III
Première étude locale des extensions de corps

1. Quelques rappels de théorie de Galois

Soit K un corps. Soit L une extension de corps de K, ce que l'on signifie par $L|K$. On dit que cette extension est *finie* si L est un K-espace vectoriel de dimension finie ; cette dimension est alors le *degré* de l'extension on la note $[L : K]$.

Rappelons quelques notions de théorie de Galois. Un élément de L est dit *séparable sur* K s'il existe un polynôme *séparable*, c'est à dire sans racine multiple, de $K[X]$ dont il est une racine. L'extension $L|K$ est dite *séparable* si tout élément de L est séparable sur K.

Si K est un corps de caractéristique 0 toute extension de K est séparable ; Cela résulte du fait que si $P \in K[X]$ possède une racine multiple x d'ordre $n \geq 2$, x est racine de $P' \neq 0$ d'ordre $n-1$. Lorsque L est un corps fini, l'extension est séparable. Cela se voit directement. L'extension $\mathbf{F}_p(T)[X]/(X^p - T)$ de $\mathbf{F}_p(T)$ n'est pas séparable, car le polynôme $X^p - T$ n'admet qu'une seule racine et il est irréductible.

L'extension $L|K$ est dite *normale* si le corps L contient aucune ou toutes les racines de tout polynôme irréductible de $K[X]$. Elle est dite *galoisienne* si elle est normale et séparable. Dans ce dernier cas, le groupe des automorphismes du corps L qui sont l'identité sur le corps K est le *groupe de Galois* de l'extension $L|K$; On le note $\mathrm{Gal}(L/K)$.

Lorsque l'extension $L|K$ est galoisienne, tout élément de L qui est invariant par $\mathrm{Gal}(L/K)$ est dans K. Si de plus l'extension $L|K$ est finie de degré $[L : K]$, le groupe $\mathrm{Gal}(L/K)$ est un groupe fini d'ordre $[L : K]$. L'extension de $\mathbf{Q}$ engendrée par une racine cubique de 2 n'est pas normale et donc pas galoisienne. Rappelons le théorème principal de la théorie de Galois pour les extensions de corps qui sont finies.

Théorème 1. — *Soit $L|K$ une extension finie et galoisienne de corps de groupe de Galois G. L'application qui à un sous-groupe H de G associe l'ensemble M des éléments de L fixés par H définit une bijection entre les sous-groupes de G et les sous-corps de L contenant K. De plus cette bijection induit une bijection entre les sous-groupes distingués de G et les sous corps M de L contenant K tels que l'extension $M|K$ soit normale.*

Supposons que l'extension $L|K$ soit finie. Soit x un élément de L. L'application $L \longrightarrow L$ qui à y associe xy est K-linéaire dont la trace (resp. le déterminant) est par définition la *trace* $\mathrm{Tr}_{L/K}(x)$ (resp. la *norme* $\mathrm{N}_{L/K}(x)$) de x. La trace est une application K linéaire et on a une relation de transitivité $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$ lorsque M est une extension finie de L.

Supposons l'extension $L|K$ est séparable. Soit $M|L$ une extension telle que $M|K$ soit galoisienne (par exemple une clôture algébrique de K contenant L). Il existe une galoisienne minimale $L'|K$ contenant L et contenue dans M qui contienne tous les conjugés de x dans M. On a alors

$$\mathrm{Tr}_{L'/K}(x) = \sum_{\sigma \in \mathrm{Gal}(L'/K)} \sigma(x)$$

et

$$\mathrm{N}_{L'/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L'/K)} \sigma(x).$$

Lorsque $L = K(x)$ la trace $\mathrm{Tr}_{L/K}(x)$ (resp. la norme $\mathrm{N}_{L/K}(x)$) est la somme (resp. le produit) des conjugués de x dans M.

L'extension L/K est séparable si et seulement si la forme K-bilinéaire symétrique $L \times L \longrightarrow K$ qui à (x, y) associe $\mathrm{Tr}_{L/K}(xy)$ est non dégénérée (voir prochain cours).

2. Extensions d'anneaux de Dedekind

Supposons désormais que L est une extension de degré fini n de K. On suppose de plus que l'extension $L|K$ est séparable, ce qui nous suffira mais n'est pas indispensable.

Soit A un anneau noethérien et intégralement clos de corps des fractions égal à K. Notons B la *clôture intégrale* de A dans L (c'est-à-dire l'ensemble des éléments de L qui sont entiers sur A). C'est un sous-anneau de L et on a $B \cap K = A$ puisque A est intégralement clos.

Proposition 1. — *L'anneau B est intégralement clos.*
Démonstration. — C'est un sous-anneau d'un corps donc un anneau intègre. Soit $x \in L$ un élément entier sur B. C'est donc la racine d'un polynôme unitaire $P \in B[X]$ de degré n. Les coefficients b_0, b_1 ... b_{n-1} de ce polynôme sont entiers sur A. Considérons l'anneau $A' = A[b_0, b_1, ..., b_{n-1}]$. C'est un module de type fini sur A puisque b_0, b_1 ... b_{n-1} sont entiers sur A. Par ailleurs $A'[x]$ est de type fini sur A' puisque x est entier sur A'. Donc $A'[x]$ est de type fini sur A. Comme A est noethérien, $A'[x]$ est un A-module noethérien. Donc le sous-A-module $A[x]$ de $A'[x]$ est de type fini sur A.

Par conséquent x est entier sur A. Il est donc dans B.

Proposition 2. — *Le corps des fractions de B est égal à L.*
Démonstration. — Soit $x \in L$. C'est une racine d'un polynôme $a_n X^n + ... + a_1 X + a_0 \in A[X]$. En multipliant ce polynôme par a_n^{n-1}, il apparaît que $a_n x$ est entier sur A. Donc x est quotient de deux éléments de B.

Proposition 3. — *Tout sous-A-module d'un A-module de type fini est de type fini.*
Démonstration. — Soit M un A-module de type fini. On peut supposer que M est de la forme A^k. En effet c'est un quotient de A^k par hypothèse ; l'assertion à démontrer passe facilement aux quotients. Notons π_i la surjection $A^k \longrightarrow A$ donnée par la i-ième

coordonnée et A_i l'image de l'injection $A \longrightarrow A^k$ sur la i-ème coordonnée. Tout sous-A-module N de A^k est déterminé par tous les $N \cap A_i$ et $\pi_i(N)$. Soit $M_1 \subset M_2 \subset .... \subset M$ une suite croissante de sous-A-modules de M. Pour tout $i \in \{1, 2, ..., k\}$, les suite d'idéaux $(M_t \cap A_i)_{t\geq 1}$ et $(\pi_i(M_t))_{t\geq 1}$ sont stationnaires puisque A est noethérien. On en déduit que la suite $(M_t)_{t\geq 1}$ constante à partir d'un certain rang. Cela revient à dire que M est de type fini (sinon une famille génératrice minimale infinie de M permettrait de construire une suite de sous-modules non stationnaire).

Remarque . — Dans la démonstration de la proposition 3, on a seulement utilisé que A est noethérien. Un A-module dont tous les sous-modules sont de type fini est dit *noethérien* (un anneau noethérien est un module noethérien sur lui-même).

Proposition 4. — *L'anneau B est un A-module de type fini lorsque l'extension $L|K$ est séparable. Il en résulte que B est un anneau noethérien.*
Démonstration. — On va démontrer que B est contenu dans un A-module de type fini ; Cela suffit d'après la proposition 3.

Soit M un sous A-module de L. Notons M^* le sous-ensemble de L formé des éléments x qui vérifient $\mathrm{Tr}_{L/K}(xy) \in A$ pour tout $y \in M$. C'est un A-module qu'on appelle la *codifférente* de M sur A. La codifférente d'un module libre est libre. En effet l'existence de la forme bilinéaire non dégénérée $(x, y) \longrightarrow \mathrm{Tr}_{L/K}(xy)$ (due à la séparabilité), permet de considérer la base duale.

Soit X une famille d'éléments de B qui est une base de L comme K-espace vectoriel. Notons V le A-module libre engendré par cette base.

Observons que l'image de B par l'application $\mathrm{Tr}_{L/K}$ est contenue dans A puisque les conjugés d'un élément entier sur A sont entiers sur A. On a donc

$$V \subset B \subset B^* \subset V^*.$$

On conclut puisque V^* est un A-module de type fini, et donc noethérien. Ainsi B est un A-module noethérien.

C'est aussi un anneau noethérien puisque toute suite croissante d'idéaux de B est une suite croissante de A-modules.

Théorème 1. — *Si A est un anneau de Dedekind, B est un anneau de Dedekind.*
Démonstration. — Compte-tenu des propositions 1, 3 et 4, il suffit de prouver que le localisé de B en tout idéal premier et non nul est un anneau de valuation discrète. Pour cela il suffit de prouver que tout idéal premier et non nul de ce localisé est maximal (caractérisation des anneaux de valuation discrète) ou encore de prouver que tout idéal premier non nul de B est maximal.

Soit $\mathcal{P}$ un idéal premier de B non maximal. Il est contenu dans un idéal maximal $\mathcal{M}$ de B. Les ensembles $\mathcal{P} \cap A$ et $\mathcal{M} \cap A$ sont des idéaux premiers non nuls de A. Puisque tout idéal premier non nul de A est maximal, ces ensembles sont égaux. Cela contredit le lemme suivant.

Lemme 2. — *Soient A et B deux anneaux tels que $A \subset B$ et B entier sur A. Soient $\mathcal{P}$ et $\mathcal{Q}$ deux idéaux premiers de B tels que $\mathcal{P} \subset \mathcal{Q}$. Supposons qu'on ait $\mathcal{P} \cap A = \mathcal{Q} \cap A$. Alors on a $\mathcal{P} = \mathcal{Q}$.*

Démonstration. — Supposons que l'inclusion $\mathcal{P} \subset \mathcal{Q}$ soit stricte. Il existe $x \in \mathcal{Q} - \mathcal{P}$. Soit $P(X) = X^n + ... + a_1 X + a_0$ un polynôme unitaire à coefficient dans A de degré minimal qui vérifie $P(x) \in \mathcal{P}$. Un tel polynôme existe puisque x est entier. Il est de degré > 1. Comme $\mathcal{P}$ est premier on a $a_0 \in \mathcal{Q} \cap A = \mathcal{P} \cap A$. Cela entraîne qu'on a $(P(x) - a_0)/x \in \mathcal{P}$ puisque $\mathcal{P}$ est premier. C'est absurde puisque P est de degré minimal. On a donc une contradiction. Cela prouve le lemme et donc le théorème.

Rappelons que l'*anneau des entiers* d'un corps de nombres L est la clôture intégrale de $\mathbf{Z}$ dans L.

Corollaire 1. — *L'anneau des entiers d'un corps de nombres est un anneau de Dedekind.*
Démonstration. — Cela résulte de l'application de la proposition à $A = \mathbf{Z}$.

3. Étude locale

Supposons désormais que A est un anneau de Dedekind. Soit $\mathcal{P}$ un idéal premier non nul de B. Posons $\mathcal{Q} = \mathcal{P} \cap A$. Dans cette situation on dit que $\mathcal{P}$ *divise* $\mathcal{Q}$ ou que $\mathcal{P}$ est *au dessus* de $\mathcal{Q}$. On note alors $\mathcal{P}|\mathcal{Q}$. Posons

$$e_{\mathcal{P}} = v_{\mathcal{P}}(\mathcal{Q}B).$$

C'est l'*indice de ramification* de $\mathcal{P}$ dans l'extension $L|K$. On a

$$\mathcal{Q}B = \prod_{\mathcal{P}|\mathcal{Q}} \mathcal{P}^{e_{\mathcal{P}}}.$$

Puisqu'on a $\mathcal{Q} \subset \mathcal{P}$, le corps $B/\mathcal{P}$ est une extension de $A/\mathcal{Q}$. Le degré $f_{\mathcal{P}}$ de cette extension est le *degré résiduel* de $\mathcal{P}$ dans l'extension $L|K$. Si $\mathcal{P}$ est le seul idéal premier qui divise $\mathcal{Q}$, et si le degré résiduel est égal à 1, on dit que l'extension $L|K$ est *totalement ramifiée* en $\mathcal{P}$.

Lorsque l'extension $(B/\mathcal{P})|(A/\mathcal{Q})$ est séparable, et que l'indice de ramification est égal à 1 on dit que l'extension $L|K$ est *non ramifiée* en $\mathcal{P}$.

Proposition 5. — *Soit $\mathcal{Q}$ un idéal maximal de A. On a*

$$n = [B/\mathcal{Q}B : A/\mathcal{Q}] = \sum_{\mathcal{P}|\mathcal{Q}} e_{\mathcal{P}} f_{\mathcal{P}}.$$

Démonstration. — Pour démontrer la seconde égalité, considérons la suite d'idéaux de B :

$$B\mathcal{Q} = \prod_{\mathcal{P}|\mathcal{Q}} \mathcal{P}^{e_{\mathcal{P}}} \subset ... \subset \mathcal{P}_1^{e_{\mathcal{P}_1}} \mathcal{P}_2^{e_{\mathcal{P}_2}} \subset ... \subset \mathcal{P}_1^{e_{\mathcal{P}_1}} \mathcal{P}_2 \subset \mathcal{P}_1^{e_{\mathcal{P}_1}} \subset ... \subset \mathcal{P}_1^2 \subset \mathcal{P}_1 \subset B.$$

Il n'y a pas d'idéal strictement compris entre deux termes successifs, puisque deux tels termes diffèrent par multiplication par un idéal maximal. Les quotients successifs sont des

espaces vectoriels de dimension 1 sur $B/\mathcal{P}_i$. En effet pour I idéal de B et $\mathcal{P}$ idéal premier non nul de B, $I/I\mathcal{P}$ est une droite sur $B/\mathcal{P}$. C'est évident si I est principal. Sinon, on peut observer que $I/I\mathcal{P}$ est isomorphe à $IB_{(\mathcal{P})}/I\mathcal{P}B_{(\mathcal{P})}$ et on se ramène au cas principal. Ainsi, $B/\mathcal{P}_i$ est de dimension $f_{\mathcal{P}_i}$ sur $A/\mathcal{P}$. Un simple comptage donne la deuxième égalité.

Démontrons maintenant la première égalité. Lorsque A est principal, elle résulte du fait qu'une base du A-module B donne une base de $B/\mathcal{P}$ comme $A/\mathcal{Q}$-module, puisque qu'un A-module de type fini et sans torsion est libre sur un anneau principal.

Nous allons nous ramener au cas principal. Considérons l'anneau de valuation discrète (donc principal) $A_{(\mathcal{Q})} = A_0$. Sa clôture intégrale dans L est égale à $A_{(\mathcal{Q})}B = B_0$. On a donc

$$n = [B_0/\mathcal{Q}B_0 : A_0/\mathcal{Q}A_0].$$

La décomposition de l'idéal $\mathcal{Q}B_0$ donne

$$\mathcal{Q}B_0 = \prod_i (B_0\mathcal{P}_i)^{e_{\mathcal{P}_i}},$$

où les $\mathcal{P}_i$ sont des idéaux premiers non nuls de B. Les $B_0\mathcal{P}_i$ sont des idéaux premiers non nuls de B_0. D'après l'égalité déjà démontrée on a

$$[B_0/\mathcal{Q}B_0 : A_0/\mathcal{Q}A_0] = \sum_i e_{\mathcal{P}_i}[B_0/B_0\mathcal{P}_i : A_0/\mathcal{Q}].$$

Puisqu'on a $A_0/\mathcal{Q}A_0 \simeq A/\mathcal{Q}A$ et $B_0/\mathcal{P}_iB_0 \simeq B/\mathcal{P}_i$, on obtient

$$n = \sum_i e_{\mathcal{P}_i} f_{\mathcal{P}_i}$$

Cela achève la démonstration.

On peut compléter la proposition précédente ainsi.

Proposition 6. — *L'anneau $B/\mathcal{Q}$ est isomorphe à $\prod_{\mathcal{P}} B/\mathcal{P}^{e_{\mathcal{P}}}$.*
Démonstration. — On a un homomorphisme d'anneau $B/\mathcal{Q}B \longrightarrow \prod_{\mathcal{P}} B/\mathcal{P}^{e_{\mathcal{P}}}$ déduit de l'application diagonale

$$B \longrightarrow \prod_{\mathcal{P}} B.$$

Démontrons qu'il s'agit de l'isomorphisme cherché. L'injectivité résulte de l'égalité $\mathcal{Q} = \cap_{\mathcal{P}} \mathcal{P}^{e_{\mathcal{P}}}$. La surjectivité se voit directement en utilisant le lemme des restes chinois.

4. Les sous-groupes de décomposition et d'inertie

Reprenons la situation de la section précédente en supposant que l'extension L/K est galoisienne.

Proposition 6. — *Soit $\mathcal{Q}$ un idéal maximal de A. Le groupe* $\mathrm{Gal}(L/K)$ *opère transitivement sur les idéaux premiers de B qui divise $\mathcal{Q}$.*
Démonstration. — Soit $\mathcal{P}$ un idéal de B qui divise $\mathcal{Q}$. L'image par un élément de $\mathrm{Gal}(L/K)$ de $\mathcal{P}$ est un sous B-module de L. Il est contenu dans B puisque le conjugué d'un élément entier est entier. C'est donc un idéal et il est premier.

Vérifions la transitivité de l'action de $\mathrm{Gal}(L/K)$. Pour $x \in L$, on a

$$\mathrm{N}_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x).$$

Comme l'application $B \to \prod_{\mathcal{P}'|\mathcal{Q}} B/\mathcal{P}'$ est sujective, il existe $x \in \mathcal{P}$ tel que $x \notin \mathcal{P}'$ pour tout $\mathcal{P}' \neq \mathcal{P}$, $\mathcal{P}'$ au dessus de $\mathcal{Q}$. Lorsque $x \in \mathcal{P}$, on a $\mathrm{N}_{L/K}(x) \in \mathcal{P} \cap A$ et donc $\mathrm{N}_{L/K}(x) \in \mathcal{Q}$. Pour tout idéal premier non nul $\mathcal{P}'$ de B au dessus de $\mathcal{Q}$, il existe $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(x) \in \mathcal{P}'$ et donc $x \in \sigma^{-1}(\mathcal{P}')$ Soit $\mathcal{P}_0$ un idéal premier de B au dessus de $\mathcal{Q}$. Il existe $\sigma \in \mathrm{Gal}(L/K)$ tel que $x \in \sigma^{-1}(\mathcal{P}_0)$. On a donc $\mathcal{P} = \sigma^{-1}(\mathcal{P}_0)$ si bien que l'action est transitive.

Corollaire 1. — *Soit $\mathcal{Q}$ un idéal premier non nul de A. Les nombres entiers $e_{\mathcal{P}}$ et $f_{\mathcal{P}}$ ne dépendent que $\mathcal{Q}$. On peut donc les noter $e_{\mathcal{Q}}$ et $f_{\mathcal{Q}}$. Notons $g_{\mathcal{Q}}$ le nombre d'idéaux premiers de A qui divisent $\mathcal{Q}$. On a*

$$[L : K] = g_{\mathcal{Q}} e_{\mathcal{Q}} f_{\mathcal{Q}}.$$

Démonstration. — Utilisation de l'action de $\mathrm{Gal}(L/K)$ qui transporte toutes les structures.

Le *sous-groupe de décomposition* $D_{\mathcal{P}}$ en $\mathcal{P}$ de $\mathrm{Gal}(L/K)$ est le sous-groupe des éléments σ qui vérifient $\sigma(\mathcal{P}) = \mathcal{P}$. C'est un sous-groupe d'indice $g_{\mathcal{Q}}$. Il ne dépend à conjugaison près que de $\mathcal{Q}$.

Le *sous-groupe d'inertie* $I_{\mathcal{P}}$ en $\mathcal{P}$ de $\mathrm{Gal}(L/K)$ est le sous-groupe des éléments σ qui vérifient $(\sigma(x) - x) \in \mathcal{P}$ pour tout $x \in B$. C'est un sous-groupe de $D_{\mathcal{P}}$.

5. Rappels sur les corps finis

Soit p un nombre premier. Rappelons que tout corps fini de caractéristique p possède un nombre d'élément égal à une puissance de p, puisque c'est un espace vectoriel sur le corps à p éléments.

Soit n un entier ≥ 1. Il existe un et un seul, à isomorphisme près, corps fini ayant $q = p^n$ éléments. Voici comment on le construit. Soit K un corps algébriquement clos de caractéristique p. L'application $K \longrightarrow K$ qui à x associe x^q est un automorphisme de K (elle préserve évidemment la multiplication ; le fait qu'elle préserve l'addition résulte de la formule du binôme). Les éléments invariants par cette application forment un sous-corps de K. CΛomme le polynôme $X^q - X$ possèdent q racines distinctes dans K (sa dérivée ne s'annule pas), ce sous-corps possède q éléments. Inversement si k est un sous-corps de

K ayant q éléments, k^* est un groupe d'ordre $q-1$. Tout élément x de k^* vérifie donc $x^{q-1}=1$. Tout élément de k est racine de $X^q - X$.

Le corps à q éléments est unique à isomorphisme non-unique près. On le note $\mathbf{F}_q$.

Soit m un nombre entier. Le corps $\mathbf{F}_{p^m}$ est isomorphe à un sous-corps de $\mathbf{F}_{p^n}$ si et seulement si $m|n$. En effet $\mathbf{F}_{p^m}$ est isomorphe au sous-corps de $\mathbf{F}_{p^n}$ formé par les racines du polynôme $X^{p^m} - X$.

Cela prouve que l'extension de corps $\mathbf{F}_{p^n}/\mathbf{F}_{p^m}$ est normale. Cette extension est séparable car les racines de l'unité sont séparables. Le groupe $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_{p^m})$ est cyclique et engendré par l'automorphisme de $\mathbf{F}_{p^n}$ qui à x associe x^{p^m}.

6. La substitution de Frobenius

Reprenons la situation de la section 3 en supposant désormais que K est un *corps de nombres*, c'est-à-dire une extension finie de $\mathbf{Q}$.

Dans ce cas, tout corps résiduel de A est un corps fini. Le corps fini $B/\mathcal{P}$ est une extension de $A/\mathcal{Q}$.

Proposition 7. — *L'application*

$$D_{\mathcal{P}} \longrightarrow \mathrm{Gal}((B/\mathcal{P})/(A/\mathcal{Q}))$$

est un homomorphisme surjectif de groupes. Son noyau est égal à $I_{\mathcal{P}}$.

Démonstration. — Seule la surjectivité n'est pas évidente. Pour l'établir, il suffit de prouver que $D_{\mathcal{P}}$ agit transitivement sur les conjugués d'un élément primitif. Soit α un élément primitif de l'extension de corps finis $(B/\mathcal{P})|(A/\mathcal{Q})$. D'après le lemme d'approximation, on peut choisir un représentant a de α dans B tel que $a \in \sigma(\mathcal{P})$ pour tout $\sigma \notin D_{\mathcal{P}}$. Considérons le polynôme $\prod_\sigma (X - \sigma(a)) \in A[X]$, où σ parcourt $\mathrm{Gal}(L/K)$. Sa réduction modulo $\mathcal{Q}$ est le produit d'une puissance de X par un polynôme de $(A/\mathcal{Q})[X]$ qui annule α. Un tel polynôme annule tous les conjugués de α. Tout conjugué de α est donc de la forme $\sigma(a) + \mathcal{P}$ avec $\sigma \in D_{\mathcal{P}}$.

Proposition 8. — *Le cardinal du groupe d'inertie $I_{\mathcal{P}}$ est égal à $e_{\mathcal{P}}$.*

Démonstration. — Cela revient à prouver que le cardinal du groupe de décomposition est égal à $e_{\mathcal{P}} f_{\mathcal{P}}$, puisqu'on vient de voir que le quotient $D_{\mathcal{P}}/I_{\mathcal{P}}$ s'identifie au groupe de Galois de l'extension résiduelle qui a pour ordre $f_{\mathcal{P}}$. Le nombre de conjugué $g_{\mathcal{P}}$ de $\mathcal{P}$ par $\mathrm{Gal}(L/K)$ est égal à l'ordre du groupe $\mathrm{Gal}(L/K)/D_{\mathcal{P}}$. Comme l'ordre de $\mathrm{Gal}(L/K)$ est égal à $g_{\mathcal{P}} e_{\mathcal{P}} f_{\mathcal{P}}$ on obtient le résultat cherché.

Tout cela est résumé en disant que les indices successifs correspondant aux inclusions de groupes

$$1 \subset I_{\mathcal{P}} \subset D_{\mathcal{P}} \subset \mathrm{Gal}(L/K)$$

sont égaux à $e_{\mathcal{P}}$, $f_{\mathcal{P}}$ et $g_{\mathcal{P}}$ respectivement.

Corollaire 1. — *L'extension $L|K$ est non ramifiée en $\mathcal{P}$ si et seulement si le sous-groupe d'inertie en $\mathcal{P}$ est trivial.*

Supposons que l'extension $L|K$ soit non ramifiée en $\mathcal{P}$. La *substitution de Frobenius* $\phi_{\mathcal{P}}$ de $D_{\mathcal{P}}$ est l'élément d'ordre $f_{\mathcal{P}}$ de $D_{\mathcal{P}}$ correspondant à l'automorphisme $x \mapsto x^q$ du corps fini $B/\mathcal{P}$, où q est l'ordre de $A/\mathcal{Q}$. Il est caractérisé par la propriété :

$$\phi_{\mathcal{P}}(x) = x^q \pmod{\mathcal{P}},$$

pour tout $x \in B$. On le note encore $(\mathcal{P}, L/K)$. Soit $\sigma \in \mathrm{Gal}(L/K)$. On a

$$(\sigma(\mathcal{P}), L/K) = \sigma(\mathcal{P}, L/K)\sigma^{-1}.$$

On dira qu'une extension de corps L/K est *abélienne* si elle est galoisienne et que le groupe $\mathrm{Gal}(L/K)$ est abélien. Toute extension de corps finis est abélienne.

Reprenons la situation étudiée au cours de cette section. Lorsque $\mathrm{Gal}(L/K)$ est un groupe abélien, la substitution de Frobenius en $\mathcal{P}$ ne dépend que de $\mathcal{Q}$. C'est le *symbole d'Artin* noté $(\mathcal{Q}, L/K)$. Cette définition se généralise à tout idéal fractionnaire I de K qui est à support en dehors des idéaux premiers ramifiés de l'extension L/K par multiplicativité, *i.e.* on pose

$$(\prod_{\mathcal{P}} \mathcal{P}^{n_{\mathcal{P}}}, L/K) = \prod_{\mathcal{P}} (\mathcal{P}, L/K)^{n_{\mathcal{P}}}.$$