XV
Les groupes de ramification

1. Le lemme de Hensel

Soit p un nombre premier. Soit K un corps p-adique, donc muni d'une valuation discrète notée v_K ou simplement v lorsqu'il n'y a pas d'ambiguïté (la théorie décrite ci-dessous s'applique en fait à des corps locaux plus généraux). Notons $\mathcal{O}_K$ l'anneau des entiers de K^*. Notons $\mathcal{Q}$ l'idéal premier non nul de $\mathcal{O}_K$. Soit π une uniformisante de $\mathcal{Q}$.

Voyons une des incarnations du *lemme de Hensel*. On trouve dans la littérature des formulations littéralement différentes mais qui expriment la même idée.

PROPOSITION 1. — *Soit $P \in \mathcal{O}_K[X]$ un polynôme de degré d. Notons $\tilde{P}$ l'image de P dans $k[X]$. Supposons que le degré de $\tilde{P}$ soit égal à d et que $\tilde{P}$ soit égal au produit de deux polynômes $\tilde{R}$ et $\tilde{Q}$ premiers entre eux. Il existe Q, $R \in \mathcal{O}_K[X]$ d'images $\tilde{Q}$ et $\tilde{R}$ dans $k[X]$ de mêmes degrés que $\tilde{Q}$ et $\tilde{R}$ respectivement et vérifiant $P = QR$.*

De plus Q (resp. R) peut être choisi unitaire lorsque $\tilde{Q}$ (resp. $\tilde{R}$) est unitaire.

Démonstration. — On construit les polynômes Q et R par approximations successives.

Soient Q_0 et R_0 deux polynômes de $\mathcal{O}_K[X]$ d'images dans $k[X]$ égales à $\tilde{Q}$ et $\tilde{R}$ et tels que $P - Q_0R_0$ soit de degré strictement inférieur à d (cela entraîne que Q_0 et R_0 sont de même degrés que $\tilde{Q}$ et $\tilde{R}$ respectivement). On a

$$P = Q_0R_0 + \pi S_1,$$

avec $S_1 \in \mathcal{O}_K[X]$ de degré $< d$. Notons $\tilde{S}_1$ l'image de S_1 dans $k[X]$. Puisque les polynômes $\tilde{P}$ et $\tilde{Q}$ sont premiers entre eux, il existe deux polynômes $\tilde{U}$, $\tilde{V} \in k[X]$ de degrés inférieurs strictement aux degrés de $\tilde{Q}$ et $\tilde{R}$ et vérifiant

$$\tilde{S}_1 = \tilde{U}\tilde{Q} + \tilde{V}\tilde{R}.$$

On a donc

$$S_1 = UQ_0 + VR_0 + \pi T,$$

avec U, V, T trois polynômes de $\mathcal{O}_K[X]$ de degrés strictement inférieurs aux degrés de R_0, Q_0 et P respectivement. Cela donne

$$P = Q_0R_0 + \pi(UQ_0 + RV_0 + \pi T) = (Q_0 + \pi V)(R_0 + \pi U) + \pi^2(T - UV).$$

Posons $Q_1 = Q_0 + \pi V$, $R_1 = R_0 + \pi U$ et $S_2 = T - UV$. Ce sont des polynômes dee mêmes degrés que Q_0 et R_0, donc de mêmes degrés que $\tilde{Q}$ et $\tilde{R}$. En itérant l'opération on obtient des suites $(Q_n)_{n\geq 0}$, $(R_n)_{n\geq 0}$ et $(S_n)_{n\geq 1}$ de polynômes de $\mathcal{O}_K[X]$ telles que

$P = Q_n R_n + \pi^{n+1} S_{n+1}$ et telles que les coefficients de $Q_{n+1} - Q_n$ (resp. $R_{n+1} - R_n$) soient dans $\mathcal{P}^{n+1}$. Les suites $(Q_n)_{n\geq 0}$ et $(R_n)_{n\geq 0}$ convergent donc vers des polynômes Q et R et on a $P = QR$.

Lorsque Q (resp. R) est un polynôme unitaire, la suite $(Q_n)_{n\geq 0}$ (resp. $(R_n)_{n\geq 0}$) peut être choisie à valeurs dans les polynômes unitaires. L'assertion subsidiaire découle de cette constatation.

COROLLAIRE . — *Soit M une extension finie de K. Il existe une extension intermédiaire $K \subset L \subset M$ telle que L soit non ramifiée sur K et telle que M soit totalement ramifiée sur L.*

Démonstration. — Notons $\tilde{M}$ et $\tilde{K}$ les corps résiduels de de M et K. Ils sont finis donc parfaits.

Soit $\tilde{x}_1 \in \tilde{M} - \tilde{K}$ de polynôme minimal $\tilde{P} \in \tilde{K}[X]$. On a $\tilde{P}(X) = (X - \tilde{x}_1)\tilde{Q}(X) \in \tilde{M}[X]$. Puisque $\tilde{M}$ est parfait, l'extension $\tilde{M}|\tilde{K}$ est séparable, donc $\tilde{x}_1$ est séparable, donc $\tilde{x}_1$ est racine simple de son polynôme minimal. Les polynômes $(X - \tilde{x}_1)$ et $\tilde{Q}$ sont donc premiers entre eux.

Soit $P \in \mathcal{O}_K[X]$ un polynôme unitaire d'image $\tilde{P}$ dans $\tilde{K}[X]$ et de même degré que $\tilde{P}$. C'est un polynôme irréductible dans $\mathcal{O}_K[X]$ puisque $\tilde{P}$ est irréductible. Utilisons le lemme de Hensel pour voir que P est le produit d'un polynôme unitaire de $\mathcal{O}_M[X]$ de degré 1 et d'un polynôme $Q \in \mathcal{O}_M[X]$. On obtient donc $P = (X - x_1)Q(X)$ avec $x_1 \in \mathcal{O}_M$ d'image $\tilde{x}_1$ dans $\tilde{M}$. L'extension $K[x_1]|K$ est non ramifiée puisque son degré est égal à son degré résiduel.

Itérons cette opération en considérant tous les éléments $\tilde{x}_1$, $\tilde{x}_2$,..., $\tilde{x}_n$ de $\tilde{M} - \tilde{K}$ et leurs représentants x_1, x_2 ..., x_n dans $\mathcal{O}_M$. L'extension $K[x_1, ..., x_n]|K$ est non ramifiée puisque la composée d'extensions non ramifiées est non ramifiée. Puisqu'on a $\tilde{M} = \tilde{K}[\tilde{x}_1, ...\tilde{x}_n]$, l'extension $\tilde{K}[\tilde{x}_1, ...\tilde{x}_n]|\tilde{K}$ est de degré égal au degré résiduel de l'extension $M|K$. Par conséquent l'extension $M|K[x_1, ..., x_n]$ est de degré égal à l'indice de ramification de l'extension $M|K$. Elle est donc totalement ramifiée. Le corps $L = K[x_1, ..., x_n]$ remplit donc les conditions recherchées.

On peut donc parler de la plus grande sous-extension non ramifiée d'une extension de corps p-adiques.

Ajoutons que la composée de deux extensions de K non ramifiées est non ramifiée. Cela se vérifie facilement en observant qu'une extension est non ramifiée si et seulement si le degré de l'extension est égal au degré résiduel.

Par ailleurs on vérifie facilement que si $M|K$ est une extension quelconque et si l'extension $L|K$ est non ramifiée alors l'extension $ML|MK$ est non ramifiée. On a utilisé implicitement cette propriété dans la démonstration du corollaire.

Le lemme de Hensel permet d'établir l'existence d'extensions ramifiées de degré quelconque de K. En effet il existe une unique extension de degré du corps résiduel de K. Cette extension est engendrée par les racines de l'unité et donc par la réduction d'un polynôme cyclotomique Φ. L'extension de K engendrée par Φ est alors de degré égal à son degré résiduel et donc non ramifiée.

Étudions maintenant les extensions totalement ramifiées.

2. Les polynômes d'Eisenstein

Reprenons les notations de la section précédente. Un polynôme

$$P(X) = X^n + a_{n-1}X^{n-1} + ... + a_0 \in K[X]$$

est dit *polynôme d'Eisenstein* si on a $a_i \in \mathcal{Q}$ pour $i = 0, 2, ..., n-1$, et $a_0 \notin \mathcal{Q}^2$.

PROPOSITION 2. — *Tout polynôme d'Eisenstein est irréductible. Toute racine d'un polynôme d'Eisenstein engendre une extension totalement ramifiée pour laquelle elle est une uniformisante de l'idéal maximal de l'anneau des entiers.*

Réciproquement, soient $L|K$ une extension totalement ramifiée et π une uniformisante de l'idéal maximal de l'anneau $\mathcal{O}_L$ des entiers de L. On a

$$L = K[\pi] \quad \text{et} \quad \mathcal{O}_L = \mathcal{O}_K[\pi].$$

De plus le polynôme minimal de π est un polynôme d'Eisenstein.

Démonstration. — Abordons d'abord la première partie. Il suffit de prouver que toute racine d'un polynôme d'Eisenstein est une uniformisante dans le corps qu'elle engendre.

Soient $P = a_n X^n + a_{n-1}X^{n-1} + ... + a_0 \in \mathcal{O}_K[X]$ un polynôme d'Eisenstein et π une racine de P. Posons $L = K[\pi]$. Posons $d = [L : K]$ et notons e l'indice de ramification de l'extension $L|K$. Notons v_L la valuation de L.

Le nombre π est entier. On a donc

$$v_L(\pi^n) = v_L(a_{n-1}\pi^{n-1} + ... + a_0) \geq \min(v_L(a_{n-1}\pi^{n-1}), ..., v_L(a_0)).$$

On a donc $v_L(\pi) \geq 1$.

Supposons qu'on ait $n > e/v_L(\pi)$. On a alors $v_L(\pi^n) > e$. Rappelons que la restriction de v_L à K coïncide avec ev_K. On a donc $v_L(a_i) = ev_K(a_i) \geq e$ et donc $v_L(a_i\pi^i) > e$ pour $i > 1$. Cela entraîne

$$v_L(\pi^n + a_{n-1}\pi^{n-1} + ... + a_1\pi) > e$$

et donc

$$v_L(a_0) = v_L(\pi^n + a_{n-1}\pi^{n-1} + ... + a_1\pi) > e.$$

Or on a $v_L(a_0) = ev_K(a_0) = e$. L'hypothèse $n > e/v_L(\pi)$ est donc absurde.

Comme on a les inégalités

$$n \geq d \geq e \geq e/v_L(\pi),$$

on obtient la relation $v_L(\pi) = 1$.

Etudions maintenant la réciproque. Soit R un système de représentants de $\mathcal{O}_K/\mathcal{Q}$. Puisque l'extension $L|K$ est totalement ramifiée, c'est aussi un système de représentants de $\mathcal{O}_L/\mathcal{P}$ (le degré résiduel est égal à 1). Supposons que $0 \in R$. Soit λ une uniformisante de $\mathcal{Q}$. Posons $\pi_{ne+s} = \lambda^s \pi^n$ (avec n et s entiers). Lorsque n parcourt $\mathbf{Z}$ et s parcourt $\{0, 1, ..., e-1\}$, les valuations des π_{ne+s} sont deux à deux distinctes et parcourent $\mathbf{Z}$.

Soit $y \in L^*$. Il s'écrit de façon unique sous la forme (c'est une variante du développement p-adique)

$$y = \sum_{k=k_0}^{\infty} r_k \pi_k$$

avec $k_0 \in \mathbf{Z}$, $r_k \in R$ et $r_{k_0} \neq 0$. On a donc

$$y = \sum_{i=0}^{e-1} \pi^i \sum_{m=k_0}^{\infty} r_{i+me} \lambda^m.$$

On a $\sum_{m=k_0}^{\infty} r_{i+me}\lambda^m \in K$, si bien que $y \in K[\pi]$. Si on suppose de plus $y \in \mathcal{O}_L$, *i.e.* $k_0 \geq 0$, on a $\sum_{m=k_0}^{\infty} r_{i+me}\lambda^m \in \mathcal{O}_K$, d'où l'égalité $\mathcal{O}_L = \mathcal{O}_K[\pi]$.

Soit $P(X) = X^d + a_{d-1}X^{d-1} + ... + a_0 \in K[X]$ le polynôme minimal de π sur K. On a $e = d$ car l'extension $L|K$ est totalement ramifiée. On a donc $a_0 = \pm \mathrm{N}_{L/K}\,\pi$ et donc

$$v_K(a_0) = \frac{e}{d} v_L(\pi) = 1.$$

Par ailleurs P est le polynôme caractéristique de la multiplication par π dans le K-espace vectoriel L. La réduction modulo $\mathcal{Q}$ de P est donc le polynôme caractéristique de la multiplication par π dans le $\mathcal{O}_K/\mathcal{Q}$-espace vectoriel $\mathcal{O}_L/\mathcal{Q}$. Cette dernière multiplication est nilpotente puisqu'on a $\pi^d \in \mathcal{Q}\mathcal{O}_L$. on a $P \equiv X^d \pmod{\mathcal{Q}}$. Cela prouve que P est un polynôme d'Eisenstein.

Remarque . — La proposition 2 assure de l'existence d'extensions totalement ramifiées de degré arbitraire. En effet, soit λ une uniformisante de $\mathcal{O}_K$. Le polynôme $X^e - \lambda$ (ou mieux $X^e - \lambda X - \lambda$) est un polynôme d'Eisenstein de degré e ; ses racines engendrent donc une extension totalement ramifiée de degré e de K.

3. Définition des groupes de ramification

Soit $L|K$ une extension galoisienne et finie. Notons $\mathcal{O}_L$ la clôture intégrale de $\mathcal{O}_K$ dans L. Soit $\mathcal{P}$ l'idéal premier non nul de $\mathcal{O}_L$ et w la valuation discrète de L associée. Soit i un entier ≥ -1. Posons

$$G_i = \{\sigma \in \mathrm{Gal}(L/K) / \sigma(x) \in x + \mathcal{P}^{i+1}, x \in \mathcal{O}_L\}.$$

C'est le *i-ième groupe de ramification* (en numérotation inférieure) de l'extension $L|K$. Les groupes G_{-1} et G_0 ne sont autres que les groupes de décomposition et d'inertie en $\mathcal{P}$ de l'extension $L|K$.

Soit $\sigma \in \mathrm{Gal}(L/K)$. Posons

$$i_{L/K}(\sigma) = \mathrm{Min}_{x \in \mathcal{O}_L} w(\sigma(x) - x)).$$

On a

$$G_i = \{\sigma \in G_{-1}/i_{L/K}(\sigma) \geq i+1\}.$$

Comme on a pour tout $\tau \in G_{-1}$,

$$i_{L/K}(\tau\sigma\tau^{-1}) = i_{L/K}(\sigma),$$

le groupe G_i est un sous-groupe distingué de G_{-1}.

PROPOSITION 3. — *Soit π_L une uniformisante de $\mathcal{P}$. Notons ϕ l'application $G_{-1} = \mathrm{Gal}(L/K) \longrightarrow \mathcal{O}_L$ qui à σ associe $\sigma(\pi_L)/\pi_L$. Soit i un entier ≥ 0.*

On a $\phi(G_i) \subset U_L^{(i)}$. L'application ϕ définit un homomorphisme injectif de groupes ϕ_i :

$$G_i/G_{i+1} \longrightarrow U_L^{(i)}/U_L^{(i+1)}$$

indépendant du choix de l'uniformisante π_L.

En particulier, G_1 est le p-sous-groupe de Sylow de G_0.

Démonstration. — La première assertion résulte de la relation $\sigma(\pi_L) \in \pi_L + \mathcal{P}^{i+1}$ pour $\sigma \in G_i$.

Soit $\sigma \in G_i$. Vérifions que la classe de $\phi(\sigma)$ dans $U_L^{(i)}/U_L^{(i+1)}$ ne dépend pas de π_L. Soit π'_L une uniformisante de $\mathcal{P}$. On a $\pi'_L = u\pi_L$, avec $u \in \mathcal{O}_K^*$. On a

$$\sigma(u\pi_L)/(u\pi_L) = (\sigma(u)/u)\phi(\sigma).$$

Comme $(\sigma(u)/u) \in U_L^{(i+1)}$, on en déduit qu'on a

$$\sigma(u\pi_L)/(u\pi_L) \in \phi(\sigma)U_L^{(i+1)}.$$

Soit $\tau \in G_i$. L'élément $\tau(\pi_L)$ est une uniformisante de $\mathcal{P}$. On a donc

$$\phi_i(\sigma\tau) = (\sigma\tau(\pi_L)/\pi_L)U_L^{(i+1)} = (\sigma\tau(\pi_L)/\tau(\pi_L))(\tau(\pi_L)/\pi_L)U_L^{(i+1)} = \phi_i(\sigma)\phi_i(\tau).$$

Cela prouve que ϕ_i est un homomorphisme de groupes.

Il reste à vérifier l'injectivité. On se ramène d'abord au cas où l'extension $L|K$ est totalement ramifiée. En effet considérons la plus grande extension non ramifiée $K'|K$ contenue dans L. Elle coïncide avec le sous corps de L fixé par G_0. Le i-ème groupe de ramification de $\mathrm{Gal}(L/K)$ coïncide avec le i-ème groupe de ramification de $\mathrm{Gal}(L/K') \subset \mathrm{Gal}(L/K)$. D'après la théorie des polynômes d'Eisenstein, on a $\mathcal{O}_L = \mathcal{O}_{K'}[\pi_L]$.

Soit $x \in \mathcal{O}_L$. Il s'écrit donc comme un polynôme en π_L à coefficients dans K'. On a donc $x = \pi_L y + z$ avec $y \in \mathcal{O}_L$ et $z \in \mathcal{O}_{K'}$. Soit $\sigma \in G_i$ tel que $\phi(\sigma) \in U_L^{(i+1)}$. On a $\sigma(\pi) \in \pi + \mathcal{P}^{i+2}$, pour toute uniformisante π de $\mathcal{P}$. Il suffit de démontrer que $\sigma \in G_{i+1}$, c'est-à-dire qu'on a $\sigma(x) - x \in \mathcal{P}^{i+2}$. Comme $\sigma \in G_0$, on a $\sigma(z) = z$. On a

$$\sigma(x) - x = \sigma(y\pi_L) - y\pi_L \in y\pi_L\mathcal{P}^{i+1} \subset \mathcal{P}^{i+2}.$$

On en déduit que G_0 est le p-sous-groupe de Sylow de G_1 en remarquant que le quotient $U_L^{(i)}/U_L^{(i+1)}$ est un p-groupe (c'est-à-dire un groupe d'ordre une puissance de p) lorsque $i \geq 1$ et que $U_L^{(0)}/U_L^{(1)}$ est d'ordre premier à p puisqu'il s'identifie au sous-groupe des éléments inversibles d'un corps fini de caractéristique p. Voir la structure des quotients $U_L^{(i)}/U_L^{(i+1)}$.

On a montré au passage que, lorsque $L|K$ est totalement ramifiée, on a

$$i_{L/K}(\sigma) = w(\sigma(\pi_L) - \pi_L)).$$

Lorsque le groupe d'inertie G_0 est trivial, rappelons que l'on dit que l'extension $L|K$ est non ramifiée. Le groupe G_1 s'appelle le *sous-groupe d'inertie sauvage*. Lorsqu'il est trivial on dit que l'extension est *modérément ramifiée*. C'est le cas si et seulement si l'indice de ramification est un nombre premier à p. Le groupe G_0/G_1 est le *groupe d'inertie modérée*.

Remarque . — La propriété $\mathcal{O}_{K'}[\pi_L] = \mathcal{O}_L$ indique que G_i est l'ensemble des éléments σ de G_0 tels que $\sigma(\pi_L) \in \pi_L + \mathcal{P}^{i+1}$, pour $i \geq 0$.

Soit s un nombre réel ≥ -1. Posons

$$G_s = \{\sigma \in G_{-1}/i_{L/K}(\sigma) \geq s + 1\}.$$

Lorsque $s = i$ est un entier ≥ -1, on a bien $G_i = G_s$.

Comparons les groupes de ramification associés aux extensions composées.

Proposition 4. — *Soit $M|K$ une extension galoisienne, finie et contenant L. Notons e' l'indice de ramification de l'extension $M|L$. Soit $\tau \in \mathrm{Gal}(L/K)$. On a*

$$i_{L/K}(\tau) = \frac{1}{e'} \sum_{\sigma \in \mathrm{Gal}(M/K), \sigma_{|L} = \tau} i_{M/K}(\sigma).$$

Démonstration. — On se ramène au cas où l'extension $M|K$ est totalement ramifiée comme dans la démonstration de la proposition 3.

Supposons que τ soit distinct de l'identité. Soient x et y deux éléments de M et L tels que $\mathcal{O}_K[x] = \mathcal{O}_M$ et $\mathcal{O}_K[y] = \mathcal{O}_L$. Notons w' la valuation de M. On a donc $e' i_{L/K}(\tau) = w'(\tau(y) - y)$ et $i_{M/K}(\sigma) = w(\sigma(x) - x)$.

Posons $a = \tau(y) - y$ et $b = \prod_{\sigma \in \mathrm{Gal}(M/K), \sigma_{|L} = \tau}(\sigma(x) - x)$. Il faut donc prouver que les valuations des éléments a et b de M sont égales. C'est-à-dire que les idéaux engendrés par a et b sont égaux.

Démontrons que l'idéal engendré par a contient b. Notons $P \in \mathcal{O}_L[X]$ le polynôme minimal de x sur L. On a $P(X) = \prod_{\rho \in \mathrm{Gal}(M/L)}(X - \rho(x))$. Le polynôme $\tau(P) - P$ est à

coefficients dans l'idéal engendré par $(\tau(y)-y)=a$. On a donc $(\tau(P)-P)(x)\in a\mathcal{O}_L$. On a $P(x)=0$ et $\tau(P)(X)=\prod_{\sigma\in\mathrm{Gal}(M/K),\sigma_{|L}=\tau}(X-\sigma(x))=\pm b$. Ainsi,on a

$$b=\pm\tau(P)(x)=\pm(\tau(P)-P)(x)\in a\mathcal{O}_L.$$

Démontrons maintenant que $a\in b\mathcal{O}_L$. Il existe $Q\in\mathcal{O}_K[X]$ tel que $y=Q(x)$. Le polynôme $(Q(X)-y)\in\mathcal{O}_L[X]$ est donc un multiple de P. Or $\tau(G)=G$. Donc $\tau(P)$ divise $\tau(Q)-\tau(y)$. On a donc

$$a=\tau(y)-y=\tau(y)-y-(\tau(Q)(x)-Q(x))=\tau(y)-\tau(Q)(x)\in\tau(P)(x)\mathcal{O}_L=b\mathcal{O}_L.$$

Cela achève la démonstration de la proposition.

La proposition 4 nous indique que les groupes de ramification ne sont pas stables par extension. Cela justifie le changement de numérotation.

4. La numérotation supérieure

Reprenons la situation que nous avons laissée dans la section précédente.

Posons $g_i=|G_i|$. Considérons la fonction continue $[-1,+\infty[\longrightarrow[-1,+\infty[$ et affine sur les intervalles $]i,i+1[$ pour $i\in\mathbf{Z}$ et qui à $s>0$ de partie entière m associe

$$\rho_{L/K}(s)=\frac{1}{g_0}(g_1+g_2+...g_m+(s-m)g_{m+1}).$$

Cette fonction est nulle en 0 et est égale à -1 en -1. Sa dérivée sur le segment $]i,i+1[$ est égale à l'indice de G_{i+1} dans G_0. On peut encore l'exprimer par l'intégrale :

$$\rho_{L/K}(s)=\int_0^s\frac{dx}{|G_0/G_x|}.$$

Ajoutons qu'elle prend des valeurs rationnelles en les nombres entiers.

Lemme 1. — *On a*

$$\rho_{L/K}(s)=\frac{1}{g_0}\sum_{\sigma\in\mathrm{Gal}(L/K)}\min(i_{L/K}(\sigma),s+1)-1.$$

Démonstration. — Comparons les deux fonctions qui apparaissent dans l'égalité. Elles valent toutes deux 0 en 0. Elles sont toutes deux continues et affines par morceaux. Il suffit de vérifier que leurs dérivées coïncident en tout nombre réel non entier s. Notons m la partie entière de s. La dérivée en s du membre de gauche figurant dans le lemme est égale à

$$\frac{1}{g_0}|\{\sigma\in G/i_{L/K}(\sigma)\geq m+2\}|.$$

Ce nombre n'est autre que l'inverse de l'indice de G_{m+1} dans G_0.

L'introduction de la numérotation supérieure est justifiée par le résultat suivant, dû à Herbrand.

PROPOSITION 5. — *Soit $M|K$ une extension galoisienne finie contenant L. Notons H_i le i-ième groupe de ramification de* $\mathrm{Gal}(M/K)$. *Posons $G' = \mathrm{Gal}(M/L)$. Soit $s \in [-1, \infty[$. Posons $t = \rho_{M/L}(s)$. On a*

$$(H_s G')/G' = G_t.$$

Démonstration. — Établissons au préalable une formule.

Lemme 2. — *Soit $\tau \in \mathrm{Gal}(L/K)$. Soit $\tilde{\tau}$ tel que $\tilde{\tau}_{|L} = \tau$ et tel que $i_{M/K}(\tilde{\tau})$ soit maximal. On a*

$$i_{L/K}(\tau) - 1 = \rho_{M/L}(i_{M/K}(\tilde{\tau}) - 1).$$

Démonstration. — Posons $m = i_{M/K}(\tilde{\tau})$. Soit $\rho \in G'$. On a la formule

$$i_{M/K}(\rho\tilde{\tau}) = \min(i_{M/K}(\rho), m);$$

Cela se vérifie immédiatement en examinant les deux cas $i_{M/K}(\rho) \geq m$ et $i_{M/K}(\rho) \leq m$ et en utilisant la relation $\rho\tilde{\tau}(x) - x = \rho\tilde{\tau}(x) - \tilde{\tau}(x) + \tilde{\tau}(x) - x$ qui donne après application des valuations le résultat cherché.

Utilisons maintenant la proposition 4. On obtient

$$i_{L/K}(\tau) = \frac{1}{e'} \sum_{\rho \in G'} i_{M/K}(\rho\tilde{\tau}) = \frac{1}{e'} \sum_{\rho \in G'} \min(i_{M/K}(\rho), m).$$

Utilisons la relation $i_{M/K}(\rho) = i_{M/L}(\rho)$ et le lemme 1. On obtient

$$i_{L/K}(\tau) = (\rho_{M/L}(m-1) + 1)\frac{|G'_0|}{e'} = \rho_{M/L}(i_{M/K}(\tilde{\tau}) - 1) + 1.$$

Cela achève de prouver le lemme.

Venons-en à la démonstration de la proposition 5. Soit $\tau \in \mathrm{Gal}(L/K)$. Soit $\tilde{\tau} \in \mathrm{Gal}(M/K)$ tel que $\tilde{\tau}_{|L} = \tau$. C'est un élément de $H_s G'/G'$ si seulement si on a $i_{M/K}(\tilde{\tau}) - 1 \geq s$, ou encore si et seulement si $\rho_{M/L}(i_{M/K}(\tilde{\tau}) - 1) \geq \rho_{M/L}(s)$ (car la fonction $\rho_{M/L}$ est croissante). D'après le lemme 2 , cela revient à dire qu'on a $i_{L/K}(\tau) - 1 \geq \rho_{M/L}(s)$, ou encore qu'on a $\tau \in G_t$. Cela prouve donc la proposition 5.

La fonction $\rho_{L/K}$ est une fonction strictement croissante et non bornée. C'est donc une bijection $[-1, +\infty[\longrightarrow [-1, +\infty[$. Considérons la fonction $\phi_{L/K} : [-1, +\infty[\longrightarrow [-1, +\infty[$ qui est réciproque de $\rho_{L/K}$. Soit t un nombre réel ≥ 1. On appelle *groupe de ramification en numérotation supérieure d'indice t* le sous-groupe

$$G^t = G_{\phi_{L/K}(t)}$$

de $\mathrm{Gal}(L/K)$.

PROPOSITION 6. — *Soit M/K une extension galoisienne finie contenant L. On a*

$$\rho_{M/K} = \rho_{L/K} \circ \rho_{M/L}$$

et

$$\phi_{M/K} = \phi_{M/L} \circ \phi_{L/K}.$$

Démonstration. — Ces deux égalités sont équivalentes. Démontrons la première. Les deux membres de l'égalité sont des fonctions continues et affines par morceaux. Elles sont toutes les deux nulles en 0. Démontrons que leurs dérivées sont égales partout où elles sont définies.

Soit s un nombre réel ≥ 1 non entier. D'après la proposition 5, on a $H_s/G'_s = G_t$ (en reprenant les notations de la proposition 5). Cela entraîne qu'on a, en notant $e_{U/V}$ l'indice de ramification de l'extension de corps p-adiques $U|V$,

$$\frac{1}{e_{M/K}}|H_s| = \frac{1}{e_{L/K}}|G_t|\frac{1}{e_{M/L}}|G'_s|.$$

On a donc, en appliquant la formule de composition des dérivées en le nombre réel non entier s,

$$\rho'_{M/K}(s) = \frac{1}{e_{L/K}}|G_t|\frac{1}{e_{M/L}}|G'_s| = \rho'_{L/K}(\rho_{M/L}(s))\rho'_{M/L}(s) = (\rho_{L/K} \circ \rho_{M/L})'(s).$$

Cela prouve la proposition 6.

Examinons le comportement des groupes de ramification en numérotation supérieure par composition d'extensions.

PROPOSITION 7. — *Soit $M|K$ une extension galoisienne finie contenant L. Notons H^i le i-ième groupe de ramification de* $\mathrm{Gal}(M/K)$ *en numérotation supérieure. Posons $G' = \mathrm{Gal}(M/L)$. Soit $s \in [-1, \infty[$. On a*

$$(H^s G')/G' = G^s.$$

Démonstration. — Posons $t = \rho_{L/K}(s)$. On a

$$(H^s G')/G' = (H_{\phi_{M/K}(t)} G')/G'.$$

D'après la proposition 5, ce dernier groupe est égal à $G_{\rho_{M/L} \circ \phi_{M/K}(t)}$. D'après la proposition 6, il est égal à

$$G_{\rho_{M/L} \circ \phi_{M/L} \circ \phi_{L/K}(t)} = G_{\phi_{L/K}(t)} = G^s.$$

Cela achève la démonstration.

5. Lien avec le discriminant

Soit $L|K$ une extension galoisienne de corps p-adiques. Considérons le discriminant $\mathcal{D}_{L/K}$ de l'extension $L|K$. On note G_i le i-ème groupe de ramification de $\mathrm{Gal}(L/K)$.

PROPOSITION 8. — *On a les formules*

$$v_K(\mathcal{D}_{L/K}) = \sum_{\sigma\in\mathrm{Gal}(L/K),\sigma\neq 1} i_K(\sigma) = \sum_{i=0}^{\infty}(|G_i|-1).$$

Démonstration. — On se ramène encore au cas où l'extension $L|K$ est totalement ramifiée puisque les deux membres de l'égalité que nous voulons démontrer ne changent pas si on remplace K par un sous-corps non ramifié.

Soit $x \in L$ tel que $\mathcal{O}_L = \mathcal{O}_K[x]$. Notons P le polynôme minimal de x sur K. On a $P(X) = \prod_{\sigma\in\mathrm{Gal}(L/K)}(X-\sigma(x))$ et donc

$$P'(x) = \prod_{\sigma\in\mathrm{Gal}(L/K),\sigma\neq 1} (X-\sigma(x))$$

D'après les propositions IV-4 et IV-5, on a

$$\mathcal{D}_{L/K} = \mathrm{N}_{L/K}(\prod_{\sigma\in\mathrm{Gal}(L/K),\sigma\neq 1} P'(x))\mathcal{O}_K.$$

On a donc, en utilisant le fait que l'extension $L|K$ est totalement ramifiée,

$$v_K(\mathcal{D}_{L/K}) = v_L(P'(x)) = \sum_{\sigma\in\mathrm{Gal}(L/K),\sigma\neq 1} v_L(x-\sigma(x)) = \sum_{\sigma\in\mathrm{Gal}(L/K),\sigma\neq 1} i_G(\sigma).$$

Passons maintenant à la deuxième égalité figurant dans la proposition. La fonction i_G est égale à i sur $G_{i-1}-G_i$. On a donc

$$\sum_{\sigma\in\mathrm{Gal}(L/K),\sigma\neq 1} i_G(\sigma) = \sum_{i=0}^{\infty} i(|G_{i-1}|-|G_i|).$$

Cela donne la formule cherchée en simplifiant le dernier membre.

PROPOSITION 9. — *Le i-ème groupe de ramification de* $\mathrm{Gal}(L/K)$ *est nul lorsqu'on a* $i > v_L(p)/(p-1)$.

Démonstration. — Supposons donc que i est un entier $> v_L(p)/(p-1)$. On se ramène encore au cas où l'extension $L|K$ est totalement ramifiée. Soit $\sigma \in G_i$. Soit π une uniformisante de l'anneau des entiers de L. On a $\sigma(\pi) = \pi(1+a)$ avec $a \in \mathcal{P}^i$.

Observons qu'on a, pour $k \geq 0$,

$$(\sigma - 1)^k(\pi) \equiv 0 \pmod{\mathcal{P}^{ki+1}}.$$

Cela se vérifie par une récurrence immédiate sur k en utilisant que $\sigma \in G_i$; En effet on a

$$\frac{\sigma((\sigma-1)^{k-1}(\pi))}{(\sigma-1)^{k-1}(\pi)} - 1 \in \mathcal{P}^i.$$

Lemme 3. — *Supposons qu'on ait* $\sigma \notin G_{i+1}$. *On a alors* $\sigma^p \in G_{i+v_L(p)} - G_{i+v_L(p)+1}$.
Démonstration. — Calculons $\sigma^p(\pi)$ grâce à la formule du binôme. On a

$$\sigma^p(\pi) = (\sigma - 1 + 1)^p(\pi) = \sum_{k=0}^{p} \binom{p}{k} (\sigma-1)^k(\pi).$$

Dans cette dernière somme, les termes correspondant à $k \neq 0$, 1, p s'écrivent sous la forme $\binom{p}{k}(\sigma-1)^{k-1}(a\pi)$; Or dans ces cas on a $p \mid \binom{p}{k}$ et $(\sigma-1)^{k-1}(a\pi) \in \mathcal{P}^{i+2}$ et donc $v_L(\binom{p}{k}(\sigma-1)^{k-1}(a\pi)) \geq i + v_L(p) + 2$.

On a donc

$$\sigma^p(\pi) - \pi \equiv (\sigma-1)^p(\pi) + pa\pi \pmod{\mathcal{P}^{i+v_L(p)+2}}.$$

D'après ce qui précède on a $(\sigma-1)^p(\pi) \in \mathcal{P}^{pi+1}$. L'hypothèse $i > v_L(p)/(p-1)$ se traduit par $pi + 1 \geq i + v_L(p) + 2$. On a donc $(\sigma-1)^p(\pi) \in \mathcal{P}^{i+v_L(p)+2}$. Cela se traduit par la congruence

$$\sigma^p(\pi) - \pi \equiv pa\pi \pmod{\mathcal{P}^{i+v_L(p)+2}}.$$

Comme $v_L(pa\pi) = v_L(p) + i + 1$, on a $\sigma^p(\pi) - \pi \in \mathcal{P}^{i+v_L(p)+1} - \mathcal{P}^{i+v_L(p)+2}$ et donc $\sigma^p \in G_{i+v_L(p)} - G_{i+v_L(p)+1}$.

Poursuivons notre raisonnement en supposant qu'on a $\sigma \notin G_{i+1}$. Comme les groupes de ramification d'indice > 0 sont des p-groupes, σ est d'ordre une puissance de p. On a donc $\sigma^{p^k} = 1$ pour un entier $k > 0$. En itérant la construction qui précède, on obtient $\sigma^{p^k} \in G_{i+kv_L(p)} - G_{i+kv_L(p)+1}$. Cela est absurde puisque $G_{i+kv_L(p)+1}$ est un sous-groupe de $\mathrm{Gal}(L/K)$ et contient donc l'élément neutre.

L'hypothèse $\sigma \notin G_{i+1}$ est donc absurde. Cela entraîne donc

$$\sigma \in \cap_{j > v_L(p)/(p-1)} G_j = \{1\}$$

et donc la trivialité du i-ème groupe de ramification.