plutôt que $Aut(\mathbf{E}/\mathbf{F})$.

Théorème 1.2.3 (Théorème fondamental de la théorie de Galois)**.**
Soit $\mathbf{E}/\mathbf{F}$ finie galoisienne de groupe de Galois G.
$\mathbf{F} \subseteq \mathbf{K} \subseteq \mathbf{E}$

1. *$\mathbf{K} \longmapsto Gal(\mathbf{E}/\mathbf{K})$ et $H \longmapsto \mathbf{E}^H$ sont des bijections réciproques l'une de l'autre.*
2. *$\mathbf{K}$ est galoisienne sur $\mathbf{F}$ si et seulement si $H \triangleleft G$. En ce cas*

$$G \to Gal(\mathbf{K}/\mathbf{F})$$
$$\sigma \mapsto \sigma|_{\mathbf{K}}$$

est un morphisme de groupes trivial sur H qui induit un isomorphisme entre G/H et $Gal(\mathbf{K}/\mathbf{F})$.

Remarque 1.2.4. *Soit $\mathbf{K} \subseteq \mathbf{F}$ et $H = Gal(\mathbf{F}/\mathbf{K})$. Soit $x \in \mathbf{K}$. On a :*

$$Tr_{\mathbf{K}/\mathbf{F}}(x) = \sum_{\sigma \in G/H} \sigma(x)$$
$$N_{\mathbf{K}/\mathbf{F}}(x) = \prod_{\sigma \in G/H} \sigma(x)$$

Définition 1.2.5. *Soit* $\mathbf{E}/\mathbf{F}$ *une extension finie. On dit que* $\mathbf{E}/\mathbf{F}$ *est abélienne si elle est galoisienne de groupe de Galois abélien.*

1.3 Isomorphismes

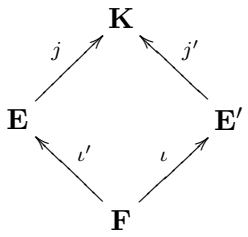
Soit $\mathbf{E}/\mathbf{F}$ une extension finie galoisienne. $\mathbf{E}$ est alors corps de décomposition sur $\mathbf{F}$ d'un polynôme séparable $P \in \mathbf{F}[X]$. Si on dispose d'une extension $\mathbf{F}'/\mathbf{F}$ qui contienne un corps de décomposition $\mathbf{E}'$ sur $\mathbf{F}$ de P (par exemple si $\mathbf{F}'$ est algébriquement clos) alors $\mathbf{E}'$ est l'unique sous-extension de $\mathbf{F}$ dans $\mathbf{F}'$ isomorphe à $\mathbf{E}/\mathbf{F}$.

Un $\mathbf{F}$-isomorphisme $\tau : \mathbf{E} \to \mathbf{E}'$ donne un isomorphisme de groupes entre $Gal(\mathbf{E}/\mathbf{F})$ et $Gal(\mathbf{E}'/\mathbf{F}')$ défini par $\sigma \mapsto \tau\sigma\tau^{-1}$.

Si $\mathbf{E}/\mathbf{F}$ est abélienne cet isomorphisme ne dépend pas du choix de τ.

1.4 Composés

Soient $\iota : \mathbf{F} \to \mathbf{E}$ et $\iota' : \mathbf{F} \to \mathbf{E}'$ deux extensions finies de $\mathbf{F}$. Une extension composée de $\mathbf{E}/\mathbf{F}$ et $\mathbf{E}'/\mathbf{F}$ est une extension $\mathbf{K}$ commune à $\mathbf{E}$ et $\mathbf{E}'$, disons $j : \mathbf{E} \to \mathbf{K}$ et $j' : \mathbf{E}' \to \mathbf{K}$ vérifiant $j \circ \iota = j' \circ \iota'$, telle que $\mathbf{K}$ soit engendrée par $j(\mathbf{E}) \cup j'(\mathbf{E}')$.



On a un morphisme d'algèbres $\mathbf{E} \otimes \mathbf{E}' \to \mathbf{K}$. Les composés (à isomorphisme près) correspondent aux corps quotients de la $\mathbf{F}$-algèbre $\mathbf{E} \otimes \mathbf{E}'$, et en particulier il en existe toujours. Si par exemple $\mathbf{L}$ est une extension algébriquement close de $\mathbf{F}$ alors il existe deux $\mathbf{F}$-isomorphismes :

$$\alpha : \mathbf{E} \to \text{un sous-corps de } \mathbf{L}$$
$$\alpha' : \mathbf{E}' \to \text{un sous-corps de } \mathbf{L}$$

et on peut prendre pour l'extension composée de $\mathbf{E}$ et $\mathbf{E}'$ le sous-corps de $\mathbf{L}$ engendré par $\alpha(\mathbf{E}) \cup \alpha'(\mathbf{E}')$.

1.5 Corps finis

Théorème 1.5.1 (Théorème de Wedderburn)**.**

Toute algèbre à division finie est un corps.

Un corps fini $\mathbf{k}$ a pour caractéristique un nombre premier p. Son sous-corps premier est isomorphe à $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Le corps $\mathbf{k}$ vu en tant qu'espace vectoriel est de dimension finie d sur $\mathbb{F}_p$ et $|\mathbf{k}| = p^d$.

Théorème 1.5.2. *Soit p premier, $q = p^d$. Alors il existe un corps fini $\mathbf{k}$ de cardinal q unique à isomorphisme près. C'est un corps de décomposition sur $\mathbb{F}_p$ de $X^q - X \in \mathbb{F}_p[X]$, noté $\mathbb{F}_q$.*

Théorème 1.5.3. *Une extension $\mathbf{l}/\mathbf{k}$ de corps finis est finie. Elle est galoisienne de groupe de Galois cyclique engendré par l'homomorphisme de Frobenius :*

$$\begin{array}{ccc} \mathbf{l} & \longrightarrow & \mathbf{l} \\ x & \longmapsto & x^q \qquad \text{où } q = |\mathbf{k}| \end{array}$$

d'ordre $d = [\mathbf{l} : \mathbf{k}]$

Remarque 1.5.4. *Si $\mathbf{k}$ est fini, $d \in \mathbb{N} - \{0\}$, il existe une extension $\mathbf{l}$ de $\mathbf{k}$ de degré d unique à $\mathbf{k}$-isomorphisme près. Elle est galoisienne et $Gal(\mathbf{l}/\mathbf{k})$ est cyclique de degré d. Pour tout $e|d$ il existe une unique extension $\mathbf{k} \subseteq \mathbf{k}_e \subseteq \mathbf{l}$ avec $[\mathbf{k}_e : \mathbf{k}] = e$. Elle est galoisienne sur $\mathbf{k}$.*

1.6 Cyclotomie

Soit $\mathbf{F}$ un corps et $n \geqslant 1$. Une extension de décomposition sur $\mathbf{F}$ du polynôme $X^n - 1 \in \mathbf{F}[X]$ s'appelle corps des racines n-ièmes de l'unité sur $\mathbf{F}$. On note souvent $\mathbf{F}(\zeta_n)$ ou $\mathbf{F}(\mu_n)$. Si on dispose d'une clôture algébrique $\bar{\mathbf{F}}$ de $\mathbf{F}$ on peut prendre l'unique corps de décomposition inclus dans $\bar{\mathbf{F}}$. Si $\mathbf{F} = \mathbb{Q}$, $\mathbb{Q}(\zeta_n)$ désigne souvent $\mathbb{Q}\left(e^{\frac{2\imath\pi}{n}}\right) \subseteq \bar{\mathbb{Q}} \subseteq \mathbb{C}$.

$$\begin{aligned} P &= X^n - 1 \\ P' &= nX^{n-1} \end{aligned}$$

donc si n est premier à la caractéristique de $\mathbf{F}$ alors P est séparable et $\mathbf{F}(\zeta_n)/\mathbf{F}$ est galoisienne. En ce cas $X^n - 1$ a exactement n racines dans $\mathbf{F}(\zeta_n)$. Ces racines forment un groupe multiplicatif μ_n cyclique car tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique. Les générateurs sont appelés racines primitives n-ièmes de l'unité. On a alors un homomorphisme de groupes

$$\begin{array}{ccc} Gal\left(\mathbf{F}(\zeta_n)/\mathbf{F}\right) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma & \longmapsto & \bar{a} \end{array}$$

où a est tel que $\sigma(\zeta) = \zeta^a$.

Définition 1.6.1.
$n \geqslant 1$. $\Phi_n \in \mathbb{C}[X]$ est défini par :

$$\Phi_n(X) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} \left(X - e^{\frac{i2k\pi}{n}}\right)$$

Proposition 1.6.2.

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Par récurrence, $\Phi_n \in \mathbb{Z}[X]$ et est unitaire de degré $\varphi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right|$.

Théorème 1.6.3. *Φ_n est irréductible dans $\mathbb{Q}[X]$.*

Corollaire 1.6.4. *$|\mathbb{Q}(\zeta_n)/\mathbb{Q}| = \varphi(n)$ car $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est galoisienne de groupe de Galois isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times$.*

En effet on sait déjà que $[\mathbb{Q}(\zeta_n)/\mathbb{Q}] \leqslant \varphi(n)$. Φ_n est irréductible sur $\mathbb{Q}$ et $\zeta^{\frac{i2\pi}{n}}$ est racine de Φ_n.

$\mathbb{Q}(\zeta_n)$ contient un corps de rupture de Φ_n sur $\mathbb{Q}$.

En particulier $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \geqslant d^\circ\Phi_n = \varphi(n)$, d'où égalité et surjectivité donc bijectivité du morphisme injectif de $Gal\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$.

Théorème 1.6.5 (Théorème de Kronecker-Weber)**.** *Toute extension abélienne finie de $\mathbb{Q}$ est cyclotomique. Plus précisément, si $\mathbf{E}/\mathbb{Q}$ est une extension abélienne alors il existe un entier $n \geqslant 1$ et une sous-extension $\mathbf{K}$ de $\mathbb{Q}(\zeta_n)$ telle que $\mathbf{E} \simeq \mathbf{K}$*

La «théorie du corps de classes» vise à décrire toutes les extensions finies abéliennes d'un corps de nombres $\mathbf{F}$.

Remarque 1.6.6. *Soit $n \geqslant 1$, on dispose de $\Phi_n \in \mathbb{Z}[X]$.*

Si p est un nombre premier, alors en général Φ_n mod $p \in \mathbb{F}_p[X]$ n'est pas irréductible. En fait, $Gal\left(\mathbb{F}_p(\zeta_n)\right)$ s'injecte dans $(\mathbb{Z}/n\mathbb{Z})^\times$: c'est le sous-groupe engendré par p mod n.

Si l'ordre de p mod n dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est d alors $\mathbb{F}_p(\zeta_n)$ est de degré d sur $\mathbb{F}_p$ et Φ_n mod p est produit de $\varphi(n)/d$ polynômes irréductibles distincts dans $\mathbb{F}_p[X]$.

La «théorie du corps de classes» vise pour un corps de nombres fixé $\mathbf{F}$ non seulement à décrire les extensions abéliennes finies $\mathbf{E}/\mathbf{F}$ mais aussi si $\mathbf{E} = \mathbf{F}[x]$ et φ est le polynôme minimal de x sur $\mathbf{F}$ à décrire la décomposition en facteurs irréductibles de φ modulo $\mathfrak{p}$ où $\mathfrak{p}$ parcourt les idéaux maximaux de $\mathcal{O}_\mathbf{F}$, anneau des entiers de $\mathbf{F}$.

Chapitre 2

Décomposition et théorie de Galois

2.1 Idéaux premiers et décomposition

Soit $\mathbf{K}$ un corps de nombres, $\mathcal{O}_{\mathbf{K}}$ son anneau des entiers, à savoir l'ensemble des éléments de $\mathbf{K}$ racines d'un polynôme unitaire à coefficients dans $\mathbb{Z}$.

L'anneau des entiers de $\mathbf{K}$, $\mathcal{O}_{\mathbf{K}}$, est un anneau de Dedekind libre comme $\mathbb{Z}$-module et de rang fini $[\mathbf{K} : \mathfrak{q}]$.

Si $\mathfrak{a}$ est un idéal non nul de $\mathcal{O}_{\mathbf{K}}$ alors $\mathcal{O}_{\mathbf{K}}/\mathfrak{a}$ est fini et on note $N(\mathfrak{a}) = |\mathcal{O}_{\mathbf{K}}/\mathfrak{a}|$ la norme de l'idéal $\mathfrak{a}$. Si $\mathfrak{b}$ est un autre idéal non nul de $\mathcal{O}_{\mathbf{K}}$ on a $N(\mathfrak{ab}) = N(\mathfrak{a})\,N(\mathfrak{b})$.

Rappel 2.1.1. *Pour les anneaux de Dedekind, voir [5] mais aussi [3].*

Un anneau de Dedekind est un anneau commutatif intègre noethérien intégralement clos dans lequel tout idéal premier est maximal.

La propriété principale des anneaux de Dedekind est que tout idéal non nul est produit d'idéaux maximaux, et que cette écriture est unique à l'ordre près des facteurs.

Si $\mathfrak{p}$ est un idéal maximal d'un anneau de Dedekind $\mathcal{A}$ et $\mathfrak{a}$ un idéal non nul, on note $\nu_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{N}$ le nombre de fois qu'intervient $\mathfrak{p}$ dans l'écriture de $\mathfrak{a}$ comme produit d'idéaux maximaux.

Si $\mathfrak{a}$ est fixé, $\nu_{\mathfrak{p}}(\mathfrak{a}) = 0$ sauf pour un nombre fini de $\mathfrak{p}$ et on écrit :

$$\mathfrak{a} = \prod_{\mathfrak{p}\ maximaux} \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})}$$

Dans un anneau de Dedekind $\mathcal{A}$, si on dispose de deux idéaux non nuls $\mathfrak{a}$ et $\mathfrak{b}$, $\mathfrak{a} \subseteq \mathfrak{b}$ équivaut à l'existence d'un idéal $\mathfrak{c}$ tel que $\mathfrak{a} = \mathfrak{bc}$.

Soit $\mathbf{E}/\mathbf{F}$ une extension finie de corps de nombres. On a alors $\mathcal{O}_{\mathbf{F}} \subseteq \mathcal{O}_{\mathbf{E}}$. Si $\mathfrak{p}$ est un idéal maximal de $\mathcal{O}_{\mathbf{F}}$ on peut former $\mathfrak{p}\mathcal{O}_{\mathbf{E}}$, l'idéal de $\mathcal{O}_{\mathbf{E}}$ engendré

par $\mathfrak{p}$. En général l'idéal $\mathfrak{p}\mathcal{O}_{\mathbf{E}}$ n'est *pas* maximal. Il peut alors s'écrire comme produit d'idéaux maximaux de $\mathcal{O}_{\mathbf{E}}$ (en effet $\mathfrak{p}\mathcal{O}_{\mathbf{E}}$ est non nul car $\mathfrak{p} \subseteq \mathfrak{p}\mathcal{O}_{\mathbf{E}}$) :

$$\mathfrak{p}\mathcal{O}_{\mathbf{E}} = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})}$$

le produit étant réalisé sur les idéaux maximaux d'$\mathcal{O}_{\mathbf{E}}$ contenant $\mathfrak{p}\mathcal{O}_{\mathbf{E}}$ et l'exposant $e(\mathfrak{q}|\mathfrak{p})$ étant strictement positif.

On dit que $\mathfrak{q}$ est *au-dessus de* $\mathfrak{p}$ et on note $\mathfrak{q}|\mathfrak{p}$.

Remarque 2.1.2. *Si l'idéal maximal d'*$\mathcal{O}_{\mathbf{E}}$ $\mathfrak{q}$ *contient* $\mathfrak{p}\mathcal{O}_{\mathbf{E}}$ *alors* $\mathfrak{q} \cap \mathcal{O}_{\mathbf{F}}$ *contient* $\mathfrak{p}$. *Mais* $\mathfrak{q} \cap \mathcal{O}_{\mathbf{F}}$ *est nécessairement un idéal de* $\mathcal{O}_{\mathbf{F}}$ *donc c'est* $\mathcal{O}_{\mathbf{F}}$ *ou* $\mathfrak{p}$. *Si* $\mathfrak{q} \cap \mathcal{O}_{\mathbf{F}} = \mathcal{O}_{\mathbf{F}}$ *alors* $1 \in \mathfrak{q}$, *ce qui est impossible. On a donc* $\mathfrak{q} \cap \mathcal{O}_{\mathbf{F}} = \mathfrak{p}$.

Définition 2.1.3. *L'exposant* $e(\mathfrak{q}|\mathfrak{p})$ *s'appelle le degré (ou indice) de ramification de* $\mathfrak{q}$ *au-dessus de* $\mathfrak{p}$.

Considérons le diagramme suivant :

$$\begin{array}{ccc} \mathcal{O}_{\mathbf{F}} & \hookrightarrow & \mathcal{O}_{\mathbf{E}} \\ \downarrow & & \downarrow \\ \mathcal{O}_{\mathbf{F}}/\mathfrak{p} & \hookrightarrow & \mathcal{O}_{\mathbf{E}}/\mathfrak{q} \end{array}$$

Remarquons que par maximalité des idéaux $\mathfrak{p}$ et $\mathfrak{q}$ la ligne du bas donne un morphisme de corps : $\mathcal{O}_{\mathbf{E}}/\mathfrak{q}$ est une extension finie de $\mathcal{O}_{\mathbf{F}}/\mathfrak{p}$.

Définition 2.1.4. *Le degré de cette extension est noté* $f(\mathfrak{q}|\mathfrak{p})$ *et appelé degré (ou indice) d'inertie de* $\mathfrak{q}$ *au-dessus de* $\mathfrak{p}$.

Définition 2.1.5. *Soit* $\mathfrak{p}$ *un idéal d'*$\mathcal{O}_{\mathbf{F}}$ *et* $\mathfrak{q}$ *un idéal d'*$\mathcal{O}_{\mathbf{E}}$ *au-dessus de* $\mathfrak{p}$.

On dit que $\mathfrak{q}$ *est non-ramifié au-dessus de* $\mathfrak{p}$ *si* $e(\mathfrak{q}/\mathfrak{p}) = 1$.

On dit que $\mathfrak{p}$ *est non-ramifié dans* $\mathbf{E}/\mathbf{F}$ *si* $e(\mathfrak{q}/\mathfrak{p}) = 1$ *pour tout* $\mathfrak{q}$ *au-dessus de* $\mathfrak{p}$.

On dit que $\mathfrak{p}$ *est totalement décomposé dans* $\mathbf{E}/\mathbf{F}$ *si on a* $e(\mathfrak{p}/\mathfrak{q}) = f(\mathfrak{q}/\mathfrak{p}) = 1$ *pour tout* $\mathfrak{q}$ *au-dessus de* $\mathfrak{p}$.

Si $\mathfrak{q}'$ est un idéal maximal de $\mathcal{O}_{\mathbf{E}'}$ au-dessus de $\mathfrak{p}$ alors $\mathfrak{q}' \cap \mathcal{O}_{\mathbf{E}}$ est un idéal maximal de $\mathcal{O}_{\mathbf{E}}$ au-dessus de $\mathfrak{p}$. La maximalité vient de :

$$\mathcal{O}_{\mathbf{E}}/(\mathfrak{q}' \cap \mathcal{O}_{\mathbf{E}}) \hookrightarrow \mathcal{O}_{\mathbf{E}'}/\mathfrak{q}'$$

et du fait qu'un sous-anneau d'un corps fini est un corps.

Propriétés de transitivité

Soit :

- $\mathfrak{p}$ un idéal maximal d'$\mathcal{O}_{\mathbf{F}}$
- $\mathfrak{q}$ un idéal maximal d'$\mathcal{O}_{\mathbf{E}}$ au-dessus de $\mathfrak{p}$
- $\mathfrak{q}'$ un idéal maximal d'$\mathcal{O}_{\mathbf{E}'}$ au-dessus de $\mathfrak{q}$

Alors on a :

- $e(\mathfrak{q}'|\mathfrak{p}) = e(\mathfrak{q}'|\mathfrak{q})\, e(\mathfrak{q}|\mathfrak{p})$
- $f(\mathfrak{q}'|\mathfrak{p}) = f(\mathfrak{q}'|\mathfrak{q})\, f(\mathfrak{q}|\mathfrak{p})$

Démonstration. En utilisant l'unicité de la décomposition en produit d'idéaux maximaux. □

Proposition 2.1.6. *Soit* $\mathbf{E}/\mathbf{F}$ *une extension finie de corps de nombres,* $\mathfrak{p}$ *un idéal maximal d'*$\mathcal{O}_\mathbf{F}$*. Alors :*

$$\sum_{\mathfrak{q}|\mathfrak{p}} e(\mathfrak{q}|\mathfrak{p})\, f(\mathfrak{q}|\mathfrak{p}) = [\mathbf{E} : \mathbf{F}]$$

Démonstration. $\mathcal{O}_\mathbf{E}/\mathfrak{p}\mathcal{O}_\mathbf{E}$ est un $\mathcal{O}_\mathbf{F}/\mathfrak{p}$-espace vectoriel. Montrons d'abord le lemme suivant :

Lemme 2.1.7. *La dimension d'*$\mathcal{O}_\mathbf{E}/\mathfrak{p}\mathcal{O}_\mathbf{E}$ *sur* $\mathcal{O}_\mathbf{F}/\mathfrak{p}$ *vaut*

$$\sum_{\mathfrak{q}|\mathfrak{p}} e(\mathfrak{q}|\mathfrak{p})\, f(\mathfrak{q}|\mathfrak{p})$$

Démonstration du lemme. Notons $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ les idéaux $\mathfrak{q}$ au-dessus de $\mathfrak{p}$ et $e_i = e(\mathfrak{q}_i|\mathfrak{p})$. On a la suite d'inclusions :

$$\mathcal{O}_\mathbf{E} \supseteq \mathfrak{q}_1 \supseteq \mathfrak{q}_1^2 \supseteq \cdots \supseteq \mathfrak{q}_1^{e_1} \supseteq \mathfrak{q}_1^{e_1}\mathfrak{q}_2 \supseteq \cdots \supseteq \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2} \supseteq \cdots \supseteq \mathfrak{p}\mathcal{O}_\mathbf{E}$$

Comme $\mathcal{O}_\mathbf{E}$ est un anneau de Dedekind, on voit facilement qu'il n'y a pas d'idéal d'$\mathcal{O}_\mathbf{E}$ entre deux termes successifs.

Remarquons que $\mathfrak{R} = \mathfrak{q}_1^{e_1} \ldots \mathfrak{q}_{\alpha-1}^{e_{\alpha-1}}\mathfrak{q}_\alpha^{\beta}/\mathfrak{q}_1^{e_1} \ldots \mathfrak{q}_{\alpha-1}^{e_{\alpha-1}}\mathfrak{q}_\alpha^{\beta+1}$ est un $\mathcal{O}_\mathbf{E}$-module annulé par $\mathfrak{q}_\alpha$ donc un $\mathcal{O}_\mathbf{E}/\mathfrak{q}_\alpha$-espace vectoriel. Le fait qu'il n'y ait pas d'idéal d'$\mathcal{O}_\mathbf{E}$ entre deux termes successifs de la suite signifie que cet espace vectoriel n'admet pas de sous-espace vectoriel strict non trivial, donc que $\dim_{\mathcal{O}_\mathbf{E}/\mathfrak{q}_\alpha} \mathfrak{R} = 1$, d'où on déduit $\dim_{\mathcal{O}_\mathbf{F}/\mathfrak{p}} \mathfrak{R} = f(\mathfrak{q}_\alpha|\mathfrak{p})$.

Comme on dispose de la tour d'extensions :

$$\mathcal{O}_\mathbf{E} \supseteq \mathfrak{q}_1 \supseteq \mathfrak{q}_1^2 \supseteq \cdots \supseteq \mathfrak{q}_1^{e_1} \supseteq \mathfrak{q}_1^{e_1}\mathfrak{q}_2 \supseteq \cdots \supseteq \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2} \supseteq \cdots \supseteq \mathfrak{p}\mathcal{O}_\mathbf{E}$$

on en déduit, $\dim_{\mathcal{O}_\mathbf{F}/\mathfrak{p}}(\mathcal{O}_\mathbf{E}/\mathfrak{p}\mathcal{O}_\mathbf{E})$ étant la somme des dimensions sur $\mathcal{O}_\mathbf{F}/\mathfrak{p}$ des quotients successifs :

$$\sum_{\mathfrak{q}|\mathfrak{p}} e(\mathfrak{q}|\mathfrak{p})\, f(\mathfrak{q}|\mathfrak{p}) = \dim_{\mathcal{O}_\mathbf{F}/\mathfrak{p}}(\mathcal{O}_\mathbf{E}/\mathfrak{p}\mathcal{O}_\mathbf{E})$$

□

Prouvons ensuite $\dim_{\mathcal{O}_\mathbf{F}/\mathfrak{p}}(\mathcal{O}_\mathbf{E}/\mathfrak{q}) = [\mathbf{E} : \mathbf{F}]$ dans le cas où $\mathcal{O}_\mathbf{F}$ est principal :

Démonstration dans le cas principal. $\mathcal{O}_{\mathbf{E}}$ est un $\mathbb{Z}$-module libre de type fini donc c'est un $\mathcal{O}_{\mathbf{F}}$-module de type fini sans torsion. Il est donc libre de type fini sur $\mathcal{O}_{\mathbf{F}}$.

On voit facilement que si $(e_1, \ldots, e_d)$ est une base de $\mathcal{O}_{\mathbf{E}}$ sur $\mathcal{O}_{\mathbf{F}}$ c'est aussi une base de $\mathbf{E}$ sur $\mathbf{F}$. Le rang de $\mathcal{O}_{\mathbf{E}}$ sur $\mathcal{O}_{\mathbf{F}}$ est alors $[\mathbf{E} : \mathbf{F}]$. Mais le rang de $\mathcal{O}_{\mathbf{E}}/\mathfrak{p}\mathcal{O}_{\mathbf{E}}$ sur $\mathcal{O}_{\mathbf{F}}/\mathfrak{p}$ est aussi $[\mathbf{E} : \mathbf{F}]$. □

Pour démontrer le résultat dans le cas général, on va se ramener au cas où $\mathcal{O}_{\mathbf{F}}$ est principal par localisation.

Rappels sur la localisation

Soit $\mathcal{A}$ un anneau commutatif intègre et $\mathbf{K}$ son corps des fractions. Supposons que $\mathcal{S} \subseteq \mathcal{A}$ est une partie multiplicative (i.e. stable par produit de deux de ses éléments) contenant 1 et pas 0.

Posons $\mathcal{S}^{-1}\mathcal{A} = \left\{s^{-1}a, s \in \mathcal{S}, a \ \in \mathcal{A}\right\}$. C'est un sous-anneau de $\mathbf{K}$ appelé *localisé de $\mathcal{A}$ en $\mathcal{S}$*.

Que se passe-t-il pour les idéaux ?

Notons $\mathcal{A}' = \mathcal{S}^{-1}\mathcal{A}$. Si $\mathfrak{a}$ est un idéal de $\mathcal{A}$ alors $\mathfrak{a}\mathcal{A} = \mathcal{S}^{-1}\mathfrak{a}$ est un idéal de $\mathfrak{a}'$. Réciproquement si $\mathfrak{a}'$ est un idéal de $\mathcal{A}'$ alors $\mathfrak{a}' \cap \mathcal{A}$ est un idéal de $\mathcal{A}$ et $\mathfrak{a}' = (\mathfrak{a}' \cap \mathcal{A})\,\mathcal{A}'$.

L'égalité ci-dessus implique en particulier que $\mathfrak{a}' \mapsto \mathfrak{a}' \cap \mathcal{A}$ est une injection (par ailleurs croissante) de l'ensemble des idéaux de $\mathcal{A}'$ dans l'ensemble des idéaux de $\mathcal{A}$.

Restreinte aux idéaux premiers, cette application est un isomorphisme d'ensembles ordonnés de l'ensemble des idéaux premiers de $\mathcal{A}'$ dans l'ensemble des idéaux premiers de $\mathcal{A}$ ne rencontrant pas $\mathcal{S}$.

Si $\mathcal{A}$ est noethérien, $\mathcal{A}'$ aussi. Si $\mathcal{A}$ est intégralement clos, $\mathcal{A}'$ aussi. Plus précisément, si $\mathcal{B}$ est la clôture intégrale de $\mathcal{A}$ dans $\mathbf{K}$, alors celle de $\mathcal{S}^{-1}\mathcal{A}$ est $\mathcal{S}^{-1}\mathcal{B}$. On déduit des résultats précédents que si $\mathcal{A}$ est de Dedekind, alors $\mathcal{A}'$ aussi.

Exemple 2.1.8. *Soit $\mathcal{A}$ un anneau de Dedekind, $\mathfrak{p}$ un idéal maximal de $\mathcal{A}$ et $\mathcal{S} = \mathcal{A} - \mathfrak{p}$. $\mathcal{S}^{-1}\mathcal{A}$ est alors un anneau de Dedekind. Le seul idéal maximal de $\mathcal{A}$ ne rencontrant pas $\mathcal{S}$ est $\mathfrak{p}$. $\mathcal{S}^{-1}\mathcal{A}$ est donc un anneau local d'idéal maximal $\mathcal{S}^{-1}\mathfrak{p} = \mathfrak{p}\mathcal{A}'$. Il est donc principal, et ses idéaux sont les $\left(\left(\mathcal{S}^{-1}\mathfrak{p}\right)^k\right)_{k\geqslant 0}$, engendrés par tout élément de $\left(\mathcal{S}^{-1}\mathfrak{p}\right)^k - \left(\mathcal{S}^{-1}\mathfrak{p}\right)^{k+1}$.*

Remarque 2.1.9. *Soit $\mathcal{A}'$ le localisé de $\mathcal{A}$ en $\mathcal{S}$. Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux de $\mathcal{A}$. Alors $(\mathfrak{a}\mathfrak{b})\,\mathcal{A}' = (\mathfrak{a}\mathcal{A}')\,(\mathfrak{b}\mathcal{A}')$.*

Application

Soient $\mathcal{A} = \mathcal{O}_{\mathbf{F}}$, $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_{\mathbf{F}}$, $\mathcal{S} = \mathcal{A} - \mathfrak{p}$. $\mathcal{A}' = \mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}$ est principal. La clôture intégrale de $\mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}$ dans $\mathbf{E}$ est $\mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}}$. C'est un $\mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}$-module libre de rang fini $[\mathbf{E} : \mathbf{F}]$.

Proposition 2.1.10. *Soit $\mathcal{A}$ un anneau intègre, $\mathcal{S}$ comme plus haut, $\mathfrak{p}$ un idéal maximal de $\mathcal{A}$ ne rencontrant pas $\mathcal{S}$. Le morphisme composé $\mathcal{A} \to \mathcal{S}^{-1}\mathcal{A} \to \mathcal{S}^{-1}\mathcal{A}/\mathcal{S}^{-1}\mathfrak{p}$ induit un isomorphisme de $\mathcal{A}/\mathfrak{p}$ sur $\mathcal{S}^{-1}\mathcal{A}/\mathcal{S}^{-1}\mathfrak{p}$.*

Démonstration. Le noyau de $\mathcal{A} \to \mathcal{S}^{-1}\mathcal{A}/\mathcal{S}^{-1}\mathfrak{p}$ est $\mathcal{S}^{-1}\mathfrak{p} \cap \mathcal{A} = \mathfrak{p}$ donc on obtient un morphisme injectif $\varphi : \mathcal{A}/\mathfrak{p} \to \mathcal{S}^{-1}\mathcal{A}/\mathcal{S}^{-1}\mathfrak{p}$. Reste à prouver la surjectivité de φ.

Soit $x = s^{-1}a, s \in \mathcal{S}, a \in \mathcal{A}$. $s \in \mathfrak{p}$ et $\mathcal{A}/\mathfrak{p}$ est un corps donc il existe $t \in \mathcal{A}$ tel que $ts = 1 \mod P$.

Alors $x - ta = s^{-1}a(1 - ts)$. $1 - ts \in \mathfrak{p}$. On obtient modulo $\mathfrak{p}$:

$x - ta \equiv 0 \mod \mathfrak{p}$

Donc $\bar{x} = \varphi(\bar{t}\bar{a})$ et φ est bien surjective ce qui achève la preuve. □

Fin de la démonstration du théorème

On applique le raisonnement utilisé dans le cas principal pour obtenir :

$$[\mathbf{E} : \mathbf{F}] = \sum_{\mathfrak{q}'|\mathfrak{p}'} e\left(\mathfrak{q}'|\mathfrak{p}'\right) f\left(\mathfrak{q}'|\mathfrak{p}'\right)$$

où $\mathfrak{p}' = \mathcal{S}^{-1}\mathfrak{p}$ est un idéal maximal de $\mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}$ et $\mathfrak{q}'$ parcourt les idéaux maximaux de $\mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}}$ au-dessus de $\mathfrak{p}'$.

Comparons :

$$\mathfrak{p}'\mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}} = \prod_{\mathfrak{q}'|\mathfrak{p}'} \mathfrak{q}'^{e(\mathfrak{q}'|\mathfrak{p}')}$$

et

$$\mathfrak{p}\mathcal{O}_{\mathbf{E}} = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})}$$

Cette dernière identité implique

$$\mathfrak{p}\mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}} = \prod_{\mathfrak{q}|\mathfrak{p}} \left(\mathcal{S}^{-1}\mathfrak{q}\right)^{e(\mathfrak{q}|\mathfrak{p})}$$

Les $\mathfrak{q}$ divisant $\mathfrak{p}$ ne rencontrent pas $\mathcal{S}$, donc les $\mathcal{S}^{-1}\mathfrak{q}$ où $\mathfrak{q}$ est au-dessus de $\mathfrak{p}$ donnent des idéaux maximaux $\mathfrak{q}$" distincts de $\mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}}$ et tels que $\mathfrak{q}" \cap \mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}} = \mathcal{S}^{-1}\mathfrak{p}$.

Par unicité de la décomposition en produit dans un anneau de Dedekind on obtient une bijection $\mathfrak{q} \mapsto \mathcal{S}^{-1}\mathfrak{q}$ entre les idéaux maximaux $\mathfrak{q}|\mathfrak{p}$ et les idéaux maximaux $\mathfrak{q}'|\mathfrak{p}'$, et $e\left(\mathcal{S}^{-1}\mathfrak{q}'|\mathcal{S}^{-1}\mathfrak{p}'\right) = e\left(\mathfrak{q}|\mathfrak{p}\right)$.

Par ailleurs, on voit que :

$$\begin{aligned} f\left(\mathfrak{q}|\mathfrak{p}\right) &= [\mathcal{O}_{\mathbf{E}}/\mathfrak{q} : \mathcal{O}_{\mathbf{F}}/\mathfrak{p}] \\ f\left(\mathcal{S}^{-1}\mathfrak{q}|\mathcal{S}^{-1}\mathfrak{p}\right) &= [\mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}}/\mathcal{S}^{-1}\mathfrak{q} : \mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}/\mathcal{S}^{-1}\mathfrak{p}] \end{aligned}$$

or par la proposition 13. on a :

$$\begin{aligned}\mathcal{O}_{\mathbf{F}}/\mathfrak{p} &\simeq \mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}/\mathcal{S}^{-1}\mathfrak{p} \\ \mathcal{O}_{\mathbf{E}}/\mathfrak{q} &\simeq \mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}}/\mathcal{S}^{-1}\mathfrak{q}\end{aligned}$$

d'où l'on déduit $f(\mathfrak{q}|\mathfrak{p}) = f\left(\mathcal{S}^{-1}\mathfrak{q}|\mathcal{S}^{-1}\mathfrak{p}\right)$ puis le résultat :

$$\sum_{\mathfrak{q}|\mathfrak{p}} e(\mathfrak{q}|\mathfrak{p})\, f(\mathfrak{q}|\mathfrak{p}) = [\mathbf{E} : \mathbf{F}]$$ □

2.2 Décomposition dans le cas galoisien

Soit $\mathbf{E} \subseteq \mathbf{F}$ une extension finie galoisienne de groupe de Galois G, où $\mathbf{F}$ est un corps de nombres. On note $n = [\mathbf{E} : \mathbf{F}]$, et on considère un idéal maximal $\mathfrak{p}$ de $\mathcal{O}_{\mathbf{F}}$.

On a

$$\mathfrak{p}\mathcal{O}_{\mathbf{E}} = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})}$$

Le groupe G agit sur $\mathcal{O}_{\mathbf{E}}$, et pour tout $\sigma \in G$ on a $\sigma.\mathcal{O}_{\mathbf{E}} = \mathcal{O}_{\mathbf{E}}$. Le $\mathbf{F}$-morphisme $\sigma \in G$ induit un isomorphisme d'anneaux de $\mathcal{O}_{\mathbf{E}}$ sur lui-même qui se restreint à l'identité sur $\mathcal{O}_{\mathbf{F}}$. Il agit sur les idéaux de $\mathcal{O}_{\mathbf{E}}$: si $\mathfrak{a}$ est un idéal de $\mathcal{O}_{\mathbf{E}}$ alors $\sigma\mathfrak{a}$ aussi.

Considérons un idéal maximal $\mathfrak{q}$ de $\mathcal{O}_{\mathbf{E}}$ au-dessus de $\mathfrak{p}$. Alors $\mathfrak{q} \cap \mathcal{O}_{\mathbf{F}} = \mathfrak{p}$ et $\sigma\mathfrak{q}$ est un idéal maximal de $\mathcal{O}_{\mathbf{E}}$ au-dessus de $\mathfrak{p}$. Le morphisme σ induit donc un morphisme de $\mathcal{O}_{\mathbf{F}}/\mathfrak{p}$-extensions $\mathcal{O}_{\mathbf{E}}/\mathfrak{q} \to \mathcal{O}_{\mathbf{E}}/\sigma\mathfrak{q}$.

Le groupe de Galois G agit donc sur les idéaux maximaux de $\mathcal{O}_{\mathbf{E}}$ au-dessus de $\mathfrak{p}$.

Théorème 2.2.1. *Cette action est transitive.*

Démonstration. On raisonne par l'absurde.

Soit $\mathfrak{q}$ un idéal maximal de $\mathcal{O}_{\mathbf{E}}$ au-dessus de $\mathfrak{p}$, $\mathfrak{q}'$ un idéal maximal de $\mathcal{O}_{\mathbf{E}}$ au-dessus de $\mathfrak{p}$ qui n'est pas dans l'orbite de $\mathfrak{q}$. On a donc :

$$(\forall \sigma \in G)\left(\mathfrak{q}' \neq \sigma\mathfrak{q}\right)$$

Par le lemme chinois on peut trouver $x' \in \mathcal{O}_{\mathbf{E}}$ tel que

$$\begin{aligned} x' &\equiv 0 \mod \mathfrak{q}' \\ x' &\equiv 1 \mod \sigma\mathfrak{q} \text{ pour tout } \sigma \in G \end{aligned}$$

$$\text{Considérons } N_{\mathbf{E}/\mathbf{F}}(x') = \prod_{\sigma \in G} \sigma x' \ \in \mathbf{F} \cap \mathfrak{q}' = \mathfrak{p}$$

Par ailleurs, $\sigma^{-1}x' \equiv 1 \mod \mathfrak{q}$ pour tout $\sigma \in G$

$$\begin{array}{rl} \text{Donc} & N_{\mathbf{E/F}}(x') \equiv 1 \mod \mathfrak{q} \\ & N_{\mathbf{E/F}}(x') \equiv 1 \mod \mathfrak{p} \end{array}$$

On obtient donc une contradiction, car $N_{\mathbf{E/F}}(x') \in \mathfrak{p}$. □

Conséquences.

Partant de $\mathfrak{p}\mathcal{O}_{\mathbf{E}} = \prod \mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})}$, pour tout $\sigma \in G$ on a :

$$\sigma\left(\mathfrak{p}\mathcal{O}_{\mathbf{E}}\right) = \mathfrak{p}\mathcal{O}_{\mathbf{E}} = \prod_{\mathfrak{q}|\mathfrak{p}} (\sigma\mathfrak{q})^{e(\mathfrak{q}|\mathfrak{p})} = \prod_{\mathfrak{q}|\mathfrak{p}} (\mathfrak{q})^{e(\mathfrak{q}|\mathfrak{p})}$$

D'où, l'action étant transitive et la décomposition de $\mathfrak{p}$ en produit d'idéaux maximaux unique, $e\left(\sigma\mathfrak{q}|\mathfrak{p}\right) = e\left(\mathfrak{q}|\mathfrak{p}\right)$.

De même σ induit un isomorphisme de $\mathcal{O}_{\mathbf{F}}/\mathfrak{p}$-extensions de $\mathcal{O}_{\mathbf{E}}/\mathfrak{q}$ sur $\mathcal{O}_{\mathbf{E}}/\sigma\mathfrak{q}$ donc $f\left(\sigma\mathfrak{q}|\mathfrak{p}\right) = f\left(\mathfrak{q}|\mathfrak{p}\right)$.

Notant e le degré de ramification commun, f le degré d'inertie commun et g le nombre d'idéaux maximaux Q de $\mathcal{O}_{\mathbf{F}}$ au-dessus de $\mathfrak{p}$, on obtient

Corollaire 2.2.2. $[\mathbf{E} : \mathbf{F}] = |G| = efg$

Définition 2.2.3. *Pour* $\mathfrak{q}|\mathfrak{p}$, $D\left(\mathfrak{q}|\mathfrak{p}\right)$ *est le stabilisateur de* $\mathfrak{q}$ *dans* G. *Il est appelé* groupe de décomposition *de* $\mathfrak{q}$ *au-dessus de* $\mathfrak{p}$.

Propriétés.

$|D\left(\mathfrak{q}|\mathfrak{p}\right)| = ef$ et pour $\sigma \in G$ $D\left(\sigma\mathfrak{q}|\mathfrak{p}\right) = \sigma D\left(\mathfrak{q}|\mathfrak{p}\right)\sigma^{-1}$. Si $\sigma \in D\left(\mathfrak{q}|\mathfrak{p}\right)$, il induit un morphisme de $\mathcal{O}_{\mathbf{F}}/\mathfrak{p}$-extensions de $\mathcal{O}_{\mathbf{E}}/\mathfrak{q}$ sur lui-même, donc un élément de $Gal\left((\mathcal{O}_{\mathbf{E}}/\mathfrak{q})/(\mathcal{O}_{\mathbf{F}}/\mathfrak{p})\right)$, d'où un homomorphisme $D\left(\mathfrak{q}|\mathfrak{p}\right) \rightarrow Gal\left((\mathcal{O}_{\mathbf{E}}/\mathfrak{q})/(\mathcal{O}_{\mathbf{F}}/\mathfrak{p})\right)$ appelé homomorphisme de réduction.

Définition 2.2.4. *Le noyau de cet homomorphisme est appelé* groupe d'inertie *de* $\mathfrak{q}|\mathfrak{p}$ *et est noté* $I\left(\mathfrak{q}|\mathfrak{p}\right)$.

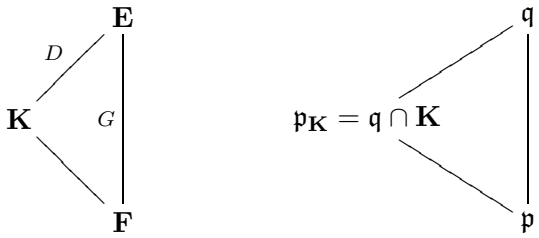
Remarque 2.2.5. *Soit* $\sigma \in G$, *on a alors* $I\left(\sigma\mathfrak{q}|\mathfrak{p}\right) = \sigma I\left(\mathfrak{q}|\mathfrak{p}\right)\sigma^{-1}$.

Théorème 2.2.6. *L'homomorphisme de réduction est surjectif.*

Corollaire 2.2.7.

$$|I\left(\mathfrak{q}|\mathfrak{p}\right)| = e = e\left(\mathfrak{q}|\mathfrak{p}\right)$$

Démonstration du théorème. Notons $\mathbf{K}$ le sous-corps de $\mathbf{E}$ fixé par $D = D\left(\mathfrak{q}|\mathfrak{p}\right)$.



D est le stabilisateur de $\mathbf{K}$ dans G et agit trivialement sur $\mathfrak{q}$. $\mathfrak{p}_\mathbf{K} = \mathfrak{q} \cap \mathbf{K}$ est un idéal maximal de $\mathcal{O}_\mathbf{K}$, $\mathfrak{q}$ est un idéal maximal de $\mathcal{O}_\mathbf{E}$ au-dessus de $\mathfrak{p}_\mathbf{K}$.

L'extension $\mathbf{E}/\mathbf{K}$ est galoisienne de groupe de Galois D donc G agit transitivement sur les idéaux maximaux de $\mathcal{O}_\mathbf{E}$ au-dessus de $\mathfrak{p}_K$. Par suite, $\mathfrak{q}$ est le seul idéal maximal de $\mathcal{O}_\mathbf{E}$ au-dessus de $\mathfrak{p}_\mathbf{K}$.

Alors $|D| = [\mathbf{E} : \mathbf{K}] = e(\mathfrak{q}|\mathfrak{p}_\mathbf{K}) f(\mathfrak{q}|\mathfrak{p}_K)$.

Par ailleurs, $|D| = e(\mathfrak{q}|\mathfrak{p}) f(\mathfrak{q}|\mathfrak{p})$. Or par transitivité pour les degrés de ramification et d'inertie, on obtient $e(\mathfrak{p}_\mathbf{K}|\mathfrak{p}) f(\mathfrak{p}_\mathbf{K}|\mathfrak{p}) = 1$ d'où $e(\mathfrak{p}_\mathbf{K}|\mathfrak{p}) = f(\mathfrak{p}_\mathbf{K}|\mathfrak{p}) = 1$.

On a alors :

$$\mathcal{O}_\mathbf{F}/\mathfrak{p} \xrightarrow{\simeq \text{ (degré 1)}} \mathcal{O}_\mathbf{K}/\mathfrak{p}_\mathbf{K} \hookrightarrow \mathcal{O}_\mathbf{E}/\mathfrak{q}$$

Il suffit donc à présent de montrer que le morphisme de groupes de $D(\mathfrak{q}|\mathfrak{p}) = Gal(\mathbf{E}/\mathbf{K})$ dans $Gal\left((\mathcal{O}_\mathbf{E}/\mathfrak{q})/(\mathcal{O}_\mathbf{K}/\mathfrak{p}_\mathbf{K})\right)$ est surjectif.

On peut donc se ramener à prouver le résultat pour $\mathfrak{p}_\mathbf{K}$ plutôt que $\mathfrak{p}$, c'est-à-dire que l'on peut supposer que le corps fixé par D est $\mathbf{F}$.

Supposons donc à présent $D = G$ et $\mathbf{F} = \mathbf{K}$.

Soit $\bar{x}$ un élément primitif pour l'extension $(\mathcal{O}_\mathbf{E}/\mathfrak{q})/(\mathcal{O}_\mathbf{F}/\mathfrak{p}) : \mathcal{O}_\mathbf{E}/\mathfrak{q} = (\mathcal{O}_\mathbf{F}/\mathfrak{p})[\bar{x}]$, et x un élément de $\mathcal{O}_\mathbf{F}$ dont la classe modulo $\mathfrak{q}$ est $\bar{x}$. Soit f le polynôme minimal de x sur F.

Le polynôme f a pour racines les conjugués de x par l'action de G, qui sont entiers, d'où l'on déduit que $f \in \mathcal{O}_\mathbf{E}[t] \cap \mathbf{F}[t] = \mathcal{O}_\mathbf{F}[t]$. On peut donc considérer sa réduction modulo $\mathfrak{p}$, $\bar{f} \in (\mathcal{O}_\mathbf{F}/\mathfrak{p})[t]$. Les racines de f sont les σx où σ décrit G. Les racines de $\bar{f}$ sont les $\bar{\sigma}\bar{x}$ où $\bar{\sigma}$ est l'élément de $(\mathcal{O}_\mathbf{E}/\mathfrak{q})/(\mathcal{O}_\mathbf{F}/\mathfrak{p})$ induit par σ via l'homomorphisme de réduction.

Un conjugué quelconque de $\bar{x}$ dans $(\mathcal{O}_\mathbf{E}/\mathfrak{q})/(\mathcal{O}_\mathbf{F}/\mathfrak{p})$ est une racine de $\bar{f}$ donc est de la forme $\bar{\sigma}\bar{x}$ pour un des $\sigma \in G$.

Or $\bar{x}$ étant un élément primitif les automorphismes de $(\mathcal{O}_\mathbf{E}/\mathfrak{q})/(\mathcal{O}_\mathbf{F}/\mathfrak{p})$ sont déterminés par leur action sur $\bar{x}$, donc sont de la forme $\bar{\sigma}$ pour un $\sigma \in G$: l'homomorphisme de réduction est donc surjectif. □

2.3 Automorphismes de Frobenius

Dans toute cette section on considère une extension $\mathbf{E}/\mathbf{F}$ galoisienne finie de corps de nombres de groupe de Galois G.

Rappel. Un idéal maximal $\mathfrak{p}$ de $\mathcal{O}_\mathbf{F}$ est dit ramifié dans $\mathbf{E}/\mathbf{F}$ s'il existe $\mathfrak{q}|\mathfrak{p}$ tel que $e(\mathfrak{q}|\mathfrak{p}) > 1$.

Proposition 2.3.1. *Seul un nombre fini d'idéaux maximaux de $\mathcal{O}_\mathbf{F}$ sont ramifiés dans $\mathbf{E}/\mathbf{F}$.*

Remarque 2.3.2. *Ce résultat s'étend aussitôt au cas où $\mathbf{E}/\mathbf{F}$ est finie en considérant sa clôture galoisienne.*

On verra que $\mathfrak{p}$ est ramifié dans $\mathbf{E}/\mathbf{F}$ si et seulement si $\mathfrak{p}|disc(\mathbf{E}/\mathbf{F})$.

Démonstration. Si l'idéal $\mathfrak{p}$ est ramifié dans $\mathbf{E}/\mathbf{F}$ alors il existe un idéal $\mathfrak{q}$ de $\mathcal{O}_\mathbf{E}$ au-dessus de $\mathfrak{p}$ tel que $I(\mathfrak{q}|\mathfrak{p}) \neq \{id\}$. On dispose alors d'un $\sigma \in I(\mathfrak{q}|\mathfrak{p})$ différent de l'identité qui agit trivialement sur le corps résiduel $\mathcal{O}_\mathbf{E}/\mathfrak{q}$.

Prenons $x \in \mathcal{O}_\mathbf{E}$ tel que $\mathbf{E} = \mathbf{F}[x]$.

Le polynôme minimal f de x sur $\mathbf{F}$ est dans $\mathcal{O}_\mathbf{F}[t]$.

$$f(t) = \prod_{\sigma \in G} (t - \sigma(x))$$

Considérons sa réduction modulo $\mathfrak{p}$: $\bar{f} \in (\mathcal{O}_\mathbf{F}/\mathfrak{p})[t] \subseteq (\mathcal{O}_\mathbf{E}/\mathfrak{q})[t]$.

$$\bar{f}(t) = \prod_{\sigma \in G} \left(t - \bar{\sigma}(\bar{x})\right)$$

Par non-trivialité de $I(\mathfrak{q}|\mathfrak{p})$ $\bar{f}$ admet une racine double modulo $\mathfrak{q}$.

Considérons $disc(f) \in \mathcal{O}_\mathbf{F}$. C'est un élément non nul de $\mathcal{O}_\mathbf{F}$ car f est irréductible et séparable dans $\mathbf{F}[t]$. Le discriminant de $\bar{f}$, $disc(\bar{f})$, qui n'est autre que la réduction modulo $\mathfrak{p}$ de $disc(f)$, est nul dans $\mathcal{O}_\mathbf{F}/\mathfrak{p}$. Cela signifie bien que $\mathfrak{p}|disc(f)\mathcal{O}_\mathbf{F}$.

Les idéaux maximaux $\mathfrak{p}$ de $\mathcal{O}_\mathbf{F}$ ramifiés dans $\mathbf{E}/\mathbf{F}$ divisent $disc(f)\mathcal{O}_\mathbf{F}$ donc ils sont en nombre fini. □

Si $\mathfrak{p}$ est un idéal maximal de $\mathcal{O}_\mathbf{F}$ non ramifié dans $\mathbf{E}/\mathbf{F}$ l'homomorphisme de réduction $D(\mathfrak{q}|\mathfrak{p}) \to Gal((\mathcal{O}_\mathbf{E}/\mathfrak{q})/(\mathcal{O}_\mathbf{F}/\mathfrak{p}))$ est un isomorphisme de groupes.

Définition 2.3.3. *Pour un tel $\mathfrak{p}$ et pour $\mathfrak{q}|\mathfrak{p}$ l'automorphisme de Frobenius $Frob(\mathfrak{q}|\mathfrak{p})$ est l'unique élément de $D(\mathfrak{q}|\mathfrak{p})$ dont l'image par l'homomorphisme de réduction est l'automorphisme de Frobenius pour le corps fini $(\mathcal{O}_\mathbf{E}/\mathfrak{q})/(\mathcal{O}_\mathbf{F}/\mathfrak{p})$.*

Propriétés.

C'est l'unique élément de G qui :

1. est dans $D(\mathfrak{q}|\mathfrak{p})$
2. vérifie $\sigma(x) \equiv x^{|\mathcal{O}_\mathbf{F}/\mathfrak{p}|} \mod \mathfrak{q}$ pour tout $x \in \mathcal{O}_\mathbf{E}$.

Il est d'ordre $f(\mathfrak{q}|\mathfrak{p})$ dans G et engendre $D(\mathfrak{q}|\mathfrak{p})$.

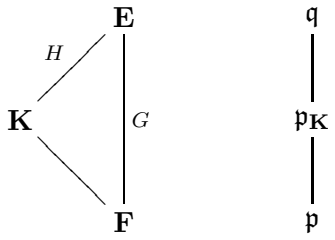
Si $\sigma \in G$ alors $Frob(\mathfrak{q}|\mathfrak{p}) = \sigma Frob(\mathfrak{q}|\mathfrak{p})\sigma^{-1}$.

En particulier si G est abélien $Frob(\mathfrak{q}|\mathfrak{p})$ ne dépend pas du choix de $\mathfrak{q}$ et se note $Frob_{\mathfrak{p}}$.

Remarque 2.3.4. *Si un idéal maximal $\mathfrak{p}$ de $\mathcal{O}_{\mathbf{F}}$ n'est pas ramifié dans $\mathbf{E}/\mathbf{F}$ alors le degré d'inertie commun f est égal à l'ordre du Frobenius, et on obtient que g, nombre d'idéaux maximaux de $\mathcal{O}_{\mathbf{E}}$ qui sont au-dessus de $\mathfrak{p}$, vaut $\frac{[\mathbf{E}:\mathbf{F}]}{f}$.*

Rappelons que $\mathfrak{p}$ est totalement décomposé dans $\mathbf{E}/\mathbf{F}$ si $f(\mathfrak{q}|\mathfrak{p}) = e(\mathfrak{q}|\mathfrak{p}) = 1$ pour tout $\mathfrak{q}$ au-dessus de $\mathfrak{p}$. Cela équivaut à dire qu'il y a exactement $[\mathbf{E} : \mathbf{F}]$ idéaux $\mathfrak{q}$ au-dessus de $\mathfrak{p}$. Dans le cas où $\mathbf{E}/\mathbf{F}$ est galoisienne cela signifie que $\mathfrak{p}$ est non ramifié dans $\mathbf{E}/\mathbf{F}$ et $Frob(\mathfrak{q}|\mathfrak{p}) = Id_{\mathbf{E}}$.

2.4 Passage aux sous-corps



$\mathfrak{q}$ idéal maximal de $\mathcal{O}_{\mathbf{E}}$

$\mathfrak{p}$ idéal maximal de $\mathcal{O}_{\mathbf{F}}$

H est un sous-groupe de G, $\mathbf{K}$ est le corps fixé par H, et on a $H = Gal(\mathbf{E}/\mathbf{K})$.

$\mathfrak{p}_{\mathbf{K}} = \mathfrak{q} \cap \mathbf{K}$ est un idéal maximal de $\mathcal{O}_{\mathbf{K}}$, avec $\mathfrak{q}|\ \mathfrak{p}_{\mathbf{K}}|\mathfrak{p}$.

L'enjeu de cette section est de déterminer $D(\mathfrak{q}|\mathfrak{p}_{\mathbf{K}})$ et $I(\mathfrak{q}|\mathfrak{p}_{\mathbf{K}})$ en fonction de $D(\mathfrak{q}|\mathfrak{p})$ et $I(\mathfrak{q}|\mathfrak{p})$.

Proposition 2.4.1.

1. $D(\mathfrak{q}|\mathfrak{p}_{\mathbf{K}}) = D(\mathfrak{q}|\mathfrak{p}) \cap H$
2. $I(\mathfrak{q}|\mathfrak{p}_{\mathbf{K}}) = I(\mathfrak{q}|\mathfrak{p}) \cap H$

Démonstration.

Pour le premier point :

$D(\mathfrak{q}|\mathfrak{p}_{\mathbf{K}}) = \{(\sigma \in H)(\sigma\mathfrak{q} = \mathfrak{q})\} = H \cap D(\mathfrak{q}|\mathfrak{p})$.

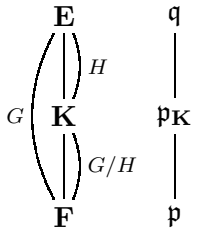
Pour le deuxième :

$$\begin{aligned} I(\mathfrak{q}|\mathfrak{p}_{\mathbf{K}}) &= \{(\sigma \in D(\mathfrak{q}|\mathfrak{p}_{\mathbf{K}}))\,(\sigma \text{ induit l'identité sur } \mathcal{O}_{\mathbf{E}}/\mathfrak{q})\} \\ &= \{(\sigma \in D(\mathfrak{q}|\mathfrak{p}) \cap H)\,(\sigma \text{ induit l'identité sur } \mathcal{O}_{\mathbf{E}}/\mathfrak{q})\} \\ &= I(\mathfrak{q}|\mathfrak{p}) \cap H \quad \square \end{aligned}$$

Si $\mathfrak{p}$ est non ramifié dans $\mathbf{E}/\mathbf{F}$ alors $\mathfrak{p}_{\mathbf{K}}$ est non ramifié dans $\mathbf{E}/\mathbf{K}$ et $Frob(\mathfrak{q}|\mathfrak{p}_{\mathbf{K}}) = Frob(\mathfrak{q}|\mathfrak{p})^{f(\mathfrak{p}_{\mathbf{K}}|\mathfrak{p})}$: en effet c'est l'unique élément de $D(\mathfrak{q}|\mathfrak{p}_{\mathbf{K}})$ qui agisse sur $OE/\mathfrak{q}$ par $x \mapsto x^{|\mathcal{O}_{\mathbf{K}}/\mathfrak{p}_{\mathbf{K}}|}$, et il en va de même pour $Frob(\mathfrak{q}|\mathfrak{p})$,

d'où le résultat cherché par multiplicativité des degrés dans une tour d'extensions.

Considérons la situation suivante :



où $G \to Gal(\mathbf{K}/\mathbf{F})$ a pour noyau H.

Proposition 2.4.2.

1. *$D(\mathfrak{p}_\mathbf{K}|\mathfrak{p})$ est l'image de $D(\mathfrak{q}|\mathfrak{p})$ dans $Gal(\mathbf{K}/\mathbf{F})$*
2. *$I(\mathfrak{p}_\mathbf{K}|\mathfrak{p})$ est l'image de $I(\mathfrak{q}|\mathfrak{p})$ dans $Gal(\mathbf{K}/\mathbf{F})$*

Démonstration.

1. Soit σ un élément de l'image de $D(\mathfrak{q}|\mathfrak{p})$ dans $Gal(\mathbf{K}/\mathbf{F})$. Alors $\sigma\mathfrak{q} = \mathfrak{q}$ et $\sigma\mathbf{K} = \mathbf{K}$, donc $\sigma\mathfrak{p}_\mathbf{K} = \sigma(\mathfrak{q} \cap \mathbf{K}) = \sigma\mathfrak{q} \cap \sigma\mathbf{K} = \mathfrak{q} \cap \mathbf{K} = \mathfrak{p}_\mathbf{K}$, donc $\sigma|_\mathbf{K} \in D(\mathfrak{p}_\mathbf{K}|\mathfrak{p})$.

   Inversement, soit $\sigma \in G$ tel que $\sigma\mathfrak{p}_\mathbf{K} = \mathfrak{p}_\mathbf{K}$.

   L'idéal $\sigma\mathfrak{q}$ est alors un idéal maximal de $\mathcal{O}_\mathbf{E}$ au-dessus de $\mathfrak{p}_\mathbf{K}$. Mais $H = Gal(\mathbf{E}/\mathbf{K})$ agit transitivement sur les idéaux maximaux de $\mathcal{O}_\mathbf{E}$ au-dessus de $\mathfrak{p}_\mathbf{K}$. On a alors : $(\exists\tau \in H)(\sigma\mathfrak{q} = \tau\mathfrak{q})$, d'où $\tau^{-1}\sigma\mathfrak{q} = \mathfrak{q}$, soit $\tau^{-1}\sigma \in D(\mathfrak{q}|\mathfrak{p})$.

   Les morphismes σ et $\tau^{-1}\sigma$ ont même image dans G/H donc σ est image dans G/H d'un élément de $D(\mathfrak{q}|\mathfrak{p})$.

2. Soit $\sigma \in I(\mathfrak{q}|\mathfrak{p})$, on voit de même que précédemment que $\sigma\mathfrak{p}_\mathbf{K} = \mathfrak{p}_\mathbf{K}$ donc $\sigma|_\mathbf{K} \in D(\mathfrak{p}_\mathbf{K}|\mathfrak{p}$; de plus σ induit l'identité sur $\mathcal{O}_\mathbf{K}/\mathfrak{p}_\mathbf{K}$ donc $\sigma|_\mathbf{K} \in I(\mathfrak{p}_\mathbf{K}|\mathfrak{p})$.

   Inversement, soit $\sigma \in G$ dont l'image dans $Gal(\mathbf{K}/\mathbf{F})$ est un élément du groupe d'inertie de $\mathfrak{p}_\mathbf{K}$ au-dessus de $\mathfrak{p}$. On peut supposer que $\sigma \in D(\mathfrak{q}|\mathfrak{p})$, et on sait en plus que σ induit l'identité sur $\mathcal{O}_\mathbf{K}/\mathfrak{p}_\mathbf{K}$.

   L'homomorphisme de réduction de $D(\mathfrak{q}|\mathfrak{p}_\mathbf{K})$ dans $Gal\left((\mathcal{O}_\mathbf{E}/\mathfrak{q})/(\mathcal{O}_\mathbf{K}/\mathfrak{p}_\mathbf{K})\right)$ est surjectif.

   Il y a donc un $\tau \in D(\mathfrak{q}|\mathfrak{p}_\mathbf{K})$ qui agit comme σ sur $\mathcal{O}_\mathbf{E}/\mathfrak{q}$, et $\tau^{-1}\sigma \in I(\mathfrak{q}|\mathfrak{p}_\mathbf{K}) \subseteq I(\mathfrak{q}|\mathfrak{p})$. Par conséquent σ et $\tau^{-1}\sigma$ ont même image dans $Gal(\mathbf{K}/\mathbf{F})$, ce qui prouve le résultat. □

Proposition 2.4.3. *Si $\mathfrak{p}$ est non ramifié dans $\mathbf{E}/\mathbf{F}$ alors $\mathfrak{p}$ est non ramifié dans $\mathbf{K}/\mathbf{F}$ et $Frob(\mathfrak{p}_\mathbf{K}|\mathfrak{p})$ est l'image de $Frob(\mathfrak{q}|\mathfrak{p})$.*

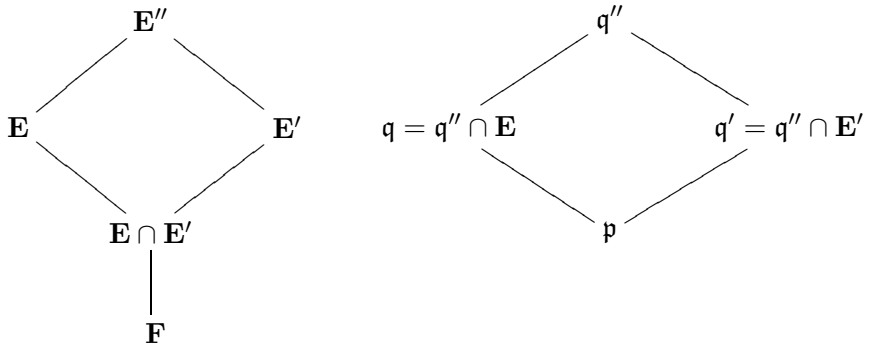
Démonstration. Le morphisme de Frobenius $Frob(\mathfrak{p}_\mathbf{K}|\mathfrak{p})$ est l'unique élément ρ de $Gal(\mathbf{K}/\mathbf{F})$ tel que $\rho \in D(\mathfrak{p}_\mathbf{K}|\mathfrak{p})$ et $\rho x \equiv x^{|\mathcal{O}_\mathbf{F}/\mathfrak{p}|} \mod \mathfrak{p}_\mathbf{K}$ pour $x \in \mathcal{O}_\mathbf{K}$.

Considérons $\tau = Frob(\mathfrak{q}|\mathfrak{p})|_\mathbf{K}$.

On a $\tau \in D(\mathfrak{p}_\mathbf{K}|\mathfrak{p})$ (par la première partie – triviale – de la proposition) et $\tau x \equiv x^{|\mathcal{O}_\mathbf{F}/\mathfrak{p}|} \mod \mathfrak{p}_\mathbf{K}$ pour $x \in \mathcal{O}_\mathbf{K}$, puisque cette égalité est déjà réalisée modulo $\mathfrak{q}$ pour $y \in \mathcal{O}_\mathbf{E}$.

Donc $\rho = \tau$. □

Remarque 2.4.4. *Soient* $\mathbf{E}/\mathbf{F}$ *et* $\mathbf{E}'/\mathbf{F}'$ *deux extensions galoisiennes finies de* $\mathbf{F}$ *de groupes respectifs* G *et* G'*, et* $\mathbf{E}$" *un composé de* $\mathbf{E}/\mathbf{F}$ *et* $\mathbf{E}'/\mathbf{F}'$*.*

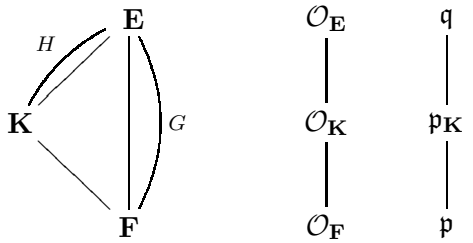


$D(\mathfrak{q}''|\mathfrak{p})$ *a pour image* $D(\mathfrak{q}|\mathfrak{p})$ *dans* G *et* $D(\mathfrak{q}'|\mathfrak{p})$ *dans* G'*.*

$I(\mathfrak{q}''|\mathfrak{p})$ *a pour image* $I(\mathfrak{q}|\mathfrak{p})$ *dans* G *et* $I(\mathfrak{q}'|\mathfrak{p})$ *dans* G'*.*

Si $\mathfrak{p}$ *est non ramifié dans* $\mathbf{E}/\mathbf{F}$ *et* $\mathbf{E}'/\mathbf{F}$ *alors il l'est dans* $\mathbf{E}''/\mathbf{F}$*. Si* $\mathfrak{p}$ *est totalement décomposé dans* $\mathbf{E}/\mathbf{F}$ *et* $\mathbf{E}'/\mathbf{F}$ *alors il l'est dans* $\mathbf{E}''/\mathbf{F}$*.*

2.5 Décomposition dans des extensions non nécessairement galoisiennes



$$\begin{aligned} D(\mathfrak{q}|\mathfrak{p}_\mathbf{K}) &= H \cap D(\mathfrak{q}|\mathfrak{p}) \\ I(\mathfrak{q}|\mathfrak{p}_\mathbf{K}) &= H \cap I(\mathfrak{q}|\mathfrak{p}) \end{aligned}$$

permet le calcul de $e(\mathfrak{p}_\mathbf{K}|\mathfrak{p})$ et $f(\mathfrak{p}_\mathbf{K}|\mathfrak{p})$.

L'idée pour la suite est que si $\mathfrak{p}'_\mathbf{K}$ est un idéal maximal de $\mathcal{O}_\mathbf{K}$ au-dessus de $\mathfrak{p}$ et $\mathfrak{q}'$ un idéal maximal de $\mathcal{O}_\mathbf{E}$ au-dessus de $\mathfrak{p}_\mathbf{K}$ alors $\mathfrak{q}'$ est un idéal maximal de $\mathcal{O}_\mathbf{E}$ au-dessus de $\mathfrak{p}$, donc $\mathfrak{q}' = \sigma\mathfrak{q}$ pour un $\sigma \in G$.

Les idéaux maximaux de $\mathcal{O}_{\mathbf{K}}$ au-dessus de $\mathfrak{p}$ sont donc de la forme $\sigma\mathfrak{q}$, $\sigma \in G$. La connaissance de $D(\sigma\mathfrak{q}|\mathfrak{p}) = \sigma D(\mathfrak{q}|\mathfrak{p})\sigma^{-1}$ et $I(\sigma\mathfrak{q}|\mathfrak{p}) = \sigma I(\mathfrak{q}|\mathfrak{p})\sigma^{-1}$ permet de calculer $e(\mathfrak{p}_{\mathbf{K}}|\mathfrak{p})$, $f(\mathfrak{p}_{\mathbf{K}}|\mathfrak{p})$ et le cas échéant $Frob(\mathfrak{p}_{\mathbf{K}}|\mathfrak{p})$.

Considérons σ, $\sigma' \in G$. Quand a-t-on $\sigma\mathfrak{q} \cap \mathcal{O}_{\mathbf{K}} = \sigma'\mathfrak{q} \cap \mathcal{O}_{\mathbf{K}}$?

Ce sont tous deux des idéaux maximaux de $\mathcal{O}_{\mathbf{K}}$ au-dessus de $\mathfrak{p}$. S'ils sont égaux, alors les idéaux $\sigma\mathfrak{q}$ et $\sigma'\mathfrak{q}$ sont deux idéaux maximaux de $\mathcal{O}_{\mathbf{E}}$ au-dessus du même idéal de $\mathcal{O}_{\mathbf{K}}$ donc il existe $\tau \in Gal(\mathbf{E}/\mathbf{K}) = H$ tel que $\sigma\mathfrak{q} = \tau\sigma\mathfrak{q}$.

Inversement, si $\tau \in Gal(\mathbf{E}/\mathbf{K}) = H$ est tel que $\sigma\mathfrak{q} = \tau\sigma'\mathfrak{q}$ alors $\sigma\mathfrak{q} \cap \mathbf{K} = \sigma'\mathfrak{q} \cap \mathbf{K}$.

La condition $\sigma\mathfrak{q} \cap \mathbf{K} = \sigma'\mathfrak{q} \cap \mathbf{K}$ équivaut donc à $(\exists \tau \in H)(\sigma\mathfrak{q} = \tau\sigma'\mathfrak{q})$, ce qui se traduit par $(\exists \rho \in D(\mathfrak{q}|\mathfrak{p}))(\sigma = \tau\sigma'\rho)$.

En conclusion, les idéaux maximaux de $\mathcal{O}_{\mathbf{K}}$ au-dessus de $\mathfrak{p}$ sont paramétrés par les doubles classes $H\sigma D$. L'ensemble des doubles classes se note en général $H\backslash G/D$.

Remarque 2.5.1. *Considérons le cas où* $\mathbf{E}/\mathbf{F}$ *est une clôture galoisienne de* $\mathbf{K}/\mathbf{F}$. *En termes de groupes ceci se traduit par : l'intersection des conjugués de* H *est triviale. En effet,* $I = \cap gHg^{-1}$ *est distingué dans* G *et* $\mathbf{E}' = \mathbf{E}^I$ *est galoisien sur* $\mathbf{F}$ *et contient* $\mathbf{K}$.

Supposons que $\mathfrak{p}$ est totalement décomposé dans $\mathbf{K}/\mathbf{F}$: pour $\mathfrak{p}_{\mathbf{K}}|\mathfrak{p}$, $e(\mathfrak{p}_K|\mathfrak{p})f(\mathfrak{p}_{\mathbf{K}}|\mathfrak{p}) = 1$. Montrons qu'alors $\mathfrak{p}$ est totalement décomposé dans $\mathbf{E}/\mathbf{F}$:

On a $|D(\mathfrak{q}|\mathfrak{p}_{\mathbf{K}})| = e(\mathfrak{q}|\mathfrak{p}_{\mathbf{K}})f(\mathfrak{q}|\mathfrak{p}_{\mathbf{K}}) = \frac{e(\mathfrak{q}|\mathfrak{p})f(\mathfrak{q}|\mathfrak{p})}{e(\mathfrak{p}_{\mathbf{K}}|\mathfrak{p})f(\mathfrak{p}_{\mathbf{K}}|\mathfrak{p})}$.

Dire que $e(\mathfrak{p}_{\mathbf{K}}|\mathfrak{p}) = f(\mathfrak{p}_{\mathbf{K}}|\mathfrak{p}) = 1$ signifie que $D(\mathfrak{q}|\mathfrak{p}_{\mathbf{K}}) = D(\mathfrak{q}|\mathfrak{p})$. Comme $D(\mathfrak{q}|\mathfrak{p}_{\mathbf{K}}) = D(\mathfrak{q}|\mathfrak{p}) \cap H$ cette égalité se traduit donc par $D(\mathfrak{q}|\mathfrak{p}) \subseteq H$ pour tout $\mathfrak{q}|\mathfrak{p}_{\mathbf{K}}$.

Comme $\mathfrak{p}$ est totalement décomposé dans $\mathbf{K}/\mathbf{F}$ c'est vrai pour tout choix de $\mathfrak{p}_{\mathbf{K}}$, donc pour tout $\mathfrak{q}$ au-dessus de $\mathfrak{p}$ on a $D(\mathfrak{q}|\mathfrak{p}) \subseteq H$.

Posons $D = D(\mathfrak{q}|\mathfrak{p})$. En fixant $\mathfrak{q}|\mathfrak{p}$ on a donc, en appliquant ce qui précède aux $\sigma\mathfrak{q}$, $\sigma \in G$:

$\sigma D\sigma^{-1} \subseteq H$ donc $D \subseteq \cap\sigma^{-1}H\sigma$, d'où $D = \{\mathbf{1}_G\}$ et $\mathfrak{p}$ est totalement décomposé dans $\mathbf{E}/\mathbf{F}$.

2.6 Lien avec les polynômes

$$\begin{array}{c}\mathbf{E}\\ \Big|\ \text{finie}\\ \mathbf{F}\end{array}$$

Soit $x \in \mathcal{O}_{\mathbf{E}}$ un élément primitif : $\mathbf{E} = \mathbf{F}[x]$ et $\mathcal{O}_{\mathbf{F}}[x] \subseteq \mathcal{O}_{\mathbf{E}}$. Soit $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_{\mathbf{F}}$ et $\mathcal{S} = \mathcal{O}_{\mathbf{F}} - \mathfrak{p}$.

Soit f le polynôme minimal de x sur F, on a $f \in \mathcal{O}_{\mathbf{F}}[t]$. On note $\bar{f}$ sa réduction dans $(\mathcal{O}_{\mathbf{F}}/\mathfrak{p})[t]$. On dispose de sa décomposition en facteurs irréductibles unitaires distincts à coefficients dans le corps résiduel :

$$\bar{f}(t) = \prod g_i(t)^{\alpha_i}$$

On fixe une famille $(h_i) \in \mathcal{O}_{\mathbf{F}}[t]$ de polynômes unitaires tels que $\bar{h_i} = g_i$.

Proposition 2.6.1. *On suppose $\mathcal{O}_{\mathbf{E}} = \mathcal{O}_{\mathbf{F}}[x]$. Alors $\mathfrak{p}\mathcal{O}_{\mathbf{E}} = \prod \mathfrak{q}_i^{\alpha_i}$ avec $\mathfrak{q}_i = (\mathfrak{p}, h_i(x))$, et les $\mathfrak{q}_i$ deux à deux distincts.*

Comme on le verra dans la démonstration, on utilise seulement que $\mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}} = \mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}[x]$. On verra plus loin les critères pour cette égalité.

Supposons pour le moment $\mathcal{O}_{\mathbf{E}} = \mathcal{O}_{\mathbf{F}}[x]$.

Démonstration.

$$\begin{aligned} \mathcal{O}_{\mathbf{E}} &\simeq \mathcal{O}_{\mathbf{F}}[t]/f(t)\mathcal{O}_{\mathbf{F}}[t] \\ \mathcal{O}_{\mathbf{E}}/\mathfrak{p}\mathcal{O}_{\mathbf{E}} &\simeq \mathcal{O}_{\mathbf{F}}[x]/(\mathfrak{p}) \\ &\simeq \mathcal{O}_{\mathbf{F}}[t]/(\mathfrak{p}, f) \\ &\simeq \mathcal{O}_{\mathbf{F}}[t]/(\mathfrak{p}\mathcal{O}_{\mathbf{F}}[t] + f\mathcal{O}_{\mathbf{F}}[t]) \\ &\simeq (\mathcal{O}_{\mathbf{F}}/\mathfrak{p})[t]/(\bar{f}) \end{aligned}$$

On a donc $\mathcal{O}_{\mathbf{E}}/\mathfrak{p}\mathcal{O}_{\mathbf{E}} \simeq (\mathcal{O}_{\mathbf{F}}/\mathfrak{p})[t]/(\bar{f})$. Or par le lemme chinois on trouve $(\mathcal{O}_{\mathbf{F}}/\mathfrak{p})[t]/\bar{f} \simeq \prod(\mathcal{O}_{\mathbf{F}}/\mathfrak{p})[t]/(g_i^{\alpha_i})$.

Les idéaux maximaux $\mathfrak{q}$ de $\mathcal{O}_{\mathbf{E}}$ contenant $\mathfrak{p}\mathcal{O}_{\mathbf{E}}$ correspondent de manière bijective aux idéaux maximaux de $\mathcal{O}_{\mathbf{E}}/\mathfrak{p}\mathcal{O}_{\mathbf{E}}$, c'est-à-dire via cette composition d'isomorphismes aux idéaux maximaux de $\mathbf{k}[t]/\bar{f}\mathbf{k}[t]$, soit aux $g_i\mathbf{k}[t]/\bar{f}\mathbf{k}[t]$ où $\mathbf{k} = \mathcal{O}_{\mathbf{E}}/\mathfrak{p}\mathcal{O}_{\mathbf{E}}$.

L'idéal g_i correspond à l'idéal $(\mathfrak{p}, h_i(x)) = \mathfrak{q}_i$.

On obtient ainsi un isomorphisme entre corps résiduels $\mathbf{k}[t]/(g_i) \simeq \mathcal{O}_{\mathbf{E}}/\mathfrak{q}_i$, qui est en particulier un isomorphisme de $\mathbf{k}$-espaces vectoriels, d'où en comparant les dimensions : $f(\mathfrak{q}_i|\mathfrak{p}) = d^\circ g_i$.

$$\begin{aligned} \mathcal{O}_{\mathbf{E}}/\mathfrak{p}\mathcal{O}_{\mathbf{E}} &\simeq \prod_{i=1}^{r} \mathcal{O}_{\mathbf{E}}/\mathfrak{q}_i^{e(\mathfrak{q}_i|\mathfrak{p})} \\ \mathbf{k}[t]/(\bar{f}\mathbf{k}[t]) &\simeq \prod_{i=1}^{r} \mathbf{k}[t]/g_i^{\alpha_i}[t] \end{aligned}$$

$e(\mathfrak{q}_i|\mathfrak{p})$ est le plus petit entier $r \geqslant 0$ tel que, notant $\bar{\mathfrak{q}_i}$ l'idéal $\mathfrak{q}_i$ réduit modulo $\mathfrak{p}\mathcal{O}_{\mathbf{E}}$, l'image de $\bar{\mathfrak{q}_i}^r$ soit nulle dans $\mathcal{O}_{\mathbf{E}}/\mathfrak{q}$. De même α_i est le plus petit entier r tel que l'image dans $\mathbf{k}[t]/g_i^{\alpha_i}(t)$ de g_i^r soit nulle.

Les deux décompositions se correspondent par l'isomorphisme de $\mathcal{O}_{\mathbf{E}}/\mathfrak{p}\mathcal{O}_{\mathbf{E}}$ sur $\mathbf{k}[t]/\bar{f}\mathbf{k}[t]$ d'où $\alpha_i = e(\mathfrak{q}_i|\mathfrak{p})$. □

Exemple : les corps quadratiques.

Soit d un entier sans facteur carré, $d \neq 0, 1$. On considère $\mathbf{K} = \mathbb{Q}(\sqrt{d})$. Alors

$$\mathcal{O}_{\mathbf{K}} = \mathbb{Z}[\sqrt{d}] \text{ si } d \equiv 2 \text{ ou } 3 \mod 4$$
$$\mathcal{O}_{\mathbf{K}} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \text{ si } d \equiv 1 \mod 4$$

On peut alors prendre selon le cas $x = \sqrt{d}$ et $f(t) = t^2 - d$ ou $x = \frac{1+\sqrt{d}}{2}$ et $f(t) = t^2 - t - \frac{d-1}{4}$.

Pour un nombre premier p fixé on considère $\bar{f} \in \mathbb{F}_p[t]$ la réduction de f modulo p. Alors

- Si $\bar{f}$ a une racine double alors p est ramifié
- Si $\bar{f}$ a deux racines simples alors $p\mathcal{O}_{\mathbf{K}} = \mathfrak{p}_1\mathfrak{p}_2$ avec $f(\mathfrak{p}_1|\mathfrak{p}) = f(\mathfrak{p}_2|\mathfrak{p}) = 1$.
- Si $\bar{f}$ est irréductible alors $p\mathcal{O}_{\mathbf{K}}$ est maximal donc $f(\mathfrak{p}\mathcal{O}_{\mathbf{K}}|\mathfrak{p}) = 2$.

Les nombres premiers ramifiés dans $\mathbf{K}$ sont donc :

- 2 et les diviseurs premiers de d si $d \equiv 2$ ou $3 \mod 4$.
- Les diviseurs premiers de d si $d \equiv 1 \mod 4$.

On suppose désormais p non ramifié dans $\mathbf{K}/\mathbb{Q}$.

$\bar{f}$ a deux racines simples si et seulement si son discriminant dans $\mathbb{F}_p^\times$ est un carré et est irréductible dans le cas contraire. Donc

- $\bar{f}$ a deux racines simples si et seulement si $\left(\frac{d}{p}\right) = 1$.
- $\bar{f}$ est irréductible si et seulement si $\left(\frac{d}{p}\right) = -1$.

Ceci vaut si $p \neq 2$.

Si $p = 2$, pour $d \equiv 2$ ou $3 \mod 4$ le nombre 2 est ramifié.

Si $d \equiv 1 \mod 4$, f se réduit en $X^2 + X$ si $d \equiv 1 \mod 8$ et en $X^2 + X + 1$ si $d \equiv 5 \mod 8$. Dans le premier cas on a deux racines simples donc 2 est totalement décomposé, dans l'autre cas le polynôme est irréductible.

2.7 Rappels sur le discriminant

Soit $\mathcal{A}$ un anneau commutatif et $\mathcal{B}$ une $\mathcal{A}$-algèbre libre de type fini comme $\mathcal{A}$-module.

Pour $x \in \mathcal{B}$, $m_x : y \longmapsto xy$ est $\mathcal{A}$-linéaire de $\mathcal{B}$ dans $\mathcal{B}$. On définit comme dans le cas des extensions de corps $Tr_{\mathcal{B}/\mathcal{A}}(x) = Tr(m_x) \in \mathcal{A}$.

Si $(e_1, \ldots, e_d)$ est une famille d'éléments de $\mathcal{B}$, on en définit le *discriminant* par :

$$disc_{\mathcal{B}/\mathcal{A}}(e_1, \ldots, e_d) = \det(Tr_{\mathcal{B}/\mathcal{A}}(e_i e_j))_{1 \leqslant i,j \leqslant d}$$

Si $f_j = \sum a_{i,j} e_i$ alors $disc_{\mathcal{B}/\mathcal{A}}(f_1, \ldots, f_d) = (\det M)^2 disc_{\mathcal{B}/\mathcal{A}}(e_1, \ldots, e_d)$ où $M = (a_{i,j})_{1 \leqslant i,j \leqslant d}$.

Le discriminant de $\mathcal{B}$ sur $\mathcal{A}$, $disc(\mathcal{B}/\mathcal{A})$, est la classe dans $\mathcal{A}/(\mathcal{A}^\times)^2$ de $disc_{\mathcal{B}/\mathcal{A}}(e_1, \ldots, e_d)$ où $(e_1, \ldots, e_d)$ est une base quelconque de $\mathcal{B}$ sur $\mathcal{A}$.

Exemple 2.7.1. *Si $f \in \mathcal{A}[T]$ est unitaire de degré d et $\mathcal{B} = \mathcal{A}[T]/f(T)$:*

$$disc_{\mathcal{B}/\mathcal{A}}(1, T, \ldots, T^{d-1}) = disc(f)$$

(où on considère les classes dans $\mathcal{B}$ des T^i)

Remarque 2.7.2. *Si $\mathcal{A} \in \mathbb{Z}$, comme $(\mathbb{Z}^\times)^2 = \{1\}$ on a $disc_{\mathcal{B}/\mathbb{Z}} \in \mathbb{Z}$. On note $d_{\mathbf{F}}$ le discriminant d'un corps de nombres $\mathbf{F}$, plutôt que $disc(\mathcal{O}_{\mathbf{F}}/\mathbb{Z})$.*

Proposition 2.7.3. *On suppose que $\mathcal{A}$ est un corps. On a équivalence entre :*
- *$disc_{\mathcal{B}/\mathcal{A}} \neq 0$*
- *$\mathcal{B}$ est produit d'extensions séparables de $\mathcal{A}$.*

Démonstration. (Démonstration partielle, se référer à [5] pour une preuve complète)
- Si $\mathcal{B}/\mathcal{A}$ est une extension finie de corps, $Tr_{\mathcal{B}/\mathcal{A}} \neq 0$ si et seulement si $\mathcal{B}/\mathcal{A}$ est séparable. Par suite $disc_{\mathcal{B}/\mathcal{A}} \neq 0$ si et seulement si $\mathcal{B}/\mathcal{A}$ est séparable.
- Si $\mathcal{B} = \prod \mathcal{B}_i$ où les $B_i, i = 1 \ldots r$ sont des A-algèbres de dimension finie, alors $disc_{\mathcal{B}/\mathcal{A}} = \prod disc_{\mathcal{B}_i/\mathcal{A}}$. Ceci donne l'implication réciproque.

Prouvons le sens direct :

Si $x \in \mathcal{B}$ est nilpotent, $x \neq 0$, alors $x\mathcal{B}$ est formé d'éléments nilpotents et $(\forall y \in \mathcal{B})(Tr_{\mathcal{B}/\mathcal{A}}(xy) = 0)$.

On considère une base $(e_1, \ldots, e_n)$ de $\mathcal{B}$ dont les d premiers éléments sont dans $x\mathcal{B}$. Alors :

$$disc_{\mathcal{B}/\mathcal{A}}(e_1, \ldots, e_n) = \begin{vmatrix} 0 & \ldots & 0 & \ldots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \ldots & 0 & \ldots & 0 \\ \vdots & & \vdots & ? & ? \\ 0 & \ldots & 0 & ? & ? \end{vmatrix} = 0$$

où seuls les éléments de la matrice carrée $(n-d, n-d)$ représentée par des points d'interrogation peuvent être non nuls.

Donc si $disc_{\mathcal{B}/\mathcal{A}} \neq 0$ alors $\mathcal{B}$ n'a pas d'élément nilpotent non nul, c'est donc un produit de corps $\mathcal{B} = \prod \mathcal{A}_i$ où $\mathcal{A}_i$ est une extension de $\mathcal{A}$.

Justifions ce point :

$\mathcal{B} = \mathcal{A}[t] \simeq \mathcal{A}[T]/P(T)$

Que $\mathcal{B}$ n'ait pas d'élément nilpotent signifie que P est produit de facteurs irréductibles distincts $P = P_1 \ldots P_r$ donc $P = \prod(\mathcal{A}[T]/P_i[T])$. Donc $disc_{\mathcal{B}/\mathcal{A}} = \prod disc_{\mathcal{A}_i/\mathcal{A}}$ est non nul si et seulement si $\mathcal{A}_i/\mathcal{A}$ est séparable pour tout i. □

Supposons que $\mathcal{A}$ est un anneau de Dedekind de corps des fractions $\mathbf{F}$, que $\mathbf{E}/\mathbf{F}$ est une extension finie séparable de degré d, et que $\mathcal{B}$ est la clôture intégrale de $\mathcal{A}$ dans $\mathbf{E}$. On sait alors que $\mathcal{B}$ est un anneau de Dedekind (cf [5] par exemple).

L'anneau $\mathcal{B}$ est alors un $\mathcal{A}$-module de type fini libre de rang d sur $\mathcal{A}$ dès que $\mathcal{A}$ est principal.

$disc_{\mathcal{B}/\mathcal{A}}$ est l'idéal de $\mathcal{A}$ engendré par les $disc_{\mathcal{B}/\mathcal{A}}(e_1,\ldots,e_d)$ où $(e_1,\ldots,e_d)$ est une famille quelconque d'éléments de $\mathcal{B}$. Si $\mathcal{B}$ est libre de type fini sur $\mathcal{A}$ on voit que $disc_{\mathcal{B}/\mathcal{A}}$ est l'idéal engendré par les discriminants des bases de $\mathcal{B}$ sur $\mathcal{A}$.

Si $\mathcal{S}$ est une partie multiplicative de $\mathcal{A}$ contenant 1 mais pas 0 alors $disc_{\mathcal{S}^{-1}\mathcal{B}/\mathcal{S}^{-1}\mathcal{A}} = \mathcal{S}^{-1}disc_{\mathcal{B}/\mathcal{A}}$.

Proposition 2.7.4. *Sous les hypothèses précédentes, soit $\mathfrak{p}$ un idéal maximal de $\mathcal{A}$, alors si on pose $\mathcal{S} = \mathcal{A} - \mathfrak{p}$, $\mathcal{A}' = \mathcal{S}^{-1}\mathcal{A}$, $\mathcal{B}' = \mathcal{S}^{-1}\mathfrak{p}$,$\mathfrak{p}' = \mathcal{S}^{-1}\mathfrak{p}$:*

$$\text{Écrivons } \mathfrak{p}\mathcal{B} = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})}$$

Alors les conditions suivantes sont équivalentes :

1. *$e(\mathfrak{q}|\mathfrak{p}) = 1$ pour tout $\mathfrak{q}|\mathfrak{p}$ et $\mathcal{B}/\mathfrak{q}$ est une extension séparable de $\mathcal{A}/\mathfrak{p}$.*
2. *$\mathfrak{p}$ ne divise pas $disc(\mathcal{B}/\mathcal{A})$.*

Cas particulier : $\mathbf{E}/\mathbf{F}$ est une extension de corps de nombres, $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_{\mathbf{F}}$, on pose $\mathcal{A} = \mathcal{O}_{\mathbf{F}}$, $\mathcal{B} = \mathcal{O}_{\mathbf{E}}$. On note alors $disc(\mathbf{E}/\mathbf{F}) = disc(\mathcal{O}_{\mathbf{E}}/\mathcal{O}_{\mathbf{F}})$.

On a équivalence entre :
– $\mathfrak{p}$ est non ramifié dans $\mathbf{E}/\mathbf{F}$.
– $\mathfrak{p}$ ne divise pas $disc(\mathbf{E}/\mathbf{F})$.

Démonstration. (voir [5] pour les détails)

En localisant en $\mathcal{S} = \mathcal{A} - \mathfrak{p}$ on se ramène à prouver le résultat demandé pour $\mathcal{A}'$, $\mathcal{B}'$ et $\mathfrak{p}'$. On prend une base $(e_1,\ldots,e_d)$ de $\mathcal{B}'$ sur $\mathcal{A}'$, qui donne une base $(\bar{e_1},\ldots,\bar{e_d})$ de $\mathcal{B}'/\mathfrak{p}\mathcal{B}'$ sur $\mathcal{A}'/\mathfrak{p}$ et le discriminant de $(e_1,\ldots,e_d)$ est la réduction modulo $\mathfrak{p}$ de $disc_{\mathcal{B}'/\mathcal{A}'}(e_1,\ldots,e_d)$.

$\mathfrak{p}'$ divise $disc_{\mathcal{B}'/\mathcal{A}'}$ signifie que $disc_{(\mathcal{B}'/\mathfrak{p}\mathcal{B}')/(\mathcal{A}'/\mathfrak{p}'\mathcal{A}')}(\bar{e_1},\ldots,\bar{e_d}) = 0$.

Par la proposition précédente, $\mathcal{B}'/\mathfrak{p}'\mathcal{B}'$ est un produit d'extensions séparables de $\mathcal{A}'/\mathfrak{p}'$. Mais :

$$\mathfrak{p}'\mathcal{B}' = \prod_{\mathfrak{q}'|\mathfrak{p}'} \mathfrak{q}'^{e(\mathfrak{q}'|\mathfrak{p}')}$$

donne $\mathcal{B}'/\mathfrak{p}'\mathcal{B}' = \prod \mathcal{B}'/\mathfrak{q}'^{e(\mathfrak{q}'|\mathfrak{p}')}$. Mézalor le fait que $\mathcal{B}'/\mathfrak{p}'\mathcal{B}'$ soit un produit d'extensions séparables de $\mathcal{A}'/\mathfrak{p}'$ se traduit par $e(\mathfrak{q}'|\mathfrak{p}') = 1$ pour tout $\mathfrak{q}'|\mathfrak{p}$ et $\mathcal{B}'/\mathfrak{q}'$ est séparable sur $\mathcal{A}'/\mathfrak{p}'$. □

Retour sur la situation du corps de nombres :

$$\begin{array}{ccc} \mathbf{E} & & \mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}} \\ {\scriptstyle finie}\,\big| & & \big| \\ \mathbf{F} & & \mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}} \qquad \mathfrak{p} \end{array}$$

Lemme 2.7.5. *Soit $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_{\mathbf{F}}$ et $\mathcal{S} = \mathcal{O}_{\mathbf{F}} - \mathfrak{p}$.*

Supposons $\mathbf{E} = \mathbf{F}[x]$, $x \in \mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}}$ et notons f le polynôme minimal de x sur $\mathbf{F}$. Supposons $disc(f) \notin \mathcal{S}^{-1}\mathfrak{p}$ (donc est inversible dans $\mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}$).

Alors $\mathfrak{p}$ est non ramifié dans $\mathbf{E}/\mathbf{F}$. On a $\mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}} = \mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}[x]$, on peut alors appliquer la proposition donnant la décomposition de $\mathfrak{p}$ en termes de $\bar{f} \in (\mathcal{O}_{\mathbf{F}}/\mathfrak{p})[T]$.

Démonstration. On a $\mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}[x] \subseteq \mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}}$, qui admettent pour bases respectivement $(1, x, \ldots, x^{d-1})$ et $(e_1, \ldots, e_d)$, où $d = d^\circ f = [\mathbf{E} : \mathbf{F}]$.

Alors $disc(f) = disc_{\mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}}/\mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}}(1, x, \ldots, x^{d-1})$.

On a vu que $disc_{\mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}}/\mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}}(1, x, \ldots, x^{d-1}) = \alpha^2 disc(e_1, \ldots, e_d)$ donc l'idéal $(disc(f))$ est un multiple de $disc(\mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}}/\mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}})$.

L'hypothèse dit que $(disc(f)) = \mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}$ donc α est une unité et comme $(e_1, \ldots, e_d)$ est une base de $\mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}}$ sur $\mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}$ alors $(1, x, \ldots, x^{d-1})$ en est aussi une base. Par suite $\mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}} = \mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}[x]$ d'où le lemme. □

Remarque 2.7.6. *Si $\mathbf{E}/\mathbf{F}$ est un corps de nombres, $\mathbf{E} = \mathbf{F}[x]$, $x \in \mathbf{F}$, alors sauf pour un nombre fini d'idéaux maximaux $\mathfrak{p}$ de $\mathcal{O}_{\mathbf{F}}$ on a $x \in \mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}$ ($\mathcal{S} = \mathcal{A} - \mathfrak{p}$) et $disc(f) \notin \mathcal{S}^{-1}\mathfrak{p}$.*

Remarque 2.7.7. *Si avec les notations précédentes on a $disc(f) \notin (\mathcal{S}^{-1}\mathfrak{p})^2$ alors $\mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}} = \mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}[x]$ mais $\mathfrak{p}$ peut être ramifié dans $\mathbf{E}/\mathbf{F}$. En effet on a toujours :*

$$disc_{\mathcal{S}^{-1}\mathcal{O}_{\mathbf{E}}/\mathcal{S}^{-1}\mathcal{O}_{\mathbf{F}}}(1, x, \ldots, x^{d-1}) = \alpha^2 disc(e_1, \ldots, e_d)$$

et l'hypothèse implique que α est une unité.

2.8 Corps cyclotomique

On se place dans la situation $\mathbf{F} = \mathbb{Q}$, $\mathbf{E} = \mathbb{Q}(e^{\frac{i2\pi}{n}}) \subseteq \mathbb{C}$. Alors $Gal(\mathbf{E}/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$. On peut supposer n impair ou multiple de 4.

Théorème 2.8.1.

1. *Les nombres premiers ramifiés dans $\mathbf{E}/\mathbb{Q}$ sont les diviseurs premiers de n.*
2. *Si p est un premier ne divisant pas n alors $Frob_p$ est $p \mod n$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Démonstration.

1. $\mathbf{E}$ est une extension de décomposition de X^n-1 sur $\mathbb{Q}$. Si p est ramifié dans $\mathbf{E}/\mathbb{Q}$ alors X^n-1 a nécessairement une racine double modulo p : $X^n-1 \in \mathbb{F}_p[X]$ n'est pas premier à sa dérivée nX^{n-1} donc $n \equiv 0 \mod p$: $p \mid n$.

   Inversement il suffit de montrer que p impair est ramifié dans $\mathbb{Q}\left(e^{\frac{\imath 2\pi}{n}}\right)/\mathbb{Q}$, et 2 est ramifié dans $\mathbb{Q}\left(e^{\imath 2\pi}4\right) = \mathbb{Q}(\imath)$, déjà vu.

   Traitons le cas où p est impair : posons $\zeta = e^{\frac{\imath 2\pi}{p}}$, racine de $\varphi_p = 1+T+\cdots+T^{p-1}$ et on a $\varphi_p(1) = p = \prod(1-\zeta^i)$, or $1-\zeta^i$ est un multiple de $1-\zeta$ dans $\mathcal{O}_{\mathbf{E}}$ ($\mathbf{E} = \mathbb{Q}(\zeta)$). p est donc un multiple de $(1-\zeta)^{p-1}$ dans $\mathcal{O}_{\mathbf{E}}$.

$$p\mathcal{O}_{\mathbf{E}} = \prod_{\mathfrak{q}\mid\mathfrak{p}} \mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})} \text{ et } \sum_{\mathfrak{q}\mid\mathfrak{p}} e(\mathfrak{q}|\mathfrak{p}) f(\mathfrak{q}|\mathfrak{p}) = p-1$$

   donc $(1-\zeta)\mathcal{O}_{\mathbf{E}}$ est un idéal maximal de $\mathcal{O}_{\mathbf{E}}$ et $p\mathcal{O}_{\mathbf{E}} = ((1-\zeta)\mathcal{O}_{\mathbf{E}})^{p-1}$ donc p est ramifié pour $p \geqslant 3$ d'où le résultat.

2. Si p ne divise pas n, $\sigma = Frob_p \in (\mathbb{Z}/n\mathbb{Z})^\times$ est caractérisé par $\sigma\mathfrak{q} = \mathfrak{q}$. Ceci doit être vrai en particulier pour $\zeta = e^{\frac{2\imath\pi}{p}}$. Mais $X^n-1 \in \mathbb{F}_p[X]$ n'a pas de racine double dans une extension. Cela implique que les ζ^a, $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ sont tous distincts modulo $\mathfrak{q}$.

   Par suite, pour obtenir $\sigma\zeta \equiv \zeta^p \mod \mathfrak{q}$ on doit prendre $\sigma = p \mod n$ d'où le résultat. □

Rappel : Si $Frob_p \in (\mathbb{Z}/n\mathbb{Z})^\times$ a pour ordre r alors :

$$p\mathcal{O}_{\mathbf{E}} = \prod_{i=1}^{\varphi(n)/r} \mathfrak{q}_i$$

avec $f(\mathfrak{q}_i/p\mathbb{Z}) = r$.

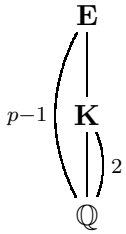
2.9 Loi de réciprocité quadratique

$\mathbf{K} = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{N}$, $d \geqslant 2$ sans facteurs carrés. On peut identifier $Gal(\mathbf{K}/\mathbb{Q})$ à $\{-1,1\}$.

Les nombres premiers ramifiés dans $\mathbf{K}/\mathbb{Q}$ sont les diviseurs premiers de d, plus 2 si $d \equiv 3 \mod 4$.

- $Frob_p = \left(\frac{d}{p}\right)$ si p est impair et ne divise pas d.
- $Frob_2 = 1$ si $d \equiv 1 \mod 8$.
- $Frob_2 = -1$ si $d \equiv 5 \mod 8$.

Fixons p premier impair et considérons $\mathbf{E} = \mathbb{Q}\left(e^{\frac{\imath 2\pi}{p}}\right)$. $Gal(\mathbf{E}/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times$ donc est isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$. On a en particulier un unique sous-groupe d'indice 2 et $\mathbf{E}$ a une unique sous-extension $\mathbf{K}/\mathbb{Q}$ où $[\mathbf{K} : \mathbb{Q}] = 2$:



Dans $\mathbf{E}/\mathbb{Q}$, le seul nombre premier ramifié est p. Il l'est *a fortiori* dans $\mathbf{K}/\mathbb{Q}$ et par conséquent on a $\mathbf{K} = \mathbb{Q}(\sqrt{p^\times})$ où $p^\times = (-1)^{\frac{p-1}{2}}p$ et $p^\times \equiv 1 \mod 4$.

$$\begin{array}{ccc} Gal(\mathbf{E}/\mathbb{Q}) & \longrightarrow & Gal(\mathbf{K}/\mathbb{Q}) \\ \sigma & \longmapsto & \sigma^{\frac{p-1}{2}} \end{array}$$

donne

$$\begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^\times & \longrightarrow & \{\pm 1\} \\ x & \longmapsto & x^{\frac{p-1}{2}} \end{array}$$

Soit q un nombre premier impair distinct de p. $Frob_q \in Gal(\mathbf{E}/\mathbb{Q})$ s'identifie à la classe de q dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

$Frob_q \in Gal(\mathbf{K}/\mathbb{Q})$ est l'image de $Frob_q \in Gal(\mathbf{E}/\mathbb{Q})$ et par suite $Frob_q \in Gal(\mathbf{K}/\mathbb{Q}) = \{\pm 1\}$ n'est autre que $\left(\frac{q}{p}\right)$. Mais on a aussi $\mathbf{K} = \mathbb{Q}(\sqrt{p^\times})$ donc $Frob_q \in Gal(\mathbf{K}/\mathbb{Q}) = \{\pm 1\}$ est $\left(\frac{p^\times}{q}\right)$. Comme $p^\times = (-1)^{\frac{p-1}{2}}p$ on a :

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

Si $q = 2$ on a encore que $Frob_2 \in Gal(\mathbf{K}/\mathbb{Q})$ et $Frob_2 = \left(\frac{2}{p}\right)$.

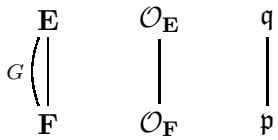
On vérifie cette fois-ci la loi par le calcul. $Frob_2 \in Gal(\mathbf{K}/\mathbb{Q})$ vaut 1 si $p^\times \equiv 1 \mod 8$ et -1 si $p^\times \equiv 5 \mod 8$, d'où :

p	mod 8	$p^\times$	mod 8	$Frob_{\mathbf{K}/\mathbb{Q}} = Frob_2$
	1		1	1
	3		5	-1
	5		5	-1
	7		1	1

Chapitre 3

Techniques analytiques

3.1 Densités



À $\mathfrak{p}$ non ramifié dans $\mathbf{E}/\mathbf{F}$ on associe $Frob(\mathfrak{q}|\mathfrak{p}) \in G$. Quelle est la répartition des $Frob(\mathfrak{q}|\mathfrak{p})$ dans G quand $\mathfrak{p}$ varie ?

On «mesure» un idéal maximal $\mathfrak{p}$ de $\mathcal{O}_{\mathbf{F}}$ par sa norme $N\mathfrak{p} = |\mathcal{O}_{\mathbf{F}}/\mathfrak{p}| \in p\mathbb{Z}$.

Soit $\mathcal{P}$ un sous-ensemble de $\mathcal{P}_{\mathbf{F}}$, ensemble des idéaux maximaux de $\mathbf{F}$.

Définition 3.1.1. *On dit que $\mathcal{P}$ a densité arithmétique $\delta \in [0,1]$ si*

$$\delta_X = \frac{|\{(\mathfrak{p} \in \mathcal{P})(N\mathfrak{p} \leqslant x)\}|}{|\{(\mathfrak{p} \in \mathcal{P}_{\mathbf{F}})(N\mathfrak{p} \leqslant x)\}|} \to \delta \quad (x \to \infty)$$

On utilisera plutôt la densité analytique :

Pour $s \in \mathbb{R}$, $s > 1$, on verra que la série $\sum_{\mathfrak{p}\in\mathcal{P}}(N\mathfrak{p})^{-s}$ converge et définit une fonction continue sur $]1, +\infty[$ (il y a une singularité au voisinage de 1).

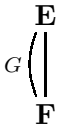
Définition 3.1.2. *On dit que $\mathcal{P}$ a densité analytique $\delta \in [0,1]$ si :*

$$\frac{\sum_{\mathfrak{p}\in\mathcal{P}}(N\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in\mathcal{P}_{\mathbf{F}}}(N\mathfrak{p})^{-s}} \to \delta \quad (s \to 1_+)$$

On sait (voir [4]) que si un ensemble a densité arithmétique δ alors il a densité analytique δ. Pour tous les ensembles que nous allons examiner, nous allons prouver qu'il existe une densité analytique et des théorèmes taubériens donneront l'existence d'une densité arithmétique, on pourra même obtenir un terme d'erreur en x.

Attention cependant, il existe des ensembles de nombres premiers admettant une densité analytique mais non une densité arithmétique. Un tel ensemble est exhibé dans [6], la preuve est donnée dans [2].

3.2 Le théorème de Čebotarev



Soit C une classe de conjugaison de G. On note $\mathcal{P}_C$ l'ensemble des idéaux maximaux de $\mathcal{O}_{\mathbf{F}}$ non ramifiés dans $\mathbf{E}/\mathbf{F}$ tels que $Frob(\mathfrak{q}|\mathfrak{p}) \in C$ pour tout $\mathfrak{q}|\mathfrak{p}$.

Théorème 3.2.1. *$\mathcal{P}_C$ admet pour densité analytique $\frac{|C|}{|G|}$*

Cas particulier :

$\mathbf{F} = \mathbb{Q}$, $\mathbf{E} = \mathbb{Q}\left(e^{\frac{i2\pi}{n}}\right)$, $G = (\mathbb{Z}/n\mathbb{Z})^\times$.

Alors p premier est non ramifié dans $\mathbf{E}/\mathbf{F}$ si et seulement si p ne divise pas n, et $Frob_p$ est la classe de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

Le théorème de Čebotarev dit : $\{p$ ne divisant pas $n | p \equiv a \mod n\}$ a pour densité analytique $\frac{1}{\varphi(n)}$. C'est le théorème de Dirichlet sur les progressions arithmétiques de nombres premiers.

3.3 Convergence

On considère des sommes ou produits infinis de nombres complexes indexés par un ensemble dénombrable I :

Soit I un ensemble dénombrable, $(x_i)_{i\in I}$ est une famille de nombres complexes. On dit que la famille $(x_i)_{i\in I}$ est sommable de somme $x \in \mathbb{C}$ si pour tout ε strictement positif il existe un sous-ensemble fini J de I tel que pour tout J' fini vérifiant $J \subseteq J' \subseteq I$ on ait :

$$\left|\left(\sum_{i\in J'} x_i\right) - x\right| \leqslant \varepsilon$$

On sait que $(x_i)_{i\in I}$ est sommable si et seulement si $(|x_i|)_{i\in I}$ est sommable ou, de manière équivalente, si et seulement si les $\sum_{i\in J} |x_i|$ ($J \subseteq I$ fini) sont majorées uniformément en J.

Si la famille est sommable, le x ci-dessus est unique et s'écrit $\sum_{i\in I} x_i$ et $|\sum x_i| \leqslant \sum |x_i|$. On dit aussi que la série $\sum x_i$ est absolument convergente.

Si on a une partition de I en $\coprod_{k\in K} J_k$ et si $(x_i)_{i\in I}$ est une famille sommable alors pour tout $k \in K$, $(x_i)_{i\in J_k}$ est sommable. Si y_k est sa somme, $(y_k)_{k\in K}$ est sommable et $\sum_{k\in K} y_k = \sum_{i\in I} x_i$.

Fonction ζ de Riemann :

Pour $\Re(s) > 1$ on définit :

$$\zeta(s) = \sum_{n \geqslant 1} n^{-s} = \prod_{p \text{ premier}} \left(\frac{1}{1 - p^{-s}} \right)$$

Formellement, ceci correspond simplement à l'unicité de la décomposition des entiers en facteurs premiers. Il convient cependant de donner un sens au produit infini :

Soit $(y_i)_{i \in I}$ une famille de nombres complexes non nuls. On dit que la famille $(y_i)_{i \in I}$ est multipliable de produit $y \in \mathbb{C}^\times$ si pour tout $\varepsilon > 0$ il existe un sous-ensemble fini J de I tel que pour tout sous-ensemble fini J' de I contenant J :

$$\left| \left(\prod_{i \in J'} y_i \right) - y \right| \leqslant \varepsilon$$

On dit alors que $\prod_{i \in I} y_i$ converge absolument.

On peut transposer le résultat obtenu plus haut pour une partition de l'ensembles des indices sans difficulté aucune.

Proposition 3.3.1. *$y_i = 1 + u_i$, $u_i \neq -1$. Alors $(y_i)_{i \in I}$ est multipliable si et seulement si $(x_i)_{i \in I}$ est sommable.*

Démonstration. Voir [1], p. 16. □

Remarque 3.3.2. *En pratique on considère des $\sum_I x_i$ où x_i est de la forme $a_i f(n_i)$, $n_i \in \mathbb{N}^\times$ dépendant de $i \in I$, $f : \mathbb{N}^\times \to \mathbb{C}$ et $i \mapsto n_i$ a des fibres finies.*

On peut alors poser

$$a(n) = \sum_{i \in I, n_i = n} a_i$$

Si la famille $\{a_i f(n_i)\}_{i \in I}$ est sommable alors $\{a(n)f(n)\}_{n \in \mathbb{N}^\times}$ l'est aussi et on a :

$$\sum_{i \in I} a_i f(n_i) = \sum_{n \in \mathbb{N}^\times} a(n) f(n)$$

La réciproque est vraie si les a_i et les $f(n_i)$ sont positifs.

Soit $S \subseteq \mathbb{C}$. On se donne une famille sommable de réels positifs $(a_i)_{i \in I}$ et pour chaque $i \in I$ une application $\alpha_i : S \to \mathbb{C}$ telle que $|\alpha_i(s)| \leqslant a_i$ pour $s \in S$. Alors pour chaque $s \in S$, $\{\alpha_i(s)\}_{i \in I}$ est sommable et :

$$\left| \sum_{i \in I} \alpha_i(s) \right| \leqslant \sum_{i \in I} a_i$$

Si les α_i sont des fonctions continues de $s \in S$ il en est de même de $\sum \alpha_i$. Si S est une partie ouverte de $\mathbb{C}$ et que les α_i sont analytiques dans S il en est de même de leur somme.

3.4 Un lemme sur les séries de Dirichlet

Définition 3.4.1. *Une série de Dirichlet est une série de la forme*

$$f(s) = \sum_{n \geqslant 1} a_n n^{-s} \text{ où } (a_n)_{n \geqslant 1} \in \mathbb{C}^{\mathbb{N}}$$

Lemme 3.4.2. *Soit $f(s) = \sum_{n \geqslant 1} a_n n^{-s}$ une série de Dirichlet, posons $S(x) = \sum_{1 \leqslant n \leqslant x} a_n$.*

On suppose qu'il existe des réels a, b tels que $|S(x)| \leqslant a x^b$ pour $x \geqslant 1$. Alors $f(s)$ converge uniformément en s dans un secteur de la forme :

$$\begin{aligned} \Re(s) &\geqslant b + \delta \\ \frac{\Re(s-b)}{|s-b|} &\geqslant \varepsilon \end{aligned}$$

pour tous δ et ε strictement positifs.

En particulier la série $f(s)$ converge pour $\Re(s) > b$.

Démonstration. Soient u et v des entiers avec $v > u \geqslant 1$, $a_n = S_n - S_{n-1}$.

$$\sum_{n=u}^{v} a_n n^{-s} = \frac{S(v)}{v^s} - \frac{S(u-1)}{u^s} + \sum_{n=u}^{v-1} \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right)$$

or

$$\frac{1}{n^s} - \frac{1}{(n+1)^s} = s \int_n^{n+1} \frac{dt}{t^{s+1}}$$

d'où pour $\sigma = \Re(s) > b$:

$$\begin{aligned} \left| \sum_{n=v}^{u} a_n n^{-s} \right| &\leqslant \frac{a}{v^{\sigma-b}} + \frac{a}{u^{\sigma-b}} + \sum_{n=u}^{v-1} \left(|s| a n^b \int_n^{n+1} \frac{dt}{t^{\sigma+1}} \right) \\ &\leqslant \frac{a}{v^{\sigma-b}} + \frac{a}{u^{\sigma-b}} + \frac{|s| a}{(\sigma-b) u^{\sigma-b}} \\ &\leqslant \frac{2a}{u^{\sigma-b}} + \frac{a|s|}{(\sigma-b) u^{\sigma-b}} \end{aligned}$$

Or on a :

$$\frac{|s|}{\sigma - b} \leqslant \frac{|s-b|}{\sigma-b} + \frac{b}{\sigma-b}$$

Et :

$$\Re(s) > b + \delta \ ; \ \frac{|s-b|}{\sigma-b} \leqslant \frac{1}{\varepsilon} \ ; \ \frac{b}{\sigma-b} \leqslant \frac{b}{\delta}$$

D'où une majoration uniforme sur S. □

Exemple 3.4.3.

- *$\zeta(s)$ converge pour $\Re(s) > 1$ et la convergence est absolue ($S(x) \leqslant x$).*
- *soit $m \geqslant 2$, $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}$ un caractère. On définit :*

$$L(\chi, s) = \sum_{n \geqslant 1, (n,m)=1} \chi(n) n^{-s}$$

Si χ n'est pas le caractère trivial, les sommes $S(x)$ sont uniformément bornées. Le lemme nous donne donc, avec $b = 0$, la convergence pour $\Re(s) > 0$, qui est uniforme sur les secteurs comme plus haut.
Si χ est le caractère trivial χ_0 on a :

$$L(\chi_0, s) = \left(\prod_{p|m} (1 - p^{-s}) \right) \zeta(s)$$

On peut prolonger ζ en une fonction méromorphe sur le demi-plan ouvert $\Re(s) > 0$ avec un pôle simple en $s = 1$.

On considère $f(s) = (1 - 2^{1-s})\zeta(s) = \sum_{n \geqslant 1} a_n n^{-s}$

avec $a_n = 1$ si n est impair et $a_n = -1$ si n est pair.

Les sommes partielles valent $1, 0, 1, 0, \ldots$ donc sont bornées d'où convergence dans $\Re(s) > 0$ vers une fonction holomorphe de s. $\zeta(s)$ est donc méromorphe dans $\Re(s) > 0$ dont les pôles éventuels sont dans $1 + \frac{2\imath\pi}{\ln 2}\,\mathbb{Z}$.

En procédant de même pour $g(s) = (1 - 3^{1-s})\zeta(s) = \sum_{n \geqslant 1} b_n n^{-s}$, on a $b_n = -2$ si $3|n$ et $b_n = 1$ sinon, on montre que les pôles éventuels de la fonction ζ sont dans $1 + \frac{2\imath\pi}{\ln 3}\,\mathbb{Z}$.

Donc ζ n'a de pôle qu'en 1, et y a bien un pôle car la série harmonique diverge.

Remarque 3.4.4. *sous les hypothèses du lemme, si $\frac{S(x)}{x} \to \mathbb{C}$ alors $(s - 1)f(s) \to C$ quand $s \to 1$ dans un secteur de la forme déjà décrite.*

3.5 La fonction ζ de Dedekind d'un corps de nombres

Soit $\mathbf{F}$ un corps de nombres, on pose :

$$\zeta_{\mathbf{F}}(s) = \sum_{\mathfrak{a} \text{ idéal non nul de } \mathcal{O}_{\mathbf{F}}} (N\mathfrak{a})^{-s}$$

Pour la convergence absolue de cette série on se ramène à la série de Dirichlet $\sum a_n n^{-s}$ où a_n est le nombre d'idéaux de $\mathcal{O}_{\mathbf{F}}$ de norme n.

Lemme 3.5.1. *Soit p un nombre premier. Il y a au plus $[\mathbf{F} : \mathbb{Q}]$ idéaux maximaux $\mathfrak{p}$ de $\mathcal{O}_{\mathbf{F}}$ dont la norme est une puissance de p.*

Démonstration. Si $N\mathfrak{p} = p^f$ alors $\mathfrak{p}|p$ et on utilise la formule :

$$\sum_{\mathfrak{p}|p} e(\mathfrak{p}|p) f(\mathfrak{p}|p) = [\mathbf{F} : \mathbb{Q}]$$

Cela implique la finitude si n est une puissance d'un nombre premier. Le cas général s'en déduit en factorisant $\mathfrak{a}$ en produit d'idéaux premiers. □

On veut appliquer le lemme en estimant $S(x) = |\{\mathfrak{a} \text{ idéal de } \mathcal{O}_\mathbf{F}; N\mathfrak{a} \leqslant x\}|$

Théorème 3.5.2. *(admis pour le moment)*
Quand $X \to \infty$ on a $S(X) = c_\mathbf{F} X + O(X^{1-\frac{1}{d}})$ où $d = [\mathbf{F} : \mathbb{Q}]$. On a pour $c_\mathbf{F}$ une expression où interviennent le nombre de racines de l'unité dans $\mathbf{F}$, le nombre de classes d'idéaux de $\mathcal{O}_\mathbf{F}$ et le régulateur (déterminant construit à partir des unités de $\mathcal{O}_\mathbf{F}$).

Corollaire 3.5.3. *La fonction $\zeta_\mathbf{F}$ se prolonge en une fonction méromorphe sur $\Re(s) > 1 - \frac{1}{d}$ avec un pôle simple en 1 et résidu $c_\mathbf{F}$.*

Démonstration. On considère $f(s) = \zeta_\mathbf{F}(s) - c_\mathbf{F}\zeta(s) = \sum a_n n^{-s}$ qui converge absolument pour $\Re(s) > 1$.

Si $T(x) = \sum_{n \leqslant x} a_n$ on voit que $T(x) \leqslant \alpha x^{1-\frac{1}{d}}$ pour un $\alpha > 0$ et $x \geqslant 1$. Par le lemme, $f(s)$ converge pour $\Re(s) > 1 - \frac{1}{d}$ vers une fonction holomorphe. □

3.6 Produit eulérien pour la fonction ζ de Dedekind

On veut établir pour $\Re(s) > 1$ l'égalité :

$$\zeta_\mathbf{F}(s) = \sum_{\mathfrak{a} \text{ idéal de } \mathcal{O}_\mathbf{F}} (N\mathfrak{a})^{-s} = \prod_{\mathfrak{p} \text{ idéal maximal de } \mathcal{O}_\mathbf{F}} \left(1 - (N\mathfrak{p})^{-s}\right)^{-1}$$

Cas particulier : $\zeta_\mathbb{Q}(s) = \zeta(s) = \prod_{p \text{ premier}} (1 - p^{-s})^{-1}$

En écrivant ceci formellement on obtient :

$$\begin{aligned} \prod_{\mathfrak{p} \text{ idéal maximal}} &= \prod_{\mathfrak{p}} \left(1 + (N\mathfrak{p})^{-s} + (N\mathfrak{p})^{-2s} + \cdots + (N\mathfrak{p})^{-ks} + \ldots\right) \\ &= \sum_{r \geqslant 0, \mathfrak{p}_i \text{ maximaux }, k_i \geqslant 1} (N\mathfrak{p}_1)^{-k_1 s} (N\mathfrak{p}_2)^{-k_2 s} \ldots (N\mathfrak{p}_r)^{-k_r s} \end{aligned}$$

L'égalité avec $\sum (N\mathfrak{a})^{-s}$ vient de l'existence et de l'unicité de la décomposition de $\mathfrak{a}$ en produit d'idéaux maximaux.

Proposition 3.6.1. *Pour $\Re(s) > 1$ on a :*

$$\zeta_{\mathbf{F}}(s) = \prod_{\mathfrak{p} \in \mathcal{P}_{\mathbf{F}}} (1 - (N\mathfrak{p})^{-s})^{-1}$$

Démonstration.

On fixe s tel que $\Re(s) > 1$ et $\varepsilon > 0$.

Il existe un ensemble fini A d'idéaux non nuls de $\mathcal{O}_{\mathbf{F}}$ tel que si B est un ensemble fini contenant A d'idéaux non nuls de $\mathcal{O}_{\mathbf{F}}$:

$$\left| \zeta_{\mathbf{F}}(s) - \sum_{\mathfrak{a} \in B} (N\mathfrak{a})^{-s} \right| \leqslant \varepsilon$$

Prenons $\mathcal{P} \subseteq \mathcal{P}_{\mathbf{F}}$ fini contenant $\mathcal{P}_A$ l'ensemble des idéaux maximaux apparaissant dans les éléments de A. Posons k_A le plus grand exposant des idéaux $\mathfrak{p} \in \mathcal{P}_A$ intervenant dans les éléments de A. Alors :

$$(1 - (N\mathfrak{p})^{-s})^{-1} = \lim_{l \to \infty} 1 + (N\mathfrak{p})^{-s} + \cdots + (N\mathfrak{p})^{-ls}$$

On peut donc trouver $k \geqslant k_A$ tel que pour $l \geqslant k$:

$$\left| \prod_{\mathfrak{p} \in \mathcal{P}} \left(1 - (N\mathfrak{p})^{-s}\right)^{-1} - \prod_{\mathfrak{p} \in \mathcal{P}} \left(\sum_{0 \leqslant \alpha \leqslant l} (N\mathfrak{p})^{-\alpha s} \right) \right| \leqslant \varepsilon$$

On a donc :

$$\left| \prod_{\mathfrak{p} \in \mathcal{P}} (1 - (N\mathfrak{p})^{-s})^{-1} - \zeta_{\mathbf{F}}(s) \right| \leqslant 2\varepsilon$$

D'où le résultat. □

Remarque 3.6.2. *En reprenant la démonstration on voit que la convergence est uniforme dans les demi-plans $\Re(s) \geqslant \delta > 1$.*

Introduisons la série :

$$\eta(s) = \sum_{\mathfrak{p} \in \mathcal{P}_{\mathbf{F}}} \sum_{n \geqslant 1} \frac{1}{n} (N\mathfrak{p})^{-ns}$$

qui converge absolument pour $\Re(s) \geqslant \delta > 1$. En effet il y a au plus $[\mathbf{F} : \mathbb{Q}]$ idéaux de $\mathcal{O}_{\mathbf{F}}$ dont la norme est de la forme p^k où p est un nombre premier fixé et k un entier plus grand que 1 fixé. Cela vient de la formule $\sum e(\mathfrak{p}|p) f(\mathfrak{p}|p) = [\mathbf{F} : \mathbb{Q}]$.

On en déduit :

$$\begin{aligned}\sum_{\mathfrak{p}\in\mathcal{P}_{\mathbf{F}}}\sum_{n\geqslant 1}\frac{1}{n}\left|(N\mathfrak{p})^{-ns}\right| &\leqslant [\mathbf{F}:\mathbb{Q}]\sum_{p \text{ premier}}\sum_{n\geqslant 1}\frac{1}{n}p^{-n\Re(s)}\\ &\leqslant d\zeta(\delta) \text{ pour } \Re(s)\geqslant\delta>1\end{aligned}$$

On en déduit que la série $\eta_{\mathbf{F}}(s)$ converge absolument dans les demi-plans $\Re(s)\geqslant\delta>1$ et y définit une fonction holomorphe de s.

Lemme 3.6.3. *Si on prend la branche du logarithme complexe réelle pour x réel on a :*

$$\eta_{\mathbf{F}}(s)=\log\zeta_{\mathbf{F}}(s)=\sum_{\mathfrak{p}\in\mathcal{P}_{\mathbf{F}}}\log\left((1-(N\mathfrak{p})^{-s})^{-1}\right)$$

Démonstration.

$$\log\left(1-(N\mathfrak{p})^{-s}\right)^{-1}=\sum_{n\geqslant 1}\frac{1}{n}(N\mathfrak{p})^{-ns}$$

pour $\Re(s)\geqslant\delta>1$ car $|(N\mathfrak{p})^{-s}|=(N\mathfrak{p})^{-\Re(s)}\leqslant(N\mathfrak{p})^{-\delta}<1$ □

La fonction $\zeta_{\mathbf{F}}$ se prolonge au demi-plan $\Re(s)>1-\frac{1}{d}$ avec pôle simple en $s=1$. En particulier, quand $s\to 1_+$ on a $\zeta_{\mathbf{F}}(s)=\frac{c}{s-1}+O(1)$ pour un $c\neq 0$. Donc quand $s\to 1_+$ on a :

$$\eta_{\mathbf{F}}(s)=\log\left(\frac{1}{s-1}\right)+O(1)$$

Rappelons que :

$$\eta_{\mathbf{F}}(s)=\sum_{\mathfrak{p}\in\mathcal{P}_{\mathbf{F}}}\sum_{n\geqslant 1}\frac{1}{n}(N\mathfrak{p})^{-ns}$$

Posons :

$$\eta_{\mathbf{F}}(s)=\left(\sum_{\mathfrak{p}\in\mathcal{P}_{\mathbf{F}}}(N\mathfrak{p})^{-s}\right)+g_{\mathbf{F}}(s)$$

Lemme 3.6.4. *$g_{\mathbf{F}}(s)$ définit une fonction holomorphe bornée au voisinage de 1.*

Démonstration. Si $\Re(s)=\delta>1/2$:

$$|g_{\mathbf{F}}(s)|=\left|\sum_{\mathfrak{p}\in\mathcal{P}_{\mathbf{F}}}\sum_{n\geqslant 2}\frac{1}{n}(N\mathfrak{p})^{-ns}\right|\leqslant[\mathbf{F}:\mathbb{Q}]\sum_{p \text{ premier}}\sum_{n\geqslant 2}\frac{1}{n}p^{-n\delta}$$

car il y a au-dessus de p au plus $[\mathbf{F}:\mathbb{Q}]$ idéaux maximaux de $\mathcal{O}_{\mathbf{F}}$. Cette série converge pour $\delta>1/2$. □

On a donc, quand $s \to 1_+$, $\sum (N\mathfrak{p})^{-s} \sim \log\left(\frac{1}{s-1}\right)$

On peut donc dans l'expression de la densité analytique remplacer le dénominateur par $\log\left(\frac{1}{s-1}\right)$.

Conséquences :

1. Une partie finie $\mathcal{P}$ de $\mathcal{P}_{\mathbf{F}}$ a densité nulle. En effet la somme qui interviendra au numérateur sera bornée pour $s \to 1_+$
2. L'ensemble des idéaux maximaux $\mathfrak{p}$ de $\mathcal{O}_{\mathbf{F}}$ d'indice d'inertie au-dessus de $\mathbb{Q}$ plus grand que 2 est de densité nulle. En effet, pour $\mathfrak{p}|p$, $N\mathfrak{p}=p^{f(\mathfrak{p}|p)} \geqslant p^2$ donc la somme sera bornée.

Remarque 3.6.5. *Si $\mathcal{P}$ a densité δ on peut lui ajouter ou retrancher un ensemble de densité nulle sans changer δ.*

3.7 Décomposition et densité

Soit $\mathbf{E}/\mathbf{F}$ une extension galoisienne finie de corps de nombres de groupe G.

Théorème 3.7.1. *L'ensemble des idéaux maximaux de $\mathcal{O}_{\mathbf{F}}$ totalement décomposés dans $\mathbf{E}/\mathbf{F}$ a pour densité $\frac{1}{d}$ où $d = [\mathbf{E} : \mathbf{F}]$.*

Remarque 3.7.2. *C'est le cas particulier du théorème de Čebotarev où $C = \{\mathbf{1}_G\}$.*

Démonstration. Soit $\mathcal{P}$ l'ensemble considéré et $\mathcal{Q}$ l'ensemble des idéaux maximaux de $\mathcal{O}_{\mathbf{E}}$ au-dessus des éléments de $\mathcal{P}$. Alors l'application de $\mathcal{Q}$ dans $\mathcal{P}$ donnée par $\mathfrak{q} \mapsto \mathfrak{q} \cap \mathcal{O}_{\mathbf{F}}$ est surjective par définition, et au-dessus de $\mathfrak{p} \in \mathcal{P}$ il y a exactement d éléments de $\mathcal{Q}$. Si $\mathfrak{q}|\mathfrak{p}$, $N\mathfrak{q} = (N\mathfrak{p})^{f(\mathfrak{q}|\mathfrak{p})} = N\mathfrak{p}$.

Il s'ensuit :

$$\sum_{\mathfrak{p}\in\mathcal{P}} (N\mathfrak{p})^{-s} = \frac{1}{d} \sum_{\mathfrak{q}\in\mathcal{Q}} (N\mathfrak{q})^{-s} \text{ pour } \Re(s) > 1$$

Considérons l'ensemble $\mathcal{P}_{\mathbf{E}} - \mathcal{Q}$. Soit $\mathfrak{q} \in \mathcal{P}_{\mathbf{E}} - \mathcal{Q}$, notons $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_{\mathbf{F}}$. Alors si $\mathfrak{p}$ est ramifié dans $\mathbf{E}/\mathbf{F}$ et alors il y a un nombre fini de possibilités pour de tels $\mathfrak{p}$ donc pour les $\mathfrak{q}$ au-dessus de $\mathfrak{p}$, et la densité de l'ensemble des $\mathfrak{q} \in \mathcal{P}_{\mathbf{E}} - \mathcal{Q}$ au-dessus d'idéaux $\mathfrak{p}$ ramifiés dans $\mathbf{E}/\mathbf{F}$ est nulle.

Si $\mathfrak{p}$ est non ramifié dans $\mathbf{E}/\mathbf{F}$ mais pas totalement décomposé, alors $f(\mathfrak{q}|\mathfrak{p}) > 1$, et l'ensemble des $\mathfrak{q} \in \mathcal{P}_{\mathbf{E}} - \mathcal{Q}$ au-dessus d'idéaux $\mathfrak{p}$ non ramifiés dans $\mathbf{E}/\mathbf{F}$ est de densité nulle.

Comme $\mathcal{P}_{\mathbf{E}}$ s'écrit comme l'union disjointe de $\mathcal{Q}$ et de $\mathcal{P}_{\mathbf{E}} - \mathcal{Q}$, et que ce dernier est de densité nulle on en déduit que $\mathcal{Q}$ a densité 1 et donc que $\mathcal{P}$ a densité $\frac{1}{d}$. □

Remarque 3.7.3. *Soit* $\mathbf{K}/\mathbf{F}$ *une extension galoisienne finie de corps de nombres et* $\mathbf{E}/\mathbf{F}$ *une clôture galoisienne de* $\mathbf{K}/\mathbf{F}$. *On a vu que les idéaux maximaux de* $\mathcal{O}_\mathbf{F}$ *qui sont totalement décomposés dans* $\mathbf{K}/\mathbf{F}$ *sont ceux qui sont totalement décomposés dans* $\mathbf{E}/\mathbf{F}$.

Il s'ensuit que l'ensemble des idéaux maximaux de $\mathcal{O}_\mathbf{F}$ *totalement décomposés dans* $\mathbf{K}/\mathbf{F}$ *a pour densité* $\frac{1}{[\mathbf{E}:\mathbf{F}]}$. *Si cette densité vaut* $\frac{1}{[\mathbf{K}:\mathbf{F}]}$ *alors* $\mathbf{K} = \mathbf{E}$ *:* $\mathbf{E}$ *est galoisienne sur* $\mathbf{F}$.

Proposition 3.7.4. *Soit* $\mathbf{E}$ *et* $\mathbf{K}$ *deux extensions finies d'un corps de nombres* $\mathbf{F}$, $\mathbf{E}/\mathbf{F}$ *étant galoisienne. Si tout idéal maximal de* $\mathcal{O}_\mathbf{F}$ *totalement décomposé dans* $\mathbf{E}/\mathbf{F}$ *l'est aussi dans* $\mathbf{K}/\mathbf{F}$ *alors* $\mathbf{K}$ *est une sous-extension de* $\mathbf{E}/\mathbf{F}$.

Démonstration. On vient de voir qu'on ne change rien en substituant à $\mathbf{K}$ sa clôture galoisienne. On peut donc supposer $\mathbf{K}$ galoisienne sur $\mathbf{F}$.

Soit $\mathbf{EK}/\mathbf{F}$ un composé de $\mathbf{E}/\mathbf{F}$ et $\mathbf{K}/\mathbf{F}$. Les idéaux maximaux de $\mathcal{O}_\mathbf{F}$ qui y sont totalement décomposés forment un ensemble de densité $\frac{1}{[\mathbf{EK}:\mathbf{F}]}$ et sont totalement décomposés dans $\mathbf{E}/\mathbf{F}$ et $\mathbf{K}/\mathbf{F}$. Inversement, les idéaux maximaux totalement décomposés dans $\mathbf{E}/\mathbf{F}$ ont densité $\frac{1}{[\mathbf{E}:\mathbf{F}]}$, le sont aussi dans $\mathbf{K}/\mathbf{F}$ par hypothèse, donc aussi dans $\mathbf{EK}/\mathbf{F}$.

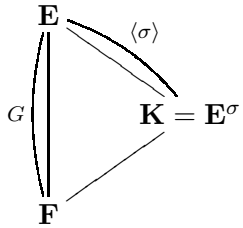
On a donc égalité des densités et $[\mathbf{E}:\mathbf{F}] = [\mathbf{EK}:\mathbf{F}]$: $\mathbf{K} \subseteq \mathbf{E}$. □

Corollaire 3.7.5. *Si* $\mathbf{E}$ *et* $\mathbf{E}'$ *sont deux extensions finies galoisiennes de* $\mathbf{F}$ *et que l'ensemble des idéaux maximaux de* $\mathcal{O}_\mathbf{F}$ *totalement décomposés dans* $\mathbf{E}/\mathbf{F}$ *diffère d'un ensemble de densité nulle de l'ensemble analogue pour* $\mathbf{E}'/\mathbf{F}$ *alors* $\mathbf{E}/\mathbf{F} \simeq \mathbf{E}'/\mathbf{F}$.

On ne sait pas, à $\mathbf{F}$ fixé, caractériser les sous-ensembles $\mathcal{P} \subseteq \mathcal{P}_\mathbf{F}$ formés des idéaux maximaux totalement décomposés dans $\mathbf{E}/\mathbf{F}$ pour une extension galoisienne finie convenable. En revanche, la théorie du corps de classes permet de le faire pour les extensions abéliennes.

3.8 Théorème de Čebotarev : réduction au cas cyclique

On va supposer que l'on dispose du théorème de Čebotarev dans le cas cyclique et l'en déduire dans le cas général.



où C est une classe de conjugaison dans G. On a $Gal(\mathbf{E}/\mathbf{K}) = \langle\sigma\rangle$: $\mathbf{E}/\mathbf{K}$ est une extension cyclique. On admet que l'on dispose du théorème

de Čebotarev dans le cas des extensions cycliques, donc que l'ensemble des idéaux maximaux de $\mathcal{O}_\mathbf{K}$ non ramifiés dans $\mathbf{E}/\mathbf{F}$ tels que $Frob_{\mathfrak{p}_\mathbf{K}} = \sigma$ a pour densité $\frac{1}{[\mathbf{E}:\mathbf{K}]} = \frac{1}{|\langle\sigma\rangle|}$.

On définit $\mathcal{Q}_\mathbf{F}$ comme l'ensemble des idéaux maximaux $\mathfrak{p}$ de $\mathcal{O}_\mathbf{F}$ non ramifiés dans $\mathbf{E}/\mathbf{F}$ tels que $Frob(\mathfrak{q}|\mathfrak{p}) = \sigma$ pour l'un des idéaux maximaux $\mathfrak{q}$ de $\mathcal{O}_\mathbf{E}$ au-dessus de $\mathfrak{p}$. C'est l'ensemble dont on souhaite estimer la densité. De même $\mathcal{Q}_\mathbf{E}$ est l'ensemble des idéaux maximaux de $\mathcal{O}_\mathbf{E}$ au-dessus d'idéaux de $\mathcal{O}_\mathbf{F}$ non ramifiés dans $\mathbf{E}/\mathbf{F}$ tels que $Frob(\mathfrak{q}|\mathfrak{q}\cap\mathcal{O}_\mathbf{F}) = \sigma$ et $\mathcal{Q}_\mathbf{K}$ l'ensemble des idéaux maximaux $\mathfrak{p}_\mathbf{K}$ de $\mathcal{O}_\mathbf{K}$ non ramifiés dans $\mathbf{E}/\mathbf{K}$ tels que $Frob(\mathfrak{q}|\mathfrak{p}_\mathbf{K}) = \sigma$ pour un idéal maximal $\mathfrak{q}$ de $\mathcal{O}_\mathbf{E}$ au-dessus de $\mathfrak{p}_\mathbf{K}$.

On sait déjà que la densité de $\mathcal{Q}_\mathbf{K}$ est $\frac{1}{|\langle\sigma\rangle|}$.

$$\begin{array}{ccc} \mathcal{Q}_\mathbf{E} & \longrightarrow & \mathcal{Q}_\mathbf{F} \\ \mathfrak{q} & \longmapsto & \mathfrak{q}\cap\mathcal{O}_\mathbf{F} \end{array}$$

est surjective par définition de $\mathcal{Q}_\mathbf{F}$.

Recherchons la fibre de $\mathfrak{p} \in \mathcal{Q}_\mathbf{F}$: on impose $\mathfrak{q}|\mathfrak{p}$ et $Frob(\mathfrak{q}|\mathfrak{p}) = \sigma$. Pour un tel $\mathfrak{q}$ on cherche les autres éléments de la fibre. Ils s'écrivent $\tau\mathfrak{q}$ où $\tau \in G$. On a $\tau\mathfrak{q} = \tau'\mathfrak{q}$ si et seulement si $\tau\langle\sigma\rangle = \tau'\langle\sigma\rangle$, et $Frob(\tau\mathfrak{q}|\mathfrak{p}) = \tau Frob(\mathfrak{q}|\mathfrak{p})\tau^{-1} = \tau\sigma\tau^{-1}$. La condition imposée à $\tau\mathfrak{q}$ est donc $\tau\sigma\tau^{-1} = \sigma$ donc que τ appartienne au centralisateur dans G de σ, noté $C_G(\sigma)$.

Le cardinal de la fibre de $\mathfrak{p} \in \mathcal{Q}_\mathbf{F}$ dans $\mathcal{Q}_\mathbf{E}$ est donc $\frac{|C_G(\sigma)|}{|\langle\sigma\rangle|}$.

Si $\mathfrak{q} \in \mathcal{O}_\mathbf{E}$ on a $\sigma = Frob(\mathfrak{q}|\mathfrak{q}\cap\mathcal{O}_\mathbf{F}) \in Gal(\mathbf{E}/\mathbf{K})$ donc en posant $\mathfrak{p}_\mathbf{K} = \mathfrak{q}\cap\mathcal{O}_\mathbf{K}$ et $\mathfrak{p} = \mathfrak{q}\cap\mathcal{O}_\mathbf{F}$on a $Frob(\mathfrak{q}|\mathfrak{p}) = Frob(\mathfrak{q}|\mathfrak{p}_\mathbf{K}) = \sigma$ et $f(\mathfrak{p}_\mathbf{K}|\mathfrak{p}) = 1$. On vient de montrer que l'application $\mathfrak{q} \mapsto \mathfrak{q}\cap\mathcal{O}_\mathbf{K}$ envoie $\mathcal{Q}_\mathbf{E}$ dans $\mathcal{Q}_\mathbf{K}$. Plus précisément elle envoie $\mathcal{Q}_\mathbf{E}$ sur le sous-ensemble de $\mathcal{Q}_\mathbf{K}$ formé des éléments $\mathfrak{p}_\mathbf{K}$ tels que :

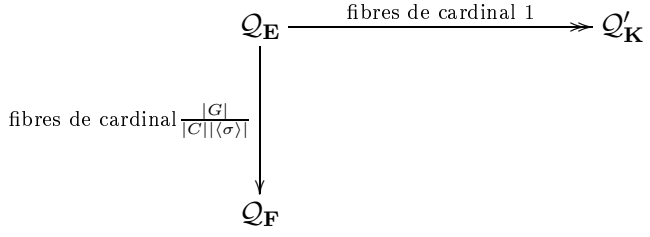
– $\mathfrak{p}_\mathbf{K}$ est au-dessus de $\mathfrak{p}$ non ramifié dans $\mathbf{E}/\mathbf{F}$.

– $f(\mathfrak{p}_\mathbf{k}|\mathfrak{p}) = 1$.

Notons $\mathcal{Q}'_\mathbf{K}$ ce sous-ensemble. $\mathcal{Q}_\mathbf{K} - \mathcal{Q}'_\mathbf{K}$ est de densité nulle en tant que réunion d'un ensemble fini (correspondant aux idéaux $\mathfrak{p}_\mathbf{K} \in \mathcal{Q}_\mathbf{K}$ au-dessus d'un idéal $\mathfrak{p}$ ramifié dans $\mathbf{E}/\mathbf{F}$) et d'un ensemble de densité nulle (pour des raisons de degré d'inertie). Par conséquent $\mathcal{Q}_\mathbf{K}$ et $\mathcal{Q}'_\mathbf{K}$ ont même densité $\frac{1}{|\langle\sigma\rangle|}$.

L'application naturelle $\mathcal{Q}_\mathbf{E} \longrightarrow \mathcal{Q}'_\mathbf{K}$ est surjective.

Si $\mathfrak{p}_\mathbf{K} \in \mathcal{Q}'_\mathbf{K}$, alors $Frob(\mathfrak{q}|\mathfrak{p}) = \sigma$ pour $\mathfrak{q}|\mathfrak{p}$. Le groupe de décomposition $D(\mathfrak{q}|\mathfrak{p})$ est engendré par σ. Or $\langle\sigma\rangle = Gal(\mathbf{E}/\mathbf{K})$, donc il y a un seul idéal $\mathfrak{q}$ au-dessus de $\mathfrak{p}_\mathbf{K}$.



Ce qui nous intéresse, c'est la densité de $\mathcal{Q}_{\mathbf{F}}$:

$$\begin{aligned}\sum_{\mathfrak{p}\in\mathcal{Q}_{\mathbf{F}}}(N\mathfrak{p})^{-s} &= \frac{|\langle\sigma\rangle||C|}{|G|}\sum_{\mathfrak{q}\in\mathcal{Q}_{\mathbf{E}}}(N(\mathfrak{q}\cap\mathcal{O}_{\mathbf{F}}))^{-s}\\ &= \frac{|\langle\sigma\rangle||C|}{|G|}\sum_{\mathfrak{p}_{\mathbf{K}}\in\mathcal{Q}_{\mathbf{K}}}(N\mathfrak{p}_{\mathbf{K}})^{-s}\end{aligned}$$

Donc la densité de $\mathcal{Q}_{\mathbf{F}}$ vaut $\frac{|\langle\sigma\rangle||C|}{|G|}$ fois la densité de $\mathcal{Q}_{\mathbf{K}}$, qui est elle-même connue et égale à $\frac{1}{|\langle\sigma\rangle|}$. On trouve donc que $\mathcal{Q}_{\mathbf{F}}$ a densité $\frac{|C|}{|G|}$.

3.9 Le théorème de Frobenius

On admet que $\zeta_{\mathbf{F}}$ a un pôle en $s = 1$. Le but de cette partie est de démontrer le théorème de Frobenius, qui est un cas particulier du théorème de Čebotarev.

Théorème 3.9.1 (Théorème de Frobenius)**.** *Soit $\mathbf{E}/\mathbf{F}$ une extension galoisienne cyclique de corps de nombres de degré d. Soit $e \geqslant 1$ divisant d. Alors l'ensemble des idéaux maximaux de $\mathcal{O}_{\mathbf{F}}$ non ramifiés dans $\mathbf{E}/\mathbf{F}$ dont le Frobenius est d'ordre e a pour densité $\frac{\varphi(e)}{d}$.*

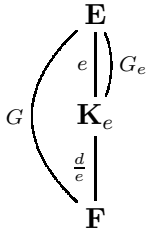
Remarque 3.9.2. *Le cas $e = 1$ correspond aux idéaux totalement décomposés dans $\mathbf{E}/\mathbf{F}$, on a déjà vu le résultat précédemment.*

Si $\sigma \in Gal(\mathbf{E}/\mathbf{F})$ a pour ordre e, les autres éléments d'ordre e dans $Gal(\mathbf{E}/\mathbf{F})$ sont les σ^k où $k \in (\mathbb{Z}/e\mathbb{Z})^\times$: il y en a $\varphi(e)$ et le théorème de Čebotarev donne bien la densité attendue $\frac{\varphi(e)}{d}$.

En utilisant la méthode de réduction du théorème de Čebotarev au cas cyclique on obtient le corollaire suivant :

Corollaire 3.9.3. *Soit $\mathbf{E}/\mathbf{F}$ une extension galoisienne finie de groupe G. Pour $\sigma \in G$ on définit la division de σ, $D(\sigma)$, comme étant l'ensemble des conjugués dans G des σ^k où k est premier à l'ordre de σ. Alors l'ensemble des idéaux maximaux $\mathfrak{p}$ de $\mathcal{O}_{\mathbf{F}}$ non ramifiés dans $\mathbf{E}/\mathbf{F}$ tels que $Frob(\mathfrak{q}|\mathfrak{p}) \in D(\sigma)$ pour $\mathfrak{q}|\mathfrak{p}$ a pour densité $\frac{|D(\sigma)|}{|G|}$.*

Démonstration du théorème de Frobenius. Soit $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_{\mathbf{F}}$ non ramifié dans $\mathbf{E}/\mathbf{F}$. Dire que $Frob_{\mathfrak{p}}$ a pour ordre e signifie qu'il engendre l'unique sous-groupe G_e de cardinal e de G donc fixe $\mathbf{K}_e = \mathbf{E}^{G_e}$:



En particulier l'idéal $\mathfrak{p}$ est totalement décomposé dans $\mathbf{K}_e/\mathbf{F}$. Plus précisément, ceci équivaut à «l'ordre de $Frob_\mathfrak{p}$ divise e».

La densité de ces idéaux maximaux est $\frac{e}{d}$. En utilisant la fonction de Moebius pour inverser cette relation, on trouve finalement que la densité des idéaux maximaux de $\mathcal{O}_\mathbf{F}$ non ramifiés dans $\mathbf{E}/\mathbf{F}$ d'ordre exactement e est $\frac{\varphi(e)}{d}$. □

3.10 Théorème de Čebotarev : fonctions L galoisiennes

Soit $\mathbf{E}/\mathbf{F}$ une extension finie abélienne de corps de nombres de groupe de Galois G. On dit que $\chi : G \to \mathbb{C}^\times$ est un caractère de G si c'est un morphisme de groupes. Si χ est un caractère on considère :

$$L(s,\chi) = \prod_{\mathfrak{p} \text{ non ramifiés}} \left(1 - \chi(Frob_\mathfrak{p})(N\mathfrak{p})^{-s}\right)^{-1}$$

Comme $|\chi(Frob_\mathfrak{p})| = 1$ pour tout $\mathfrak{p}$ on a convergence absolue pour $\Re(s) > \delta > 1$ donc on obtient une fonction holomorphe sur le demi-plan $\Re(s) > 1$.

Cas particulier : Si $\chi = \chi_0$ on a :

$$L(s,\chi_0) = \zeta_\mathbf{F}(s) \prod_{\mathfrak{p} \text{ ramifié}} (1 - (N\mathfrak{p})^{-s})$$

Proposition 3.10.1. *On a :*

$$L(s,\chi) = \sum_{\mathfrak{a} \text{ idéal} \neq \{0\}} \chi(\mathfrak{a})(N\mathfrak{a})^{-s}$$

avec $\chi(\mathfrak{a}) = 0$ si $\mathfrak{a}$ est divisible par un idéal ramifié dans $\mathbf{E}/\mathbf{F}$, et $\chi(\mathfrak{a}) = \prod \chi(\mathfrak{p}_i)$ si $\mathfrak{a} = \prod \mathfrak{p}_i$ où les $\mathfrak{p}_i$ sont non ramifiés dans $\mathbf{E}/\mathbf{F}$.

On montrera plus tard le résultat suivant :

Théorème 3.10.2. *Si $\chi : G \to \mathbb{C}^\times$ est un caractère non trivial alors $L(s,\chi)$ se prolonge au voisinage de $s = 1$ en une fonction holomorphe non nulle.*

On va en déduire le théorème de Čebotarev dans le cas abélien, donc *a fortiori* dans le cas cyclique dont on a remarqué qu'il suffit à démontrer le cas général.

On définit :

$$\eta_\chi(s) = \sum_{\mathfrak{p} \text{ non ramifié}} \sum_{n \geqslant 1} \frac{1}{n} \chi(Frob_\mathfrak{p})(N\mathfrak{p})^{-ns} = \log\left(L(s,\chi)\right)$$

pour $\Re(s) > 1$. Par le théorème, $\eta_\chi(s)$ est borné au voisinage de $s = 1$. On pose :

$$\eta_\chi(s) = \sum_{\mathfrak{p} \text{ non ramifié}} \chi(Frob_\mathfrak{p})(N\mathfrak{p})^{-s} + g_\chi(s)$$

et comme tout à l'heure $g_\chi(s)$ converge absolument pour $\Re(s) > \delta$ donc $\sum_{\mathfrak{p} \text{ non ramifié}} \chi(Frob_\mathfrak{p})(N\mathfrak{p})^{-s}$ est bornée au voisinage de $s = 1$. Si $\chi = \chi_0$ on a $\sum \chi_0(Frob\mathfrak{p})(N\mathfrak{p})^{-s} = \log\left(\frac{1}{s-1}\right) + O(1)$ au voisinage de 1.

On utilise ensuite l'orthogonalité des caractères : pour $g \in G$, $\sum_\chi \chi(g) = 0$ si $g \neq \mathbf{1}_G$, $|G|$ si $g = \mathbf{1}_G$.

Si $\mathfrak{p}$ est un idéal maximal de $\mathcal{O}_\mathbf{F}$ non ramifié dans $\mathbf{E}/\mathbf{F}$ et si $g \in G$:

$$\sum_{\chi \text{ caractère de } G} \chi(Frob_\mathfrak{p})\chi^{-1}(g) = 0 \text{ si } g \neq Frob_\mathfrak{p} \text{ , } |G| \text{ si } G = Frob_\mathfrak{p}$$

On fixe $g \in G$ et on considère :

$$\sum_{\chi \text{ caractère de } G} \chi^{-1}(g) \sum_{\mathfrak{p} \text{ non ramifié}} \chi(Frob_\mathfrak{p})(N\mathfrak{p})^{-s} \sim_{s\to 1} \log\left(\frac{1}{s-1}\right)$$

Ceci est aussi égal à :

$$\sum_{\mathfrak{p} \text{ non ramifié}} \left(\sum_\chi \chi(Frob_\mathfrak{p})\chi(g)^{-1}\right)(N\mathfrak{p})^{-s} = |G| \sum_{\mathfrak{p} \text{ non ramifié}, Frob_\mathfrak{p} = g} (N\mathfrak{p})^{-s}$$

On en déduit :

$$\sum_{\mathfrak{p} \text{ non ramifié}, Frob_\mathfrak{p} = g} (N\mathfrak{p})^{-s} \sim_{s\to 1} \frac{1}{|G|} \log\left(\frac{1}{s-1}\right)$$

Donc en passant à la densité on obtient le théorème de Čebotarev.

Chapitre 4

Corps valués

Le corps, dans ce chapitre, s'appellera $\mathbf{K}$.

4.1 Valeurs absolues

Définition 4.1.1. *Une valeur absolue sur* $\mathbf{K}$ *est une fonction de* $\mathbf{K}$ *dans* $\mathbb{R}_+^\times$ *vérifiant :*

1. $|x| = 0$ *si et seulement si* $x = 0$
2. $|xy| = |x||y|$ *pour* $x, y \in \mathbf{K}$.
3. $|x + y| \leqslant |x| + |y|$ *pour* $x, y \in \mathbf{K}$.

elle est dite ultramétrique si l'on a la condition plus forte $|x+y| \leqslant \max(|x|, |y|)$. *Une valeur absolue est dite* archimédienne *si elle n'est pas ultramétrique,* triviale *si elle vaut 1 pour tout* $x \neq 0$.

On a $|1| = 1$, $|-1| = 1$ et plus généralement $|-x| = |x|$. On montre facilement l'inégalité $|x - y| \geqslant ||x| - |y||$.

Proposition 4.1.2. *Soit* $|\ |$ *une valeur absolue ultramétrique, prenons* $x, y \in \mathbf{K}$ *tels que* $|x| \neq |y|$. *Alors* $|x + y| = |x - y| = \max(|x|, |y|)$

Démonstration. Supposons $|x| < |y|$. On a donc $|x + y| < |y|$. D'autre part, $|y| = |x + y - x| \leqslant \max(|x + y|, |x|)$, donc on a aussi $|y| \leqslant |x + y|$ d'où le résultat. □

Ainsi en ultramétrique tout triangle est isocèle !

Définition 4.1.3. *Une valuation discrète sur* $\mathbf{K}$ *est une application* v *surjective de* $\mathbf{K}^\times$ *dans* $\mathbb{Z}$ *telle que :*
- $v(xy) = v(x) + v(y)$
- $v(x + y) \geqslant \min(v(x), v(y))$ *quand* $x + y \neq 0$.[1]

[1] On peut aussi prolonger v à $\mathbb{Z} \cup \{\infty\}$ en posant $v(0) = \infty$.

Si v est une valuation discrète sur $\mathbf{K}$ alors pour $\alpha \in \mathbb{R}$, $\alpha > 1$ on obtient une valeur absolue ultramétrique sur $\mathbf{K}$ par :

- $|0| = 0$.
- $|x| = \alpha^{-v(x)}$ pour $x \neq 0$.

L'ensemble des valeurs de cette valeur absolue, $|\mathbf{K}^\times|$, est $\alpha^{\mathbb{Z}}$, discret dans $\mathbb{R}_+^\times$. Inversement, si $|\ |$ est une valeur absolue ultramétrique sur $\mathbf{K}$ de groupe des valeurs $\alpha^{\mathbb{Z}}$, $\alpha > 1$, on peut poser $v(x) = -\frac{\log|x|}{\log\alpha}$ et on obtient ainsi une valuation sur $\mathbf{K}$.

Exemple 4.1.4.

1. *Sur $\mathbf{K} = \mathbb{R}$ on dispose de la valeur absolue usuelle, notée $|\ |_\infty$, qui est archimédienne. Idem si $\mathbf{K} = \mathbb{C}$.*
2. *Si $\mathbf{F}$ est un corps et $\sigma : \mathbf{F} \to \mathbb{R}$ ou $\mathbb{C}$ est un plongement, alors $x \mapsto |\sigma(x)|$ est une valeur absolue archimédienne sur $\mathbf{F}$.*
3. *Si p est un nombre premier on a une valeur absolue $|\ |_p$ sur $\mathbb{Q}$ définie par :*
   - $|0|_p = 0$.
   - $\left|\frac{a}{b}\right|_p = \mathfrak{p}^{-(v_p(a)-v_p(b))}$ *où $v_p(n)$ est l'exposant de p dans la décomposition de n en facteurs premiers*[2].
4. *Soit $\mathbf{K}$ un corps de nombres, $\mathfrak{p}$ un idéal maximal de $\mathcal{O}_\mathbf{K}$, $x \in \mathbf{K}^\times$. $x\mathcal{O}_\mathbf{K}$ est un idéal fractionnaire de $\mathcal{O}_\mathbf{K}$. On peut donc l'écrire de manière unique :*

$$x\mathcal{O}_\mathbf{K} = \prod_{\mathcal{P}\ \text{idéal maximal}} \mathfrak{p}^{\alpha_\mathfrak{p}}$$

où $(\alpha_\mathfrak{p})$ est un entier nul pour presque tout $\mathfrak{p}$. On pose alors $v_\mathfrak{p}(x) = \alpha_\mathfrak{p}$. $v_\mathfrak{p}$ est une valuation si $\mathfrak{p}$ est principal : en effet 1 est alors atteint et le groupe des valeurs est $\mathbb{Z}$ entier. S'il ne l'est pas, l'une de ses puissances l'est puisque le groupe de classes d'idéaux est fini, d'ordre noté h. On a alors que $v_\mathfrak{p}(\mathbf{K}^\times)$ est un sous-groupe de $\mathbb{Z}$ contenant $h\mathbb{Z}$ donc un $d\mathbb{Z}$ avec $d|h$, $d > 0$. Alors $x \mapsto \frac{v_\mathfrak{p}(x)}{d}$ est une valuation. On obtient ainsi une valeur absolue sur $\mathbf{K}$ donnée par :

$$|x|_\mathfrak{p} = (N\mathfrak{p})^{-v_\mathfrak{p}(x)}$$

4.2 Topologie associée à une valeur absolue

Si $|\ |$ est une valeur absolue sur $\mathbf{K}$, $(x, y) \mapsto |x - y|$ définit une distance sur $\mathbf{K}$ sui hérite ainsi d'une structure d'espace métrique. La valeur absolue triviale donne la topologie discrète sur $\mathbf{K}$.

[2] À titre d'exercice, on pourra vérifier que c'est une valuation indépendante du représentant choisi, et qui vaut 1 en p.

Définition 4.2.1. *On dit que deux valeurs absolues sur* $\mathbf{K}$ *sont équivalentes si elles définissent la même topologie.*

Proposition 4.2.2. *Soient* $|\ |$ *et* $|\ |'$ *deux valeurs absolues sur* $\mathbf{K}$*. Elles sont équivalentes si et seulement si il existe* $a > 0$ *tel que* $|x|' = |x|^a$ *pour tout* $x \in \mathbf{K}^\times$*.*

Remarque 4.2.3. *Attention, il n'est pas vrai en général que* $x \mapsto |x|^a$ *soit une valeur absolue quand* $|\ |$ *en est une.*

Démonstration. Si l'égalité est vérifiée il est clair que les topologies induites sont les mêmes.

Supposons que $|\ |$ et $|\ |'$ soient équivalentes. Prenons $x \in \mathbf{K}$, $x \neq 0$. On a $|x| < 1$ si et seulement si x^n tend vers 0 pour la topologie induite par $|\ |$. On voit donc que $|x| < 1$ si et seulement si $|x|' < 1$, et de même on a équivalence entre $|x| = 1$ et $|x|' = 1$, $|x| > 1$ et $|x|' > 1$.

En particulier si l'une des valeurs absolues est triviale, l'autre l'est aussi. Supposons-les donc toutes deux non triviales. On choisit $y \in \mathbf{K}^\times$ tel que $|y| > 1$. On a alors $|y|' > 1$.

Soit $x \in \mathbf{K}^\times$. Pour m et n entiers, $m \geqslant 1$ on a :

$$\left|\frac{x^m}{y^n}\right| < 1 \text{ si et seulement si } \left|\frac{x^m}{y^n}\right|' < 1$$

Donc $\frac{\log|x|}{\log|y|}$ et $\frac{\log|x|'}{\log|y|'}$ définissent la même coupure de Dedekind : ils sont égaux. On en déduit que $\frac{\log|x|}{\log\ |x|'}$ est constant. En notant a sa valeur, on a pour tout $x \neq 0$: $|x|' = |x|^a$. □

4.3 Valeurs absolues ultramétriques

Proposition 4.3.1. *Soit* $\mathbf{K}$ *un corps,* $|\ |$ *une valeur absolue non triviale. Alors* $|\ |$ *est ultramétrique si et seulement si elle est bornée sur le sous-anneau premier.*

Démonstration. Soit $n \in \mathbb{N}$. On a $|n\mathbf{1_K}| = |\mathbf{1_K} + \cdots + \mathbf{1_K}|$ (n fois). On a donc $|n\mathbf{1_K}| \leqslant |\mathbf{1_K}| = 1$. Ceci reste trivialement vrai pour $n \in \mathbb{Z}$ donc la valeur absolue est bornée.

Réciproquement supposons que $|\ |$ est bornée sur le sous-anneau premier de $\mathbf{K}$ par $N \in \mathbb{N}$. Prenons $x, y \in \mathbf{K}$ tels que $|x| \leqslant |y|$. Prouvons que $|x+y| \leqslant |y|$. On sait déjà que $|x + y| \leqslant |x| + |y|$.

Pour $k \in \mathbb{N}^\times$:

$$(x+y)^k = \sum_{i=0}^{k} \binom{k}{i} x^i y^{k-i}$$

D'où l'on déduit par inégalité triangulaire :

$$\begin{aligned} |x+y|^k &\leqslant \sum_{i=0}^{k} \left| \binom{k}{i} \mathbf{1_K} \right| |x|^i |y|^{k-i} \\ &\leqslant N \sum_{i=0}^{k} |y|^k \\ &\leqslant N(k+1)|y|^k \\ |x+y| &\leqslant N^{\frac{1}{k}}(k+1)^{\frac{1}{k}}|y| \\ &\leqslant |y| \text{ en faisant tendre } n \text{ vers l'infini} \quad \square \end{aligned}$$

Corollaire 4.3.2. *Si* $\mathbf{K}$ *est de caractéristique non nulle alors toute valeur absolue sur* $\mathbf{K}$ *est ultramétrique : en effet le sous-anneau premier est alors fini.*

Lemme 4.3.3. *Soit* $|\ |$ *une valeur absolue ultramétrique sur* $\mathbf{K}$*. On note :*

- $\mathcal{R} = \{x \in \mathbf{K}, |x| \leqslant 1\}$
- $\mathcal{P} = \{x \in \mathbf{K}, |x| < 1\}$

Alors $\mathcal{R}$ *est un anneau local d'idéal maximal* $\mathcal{P}$ *et de corps des fractions* $\mathbf{K}$*. Si la valeur absolue est discrète alors* $\mathbb{R}$ *est un anneau local principal dont les idéaux non nuls sont les* $\mathcal{P}^k, k \neq 0$*.*

Démonstration. On a pour $x, y \in \mathbf{K}$, : $|xy| = |x||y|$ et $|x+y| \leqslant \max(|x|, |y|)$ donc $\mathcal{R}$ est bien un sous-anneau de $\mathbf{K}$ et $\mathcal{P}$ en est bien un idéal. Si $x \in \mathbf{K} - \mathcal{R}$ alors $|x| > 1$ et $|x^{-1}| < 1$ donc $x^{-1} \in \mathcal{P} \subseteq \mathcal{R}$. $\mathbf{K}$ est ainsi le corps des fractions de $\mathcal{R}$.

Un élément $x \in \mathbf{K}$ est dans $\mathcal{R} - \mathcal{P}$ si et seulement si $|x| = 1$. Alors $|x^{-1}| \in \mathcal{R} - \mathcal{P}$. On voit donc que $\mathcal{R}^\times = \mathcal{R} - \mathcal{P}$ ce qui implique que $\mathcal{P}$ est un idéal maximal de $\mathcal{R}$ et que c'en est le seul.

Supposons que $|\mathbf{K}^\times| = \alpha^{\mathbb{Z}}$ avec $\alpha > 1$. Choisissons $\pi \in \mathcal{P}$ tel que $|\pi| = \alpha^{-1}$, alors tout élément $x \in \mathbf{K}^\times$ s'écrit de façon unique $x = \pi^k u$ où $k \in \mathbb{Z}$ et $u \in \mathcal{R}^\times$. Le reste du lemme en découle facilement : soit $\mathcal{I} \subseteq \mathcal{P}$ un idéal non nul de $\mathcal{R}$. Soit x un élément de valeur absolue maximale de $\mathcal{I}$, posons $x = \pi^k u$. Pour tout $y \in \mathcal{P}^k$, on peut écrire $y = \pi^l v$ où $l \geqslant k$ et $v \in \mathcal{R}^\times$, ce qui montre que y est un multiple de x donc qu'il est dans $\mathcal{I}$ et finalement que $\mathcal{I} = \langle x \rangle = \mathcal{P}^k$. $\square$

Remarque 4.3.4.

- *Supposons que la valeur absolue est discrète. Soit* $v : \mathbf{K}^\times \to \mathbb{Z}$ *la valuation correspondante. Un élément* π *de* $\mathbf{K}$ *de valuation* 1 *est appelé une uniformisante de* $\mathbf{K}$*.*
- $\mathcal{R}$ *est appelé l'anneau des entiers de* $\mathbf{K}$*.*

4.4 Valeurs absolues sur $\mathbb{Q}$

Proposition 4.4.1. *Une valeur absolue non triviale sur $\mathbb{Q}$ est équivalente soit à $|\ |_\infty$ soit à $|\ |_p$ pour un nombre premier p. Ces valeurs absolues sont deux à deux non équivalentes. De plus on a la formule du produit :*

$$|x|_\infty \prod_{p\ premier} |x|_p = 1 \text{ pour tout } x \in \mathbb{Q}^\times$$

Démonstration. La formule du produit est immédiate à partir de la décomposition de x en facteurs premiers.

Soit p premier. On a $|p|_\infty > 1$, $|p|_p < 1$ et $|p|_q = 1$ pour q un nombre premier différent de p. Ceci suffit à montrer que les valeurs absolues considérées sont deux à deux non équivalentes.

Soit $|\ |$ une valeur absolue non triviale sur $\mathbb{Q}$. Soient $m, n > 1$ deux entiers. Écrivons m en base n :

$$m = a_0 + a_1 n + \cdots + a_r n^r, 0 \leqslant a_i < n, a_r \neq 0$$

On a $|a_i| \leqslant n$, $r \leqslant \frac{\log m}{\log n}$,et en posant $N = \max(1, |n|)$ on obtient :

$$|m| \leqslant \left(1 + \frac{\log m}{\log n}\right) n N^{\frac{\log m}{\log n}}$$

En remplaçant m par m^s on trouve :

$$\begin{aligned} |m|^s &\leqslant \left(1 + s\frac{\log m}{\log n}\right) n N^{s\frac{\log m}{\log n}} \\ |m| &\leqslant \left(1 + s\frac{\log m}{\log n}\right)^{frac1s} n^{\frac{1}{s}} N^{\frac{\log m}{\log n}} \\ &\leqslant N^{\frac{\log m}{\log n}} \text{ en faisant tendre } s \text{ vers l'infini.} \end{aligned}$$

Deux cas sont à étudier :

– Il existe $n > 1$ avec $|n| \leqslant 1$. On choisit un tel n, pour lequel $N = 1$. Alors $|m| \leqslant 1$ pour tout $m > 1$ donc pour $m \in \mathbb{Z}$. La valeur absolue est donc ultramétrique, non triviale par hypothèse.
Soit $\mathcal{P}_\mathbb{Z}$ l'idéal de $\mathbb{Z}$ formé des entiers relatifs de valeur absolue strictement inférieure à 1. $\mathcal{P}_\mathbb{Z} \neq \{0\}$ (sinon la valeur absolue serait triviale). Avec les notations $\mathcal{R}$ et $\mathcal{P}$ adoptées précédemment, $\mathcal{P}_\mathbb{Z} = \mathbb{Z} \cap \mathcal{P}$. $\mathbb{Z} \subseteq \mathbb{R}$ donc on a un morphisme injectif d'anneaux $\mathbb{Z}/\mathcal{P}_\mathbb{Z} \to \mathcal{R}/\mathcal{P}$. $P_\mathbb{Z}$ est donc un idéal premier non nul de $\mathbb{Z}$, donc de la forme $p\mathbb{Z}$ pour un unique nombre premier p.
Pour $m \in \mathbb{Z} - p\mathbb{Z}$, on a donc $|m| = 1$, et pour $x \in \mathbb{Z}$ on a $|x| = |p|^{v_p(x)}$ (pour $x \neq 0$), ce qui reste vrai pour $x \in \mathbb{Q}^\times$. La valeur absolue est donc équivalente à la valeur absolue p-adique.

– $n > 1$ entraîne $|n| > 1$. Alors, avec n, m comme précédemment on a $N = \max(1, |n|) = |n|$ donc $|m|^{\frac{1}{\log m}} \leqslant |n|^{\frac{1}{\log |n|}}$ pour $m, n > 1$.
On a donc l'égalité $|m|^{\frac{1}{\log m}} = |n|^{\frac{1}{\log |n|}} = c > 1$ et pour $x \in \mathbb{Q}^\times$ on a $x = c^{\log |x|_\infty} = |x|_\infty^{\log c}$ donc la valeur absolue est équivalente à la valeur absolue usuelle.

□

4.5 Approximation faible

Théorème 4.5.1 (Théorème d'approximation faible)**.** *Soit* $\mathbf{K}$ *un corps et* $|\ |_1, \ldots, |\ |_n$ *n valeur absolue sur* $\mathbf{K}$ *non triviales deux à deux non équivalentes. Soit* $\varepsilon > 0$ *et* $x_1, \ldots, x_n \in \mathbf{K}$*. Alors il existe* $y \in \mathbf{K}$ *tel que* $|y - x_i|_i < \varepsilon$ *pour* $1 \leqslant i \leqslant n$*.*

Lemme 4.5.2. *Il existe* $a \in \mathbf{K}^\times$ *tel que* $|a|_1 > 1$ *et* $|a|_i < 1$ *pour* $i > 1$*.*

Démonstration du lemme. On procède par récurrence sur n, le cas $n = 2$ étant acquis (c'est une conséquence immédiate de la non-équivalence des valeur absolue considérées.).

Supposons le résultat acquis jusqu'à $n - 1 \geqslant 2$. On a un $b \in \mathbf{K}$ tel que :

$$|b|_1 > 1, |b|_2 < 1, \ldots, |b|_{n-1} < 1$$

Fixons un $c \in \mathbf{K}$ tel que $|c|_1 > 1$ et $|c|_n < 1$. Alors :
– Si $|b|_n < 1$, $a = b$ convient.
– Si $|b|_n = 1$, $a = cb^r$ convient pour r assez grand.
– Si $|b|_n > 1$, $a = cb^r \frac{1}{1+b^r}$ convient pour r assez grand.
Seul le dernier cas mérite démonstration :

$$|a|_1 = \frac{|c|_1 |b|_1^r}{|1 + b^r|_1}$$

Or $|b|_1^r \geqslant |1 + b^r|_1 \geqslant |b|_1^r - 1$ donc $|1 + b^r|_1 \ \sim |b|_1^r$ et $|a|_1 > 1$ à partir d'un certain r.

Pour $2 \leqslant i \leqslant n - 1$, $|b|_1 < 1$ et on trouve de même que $|a|_i \to 0$. Pour $i = n$ on fonctionne de même. □

Démonstration du théorème. On choisit pour chaque valeur absolue un élément $a_j \in \mathbf{K}$ tel que $|a_j|_j > 1$ et $|a_j|_i < 1$ pour $i \neq j$.

Pour r entier, quand r tend vers l'infini :

$$\text{Pour } i \neq j \quad \left| \frac{a_j^r}{1 + a_j^r} \right|_i \to 0 \text{ et } \left| \frac{a_j^r}{1 + a_j^r} - 1 \right|_j \to 0$$

En prenant y défini par :

$$y = \sum_{j=1}^{n} \left(\frac{a_j^r}{1 + a_j^r} x_j \right)$$

Pour r assez grand on aura bien $|y - x_i|_i < \varepsilon$ pour tout i d'où le résultat. □

4.6 Complétés

Soit $\mathbf{K}$ un corps muni d'une valeur absolue $|\ |_{\mathbf{K}}$. On considère l'ensemble des suites de Cauchy $(x_n)_{n\in\mathbb{N}}$ à valeurs dans $\mathbf{K}$, noté $\mathcal{C}$, muni de la multiplication et de l'addition composante par composante. C'est un anneau. L'enemble $\mathcal{C}_0$ des suites convergeant vers 0 en est un idéal (les suites de Cauchy étant bornées). Cet idéal est maximal :

Soit $s = (s_n) \in \mathcal{C}$ ne convergeant pas vers 0. Il existe donc $\varepsilon > 0$ tel que pour tout $N > 0$ il existe $n \geqslant N$pour lequel $|s_n| > \varepsilon$. La suite s étant de Cauchy il existe $N > 0$ tel que pour $p, q \geqslant N$ on ait $|s_p - s_q| < \frac{\varepsilon}{2}$. Fixant de tels ε et N, ainsi que $n \geqslant N$ tel que $|s_n| > \varepsilon$, on trouve que $|s_p| > \frac{\varepsilon}{2}$pour $p \geqslant N$. On pose $t_p = s_p^{-1}$ pour $p \geqslant N$ et $t_p = 1$ pour $p < N$. Alors, pour $p, q \geqslant N$, $|t_p - t_q| = \frac{|s_p - s_q|}{|s_p s_q|} \leqslant \frac{4}{\varepsilon^2}|s_p - s_q|$. La suite s étant de Cauchy il en est donc de même de la suite t, et $(s_n t_n)$ est congrue à la suite constante de valeur 1 modulo $\mathcal{C}_0$. La suite s est donc inversible modulo $\mathcal{C}_0$ et l'anneau quotient $\mathcal{C}/\mathcal{C}_0$ est bien un corps.

Définition 4.6.1. *Le corps $\mathcal{C}/\mathcal{C}_0$ est appelé le* complété de $\mathbf{K}$ *pour la valeur absolue $|\ |$. On le note en général $\hat{\mathbf{K}}$.*

Si à $x \in \mathbf{K}$ on associe la suite constante de valeur x on obtient un plongement de $\mathbf{K}$ dans $\hat{\mathbf{K}}$ qui est un homomorphisme de corps. Pour $s \in \mathcal{C}$ la suite des $|s_n|$ est de Cauchy dans $\mathbb{R}$ donc converge vers un élément $|s| \in \mathbb{R}$. On vérifie facilement que $|s+t| \leqslant |s|+|t|$, d'où l'on déduit que $|s+t| = |s-t| = |s|$ si $t \in \mathcal{C}_0$. La fonction valeur absolue passe donc au quotient et on obtient ainsi sur $\hat{\mathbf{K}}$ une valeur absolue qui étend celle de $\mathbf{K}$, donc une métrique. Remarquons que $\mathbf{K}$ est dense dans son complété $\hat{\mathbf{K}}$.

Proposition 4.6.2. *(admise)*
Pour cette métrique, $\hat{\mathbf{K}}$ est complet.

Exemple 4.6.3.
- $\mathbf{K} = \mathbb{Q}$, $|\ | = |\ |_\infty$ *: le complété est* $\mathbb{R}$.
- *Si p est un nombre premier le complété de $\mathbb{Q}$ pour la valeur absolue $|\ |_p$ est noté $\mathbb{Q}_p$ et s'appelle le corps des nombres p-adiques. Il est muni d'une valeur absolue discrète à valeurs $p^{\mathbb{Z}}$. La valuation correspondante se note $v_p : \mathbb{Q}_p^\times \to \mathbb{Z}$ et vérifie $v_p(p) = 1$. L'anneau des $x \in \mathbb{Q}_p$ tels que*

$|x|_p \leqslant 1$ se note $\mathbb{Z}_p$ et s'appelle l'anneau des entiers p-adiques. C'est un anneau local d'idéal maximal $p\mathbb{Z}_p$.

Remarque 4.6.4. *Si on remplace la valeur absolue sur $\mathbf{K}$ par une valeur absolue équivalente les complétés sont topologiquement isomorphes.*

On peut interpréter le théorème d'approximation faible en disant que si l'on a des valeur absolue sur $\mathbf{K}$ deux à deux non équivalentes, alors en notant $\hat{\mathbf{K}}_i$ le complété de $\mathbf{K}$ pour $|\ |_i$ le plongement :

$$\begin{array}{ccc} \mathbf{K} & \longrightarrow & \hat{\mathbf{K}}_1 \times \cdots \times \hat{\mathbf{K}}_n \\ x & \longmapsto & (x, \ldots, x) \end{array}$$

est d'image dense.

4.7 Places des corps de nombres – cas archimédien

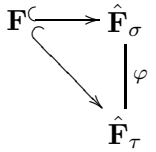
Définition 4.7.1. *Une place d'un corps de nombres $\mathbf{F}$ est une classe d'équivalence de valeurs absolues non triviales sur $\mathbf{F}$. Une telle place est dite* archimédienne *ou* infinie *si les valeurs absolues dans la classe le sont,* ultramétrique *ou* finie *dans le cas contraire.*

Soit $\mathbf{F}$ un corps de nombres, notons $\sigma_1, \ldots, \sigma_r$ ses plongements réels et $\sigma_{r+1}, \bar{\sigma}_{r+1}, \ldots, \sigma_{r+s}, \bar{\sigma}_{r+s}$ ses plongements complexes. On a $[\mathbf{F} : \mathbb{Q}] = r + 2s$.

Pour chaque tel plongement σ on a une valeur absolue sur $\mathbf{F}$ définie par $|x|_{\sigma_i} = |\sigma_i x|_\infty$ et ces valeurs absolues ne sont pas deux à deux équivalentes :

Supposons que les valeurs absolues attachées à σ et τ (plongements de $\mathbf{F}$ dans $\mathbb{R}$ ou $\mathbb{C}$) sont équivalentes. En ce cas les complétés $\hat{\mathbf{F}}_\sigma$ et $\hat{\mathbf{F}}_\tau$ sont isomorphes en tant que corps topologiques. Ces complétés sont $\mathbb{R}$ ou $\mathbb{C}$ suivant que les plongements sont réels ou complexes, de sorte que les complétés sont nécessairement tous deux $\mathbb{R}$ ou tout deux $\mathbb{C}$.

Or le seul isomorphisme de corps topologique de $\mathbb{R}$ sur lui-même est l'identité. Les seuls automorphismes de corps topologique de $\mathbb{C}$ sont l'identité et la conjugaison complexe. φ est donc l'identité ou la conjugaison complexe dans le diagramme suivant :



On a ainsi produit $r + s$ places infinies de $\mathbf{F}$: r places «réelles» (une par plongement réel) et s places «complexes» (une par paire de plongements complexes).

Proposition 4.7.2. *Ce sont les seules places archimédiennes de $\mathbf{F}$. (On connaît déjà le résultat pour $\mathbf{F} = \mathbb{Q}$.)*

Démonstration. On se donne une valeur absolue non triviale $|\ |$ sur $\mathbf{F}$, et on considère le complété $\hat{\mathbf{F}}$ de $\mathbf{F}$ pour cette valeur absolue, ainsi que le complété $\hat{\mathbb{Q}}$ de $\mathbb{Q}$ dans $\hat{\mathbf{F}}$. C'est un sous-corps de $\hat{\mathbf{F}}$ dans lequel $\mathbb{Q}$ est dense. Comme $|\ |$ restreinte à $\mathbb{Q}$ est archimédienne elle est équivalente à $|\ |_\infty$ et on a un isomorphisme de corps topologiques entre $\hat{\mathbb{Q}}$ et $\mathbb{R}$ prolongeant l'identité. On identifie $\hat{\mathbb{Q}}$ à $\mathbb{R}$, de sorte que $\hat{\mathbf{F}}$ est vu comme une extension de $\mathbb{R}$, en particulier comme un $\mathbb{R}$-espace vectoriel.

L'homomorphisme de corps de $\mathbf{F}$ dans $\hat{\mathbf{F}}$ correspond à l'homomorphisme d'algèbres :

$$\begin{array}{rcl} \varphi : \mathbf{F} \otimes_{\mathbb{Q}} \mathbb{R} & \longrightarrow & \hat{\mathbf{F}} \\ x \otimes \lambda & \longmapsto & x\lambda \end{array}$$

L'algèbre $\mathbf{F} \otimes_{\mathbb{Q}} \mathbb{R}$ est de dimension finie $[\mathbf{F} : \mathbb{Q}]$ sur $\mathbb{R}$ donc $\varphi(\mathbf{F} \otimes_{\mathbb{Q}} \mathbb{R})$ est un $\mathbb{R}$-sous-espace vectoriel de dimension finie de $\hat{\mathbf{F}}$. Le corps $\hat{\mathbf{F}}$ est muni d'une valeur absolue $|\ |$ et sa restriction à l'image de φ y définit sa topologie d'espace vectoriel de dimension finie.

L'image de φ est une partie complète donc fermée de $\hat{\mathbf{F}}$. Mais $\mathbf{F}$ est dense dans $\hat{\mathbf{F}}$ donc *a fortiori* l'image de φ l'est. On a donc que $\varphi(\mathbf{F} \otimes_{\mathbb{Q}} \mathbb{R}) = \hat{\mathbf{F}}$, et $\hat{\mathbf{F}}$ peut se décrire en tant qu'extension de $\mathbb{R}$ comme un quotient de l'algèbre :

$$\mathbf{F} \otimes_{\mathbb{Q}} \mathbb{R} = \left(\prod_{\sigma \text{ réel}} \mathbb{R} \right) \times \left(\prod_{\sigma, \bar{\sigma} \text{ complexes}} \mathbb{C} \right)$$

On peut ainsi décrire la $\mathbb{R}$-algèbre $\mathbf{F} \otimes_{\mathbb{Q}} \mathbb{R}$ comme un produit de corps $\mathbf{F}_i$: soit $x \in \mathbf{F}$ un élément primitif de polynôme minimal f. Alors $\mathbf{F} = \mathbb{Q}[T]/f(T)$, donc :

$$\mathbf{F} \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}[T]/f(T) \simeq \prod_{i=1}^{r} \mathbb{R}[T]/f_i(T)$$

où $f = \prod_{i=1}^{r} f_i$ est l'écriture de f comme produit d'irréductibles.

En notant $\mathbf{F}_i = \mathbb{R}[T]/f_i(T)$ on a $\mathbf{F}_i = \mathbb{R}$ si f_i est un facteur linéaire, auquel cas on obtient un plongement réel, $\mathbf{F}_i = \mathbb{C}$ si f_i est un facteur quadratique, auquel cas on obtient une paire de plongements complexes.

Suivant que $\mathbf{F}_i = \mathbb{R}$ ou $\mathbb{C}$ en tant que $\mathbb{R}$-espace vectoriel de dimension finie donc en tant qu'espace vectoriel topologique sur $\mathbb{R}$ on obtient par le plongement de $\mathbf{F}$ dans $\hat{\mathbf{F}}$ un plongement de $\mathbf{F}$ dans $\mathbb{R}$ ou $\mathbb{C}$. En effet, un plongement de $\mathbf{F}$ dans $\hat{\mathbf{F}} \simeq \mathbf{F} \otimes_{\mathbb{Q}} \mathbb{R}$ se factorise à travers l'isomorphisme entre $\mathbf{F} \otimes_{\mathbb{Q}} \mathbb{R}$ et $\prod \mathbf{F}_i$. La topologie usuelle sur $\mathbb{R}$ ou $\mathbb{C}$ est aussi celle qui provient de la valeur absolue de $\mathbf{F}$ donc $|\ |$ est équivalente à la valeur absolue associée au plongement considéré. □

Remarque 4.7.3. *Soit $x \in \mathbf{F}$. La multiplication par x vue comme endomorphisme du $\mathbb{Q}$-espace vectoriel $\mathbf{F}$ a même polynôme caractéristique S que la multiplication par $x \otimes 1$ vue comme endomorphisme du $\mathbb{R}$-espace vectoriel $\mathbf{F} \otimes_{\mathbb{Q}} \mathbb{R}$ (Pour le voir il suffit de considérer une base de $\mathbf{F}$ sur $\mathbb{Q}$.).*

Or $\mathbf{F} \otimes_{\mathbb{Q}} \mathbb{R} \simeq \prod \mathbf{F}_i$ et le polynôme S est le produit des polynômes caractéristiques S_i de la mumtiplication par x dans $\mathbf{F}_i$ vu comme $\mathbb{R}$-espace vectoriel.

On en déduit :

$$\begin{aligned} Tr_{\mathbf{F}/\mathbb{Q}}(x) &= \sum_{i=1}^{r+s} Tr_{\mathbf{F}_i/\mathbb{Q}}(x) \\ N_{\mathbf{F}/\mathbb{Q}}(x) &= \prod_{i=1}^{r+s} N_{\mathbf{F}_i/\mathbb{Q}}(x) \end{aligned}$$

On peut généraliser ces raisonnements : si $\mathbf{E}/\mathbf{F}$ est une extension de corps de nombres et que l'on se donne une place infinie de $\mathbf{F}$ pour laquelle on note $\mathbf{F}_\infty$ le complété correspondant, on cherche à déterminer les places infinies de $\mathbf{E}$ «au-dessus» de celles de $\mathbf{F}$. On dira qu'une place de $\mathbf{E}$ est au-dessus d'une place de $\mathbf{F}$ si les valeurs absolues de la place considérée sur $\mathbf{E}$ donnent par restriction à $\mathbf{F}$ des valeurs absolues de la place considérée sur $\mathbf{F}$.

On procède comme précédemment : on forme $\mathbf{E} \otimes_{\mathbf{F}} \mathbf{F}_\infty$ que l'on écrit comme un produit de corps $\mathbf{E}_i$, et alors chaque $\mathbf{E}_i$ correspond à exactement une place de $\mathbf{E}$ au-dessus de celle donnée sur $\mathbf{F}$. On a les mêmes résultats sur les normes et les traces :

$$\begin{aligned} Tr_{\mathbf{E}/\mathbf{F}}(x) &= \sum_{i=1}^{\alpha} Tr_{\mathbf{E}_i/\mathbf{F}}(x) \\ N_{\mathbf{E}/\mathbb{Q}}(x) &= \prod_{i=1}^{\alpha} N_{\mathbf{E}_i/\mathbf{F}}(x) \end{aligned}$$

4.8 Places des corps de nombres – cas fini

Proposition 4.8.1. *Soit $\mathbf{F}$ un corps de nombres et $|\ |$ une valeur absolue ultramétrique non triviale sur $\mathbf{F}$. Alors il existe un unique idéal maximal $\mathfrak{p}$ de $\mathcal{O}_{\mathbf{F}}$ tel que $|\ |$ soit équivalente à $|\ |_{\mathfrak{p}}$.*

Démonstration. La restriction de $|\ |$ à $\mathcal{O}_{\mathbf{F}}$ est non triviale (sinon elle serait triviale sur le corps des fractions de $\mathcal{O}_{\mathbf{F}}$, à savoir $\mathbf{F}$). Un élément x de $\mathcal{O}_{\mathbf{F}}$ est entier sur $\mathbb{Z}$ donc racine d'un polynôme unitaire $f \in \mathbb{Z}[T]$:

$$x^d = a_1 x^{d-1} + \cdots + a_d \text{ où } a_i \in \mathbb{Z}$$

Cela implique que $|x| \leqslant 1$: si on a $|x| > 1$ alors $|x|^d > |x|^i$ pour $0 \leqslant i \leqslant d$, et comme la valeur absolue est ultramétrique $|x|^d > |a_1 x^{d-1} + \cdots + a_d|$ (en effet $|a_i| \leqslant 1$ pour $a_0 \in \mathbb{Z}$), en contradiction avec l'hypothèse. On a donc $|x| \leqslant 1$ donc $x \in \mathcal{O}_{\mathbf{F}}$. □

4.9 Calcul dans les corps complets non archimédiens

4.10 Espaces vectoriels de dimension finie sur un corps complet non archimédien

4.11 Extensions finies d'un corps complet ultramétrique

4.12 Complétés ultramétriques des corps de nombres

4.13 Formule du produit

4.14 Cas galoisien

Chapitre 5

Adèles et idèles

Bibliograhie

Bibliographie

[1] Bourbaki. *Topologie Générale VIII.*

[2] Ellison et Mendès-France.

[3] John Milnor. *Introduction to algebraic K-theory.* Princeton University Press, 1971.

[4] Narkiewicz.

[5] Pierre Samuel. *Théorie algébrique des nombres.* Hermann, 1971.

[6] Jean-Pierre Serre. *Cours d'arithmétique.* Presses universitaires de France.