جامعة محمد الأول – وجدة
Université Mohammed Premier – Oujda
كلية العلـوم
Faculté des Sciences
شعبـة الرياضيات
Département de Mathématiques

Master de Théorie des Nombres

Semestre 2

CORPS D'INERTIE ET DE DECOMPOSITION

Les chapitres I et II

Professeur : Moulay Chrif ISMAILI

Année Universitaire : 2019/2020

CHAPITRE I

GROUPES D'INERTIE ET DE DÉCOMPOSITION

1.1 Décomposition dans le cas galoisien

Parmi les résultats principaux vus dans le cours d'Introduction à la Théorie des Nombres, on rappelle le théorème suivant :

Théorème 1.1.1 *Soit A un anneau de Dedekind de corps des fractions K, soient L une extension séparable finie de K de degré n et B la fermeture intégrale de A dans L. Si P est un idéal premier de A, alors :*

$$\sum_{\mathcal{P} \mid P} e_{L/K}(\mathcal{P}) f_{L/K}(\mathcal{P}) = n = [L : K].$$

Cas des extensions galoisiennes

Les notations étant celles du théorème précédent. On suppose de plus que l'extension L/K est galoisienne.

Théorème 1.1.2 *Le groupe de Galois de L sur K opère transitivement sur l'ensemble des idéaux premiers de B au dessus d'un idéal premier non nul P de A donné.*

Démonstration :
La démonstration de ce théorème repose sur le lemme d'évitement des idéaux premiers (voir *P. Samuel*, page 105), qui dit que :

Lemme 1.1.1 *Soient R un anneau, $P_1, \cdots, P_q$ une famille finie d'idéaux premiers de R, et I un idéal de R tel que $I \not\subset P_i$ pour tout i. Alors il existe $a \in I$ tel que $a \notin P_i$ pour tout i.*

Soit P un idéal premier non nul de A.
Soient $\mathcal{P}_1$ et $\mathcal{P}_2$ deux idéaux premiers de B au dessus de P, et soit $\mathrm{Gal}(L/K)$ le groupe de Galois de L/K. on suppose que $\mathcal{P}_1 \notin \{\mathcal{P}_2^\sigma \mid \sigma \in \mathrm{Gal}(L/K)\}$, alors d'après le lemme d'évitement des idéaux premiers, il existe un élément $x \in \mathcal{P}_1$ et $x \notin \mathcal{P}_2^\sigma \ \forall \sigma$.
On a $N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x)$; $x \in \mathcal{P}_1 \Rightarrow N_{L/K}(x) \in \mathcal{P}_1 \cap K = P$, or $P \subset \mathcal{P}_2$, donc

$N_{L/K}(x) \in \mathcal{P}_2$, et comme $\mathcal{P}_2$ est un idéal premier, $\exists \sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(x) \in \mathcal{P}_2$, d'où $x \in \mathcal{P}_2^{\sigma^{-1}}$, absurde.
Ainsi $\exists \sigma \in \mathrm{Gal}(L/K)$ tel que $\mathcal{P}_1 = \mathcal{P}_2^{\sigma} = \sigma(\mathcal{P}_2)$. □

Corollaire 1.1.1 Si $\mathcal{P}$ est un idéal de B au dessus de P, et si e, f et g désignent respectivement l'indice de ramification de $\mathcal{P}$ dans L/K ; le degré résiduel de $\mathcal{P}$ dans L/K, et g le nombre d'idéaux premiers de B au dessus de P, alors :
1) Tous les idéaux premiers de B au dessus de P ont même indice de ramification e et même degré résiduel f.
2) $n = efg$.

Démonstration :
1) Soit $PB = \prod_{i=1}^{g} \mathcal{P}_i^{e_i}$ la décomposition de PB dans B, comme $\mathcal{P}_i = \sigma_i(\mathcal{P}_1)$, alors

$$PB = \prod_{i=1}^{g} \mathcal{P}_i^{e_i} = \prod_{i=1}^{g} \sigma_i(\mathcal{P}_1)^{e_i}.$$

Par ailleurs, il est très facile de vérifier que $\forall \sigma \in \mathrm{Gal}(L/K)$; $\sigma(PB) = PB$ (car $\sigma(B) = B$), en appliquant σ_j^{-1} à $PB = \prod_{i=1}^{g} \sigma_i(\mathcal{P}_1)^{e_i}$, et en utilisant l'unicité de la décomposition, on trouve que $e_j = e_1$, $\forall 1 \leq j \leq g$.
On vérifie sans peine que si $\mathcal{P}$ est un idéal premier non nul de B, et $\sigma \in \mathrm{Gal}(L/K)$, alors $B/\mathcal{P} \simeq B/\sigma(\mathcal{P})$. Cet isomorphisme permet de montrer que les idéaux premiers de B au dessus de $\mathcal{P}$ ont même degré résiduel.
2) En posant $e = e_i$ et $f = f_i$, alors $n = \sum_i e_i f_i$, on trouve que $n = efg$. □

Remarque 1.1.1 Dans le cas Galoisien, on voit que l'indice de ramification et le degré résiduel dépendent de l'idéal premier P, dans ce cas on dira indice de ramification et degré résiduel de P. On dira aussi que P est ramifié, si l'un des idéaux premiers quelconques de B au dessus de P est ramifié dans L/K.

Définition 1.1.1 *Soit L/K galoisienne, et soit P un idéal premier non nul de K. On dit que P se décompose complétemnent ou est totalement décomposé dans L/K si $e = f = 1$ et $g = n$ où $n = [L : K]$.*
On dit que l'idéal P est inerte si $e = g = 1$ ($f = n$).

1.2 Corps de décomposition et corps d'inertie

Corps de décomposition

Soit L/K une extension galoisienne finie, dont le groupe de Galois est noté $\mathrm{Gal}(L/K)$. On suppose que K est le corps des fractions d'un anneau de Dedekind A, et on désigne par B la clôture intégrale de A dans L.
Soit P un idéal premier non nul de A et soit $\mathcal{P}$ un idéal premier de B au dessus de P. On pose :

$$D_{\mathcal{P}} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathcal{P}) = \mathcal{P}\}.$$

Définition 1.2.1 *$D_{\mathcal{P}}$ est un sous-groupe de $Gal(L/K)$ qui dépend de $\mathcal{P}$; on l'appelle le groupe de décomposition de $\mathcal{P}$ dans L/K.*
Soit K_D le corps intermédiaire de L/K fixe par $D_{\mathcal{P}}$; on l'appelle le corps de décomposition de $\mathcal{P}$ dans l'extension L/K.

On désigne par e et f respectivement l'indice de ramification et le degré résiduel de $\mathcal{P}$ dans L/K, soit g le nombre des idéaux premiers de B au dessus de P, comme L/K est galoisienne $[L : K] = efg$.

Proposition 1.2.1 *Le groupe de décomposition $D_{\mathcal{P}}$ est d'ordre ef.*

Démonstration :
Considérons l'ensemble des classes à gauche modulo $D_{\mathcal{P}}$ des éléments de $\mathrm{Gal}(L/K)$, et soit r le nombre de ces classes ; on sait que $[L : K] = n = r|D_{\mathcal{P}}|$, où $|D_{\mathcal{P}}|$ est l'ordre de $D_{\mathcal{P}}$.
Soient $\overline{\sigma_1}, \cdots, \overline{\sigma_r}$ ces classes ; $\overline{\sigma_i} = \sigma_i D_{\mathcal{P}}$ et $\forall \tau \in D_{\mathcal{P}}$; $\sigma_i\tau(\mathcal{P}) = \sigma_i(\mathcal{P})$. Les $\sigma_i(\mathcal{P})$ pour $1 \leq i \leq r$ sont des idéaux premiers de B distincts deux à deux, en effet, si $\sigma_i(\mathcal{P}) = \sigma_j(\mathcal{P})$, alors $\sigma_j^{-1}\sigma_i(\mathcal{P}) = \mathcal{P} \Rightarrow \sigma_j^{-1}\sigma_i \in D_{\mathcal{P}} \Rightarrow \sigma_i \in \sigma_j D_{\mathcal{P}} \Rightarrow \overline{\sigma_i} = \overline{\sigma_j}$.
On en déduit que $\sigma_1(\mathcal{P}), \cdots, \sigma_r(\mathcal{P})$ sont tous les idéaux premiers de B au dessus de P distincts deux à deux (grâce à l'operation transitive de $\mathrm{Gal}(L/K)$), ainsi $r = g$, par suite $|D_{\mathcal{P}}| = ef$.

Corps d'inertie On garde les mêmes notations et on fixe $\mathcal{P}$, $P = \mathcal{P} \cap A$, on pose $\overline{K} = A/P$, $\overline{L} = B/\mathcal{P}$ et $[\overline{L} : \overline{K}] = f$. On pose aussi $G = \mathrm{Gal}(L/K)$.
Comment construire un $\overline{K}$-automorphisme de $\overline{L}$?
Soit $\sigma \in D_{\mathcal{P}}$; alors l'application $\overline{\sigma}$ définie par $\overline{\sigma}(\overline{b}) = \overline{\sigma(b)}$ la classe de $\sigma(b)$ modulo $\mathcal{P}$, est un $\overline{K}$-automorphisme de $\overline{L}$. L'extension $\overline{L}$ de $\overline{K}$ n'est pas nécessairement galoisienne car non nécessairement séparable.
On désigne par $\mathrm{Gal}\ (\overline{L}/\overline{K})$ le groupe des $\overline{K}$-automorphismes de $\overline{L}$. Soit l'application $\varphi_{\mathcal{P}}$ définie par :

$$\begin{array}{rccc} \varphi_{\mathcal{P}} : & D_{\mathcal{P}} & \longrightarrow & \mathrm{Gal}\ (\overline{L}/\overline{K}) \\ & \sigma & \longmapsto & \overline{\sigma} \end{array}$$

$\varphi_{\mathcal{P}}$ est un homomorphisme de groupes. Ker $\varphi_{\mathcal{P}}$ est un sous-groupe distingué de $D_{\mathcal{P}}$; on l'appelle le groupe d'inertie de $\mathcal{P}$ dans l'extension L/K, et on le note $T_{\mathcal{P}}$.
Soit K_T le sous-corps de L fixe par $T_{\mathcal{P}}$; on appelle K_T le corps d'inertie de $\mathcal{P}$ dans L/K.
On a le diagramme suivant : K———— K_D———— K_T———— L ; il est clair que K_T est galoisienne sur K_D dont le groupe de Galois est Gal $(K_T/K_D) = D_{\mathcal{P}}/T_{\mathcal{P}}$; où $T_{\mathcal{P}} = \text{Ker } \varphi_{\mathcal{P}} = \{\sigma \in D_{\mathcal{P}} \mid \overline{\sigma} = \overline{1}\}$; évidemment $\overline{1} = 1_{\overline{L}}$.
En fait $\overline{\sigma} = \overline{1} \Leftrightarrow \forall \overline{b} \in \overline{L},\ \overline{\sigma}(\overline{b}) = \overline{b} = \overline{\sigma(b)}$; ainsi $\sigma \in T_{\mathcal{P}} \Leftrightarrow \sigma(b) - b \in \mathcal{P}\ \forall b \in B$.
Soit $v_{\mathcal{P}}$ la valuation associée à $\mathcal{P}$ définie sur L , alors $v_{\mathcal{P}}(\sigma(b) - b) \geq 1,\ \forall b \in B$, et $\sigma \in T_{\mathcal{P}} \Leftrightarrow v_{\mathcal{P}}(\sigma(b) - b) > 0,\ \forall b \in B$.
On définit sur $D_{\mathcal{P}}$ une filtration $G_i = \{\sigma \in D_{\mathcal{P}} \mid v_{\mathcal{P}}(\sigma(b) - b) \geq i + 1,\ \forall b \in B\}$; G_i est une suite décroissante et on a $T_{\mathcal{P}} = G_0$ et $D_{\mathcal{P}} = G_{-1}$.

Proposition 1.2.2 *L'extension résiduelle $\overline{L}$ de $\overline{K}$ est normale et l'application $\varphi_{\mathcal{P}} :\ D_{\mathcal{P}} \to Gal\ (\overline{L}/\overline{K})$ définit un homomorphisme surjectif ; c.à.d. $D_{\mathcal{P}}/T_{\mathcal{P}} \simeq Gal\ (\overline{L}/\overline{K})$.*

Démonstration :
Soit $\overline{b} \in \overline{L}$ où $b \in B$, b est racine du polynôme $P(X) = \prod_{\sigma \in G}(X - \sigma(b)) \in A[X]$. Si $P(X) = X^n + a_1X^{n-1} + \cdots + a_n$, où $a_i \in A$ et $\overline{a_i}$ est la classe de a_i modulo $\mathcal{P}$, on pose $\overline{P}(X) = X^n + \overline{a_1}X^{n-1} + \cdots + \overline{a_n} = \prod_{\sigma \in G}(X - \overline{\sigma(b)}) \in \overline{K}[X]$ et $\overline{\sigma(b)} \in \overline{L}$. Ainsi $\overline{L}$ est normale sur $\overline{K}$.
Soit $\tau \in$ Gal $(\overline{L}/\overline{K})$, montrons que $\exists \sigma \in D_{\mathcal{P}}$ tel que $\overline{\sigma} = \tau$.
Soit $\overline{L}_s$ la clôture séparable de $\overline{K}$ dans $\overline{L}$, on a $\overline{L}_s = \overline{K}(\overline{\theta})$, où $\overline{\theta} \in \overline{L}$. $\tau(\overline{\theta})$ est évidemment une racine de Irr $(\overline{\theta}, \overline{K})$. D'après le théorème du reste chinois, on peut trouver un élément $b \in B$ tel que : $b \equiv \theta \bmod \mathcal{P}$ et $b \equiv 0 \bmod \sigma'^{-1}(\mathcal{P})$ pour tout $\sigma' \notin D_{\mathcal{P}}$; ainsi $\overline{b} = \overline{\theta},\ \sigma'(b) \equiv 0 \bmod \mathcal{P}$, on en déduit que si $P(X) = \prod_{\sigma \in G}(X - \sigma(\theta)) \in A[X]$, alors $\overline{P_1(X)} = \prod_{\sigma \in D_{\mathcal{P}}}(X - \overline{\sigma(\theta)}) \in \overline{K}[X]$ est un polynôme de $\overline{K}[X]$ annulé par $\overline{\theta}$, donc divisible par Irr $(\overline{\theta}, \overline{K})$, par suite $\tau(\overline{\theta})$ est une racine de $\overline{P_1(X)}$, il existe donc $\sigma \in D_{\mathcal{P}}$ tel que $\tau(\overline{\theta}) = \overline{\sigma(\theta)} = \overline{\sigma}(\overline{\theta})$, c.à.d. que τ et $\overline{\sigma}$ coinçident sur $\overline{L_s}$, par suite sur $\overline{L}$, ainsi $\tau = \overline{\sigma}$.
Conclusion : $D_{\mathcal{P}}/T_{\mathcal{P}} \simeq$ Gal $(\overline{L}/\overline{K})$. □

Proposition 1.2.3 *On garde les notations précédentes et on suppose que $\overline{L}$ est une extension séparable de $\overline{K}$, alors :*
1) $[L : K_T] = e$.
2) $\mathcal{P}$ est totalement ramifié dans L/K_T.
3) $\mathcal{P} \cap K_T$ est non ramifié dans K_T/K_D et il est de degré résiduel f dans K_T/K_D.
4) $\mathcal{P} \cap K_D$ est non ramifié dans K_D/K et de degré résiduel égal à 1 dans K_D/K. Autrement dit ; $\overline{K_T} = \overline{L}$ et $\overline{K_D} = \overline{K}$. ($\overline{K_T}$ est le corps résiduel de $\mathcal{P} \cap K_T$ et $\overline{K_D}$ celui de $\mathcal{P} \cap K_D$).

Démonstration :
$D_{\mathcal{P}}/T_{\mathcal{P}} \simeq$ Gal $(\overline{L}/\overline{K})$; comme $\overline{L}/\overline{K}$ est séparable, alors $|\text{Gal }(\overline{L}/\overline{K})| = [\overline{L} : \overline{K}] = f$, d'où $|T_{\mathcal{P}}| = e$ donc $[L : K_T] = e$ et $[K_T : K_D] = f$.
Le groupe de décomposition D' de $\mathcal{P}$ dans L/K_T est $T_{\mathcal{P}}$, car Gal $(L/K_T) = T_{\mathcal{P}} \subset D_{\mathcal{P}}$. Il est évident que le groupe d'inertie T' de $\mathcal{P}$ dans L/K_T est égal à $T_{\mathcal{P}}$. Ainsi D'/T' est d'ordre 1, donc $[\overline{L} : \overline{K_T}] = 1$ donc $\mathcal{P}$ est totalement ramifié dans L/K_T.
Comme $e_{L/K}(\mathcal{P}) = e = e_{L/K_T}(\mathcal{P}) = e_{L/K_T}(\mathcal{P}).e_{K_T/K_D}(\mathcal{P} \cap K_T).e_{KD/K}(\mathcal{P} \cap K_D)$, alors $e_{K_T/K_D}(\mathcal{P} \cap K_T) = e_{KD/K}(\mathcal{P} \cap K_D) = 1$. Le même raisonnement sur les degrés résiduels permet de montrer que $[\overline{K_T} : \overline{K_D}] = f$ et $[\overline{K_D} : \overline{K}] = 1$. □

Proposition 1.2.4 *On garde les mêmes notations mais on suppose que $\overline{L}$ n'est pas nécessairement séparable sur $\overline{K}$. Soit p la caractéristique de $\overline{K}$ et soient f_s et p^m respectivement le degré de séparabilité et le degré d'inséparabilité de $\overline{L}/\overline{K}$. Alors :*
1) Le corps d'inertie K_T est une extension galoisienne de K_D de degré f_s et on a $[L : K_T] = ep^m$.
2) L'indice de ramification de $\mathcal{P}$ (resp. $\mathcal{P} \cap K_T$, resp. $\mathcal{P} \cap K_D$) dans L/K_T (resp. K_T/K_D, resp. K_D/K) est égal à e (resp. 1, resp. 1).
3) Si $\overline{L_s}$ est la clôture séparable de $\overline{L}/\overline{K}$, $\overline{K_T}$, (resp. $\overline{K_D}$) le corps résiduel de $\mathcal{P} \cap K_T$ (resp. de $\mathcal{P} \cap K_D$). Alors :
$\overline{K_T} = \overline{L_s}$; $\overline{K_D} = \overline{K}$; $[\overline{L} : \overline{K_T}] = p^m$ *et* $[\overline{K_T} : \overline{K_D}] = f_s$.

Démonstration :
On a $[\overline{L} : \overline{K}] = f = f_s p^m$ et $D_{\mathcal{P}}/T_{\mathcal{P}} \simeq$ Gal $(\overline{L}/\overline{K})$, d'où $|D_{\mathcal{P}}/T_{\mathcal{P}}| = f_s$, par suite $|T_{\mathcal{P}}| = ep^m$.
On considère L/K_T et on remarque que $T_{\mathcal{P}}$ est à la fois le groupe de décomposition $D'_{\mathcal{P}}$ et le groupe d'inertie $T'_{\mathcal{P}}$ de $\mathcal{P}$ dans L sur K_T. Comme $D'_{\mathcal{P}}/T'_{\mathcal{P}} \simeq$ Gal $(\overline{L}/\overline{K_T})$ est d'ordre 1, alors $\overline{K_T} = \overline{L_s}$ et $[\overline{L} : \overline{K_T}] = p^m$ □

Remarque 1.2.1 Dans les deux cas qui suivent l'extension $\overline{L}/\overline{K}$ est séparable :
1) $\overline{K}$ est un corps parfait (cas lorsque K est un corps de nombres).
2) Le degré résiduel $[\overline{L} : \overline{K}]$ est premier avec la caractéristique de $\overline{K}$; si $p =$ car $(\overline{K})$ on a $pA \subset P$.

Corollaire 1.2.1 Si $\overline{K}$ est un corps fini alors le groupe quotient $D_{\mathcal{P}}/T_{\mathcal{P}}$ est cyclique.

Démonstration :
$D_{\mathcal{P}}/T_{\mathcal{P}} \simeq$ Gal $(\overline{L}/\overline{K})$, et comme toute extension algébrique finie d'un corps fini est une extension cyclique, on déduit alors le résultat facilement.

Remarque 1.2.2 C'est le cas lorsque K est un corps de nombres.

Proposition 1.2.5 *On garde les mêmes notations du début de ce paragraphe et soit M un corps intermédiaire de L/K. Soient $D_{\mathcal{P}}(L/M)$ et $T_{\mathcal{P}}(L/M)$ les groupes de décomposition et d'inertie de $\mathcal{P}$ dans L/M, alors :*

$$D_{\mathcal{P}}(L/M) = D_{\mathcal{P}} \cap Gal\,(L/M) \;\; et \;\; T_{\mathcal{P}}(L/M) = T_{\mathcal{P}} \cap Gal\,(L/M).$$

Cas abélien

Théorème 1.2.1 *On suppose que L est une extension abélienne de K.*
1) Si P est un idéal premier non nul de K alors tous les idéaux premiers de L au dessus de P ont même corps de décomposition et même corps d'inertie.
2) Le corps de décomposition (resp. d'inertie) d'un idéal premier non nul P de K est le plus grand corps intermédiaire de L/K dans lequel P se décompose complétement (resp. P est non ramifié).

Démonstration :
1) Soit $\tau \in$ Gal (L/K) et soit $D_{\mathcal{P}}$ le groupe de décomposition de $\mathcal{P}$ dans L/K. Il est facile de vérifier que $D_{\tau(\mathcal{P})} = \tau D_{\mathcal{P}} \tau^{-1}$ et $T_{\tau(\mathcal{P})} = \tau T_{\mathcal{P}} \tau^{-1}$, comme L/K est abélienne, on a le résultat.
2) Soient e et f l'indice de ramification et le degré résiduel de P dans l'extension L/K et soit $K \subset K' \subset L$, $D_{\mathcal{P}}(L/K') = D_{\mathcal{P}} \cap$ Gal $(L/K') \subset D_{\mathcal{P}}$. Si P se décompose complétement dans K' alors $[L : K']$ est un multiple de ef c.à.d. $K' \subset K_D$, or $|D_{\mathcal{P}}(L/K')| = ef = |D_{\mathcal{P}}|$. □

Remarque 1.2.3 Dans le cas non abélien les corps de décomposition sont conjugués deux à deux, et les corps d'inertie sont conjugués deux à deux.

CHAPITRE II

AUTOMORPHISME DE FROBENIUS ET APPLICATION D'ARTIN

2.1 Automorphisme de Frobenius

Soit K un corps de nombres et L une extension galoisienne finie de K. On désignera par A l'anneau des entiers de K et B celui de L. On considère P un idéal premier de K non ramifié dans L et $\mathcal{P}$ un idéal premier de L au dessus de P. Dans ce cas, le groupe d'inertie $T_{\mathcal{P}}$ est d'ordre $e = 1$. Ainsi, le groupe de décomposition $D_{\mathcal{P}} \simeq \text{Gal}\ (\overline{L}/\overline{K})$. Or on sait que le groupe de Galois d'une extension finie d'un corps fini est cyclique (voir P. Samuel page 104, exemple 3), d'où le groupe de décomposition $D_{\mathcal{P}}$ est cyclique d'ordre f (le degré résiduel). Si On note par $\mathbf{F_q}$ un corps fini à q éléments et $\mathbf{F_{q^f}}$ une extension finie de degré f sur $\mathbf{F_q}$, on vérifie que le l'automorphisme $y \mapsto y^q$ est un générateur du groupe de Galois de $\mathbf{F_{q^f}}$ sur $\mathbf{F_q}$, qu'on appelle l'automorphisme de Frobenius.

Définition 2.1.1 *L'automorphisme de Frobenius de l'idéal premier $\mathcal{P}$ est l'unique automorphisme du groupe de décomposition $D_{\mathcal{P}}$ vérifiant :*

$$\sigma(x) \equiv x^q \ \ mod\ \mathcal{P}\ \ pour\ x \in B,$$

et q le cardinal de $\overline{K}$.

L'automorphisme de Frobenius de l'idéal premier $\mathcal{P}$ sera noté par :

$$\sigma = \left[\frac{L/K}{\mathcal{P}}\right].$$

Dans la suite, on va établir certaines propriétés de l'automorphisme de Frobenius.

Propriété 2.1.1 *Pour tout automorphisme $\tau \in Gal(L/K)$, on a :*

$$\left[\frac{L/K}{\tau(\mathcal{P})}\right] = \tau \left[\frac{L/K}{\mathcal{P}}\right] \tau^{-1}.$$

Démonstration : Tout élément de B peut être écrit sous la forme $\tau^{-1}(x)$ avec x un entier algébrique. Nous avons alors $\left[\frac{L/K}{\mathcal{P}}\right] \tau^{-1}(x) \equiv \tau^{-1}(x)^q \mod \mathcal{P}$. En appliquant τ à cette égalité, on obtient $\tau \left[\frac{L/K}{\mathcal{P}}\right] \tau^{-1}(x) \equiv x^q \mod \tau(\mathcal{P})$. L'unicité de l'automorphisme de Frobenius force le résultat. □

Supposons $L \supset E \supset K$ et posons $\mathcal{P} \cap E = P_0$. Comme $\mathcal{P}$ est non ramifié dans L, alors P_0 est forcément non ramifié dans L. Nous pouvons donc parler de l'automorphisme de Frobenius de $\mathcal{P}$ dans l'extension L/E qui est relié à celui de $\mathcal{P}$ dans L/K par la :

Propriété 2.1.2

$$\left[\frac{L/K}{\mathcal{P}}\right]^{f(P_0/P)} = \left[\frac{L/E}{\mathcal{P}}\right].$$

Démonstration : Les corps résiduels des anneaux des entiers dans L, E et K relativement à $\mathcal{P}$, P_0 et P vérifient $\overline{L} \supset \overline{E} \supset \overline{K}$. De plus, si $q = |\overline{K}|$, alors $q^{f_0} = |\overline{E}|$ et $q^f = |\overline{L}|$, où $f_0 = f(P_0/P)$. Le générateur du groupe de Galois de $\overline{L}$ sur $\overline{E}$ est défini par $x \mapsto x^{q^{f_0}}$. Ce n'est rien d'autre que la f_0-ème puissance du générateur de $\mathrm{Gal}(\overline{L}/\overline{K})$. L'unicité et la définition de l'automorphisme de Frobenius permettent de conclure. □

Supposons maintenant $L \supset E \supset K$, et de plus E normale sur K. nous avons donc le droit de parler de l'automorphisme de Frobenius de P_0 dans E/K, et on a :

Propriété 2.1.3

$$\left[\frac{E/K}{P_0}\right] = \left[\frac{L/K}{\mathcal{P}}\right]|E \quad \textit{la restriction à } E.$$

Démonstration : Pour un entier algébrique x dans E, une congruence du type $\sigma(x) \equiv x^q \mod \mathcal{P}$ est équivalente à la congruence $\sigma(x) \equiv x^q \mod P_0$, car $\mathcal{P} \cap E = P_0$ est envoyé sur lui même par $D_{\mathcal{P}}$ lorsque E est normale sur K. Donc si on pose $\sigma = \left[\frac{L/K}{\mathcal{P}}\right]$, alors la restriction de σ à E n'est rien d'autre que $\left[\frac{E/K}{P_0}\right]$. □

Maintenant on suppose que E_1 et E_2 sont des extensions normales sur K et $L = E_1E_2$. Posons $\mathcal{P} \cap E_i = P_i$ pour $i = 1,\ 2$. Les automorphismes de Frobenius suivants :

$$\left[\frac{E_1E_2/K}{\mathcal{P}}\right],\ \left[\frac{E_1/K}{P_1}\right] \text{ et } \left[\frac{E_2/K}{P_2}\right]$$

sont bien définis, mais appartiennent à des groupes différents. Soit donc l'application :

$$\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(E_1/K) \times \mathrm{Gal}(E_2/K)$$

définie par :

$$\sigma \longmapsto (\sigma|E_1, \sigma|E_2).$$

C'est une application injective, car tout automorphisme agissant comme l'identité sur E_1 et E_2 en même temps est égal à l'identité sur $L = E_1E_2$. En identifiant $\mathrm{Gal}(L/K)$ à son image dans le produit direct de $\mathrm{Gal}(E_1/K)$ par $\mathrm{Gal}(E_2/K)$ et en utilisant la propriété 1.4.3 on a facilement :

Propriété 2.1.4 $\left[\frac{E_1E_2/K}{\mathcal{P}}\right] = \left[\frac{E_1/K}{P_1}\right] \times \left[\frac{E_2/K}{P_2}\right]$.

Définition 2.1.2 *On dit qu'un premier P se décompose complètement dans L si P admet $[L : K]$ distincts diviseurs premiers dans L.*

Il est facile de voir que cela est équivalent à dire que pour tout idéal premier $\mathcal{P}$ de L au dessus de P, on a $e(\mathcal{P}/P) = f(\mathcal{P}/P) = 1$, qu'on peut formuler comme suit :

Propriété 2.1.5 *L'idéal premier se décompose complètement dans dans L/K si et seulement si*

$$\left[\frac{L/K}{\mathcal{P}}\right] = 1.$$

Démonstration : La définition de $\left[\frac{L/K}{\mathcal{P}}\right]$ implique que c'est un générateur du groupe de décomposition $D_{\mathcal{P}}$. Cependant, P se décompose complètement dans L/K si et seulement si $|D_{\mathcal{P}}| = ef = 1$. □

Corollaire 2.1.1 Soient E_1 et E_2 deux extensions normales sur K et $L = E_1E_2$. L'idéal premier P de K se décompose complètement dans L si et seulement si P se décompose complètement dans E_1 et E_2.

Démonstration : La propriété 1.4.4 implique : $\left[\frac{L/K}{\mathcal{P}}\right] = 1$ si et seulement si $\left[\frac{E_i/K}{P_i}\right] = 1$ pour $i = 1,\ 2$. □

2.1.1 Factorisation dans les extensions non normales

Dans le cas d'une extension normale L/K, l'automorphisme de Frobenius est porteur de toutes les informations concernant la factorisation des premiers non ramifiés puisque $\left[\frac{L/K}{\mathcal{P}}\right]$ est d'ordre f (car il engendre $D_{\mathcal{P}}$) et le nombre des facteurs premiers de L au dessus de P est $g = [L : K]/f$.

Nous allons maintenant voir comment l'automorphisme de Frobenius peut être utilisé pour décrire la factorisation de P dans une extension non normale.

Soit donc la tour de corps de nombres $K \subset E \subset L$ avec E/K non nécessairement normale. Soit H le sous-groupe de $G = \mathrm{Gal}(L/K)$ tel que E est le corps fixe par H. On considère une décomposition de G en classes à droite modulo H, de sorte que :

$$G = H\sigma_1 \cup \cdots \cup H\sigma_k.$$

Tout élément σ dans G permute ces classe par multiplication à droite : $H\sigma_i \to H\sigma_i\sigma$. *Un cycle de longueur* t pour σ est la donnée d'une suite de classes :

$$H\sigma_i,\ H\sigma_i\sigma,\ H\sigma_i\sigma^2, \cdots, H\sigma_i\sigma^{t-1},$$

telle que les t classes sont distinctes et $H\sigma_i = H\sigma_i\sigma^t$. Cette définition rappelle celle de la notion de cycle du groupe des permutations. La collection de toutes les classes est partitionnée en cycles disjoints de σ.

Nous voulons décrire comment le premier P de K se factorise en produit de premiers de E. Nous supposons que P est non ramifié dans L et que $\mathcal{P}$ est un facteur premier de P dans L.

Proposition 2.1.1 *Soit σ l'automorphisme de Frobenius de $\mathcal{P}$ dans L/K. Supposons qu'en agissant sur les classes à droite modulo H l'automorphisme σ admet s cycles de longueur $t_1, \cdots,\ t_s$. Alors P est le produit de s premiers distincts de E, de degré résiduels respectifs $t_1, \cdots,\ t_s$.*

Démonstration : Soit $H\tau$ un représentant d'un cycle de longueur t pour σ. Posons $P_0 = \tau(\mathcal{P}) \cap E$. Il est clair que P_0 est un premier de E au dessus de $\tau(\mathcal{P}) \cap K = P$. Le degré résiduel $f(P_0/P) = f$ peut être calculé de la façon suivante.

Le degré résiduel de $\tau(\mathcal{P})$ sur P_0 est l'ordre du groupe de décomposition $H(\tau(\mathcal{P}))$, c.-à-d. le sous-groupe de $H = \mathrm{Gal}(L/E)$ laissant fixe $\tau(\mathcal{P})$. Ce sous-groupe est donné par :

$$H(\tau(\mathcal{P})) = \mathcal{H} \cap \mathcal{D}_{\tau(\mathcal{P})}.$$

Comme σ est un générateur du groupe de décomposition $D_{\mathcal{P}}$, alors $D_{\tau(\mathcal{P})} = \tau D_{\mathcal{P}} \tau^{-1} =$

$< \tau\sigma\tau^{-1} >$. On en déduit que

$$H \cap < \tau\sigma\tau^{-1} > = < \tau\sigma^t\tau^{-1} >,$$

où t est le plus petit entier positif tel que $H\tau = H\tau\sigma^t$. Cela conduira au fait que le groupe $H(\tau(\mathcal{P})) = < \tau\sigma^t\tau^{-1} >$. On en déduit que :

$$f(P_0/P) = f(\mathcal{P}/P)/f(\mathcal{P}/P_0) = |D_{\mathcal{P}}|/|H(\tau(\mathcal{P}))| = | < \sigma > |/| < \tau\sigma^t\tau^{-1} > | = t.$$

Par conséquent, un cycle de σ de longueur t correspond à un premier de E au dessus de P, de degré résiduel t. Dans la suite, nous allons montrer que cette correspondance est bijective.

Supposons que $H\tau$ et $H\lambda$ sont des classes modulo H telles que :

$$P_0 = \lambda(\mathcal{P}) \cap E = \tau(\mathcal{P}) \cap E.$$

Alors $\lambda(\mathcal{P})$ et $\tau(\mathcal{P})$ sont deux idéaux premiers de L divisant P_0. Comme le groupe de Galois H agit transitivement sur les premiers au dessus de P_0, il existe $\gamma \in H$ tel que $\gamma\lambda(\mathcal{P}) = \tau(\mathcal{P})$. Il s'ensuit que $\tau^{-1}\gamma\lambda \in D_{\mathcal{P}} = < \sigma >$, d'où $\tau^{-1}\gamma\lambda = \sigma^i$ pour un certain i. Ainsi :

$$H\tau\sigma^i = H\gamma\lambda = H\lambda,$$

par suite, $H\tau$ et $H\lambda$ appartiennent au même cycle.

La dernière étape consiste à montrer que tout diviseur premier de P dans E à été obtenu de cette façon.Chacun des s cycles de σ correspond à un premier P_i de E au dessus de P et de degré résiduel $t_i = f(P_i/P)$ de sorte que :

$$\Sigma t_i = [G : H] = [E : K],$$

et en utilisant le théorème 1.2.1 on s'aperçoit que tous les diviseurs premiers de P dans E ont été comptés.

Corollaire 2.1.2 Le nombres des premiers de E divisant P et de degré résiduel 1 est égal au nombre de représentants de classes σ_i satisfaisant :

$$\sigma_i D_{\mathcal{P}} \sigma_i^{-1} \subseteq H.$$

Démonstration : Comme $D_{\mathcal{P}} =< \sigma >$, alors $\sigma_i D_{\mathcal{P}} \sigma_i^{-1} \subseteq H \Leftrightarrow \sigma_i \sigma \sigma_i^{-1} \in H \Leftrightarrow H\sigma_i\sigma = H\sigma_i \Leftrightarrow \sigma_i$ appartient à un cycle de longueur 1. Le résultat est alors acquis grâce à la proposition précédente.

2.2 L'application d'Artin pour les extensions abéliennes

Dans cette section nous supposons que L est normale sur K at que $G = \mathrm{Gal}(L/K)$ est abélien. Nous savons (propriété 1.4.1) que si P est un idéal premier non ramifié de K et si $\mathcal{P}$ et $\tau(\mathcal{P})$ sont deux diviseurs premiers de P dans L, alors les automorphismes de Frobenius correspondants sont égaux puisque :

$$\left[\frac{L/K}{\tau(\mathcal{P})}\right] = \tau \left[\frac{L/K}{\mathcal{P}}\right] \tau^{-1} = \left[\frac{L/K}{\mathcal{P}}\right].$$

Cela montre que l'automorphisme de Frobenius ne dépend pas vraiment de $\mathcal{P}$ mais plutôt de l'idéal premier P de K. Nous pouvons donc changer de notation et écrire :

$$\left[\frac{L/K}{P}\right] \quad \text{au lieu de} \quad \left[\frac{L/K}{\mathcal{P}}\right]$$

qu'on appellera l'*automorphisme de Frobenius de* P.

De cette façon, l'automorphisme de Frobenius peut être vu comme une correspondance entre les premiers non ramifiés et certains éléments du groupe de Galois abélien.

On notera par $\mathbf{I_K}$ le groupe des idéaux fractionnaires non nuls de K. On posera aussi S un ensemble fini de premiers de K incluant tous les idéaux premiers ramifiés dans L. On notera aussi par ${\mathbf{I_K}}^S$ ou simplement $\mathbf{I}^S$ le sous-groupe de $\mathbf{I_K}$ engendré par tous les premiers n'appartenant pas à S. Pour chaque idéal fractionnaire $\mathcal{A}$ dans $\mathbf{I}^S$

nous définirons un élément $\varphi_{\mathbf{L/K}}(\mathcal{A})$ dans G comme suit : Si $\mathcal{A}$ se factorise sous la forme

$$\mathcal{A} = \prod_P P^{\alpha(P)}$$

alors on pose

$$\varphi_{\mathbf{L/K}}(\mathcal{A}) = \prod_P \left[\frac{L/K}{P}\right]^{\alpha(P)}.$$

Le produit est bien défini car G est abélien. La fonction $\varphi_{\mathbf{L/K}}$ est un homomorphisme de $\mathbf{I}^S$ dans G qu'on appelle l'*application d'Artin* pour l'extension L/K. Nous insistons sur le fait que $\varphi_{\mathbf{L/K}}$ est définie uniquement pour les idéaux dont la factorisation ne comporte que des premiers non ramifiés. Évidemment, lorsque P est un premier non ramifié dans L, $\varphi_{\mathbf{L/K}}(P)$ n'est rien d'autre que l'automorphisme de Frobenius de P.

Supposons que E est une extension finie de K. On peut translater l'extension abélienne L/K par E pour obtenir une extension abélienne EL/E dont le groupe de Galois H peut être identifié à un sous-groupe de G par restriction. Si on note par ${\mathbf{I}_\mathbf{E}}^S$ la partie du groupe des idéaux fractionnaires de E engendrée par les premiers de E qui ne divisent aucun premier de S, alors la relation entre les applications d'Artin pour les extensions EL/E et L/K est donnée par la

Proposition 2.2.1 *Lorsque $Gal(EL/E)$ est identifié (par restriction) à un sous-groupe de $Gal(L/K)$, alors :*

$$\varphi_{\mathbf{EL/E}} = \varphi_{\mathbf{L/K}} \cdot N_{\mathbf{E/K}} \ \textit{sur} \ {\mathbf{I}_\mathbf{E}}^S.$$

Démonstration : Si $\mathcal{P}$ désigne un idéal premier de EL, on posera les idéaux premiers $\mathcal{P}_L = \mathcal{P} \cap L$, $\mathcal{P}_E = \mathcal{P} \cap E$ et $\mathcal{P}_K = \mathcal{P} \cap K$. Posons $N_{\mathbf{K}/\mathbb{Q}}(\mathcal{P}_K) = q$ une puissance d'un nombre premier et $N_{\mathbf{E/K}}(\mathcal{P}_E) = \mathcal{P}_K^f$. Posons $\sigma = \varphi_{\mathbf{EL/E}}(\mathcal{P}_E)$. Tout entier algébrique x dans EL vérifie :

$$\sigma(x) \equiv x^{q^f} \mod \mathcal{P}.$$

Lorsque x appartient aussi à L alors :

$$\sigma(x) \equiv x^{q^f} \mod \mathcal{P}_L.$$

On utilise ici le fait que $\sigma(\mathcal{P}) = \mathcal{P}$ et $\sigma(\mathcal{P}_L) = \mathcal{P}_L$. Maintenant posons $\tau = \varphi_{\mathbf{L/K}}(\mathcal{P}_K)$. Pour tout entier algébrique de L, nous avons donc :

$$\tau(x) \equiv x^q \mod \mathcal{P}_L \ \text{ et } \ \tau^f(x) \equiv x^{q^f} \mod \mathcal{P}_L.$$

À cause de l'unicité on a $\tau^f = \sigma$ sur L. Ainsi :

$$\varphi_{\mathbf{EL/E}}(\mathcal{P}_E) = \varphi_{\mathbf{L/K}}(\mathcal{P}_K)^f = \varphi_{\mathbf{L/K}} N_{\mathbf{E/K}}(\mathcal{P}_E).$$

Cela prouve l'égalité pour les premiers de ${\mathbf{I}_\mathbf{E}}^S$. Comme toutes les applications considérées sont multiplicatives, on ne déduit le résultat sur ${\mathbf{I}_\mathbf{E}}^S$ tout entier.

Corollaire 2.2.1

$$N_{\mathbf{L/K}}(\mathbf{I_L}^S) \subseteq \ker(\varphi_{\mathbf{L/K}}).$$

Démonstration : Prendre dans la proposition précédente $E = L$ pour avoir :

$$\varphi_{\mathbf{L/K}} \cdot N_{\mathbf{L/K}} = \varphi_{\mathbf{L/L}} = \text{l'automorphisme identité.}$$

Ce résultat décrit une partie du noyau de l'application d'Artin. L'un des objectifs principaux (des autres cours) est justement de décrire le noyau et l'image de l'application d'Artin. On verra (dans les cours concernés) que l'application d'Artin est toujours surjective sur le groupe de Galois $\mathrm{Gal}(L/K)$, et on donnera aussi la description explicite de son noyau. le cas des extensions cyclotomiques est un exemple parfait d'illustration de ces idées.

Soit m un entier positif et θ un racine primitive m-ème de l'unité. Soit aussi $K = \mathbb{Q}$ le corps des nombres rationnels et $L = \mathbb{Q}(\theta)$ le m-ème corps cyclotomique. On sait que le groupe de Galois G de L sur K est formé des automorphismes σ_t définis de façon unique par la condition :

$$\sigma_t(\theta) = \theta^t,$$

où t est un entier positif premier à m. Soit p un nombre premier ne divisant pas m, alors l'idéal premier (p) est non ramifié dans L, et l'auromorphisme σ_p satisfait les propriétés définissant l'automorphisme de Frobenius de (p). Ainsi :

$$\varphi_{\mathbf{L}/\mathbb{Q}}(p) = \sigma_p.$$

Pour un entier positif $a = \Pi p_i^{c_i}$ relativement premier à m nous avons :

$$\varphi_{\mathbf{L}/\mathbb{Q}}(a) = \Pi \varphi_{\mathbf{L}/\mathbb{Q}}(p_i)^{c_i} = \Pi(\sigma_{p_i})^{c_i} = \sigma_a.$$

Pour tout entier positif b premier à m il existe un entier positif b^* tel que :

$$bb^* \equiv \ 1 \mod m.$$

On en déduit facilement que :

$$\varphi_{\mathbf{L}/\mathbb{Q}}(1/b) = \varphi_{\mathbf{L}/\mathbb{Q}}(b^*) = \sigma_{b^*},$$

et plus généralement :

$$\varphi_{\mathbf{L}/\mathbb{Q}}(a/b) = \sigma_{ab^*}.$$

Maintenant on est en mesure de décrire le noyau et l'image de $\varphi_{\mathbf{L}/\mathbb{Q}}$.

Proposition 2.2.2 *Soit S l'ensemble des idéaux premier contenant (m). L'application d'Artin $\varphi_{\mathbf{L}/\mathbb{Q}}$ envoie de façon surjective $\mathbf{I}_{\mathbb{Q}}{}^S$ sur $G(L/\mathbb{Q})$ et le noyau est l'ensemble des idéaux fractionnaires (a/b) où a et b sont des entier positifs satisfaisant $a \equiv \ b \mod m$.*

Démonstration : Il est clair que $\varphi_{\mathbf{L}/\mathbb{Q}}$ est surjective sur $G(L/\mathbb{Q})$. L'idéal(a/b) est dans le noyau si et seulement si $\sigma_{ab^*} = \sigma_1$ qui est l'application identité. Cette égalité se traduit par $a \equiv \ b \mod m$.