

La seconde inégalité fondamentale

Olivier Wittenberg

19 mai 2003

Résumé

On prouve ici la seconde inégalité fondamentale de la théorie du corps de classes global, en suivant plus ou moins les notes d'Artin-Tate [1]. Le théorème de Tsen permettant avantageusement de traiter le cas des corps de fonctions, on se restreindra à celui des corps de nombres.

1 Notations et énoncé

Si k est un corps global, on notera comme d'habitude Ω_k l'ensemble de ses places, \mathcal{O}_k son anneau d'entiers, k_v (resp. $\mathcal{O}_{k,v}$) le complété de k (resp. de \mathcal{O}_k) en $v \in \Omega_k$, $\text{Pic}(\mathcal{O}_k)$ le groupe des classes d'idéaux de k , J_k le groupe des idèles de k , et enfin C_k celui des classes d'idèles. De plus, pour $S \subset \Omega_k$ fini, on notera $\mathcal{O}_{k,S}$ ou \mathcal{O}_S l'anneau des S -entiers de k (c'est l'ensemble des éléments de k entiers aux places finies de $\Omega_k \setminus S$), $J_{k,S}$ ou J_S le groupe des S -idèles, $C_{k,S}$ ou C_S celui des classes de S -idèles, et $\text{Pic}(\mathcal{O}_{k,S})$ le quotient de $\text{Pic}(\mathcal{O}_k)$ par les classes des places finies de S . Rappelons que $\text{Pic}(\mathcal{O}_k)$ est fini si k est un corps de nombres, de sorte que $\text{Pic}(\mathcal{O}_{k,S}) = 0$ si S est assez grand. Sous cette hypothèse, la suite exacte

$$0 \longrightarrow C_{k,S} \longrightarrow C_k \longrightarrow \text{Pic}(\mathcal{O}_{k,S})$$

montre que $C_k = C_{k,S}$, i.e. $J_k = k^* J_{k,S}$.

Si K/k est une extension, on notera souvent simplement N la norme de K à k . Si K/k est galoisienne de groupe G et si w est une place de K , le groupe de décomposition en w sera noté G_w . Enfin, $h^i(G, A)$ désignera le cardinal d'un groupe de cohomologie $H^i(G, A)$.

Théorème (Seconde inégalité) — *Si K/k une extension finie galoisienne de corps globaux, $(C_k : NC_K)$ divise $[K : k]$.*

Lorsque K/k est cyclique de groupe G , $(C_k : NC_K)$ est égal à $h^2(G, C_K)$. Rappelons que l'on dispose, sous cette hypothèse, de la première inégalité fondamentale : $h^2(G, C_K) = h^1(G, C_K)[K : k]$. Du théorème découle donc la nullité de $H^1(G, C_K)$ pour une extension cyclique, ce qui est l'un des axiomes des formations de classes. Un dévissage facile à l'aide de sous-groupes de Sylow et des propriétés des p -groupes permet ensuite d'établir que $H^1(G, C_K) = 0$ pour toute extension finie (voir [2] p. 174).

Soit k un corps de fonctions. On a vu lors d'un précédent exposé l'exactitude de la suite

$$0 \longrightarrow \text{Br}(k) \longrightarrow \bigoplus_{v \in \Omega_k} \text{Br}(k_v) \longrightarrow \mathbf{Q}/\mathbf{Z} \longrightarrow 0.$$

Si l'on écrit cette suite au niveau de k et au niveau d'une extension finie galoisienne K/k de groupe G , on en déduit l'injectivité de $H^2(G, K^*) \rightarrow H^2(G, J_K)$, puisque $H^2(G, K^*) = \text{Ker}(\text{Br}(k) \rightarrow \text{Br}(K))$ et de même pour les idèles. La suite exacte

$$0 \longrightarrow K^* \longrightarrow J_K \longrightarrow C_K \longrightarrow 0$$

montre maintenant que le bord $H^1(G, C_K) \rightarrow H^2(G, K^*)$ est nul. Pour obtenir la seconde inégalité, il suffit donc de la nullité de $H^1(G, J_K)$, mais celle-ci découle du théorème de Hilbert 90 puisque $H^1(G, J_K)$ est une somme directe de $H^1(G_w, K_w^*)$ pour des $w \in \Omega_K$ (lemme de Shapiro).

2 Préliminaire : une conséquence de la première inégalité

Nous aurons besoin d'un théorème sur l'existence de premiers vérifiant certaines conditions de décomposition dans des extensions cycliques données d'un corps global. On pourrait se servir du théorème de Čebotarev, mais la première inégalité fondamentale suffira à l'établir.

Proposition 2.2 — *Soit K/k une extension finie galoisienne non triviale de corps globaux. Il existe une infinité de places de k qui ne se décomposent pas totalement dans K .*

Démonstration — Comme le groupe de Galois de K/k contient un sous-groupe cyclique non trivial, on peut supposer K/k cyclique. Soit S l'ensemble des places de k qui ne se décomposent pas totalement dans K . Procédons par l'absurde et supposons S fini. D'après la première inégalité fondamentale, tout ce qu'il reste à montrer est la surjectivité de la norme $C_K \rightarrow C_k$, i.e. l'égalité $J_k = k^* N J_K$. Soit $a \in J_k$. Dans une extension de corps locaux, les normes forment un ouvert¹, de sorte que la finitude de S et le lemme d'approximation fournissent un $b \in k^*$ tel que ba soit une norme en toute place de S . Les places hors de S étant totalement décomposées dans K , ba est une norme en toute place, d'où le résultat. \square

Proposition 2.3 — *Soient k un corps global, p un nombre premier et K_1, \dots, K_s des extensions cycliques de k de degré p « globalement k -linéairement disjointes », au sens où $K_1 \otimes_k \dots \otimes_k K_s$ est un corps. Il existe une infinité de places de k totalement décomposées dans K_i pour $i > 1$ et inertes dans K_1 .*

Démonstration — Soient $M = K_2 \otimes_k \dots \otimes_k K_s$ et $L = K_1 \otimes_k M$. Ce sont des corps. L'extension L/M est cyclique de degré p , de sorte qu'il existe une infinité de places w de M qui ne se décomposent pas totalement dans L , d'après la proposition 2.2, et y sont donc inertes. On notera encore w la place de L au-dessus de $w \in \Omega_M$. Montrons que la trace v sur k d'une telle place w de M convient dès lors qu'elle ne se ramifie pas dans L . Les corps résiduels étant finis, l'extension L_w/k_v est alors nécessairement cyclique. Son degré divise celui de L/k , qui est une puissance de p , donc divise p . Comme par ailleurs L_w/M_w est de degré p , cela montre que $M_w = k_v$, i.e. v se décompose totalement dans M et donc dans K_i pour $i > 1$. Enfin, v est inerte dans K_1 puisqu'elle n'est pas totalement décomposée dans L . \square

Mentionnons enfin un résultat général sur les corps p -adiques qui nous sera utile par la suite.

Proposition 2.4 — *Soient L un corps p -adique et $n \in \mathbf{N}^*$. On suppose que L contient une racine primitive n -ème de l'unité. Alors*

$$(\mathcal{O}_L^* : \mathcal{O}_L^{*n}) = \frac{n}{|n|} \quad \text{et} \quad (L^* : L^{*n}) = \frac{n^2}{|n|},$$

où $|\cdot|$ désigne la valeur absolue normalisée sur L , i.e. vérifiant $|p| = p^{-[L:\mathbf{Q}_p]}$.

Démonstration — L'exponentielle $x \mapsto \sum_{j=0}^{\infty} x^j/j!$ converge sur un disque ouvert de \mathcal{O}_L contenant 0; le logarithme $x \mapsto \sum_{j=1}^{\infty} (-1)^j (x-1)^j/j$ converge sur un disque ouvert de \mathcal{O}_L^* contenant 1. Comme \mathcal{O}_L et \mathcal{O}_L^* sont des groupes profinis, leurs sous-groupes ouverts forment une base de voisinages du neutre et sont d'indice fini. De plus, l'exponentielle et le logarithme sont des morphismes de groupes là où ils sont définis, de sorte qu'il existe un sous-groupe d'indice fini de \mathcal{O}_L isomorphe à un sous-groupe d'indice fini de \mathcal{O}_L^* . En notant $h(M)$ le quotient de Herbrand d'un $\mathbf{Z}[\mathbf{Z}/n\mathbf{Z}]$ -module M , on a donc $h(\mathcal{O}_L) = h(\mathcal{O}_L^*)$ (où l'action de $\mathbf{Z}/n\mathbf{Z}$ est triviale). Par ailleurs, $h(\mathcal{O}_L) = (\mathcal{O}_L : n\mathcal{O}_L) = 1/|n|$ puisque \mathcal{O}_L est sans torsion. De plus, $h(\mathcal{O}_L^*) = (\mathcal{O}_L^* : \mathcal{O}_L^{*n})/n$ puisque L contient une racine primitive n -ème de l'unité. La première assertion est maintenant établie; la seconde découle de la première et de la suite exacte $0 \longrightarrow \mathcal{O}_L^* \longrightarrow L^* \longrightarrow \mathbf{Z} \longrightarrow 0$. \square

3 Preuve pour les corps de nombres

On prendra dorénavant pour k un corps de nombres. Si E/F est une extension de corps de nombres, on notera $I(E/F) = (C_F : N_{E/F} C_E)$. Commençons par quelques propriétés élémentaires de $I(\cdot/\cdot)$.

¹En effet, elles sont d'indice fini, ce qui est une conséquence immédiate de la théorie du corps de classes local, mais aussi plus directement de la finitude de L^*/L^{*n} pour tout entier $n > 0$ lorsque L est un corps local.

Proposition 3.5 — Soit E/F une extension de corps de nombres. L'indice $I(E/F)$ est fini.

Démonstration — Soit D une clôture galoisienne de E sur F . Il suffit de prouver la finitude de $I(D/F)$. Choisissons un ensemble fini S de places de F contenant les places infinies et celles qui se ramifient dans D , assez grand pour que $\text{Pic}(\mathcal{O}_{F,S}) = 0$ et $\text{Pic}(\mathcal{O}_{D,S_D}) = 0$ en notant $S_D \subset \Omega_D$ l'ensemble des places de D au-dessus d'une place de S . On a alors $C_F = C_{F,S}$ et $C_D = C_{D,S_D}$, de sorte que

$$C_F/NC_D = C_{F,S}/NC_{D,S_D} = J_{F,S}/(\mathcal{O}_{F,S}^* NJ_{D,S_D})$$

est un quotient de

$$J_{F,S}/NJ_{D,S_D} = \prod_{v \in S} F_v^*/ND_v^* \times \prod_{v \notin S} \mathcal{O}_{F,v}^*/N\mathcal{O}_{D,v}^*,$$

où D_v (resp. $\mathcal{O}_{D,v}$) désigne le produit des D_w (resp. $\mathcal{O}_{D,w}$) pour $w \in \Omega_D$ divisant v . Notons que si w est une place de D au-dessus de $v \in \Omega_F$, on a $\mathcal{O}_{F,v}^*/N\mathcal{O}_{D,v}^* = \mathcal{O}_{F,v}^*/N\mathcal{O}_{D,w}^*$ et $F_v^*/ND_v^* = F_w^*/ND_w^*$. Pour toute place w de D au-dessus d'une place $v \notin S$, la norme $\mathcal{O}_{D,w}^* \rightarrow \mathcal{O}_{F,v}^*$ est surjective puisque v ne se ramifie pas dans D (calculs de normes et surjectivité de la norme d'une extension de corps finis, cf. [2] p. 90). De plus, sans restriction sur v , F_v^*/ND_w^* est un groupe fini. Comme S lui-même est fini, ceci permet de conclure. \square

Corollaire 3.6 — L'indice $I(E/F)$ divise une puissance de $[E : F]$.

Démonstration — Notons $n = [E : F]$. La puissance n -ème d'un idèle de F est évidemment une norme, de sorte que le groupe abélien fini $C_F/N_{E/F}C_E$ est tué par n ; son ordre divise donc une puissance de n . \square

Proposition 3.7 — Soient F/k et E/F des extensions finies. L'entier $I(E/k)$ divise $I(E/F)I(F/k)$.

Démonstration — La suite de groupes abéliens finis

$$C_F/N_{E/F}C_E \xrightarrow{N_{F/k}} C_k/N_{E/k}C_E \longrightarrow C_k/N_{F/k}C_F \longrightarrow 0$$

est évidemment exacte, d'où le résultat. \square

Soit K/k une extension finie galoisienne. Procédons d'abord à quelques réductions. Dans les énoncés qui suivent, il sera bien évidemment sous-entendu que l'on cherche à démontrer que $I(K/k)$ divise $[K : k]$.

Proposition 3.8 — On peut supposer K/k cyclique de degré premier.

Démonstration — L'astuce est de décomposer $I(K/k)$ et $[K : k]$ en produit de facteurs premiers. Notons G le groupe de Galois de K/k . Soient p un nombre premier, H un p -Sylow de G et $F = K^H$. La proposition 3.7 montre que $I(K/k)$ divise $I(K/F)I(F/k)$. L'extension F/k étant de degré premier à p , $I(F/k)$ l'est aussi (corollaire 3.6). Il s'ensuit que $I(K/k)$ divise $I(K/F)[F : k]$ dans \mathbf{Z}_p , et il reste seulement à prouver que $I(K/F)$ divise $[K : F]$. Comme H est un p -groupe, il existe une suite de sous-groupes

$$1 = H_0 \subset H_1 \subset \cdots \subset H_s = H$$

telle que H_i soit distingué dans H_{i+1} et que les quotients successifs soient cycliques d'ordre p (procéder par récurrence sur l'ordre de H ; le résultat est clair si H est commutatif, et sinon quotienter par le centre, qui est non trivial). Notons $F_i = K^{H_i}$; par hypothèse, l'extension F_i/F_{i+1} étant cyclique d'ordre premier, $I(F_i/F_{i+1})$ divise $[F_i : F_{i+1}]$. La proposition 3.7 permet d'en déduire que $I(K/F)$ divise $[K : F]$, d'où le résultat. \square

Proposition 3.9 — On peut de plus supposer que k contient une racine primitive ℓ -ème de l'unité, où $\ell = [K : k]$.

Démonstration — Soit ζ une racine primitive ℓ -ème de l'unité. L'indice $I(K/k)$ divise évidemment $I(K(\zeta)/k)$, qui divise $I(K(\zeta)/k(\zeta))I(k(\zeta)/k)$ d'après la proposition 3.7. Comme $[k(\zeta) : k]$ est premier à ℓ , le corollaire 3.6 appliqué deux fois permet d'en déduire que $I(K/k)$ divise $I(K(\zeta)/k(\zeta))$, d'où le résultat. \square

Supposons donc que k contient une racine primitive ℓ -ème de l'unité, et que K/k est une extension cyclique de degré ℓ . D'après la théorie de Kummer, il existe $a \in k^*$ tel que $K = k(a^{1/\ell})$. Soit $S \subset \Omega_k$ fini, contenant les

places archimédiennes, assez grand pour que a et ℓ soient des unités en-dehors de S et pour que $\text{Pic}(\mathcal{O}_S) = 0$. Notons s son cardinal, et posons

$$D = \prod_{v \in S} k_v^{\star \ell} \times \prod_{v \in T} k_v^{\star} \times \prod_{v \notin S \cup T} \mathcal{O}_v^{\star},$$

où T est un ensemble fini de places de k totalement décomposées dans K que l'on précisera par la suite.

Lemme 3.10 — *On a $D \subset N_{K/k} J_K$.*

Démonstration — Cela se teste place par place. Comme l'extension K/k est de degré ℓ , les puissances ℓ -èmes dans k_v^{\star} sont évidemment des normes. Les places de T étant totalement décomposées dans K , les éléments de k_v^{\star} sont des normes pour $v \in T$. Enfin, l'extension K/k est non ramifiée en-dehors de $S \cup T$, de sorte que les unités v -adiques sont des normes pour $v \notin S \cup T$. \square

Lemme 3.11 — *Pour tout $V \subset \Omega_k$ fini contenant les places archimédiennes, $\dim_{\mathbf{F}_\ell} (\mathcal{O}_V^{\star} / \mathcal{O}_V^{\star \ell}) = \text{Card}(V)$.*

Démonstration — Le théorème de Dirichlet affirme que \mathcal{O}_V^{\star} est le produit d'un \mathbf{Z} -module libre de rang $\text{Card}(V) - 1$ (puisque V contient les places archimédiennes) par le groupe des racines de l'unité de k . Or ce dernier groupe est cyclique, et son ordre divise ℓ puisque k contient une racine primitive ℓ -ème de l'unité. \square

Proposition 3.12 — *Il existe un ensemble $T \subset \Omega_k$ fini, disjoint de S , de cardinal $s - 1$, ne contenant que des places totalement décomposées dans K , tel que la flèche canonique*

$$\mathcal{O}_S^{\star} / \mathcal{O}_S^{\star \ell} \longrightarrow \prod_{v \in T} \mathcal{O}_v^{\star} / \mathcal{O}_v^{\star \ell}$$

soit surjective.

Démonstration — Soit (a_1, \dots, a_s) une base de $\mathcal{O}_S^{\star} / \mathcal{O}_S^{\star \ell}$ sur \mathbf{F}_ℓ telle que a_1 soit la classe de $a \in \mathcal{O}_S^{\star}$. Posons $K_i = k(a_i^{1/\ell})$. La proposition 2.3 fournit, pour chaque $i \in \{2, \dots, s\}$, une place $v_i \in \Omega_k \setminus S$ inerte dans K_i et totalement décomposée dans K_j pour $j \neq i$. Prenons $T = \{v_i; 2 \leq i \leq s\}$. Les groupes $\mathcal{O}_v^{\star} / \mathcal{O}_v^{\star \ell}$ pour $v \in T$ sont cycliques d'ordre ℓ (d'après la proposition 2.4 ou bien le lemme de Hensel), et l'image de a_i dans $\mathcal{O}_{v_j}^{\star} / \mathcal{O}_{v_j}^{\star \ell}$ est nulle si et seulement si v_j est totalement décomposée dans K_i , i.e. si et seulement si $j \neq i$, ce qui permet de conclure. \square

La proposition suivante a un intérêt dans d'autres contextes; nous en donnons donc un énoncé général.

Proposition 3.13 — *Soient $n \in \mathbf{N}^{\star}$, L un corps de nombres contenant une racine primitive n -ème de l'unité, S un ensemble fini de places de L contenant les places archimédiennes et assez grand pour que $\text{Pic}(\mathcal{O}_{L,S}) = 0$ et pour que n soit une S -unité. Soit T un ensemble de places de L disjoint de S et tel que la flèche*

$$\mathcal{O}_{L,S}^{\star} / \mathcal{O}_{L,S}^{\star n} \longrightarrow \prod_{v \in T} \mathcal{O}_{L,v}^{\star} / \mathcal{O}_{L,v}^{\star n}$$

soit surjective. Alors la flèche canonique

$$\mathcal{O}_{L,S \cup T}^{\star} / \mathcal{O}_{L,S \cup T}^{\star n} \longrightarrow \prod_{v \in S} L_v^{\star} / L_v^{\star n}$$

est injective.

Démonstration — Soit $x \in \mathcal{O}_{L,S \cup T}^{\star}$ dont l'image dans L_v^{\star} soit une puissance n -ème pour tout $v \in S$ et posons $M = L(x^{1/n})$. Comme L contient toutes les racines n -èmes de l'unité, M/L est une extension cyclique. On dispose dans ce cadre de la première inégalité fondamentale; pour montrer que $M = L$, il suffit donc d'établir la surjectivité de la norme $C_M \rightarrow C_L$. Soit

$$R = \prod_{v \in S} L_v^{\star} \times \prod_{v \in T} \mathcal{O}_{L,v}^{\star n} \times \prod_{v \notin S \cup T} \mathcal{O}_{L,v}^{\star}.$$

On a $J_L = L^* J_{L,S}$ puisque $\text{Pic}(\mathcal{O}_{L,S}) = 0$. L'hypothèse de surjectivité entraîne que $J_{L,S} \subset L^* R$. Ainsi, il suffit de voir que $R \subset N_{M/L} J_M$, ce qui se vérifie place par place. L'extension M/L est non ramifiée en-dehors de $S \cup T$ donc les unités v -adiques sont des normes pour $v \notin S \cup T$. De plus, les places $v \in S$ sont totalement décomposées dans M , et tout élément de k_v^* est donc une norme. Finalement, les éléments de $\mathcal{O}_{L,v}^{*n}$ sont des normes puisque l'extension M/L est de degré n . \square

Nous avons maintenant tous les outils nécessaires pour prouver la seconde inégalité. La suite

$$1 \longrightarrow \mathcal{O}_{S \cup T}^* / (D \cap \mathcal{O}_{S \cup T}^*) \longrightarrow J_{k, S \cup T} / D \longrightarrow J_k / (k^* D) \longrightarrow 1$$

est exacte (la surjectivité provient de ce que $\text{Pic}(\mathcal{O}_S) = 0$). D'après la proposition 3.13, $D \cap \mathcal{O}_{S \cup T}^* = \mathcal{O}_{S \cup T}^{*\ell}$, de sorte que la suite exacte précédente s'identifie à

$$1 \longrightarrow \mathcal{O}_{S \cup T}^* / \mathcal{O}_{S \cup T}^{*\ell} \longrightarrow \prod_{v \in S} k_v^* / k_v^{*\ell} \longrightarrow J_k / (k^* D) \longrightarrow 1.$$

D'après le lemme 3.11, $\text{Card}(\mathcal{O}_{S \cup T}^* / \mathcal{O}_{S \cup T}^{*\ell}) = \ell^{\text{Card}(S \cup T)} = \ell^{2s-1}$. Par ailleurs, $|\ell|_v = 1$ pour $v \notin S$ puisque ℓ est une S -unité et que S contient les places archimédiennes, de sorte que la formule du produit et la proposition 2.4 montrent que

$$\text{Card} \left(\prod_{v \in S} k_v^* / k_v^{*\ell} \right) = \ell^{2s}.$$

D'où finalement $(J_k : k^* D) = \ell$, et le lemme 3.10 permet de conclure.

Bibliographie

- [1] E. ARTIN, J. TATE, Class field theory, *Benjamin, New York*, 1967.
- [2] J-P. SERRE, Corps locaux, *Hermann, Paris*, 1968.