[9] H. Hasse, *Arithmetische Theorie der kubischen Zahlkörper auf Klassenkörpertheoretischer Grundlage*, Math. Zeitschr. 31 (1930), pp. 565–582.
[10] S. Kobayashi, *On the 3-rank of the ideal class groups of certain pure cubic fields*, J. Fac. Sci. Univ. Tokyo, Sec. IA 20 (1973), p. 209–216.
[11] — *On the 3-rank of the ideal class groups of certain pure cubic fields II*, to appear.
[12] S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, Mass., 1970.
[13] H. Reichardt, *Arithmetische Theorie der kubischen Körper als Radikalkörper*, Monatshefte Math. Phys. 40 (1933), pp. 323–350.
[14] D. Shanks, *On Gauss's class number problems*, Math. Comp. 23 (1969), pp. 151–163.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TEXAS
Austin, Texas, U.S.A.

*Received on 25. 9. 1974* (623)

ACTA ARITHMETICA
XXX (1976)

# Filtration de $K^*/K^{*p}$ et ramification sauvage

par

THONG NGUYEN-QUANG-DO (Paris)

Si $k$ est un corps local de caractéristique 0, de caractéristique résiduelle $p \neq 0$, le groupe multiplicatif $k^*/k^{*p}$ est filtré de façon naturelle par les sous-groupes $U_k^i k^{*p}/k^{*p}$ (sections 1 et 2). L'objet principal de cet article est d'étudier comment cette filtration se transforme dans une extension galoisienne $K/k$, plus précisément via l'homomorphisme naturel $\eta$: $k^*/k^{*p} \to K^*/K^{*p}$ (section 3): la façon dont $\eta$ transforme la fonction d'ordre de la filtration est décrite par une fonction $\delta_{K/k}$ attachée à la fonction classique $\psi_{K/k}$ et jouissant de propriétés analogues. Dans la section 4, nous appliquons les résultats obtenus à la construction de $p$-extensions cycliques de $k$ ayant des nombres de ramification donnés.

**0. Notations générales.** Dans toute la suite, sauf mention expresse du contraire, nous entendrons par „corps local" $k$, un corps $k$ qui est complet pour une valuation discrète, qui est de caractéristique 0, et dont le corps résiduel $\bar{k}$ est *parfait*, de caractéristique $p \neq 0$.

Nous noterons $\mathrm{ord}_k$ la valuation additive normalisée de $k$, i.e. telle que $\mathrm{ord}_k k = \mathbf{Z} \cup \{\infty\}$.

Nous poserons $e_k = \mathrm{ord}_k p$ et $e'_k = e_k/(p-1)$ (c'est un entier si $k$ contient les racines $p$-ièmes de l'unité). Pour tout $x \in k^*$, il sera commode de noter: $d_k(x) = \mathrm{ord}_k(1-x)$.

Comme d'habitude, nous introduisons les groupes multiplicatifs:

$U_k = U_k^0 = \{x \in k^*;\ \mathrm{ord}_k x = 0\}$,

$U_k^i = \{x \in k^*;\ d_k(x) \geqslant i\}$ pour tout entier $i \geqslant 1$.

Enfin, pour tout entier $i \geqslant 0$, nous noterons $\overline{U}_k^i = U_k^i/U_k^{i+1}$. On sait que $\overline{U}_k^0 \cong \bar{k}^*$ (groupe multiplicatif de $\bar{k}$) et que, pour tout entier $i \geqslant 1$, $\overline{U}_k^i$ est isomorphe au groupe additif de $\bar{k}$ (de façon non canonique, par le choix d'une uniformisante).

Dans la suite, lorsqu'il n'y aura pas d'ambiguïté possible, on sous-entendra l'indice $k$, et l'on écrira: $\mathrm{ord}(x)$, $d(x)$, $e$, $e'$, etc... au lieu de $\mathrm{ord}_k(x)$, $d_k(x)$, $e_k$, $e'_k$, etc...

**1. La fonction „Défaut".** Suivant [6], introduisons la notion de défaut d'un élément de $k^*$ de la façon suivante:

**1.1.** Définition. Pour tout $x \in k^*$, on pose: *défaut de* $x = \mathrm{def}_k(x) = \sup d_k(y)$, pour $y \in xk^{*p}$.

On écrira $\mathrm{def}(x)$ au lieu de $\mathrm{def}_k(x)$ s'il n'y a pas de confusion possible.

Notre but dans cette section va être de déterminer l'ensemble des valeurs prises sur $k^*$ par la fonction $\mathrm{def}_k$ (le résultat final figure dans [6], mais avec une erreur).

L'outil principal sera le théorème bien connu suivant:

**1.2.** Théorème. *Soit* $\lambda: k^* \to k^*$ *l'homomorphisme d'élévation à la puissance* $p$*-ième, défini par* $\lambda(x) = x^p$. *Alors:*

(i) *Pour tout entier* $m \geqslant 0$, $\lambda(U^m) \subset U^{P(m)}$ *et* $\lambda(U^{m+1}) \subset U^{P(m)+1}$, *où* $P(m) = \min(pm, m+e)$;

(ii) $\lambda$ *induit par passage au quotient, un isomorphisme* $\lambda_0 = \overline{U}^0 \to \overline{U}^0$;

(iii) *Pour tout entier* $m \geqslant 1$, $\lambda$ *induit, par passage au quotient, un homomorphisme* $\lambda_m: \overline{U}^m \to \overline{U}^{P(m)}$ *tel que, si l'on identifie* $\overline{U}^m$ *et* $\overline{U}^{P(m)}$ *à* $\bar{k}$ *par le choix d'une uniformisante* $\overline{\omega}$ *de* $k$, $\lambda_m$ *est défini par:*

(a) *Si* $m < e'$, $\lambda_m(\bar{a}) = \bar{a}^p$. *Dans ce cas* $\lambda_m$ *est un isomorphisme.*

(b) *Si* $m > e'$, $\lambda_m(\bar{a}) = \bar{A}\bar{a}$, *où* $\bar{A}$ *désigne l'image dans* $\bar{k}$ *de* $p/\overline{\omega}^e$. *Dans ce cas,* $\lambda_m$ *est un isomorphisme.*

(c) *Si* $m = e'$, $\lambda_m(\bar{a}) = \bar{a}^p + \bar{A}\bar{a}$. *Dans ce cas,* $\mathrm{Ker}\,\lambda_m$ *est l'image du groupe des racines* $p$*-ièmes de l'unité contenues dans* $\bar{k}$, *et* $\lambda_m$ *est surjectif si* $\bar{k}$ *est algébriquement clos.*

Démonstration. Standard (cf. par exemple [2], § 15).

Nous allons maintenant établir les propriétés de la fonction „défaut" dans une série de lemmes:

**1.3.** Lemme. (a) *Pour tout* $x \in k^*$, *on a:* $0 \leqslant \mathrm{def}(x) \leqslant +\infty$, *avec* $\mathrm{def}(x) = +\infty$ *si et seulement si* $x \in k^{*p}$, *et* $\mathrm{def}(x) = 0$ *si et seulement si* $\mathrm{ord}(x) \not\equiv 0 \pmod p$.

(b) *Pour tous* $x, y \in k^*$ *tels que* $xy^{-1} \in k^{*p}$, *on a:* $\mathrm{def}(x) = \mathrm{def}(y)$.

Démonstration. C'est clair, d'après la définition de la fonction def.

**1.4.** Lemme. *Tout* $x \in k^*$ *et tel que* $\mathrm{ord}\,x \equiv 0 \pmod p$ *est congru multiplicativement* $\mathrm{mod}\,k^{*p}$ *à un élément* $y$ *de* $U^1$ *tel que* $d(y) = m$, *avec soit* $m \geqslant pe'$, *soit* $0 < m < pe'$ *et* $(m, p) = 1$.

Démonstration. Cela résulte immédiatement du théorème 1.2.

**1.5.** Lemme. *Soit* $y \in U^1$ *et soit* $m' = d(y)$. *Alors:*

(a) *Si* $0 < m < pe'$ *et* $(m, p) = 1$, $\mathrm{def}(y) = m$.

(b) *Si* $m = pe'$, $\mathrm{def}(y) = pe'$ *ou* $+\infty$.

(c) *Si* $m > pe'$, $\mathrm{def}(y) = +\infty$.

Démonstration. (a) Puisque 1 est une puissance $p$-ième, on a toujours $\mathrm{def}(y) \geqslant d(y) = m$. Supposons que $\mathrm{def}(y) > m$: cela signifierait qu'il existe $z \in k^*$ t.q. $d(yz^p) \geqslant m+1$, et cela impliquerait que $d(z^p) = d(y)$, soit, puisque $m < pe'$, que $m = pd(z)$, ce qui est contraire à l'hypothèse.

(b) Si $m = pe'$ et si $y$ n'est pas congru $\mathrm{mod}\,k^{*p}$ à un élément de $U^{pe'+1}$, $\mathrm{def}(y) = pe'$. Sinon, on tombe dans le cas (c).

(c) Si $m > pe'$, il résulte du théorème 1.2 que $y \in k^{*p}$, donc $\mathrm{def}(y) = +\infty$. ∎

Les lemmes 1.3, 1.4 et 1.5 mis ensemble donnent immédiatement le théorème suivant:

**1.6.** Théorème. *Soit* $D(k)$ *l'ensemble des entiers* $m$ *tels que* $0 \leqslant m \leqslant pe'_k$, *et* $(m, p) = 1$ *si* $m \neq 0$ *et* $m \neq pe'_k$. *Alors* $\mathrm{def}_k(k^*) \subset D(k) \cup \{+\infty\}$.

**2. Filtration de $k^*/k^{*p}$.**

**2.1.** Désignons par $\Gamma_k$ le groupe multiplicatif $k^*/k^{*p}$. Si $\bar{x} \in \Gamma_k$, $\mathrm{def}_k(x)$ ne dépend pas du choix du représentant $x$ de $\bar{x}$ dans $k^*$. Posons $\mathrm{def}_k(\bar{x}) = \mathrm{def}_k(x)$. Pour tout entier $m \geqslant 0$, posons $\Gamma_k^m = \{\bar{x} \in \Gamma_k,\ \mathrm{def}_k(\bar{x}) \geqslant m\}$. Il est clair que $\Gamma_k^m$ est un sous-groupe de $\Gamma_k$, et que la famille des $\Gamma_k^m$ munit $\Gamma_k$ d'une filtration dont la fonction d'ordre est $\mathrm{def}_k$. De plus, on a $\Gamma_k^0 = \Gamma_k$ et $\Gamma_k^m = \{1\}$ si $m > pe'_k$. Les sauts de la filtration (i.e. les entiers $m$ tels que $\Gamma_k^m \neq \Gamma_k^{m+1}$) sont inclus dans l'ensemble $D(k)$ (théorème 1.6). Pour tout entier $m \geqslant 0$, posons $\bar{\Gamma}_k^m = \Gamma_k^m/\Gamma_k^{m+1}$. Nous sous-entendrons l'indice $k$ s'il n'y a pas de confusion possible.

**2.2.** Théorème. (i) *Soit* $\bar{x} \in \Gamma^0$ *et soit* $x$ *un représentant de* $\bar{x}$ *dans* $k^*$. *La classe modulo* $p$ *de* $\mathrm{ord}(x)$ *ne dépend pas du choix de* $x$, *et définit par passage au quotient un isomorphisme* $\mu_0$ *de* $\bar{\Gamma}^0$ *sur* $\mathbf{Z}/p\mathbf{Z}$.

(ii) *Soit* $m \in D(k)$ *et tel que* $m \neq 0$ *et* $m \neq pe'$. *Soit* $\bar{x} \in \bar{\Gamma}^m$ *et soit* $x$ *un représentant de* $\bar{x}$ *dans* $k^*$ *tel que* $d(x) = \mathrm{def}(\bar{x})$. *Alors la classe de* $x$ *modulo* $U^{m+1}$ *ne dépend pas du choix de* $x$, *et définit par passage au quotient un isomorphisme* $\mu_m$ *de* $\bar{\Gamma}^m$ *sur* $\overline{U}^m$.

(iii) *Si* $e'$ *est un entier, soit* $\overline{\omega}$ *une uniformisante de* $k$ *et soit* $\bar{A}$ *la classe de* $p/\overline{\omega}^e$ *dans* $\bar{k}$. *Soit* $\lambda_{e'}$ *l'homomorphisme du groupe additif de* $\bar{k}$ *dans lui-même défini par* $\lambda_{e'}(\bar{a}) = \bar{a}^p + \bar{A}\bar{a}$. *Soit* $\bar{x} \in \bar{\Gamma}^{pe'}$ *et soit* $x = 1 + b\overline{\omega}^{pe'}$ *un représentant de* $\bar{x}$ *dans* $U^{pe'}$. *La classe de l'image* $\bar{b}$ *de* $b$ *dans* $\bar{k}$, *modulo* $\mathrm{Im}\,\lambda_{e'}$, *ne dépend pas du choix de* $x$ *et définit un isomorphisme de* $\bar{\Gamma}^{pe'} = \Gamma^{pe'}$ *sur* $\mathrm{Coker}\,\lambda_{e'}$. *Si* $\bar{k}$ *est algébriquement clos,* $\Gamma^{pe'} = \{1\}$.

Démonstration. (i) est immédiat.

(ii). Soit $m \in D(k) - \{0, pe'\}$ et soit $\bar{x} \in \Gamma^m$. Il résulte des propriétés de la fonction défaut qu'il existe un représentant $x$ de $\bar{x}$ dans $k^*$ tel que $d(x) = \mathrm{def}(\bar{x})$. Si $\mathrm{def}(\bar{x}) > m$, la classe de $x$ mod $U^{m+1}$ est 1. Si $\mathrm{def}(\bar{x}) = m$, soit $y$ un autre représentant de $\bar{x}$ dans $k^*$ tel que $d(x) = \mathrm{def}(\bar{x}) = m$. Alors $y$ est de la forme $y = xz^p$, $z \in k^*$, d'où $d(z^p) \geqslant m$, et comme $m < pe'$, on ne peut avoir $d(z^p) = m$. Donc les classes de $x$ et $y$ mod $U^{m+1}$ coïncident. Le reste de (ii) est évident.

(iii). Soit $\bar{x} \in \bar{\Gamma}^{pe'}$ et soit $x = 1 + b\bar{\omega}^{pe'}$ un représentant de $\bar{x}$ dans $U^{pe'}$ (i.e. $\operatorname{ord} b \geqslant 0$). Si $y$ est un autre représentant de $\bar{x}$ dans $U^{pe'}$, $y$ est de la forme $y = xz^p$, $z \in k^*$, d'où $d(z^p) \geqslant pe'$. On sait dans ce cas (théorème 1.2) que $z$ est de la forme $z = 1 + c\bar{\omega}^{e'}$, avec $\operatorname{ord} c \geqslant 0$ et $z^p \equiv 1 + (c^p + Ac)\bar{\omega}^{pe'}$ (mod $U^{pe'+1}$). Cela montre que la classe de $\bar{b} \bmod \operatorname{Im}\lambda_{e'}$ ne dépend pas du choix de $x$. On définit ainsi un homomorphisme $\mu_{pe'}$ de $\bar{\Gamma}^{pe'} = \Gamma^{pe'}$ dans $\operatorname{Coker}\lambda_{e'}$. La surjectivité de $\mu_{pe'}$ est évidente.

Montrons l'injectivité:

Soit $x = 1 + b\bar{\omega}^{pe'}$ tel que $\bar{b} \in \operatorname{Im}\lambda_{e'}$. Alors $\bar{b}$ est de la forme $\lambda_{e'}(\bar{c})$, autrement dit, il existe $z = 1 + c\bar{\omega}^{e'}$, $\operatorname{ord} c \geqslant 0$, tel que $x \equiv z^p$ (mod $U^{pe'+1}$).

Il en résulte que $x \in k^{*p}$, ce qui montre l'injectivité de $\mu_{pe'}$. La fin de l'assertion (iii) est évidente. ∎

Remarque. Les isomorphismes définis dans (i) et (ii) sont canoniques, alors que celui de (iii) dépend du choix de l'uniformisante $\bar{\omega}$.

**3. Etude l'homomorphisme** $k^*/k^{*p} \to K^*/K^{*p}$. $k$ vérifiant toujours les conditions de la section 1, soit $K$ une extension galoisienne de $k$. De la même manière que dans 2, le groupe $\Gamma_K = K^*/K^{*p}$ est filtré par la fonction $\mathrm{def}_K$. L'injection naturelle $k^* \to K^*$ définit, par passage au quotient, un homomorphisme $\eta_{K/k}$: $\Gamma_k \to \Gamma_K$ (en abrégé: $\eta$) dont nous nous proposons d'étudier l'effet sur la filtration des $\Gamma_k^m$. L'étude étant très simple dans le cas où l'extension est non ramifiée ou modérément ramifiée, nous nous bornerons au cas sauvagement ramifié, i.e. au cas où $K/k$ est une $p$-extension totalement ramifiée. Nous examinerons d'abord le cas où $K/k$ est cyclique de degré $p$, puis nous poserons au cas général par „dévissage".

**3.1. Rappels et définitions.** Soit $K/k$ une extension galoisienne de degré fini, de groupe de Galois $G$. Rappelons les faits suivants concernant la ramification dans l'extension $K/k$ (cf. par exemple [4], chap. 4):

**3.1.1.** Groupes de ramification. Pour tout $\sigma \in G$, on pose: $i_{K/k}(\sigma) = \operatorname{inf}\operatorname{ord}_K(\sigma(x) - x) - 1$ où $x$ parcourt l'anneau des entiers de $K$. On pose $G_{-1} = G$ et pour tout entier $i \geqslant 0$, $G_i = \{\sigma \in G;\ i_{K/k}(\sigma) \geqslant i\}$. Les $G_i$ sont des sous-groupes de $G$, appelés groupes de ramification en notation inférieure, et munissent $G$ d'une filtration décroissante dont la fonction d'ordre est $i_{K/k}$. Un entier $i$ tel que $G_i \neq G_{i+1}$ sera appelé saut inférieur de ramification de l'extension $K/k$.

Pour tout réel $t \geqslant 0$, soit $G_t = G_i$, où $i$ est le plus petit entier $\geqslant t$. Pour tout réel $u \geqslant 0$, on pose $\varphi_{K/k}(u) = \varphi(u) = \int_0^u (G_0 : G_t)^{-1} dt$, et l'on convient de prolonger $\varphi$ par $\varphi(u) = u$ si $u \leqslant 0$. La fonction $\varphi$ est continue, linéaire par morceaux, strictement croissante. Soit $\psi_{K/k} = \psi$ la fonction réciproque. On définit la numérotation supérieure des groupes de ramification en posant $G^v = G\psi(v)$ pour tout $v$ réel. Un réel $v$ tel que $G^v \neq G^{v+\varepsilon}$ pour tout $\varepsilon > 0$ sera appelé saut supérieur de ramification de l'extension $K/k$. Si l'extension $K/k$ est abélienne, les sauts supérieurs sont des entiers (théorème de Hasse–Arf).



**3.1.2.** La fonction $\delta_{K/k}$. Introduisons une fonction $\delta_{K/k}$: $\boldsymbol{R} \to \boldsymbol{R}$ (en abrégé: $\delta$) en posant:

$$\delta_{K/k}(t) = pe'_K - \psi_{K/k}(pe'_k - t), \quad \text{pour tout } t \in \boldsymbol{R}.$$

Il résulte des propriétés de la fonction $\psi_{K/k}$ que la fonction $\delta_{K/k}$ est continue, strictement croissante et transitive, i.e. telle que si $M$ est une sous-extension de $K$ galoisienne sur $k$, on a: $\delta_{K/k} = \delta_{K/M} \circ \delta_{M/k}$. C'est la fonction $\delta$ qui jouera le rôle principal dans l'étude de l'homomorphisme $\eta$.

Dans la suite, nous aurons souvent besoin du lemme technique suivant:

**3.1.3.** Lemme. *Soit $K/k$ une extension galoisienne de degré fini, totalement ramifiée, de groupe de Galois $G$. Soit $\sigma \in G$, $\sigma \neq 1$, et soit $s = i_{K/k}(\sigma)$. Soit $f: K^* \to K^*$ l'application définie par $f(x) = \sigma x/x$. Alors pour tout entier $m$, $f(U_K^m) \subset U_K^{s+m}$ et pour tout entier $m \not\equiv 0 \pmod p$, $f$ définit par passage au quotient un isomorphisme $f_m$ de $\overline{U}_K^m$ sur $\overline{U}_K^{s+m}$ tel que, en identifiant $\overline{U}_K^m$ et $\overline{U}_K^{s+m}$ à $\bar{K}$ par le choix d'une uniformisante $\pi$ de $K$, $f_m$ est donné par: $f_m(\bar{a}) = m\bar{s}\bar{a}$, où $\bar{s}$ est l'image dans $\bar{K}$ de $\left(\frac{\sigma\pi}{\pi} - 1\right)/\pi^s$.*

Démonstration. C'est un calcul standard de développements limités (cf. par exemple [6], théorème 22, p. 147).

**3.2. Cas où $K/k$ est cyclique de degré $p$, totalement ramifiée.** Dans ce cas, en désignant par $s$ l'unique saut de ramification de $K/k$, on sait que $s \leqslant pe'_k$, avec $s = pe'_k$ si et seulement si $s \equiv 0 \pmod p$ ([6], p. 144).

La fonction $\delta$ est alors définie par:

$$\delta(t) = \begin{cases} pt + ps - s & \text{si} \quad s + t \leqslant pe'_k, \\ t + pe_k & \text{si} \quad s + t \geqslant pe'_k. \end{cases}$$

**3.2.1.** Proposition. *Soit $D(k)$ l'ensemble défini dans* 1.6. *Alors pour tout $m \in D(k)$,*

$$\eta(\Gamma_k^m) \subset \Gamma_K^{\delta(m)} \quad \text{et} \quad \eta(\Gamma_k^{m+1}) \subset \Gamma_K^{\delta(m)+1}.$$

Nous démontrerons cette proposition un peu plus loin. Notons qu'elle permet de définir, par passage au quotient, des homomorphismes $\eta_{K/k}^m$: $\Gamma_k^m \to \Gamma_K^{\delta(m)}$ (en abrégé: $\eta^m$) pour tout $m \in D(k)$. Remarquons que si $m \in D(k)$, $\delta(m) \in D(K)$ donc, pour préciser ces homomorphismes, on pourra identifier (théorème 2.2) $\Gamma_k^0$ à $\boldsymbol{Z}/p\boldsymbol{Z}$ et $\Gamma_k^m$ (resp. $\Gamma_K^{\delta(m)}$) à $\bar{k}$ (resp. à $\bar{K} = \bar{k}$) par le choix d'une uniformisante $\bar{\omega}$ de $k$ (resp. $\pi$ de $K$) pour tout $m \in D(k) - \{0, pe'_k\}$. Il vient:

**3.2.2.** PROPOSITION. *Soit $K/k$ une extension cyclique de degré $p$, totalement ramifiée, de groupe de Galois $G$. Soit $\pi$ une uniformisante de $K$ et soit $\varpi = N_{K/k}\pi$ une uniformisante de $k$. Soit $\sigma$ un générateur de $G$ et soit $s = i_{K/k}(\sigma)$ l'unique saut de ramification de $K/k$. Soient $\bar{A}$ et $\bar{\varepsilon}$ respectivement images de $p/\pi^{e_K}$ et $\left(\frac{\sigma\pi}{\pi}-1\right)/\pi^s$ dans $\bar{K} = \bar{k}$. Alors:*

(i) *si $e'_k$ est un entier, $\eta^{pe'_k}: \Gamma_k^{pe'_k} \to \Gamma_K^{pe'_K}$ est un isomorphisme,*

(ii) *$\eta^0: \Gamma_k^0 \to \Gamma_K^{\delta(0)}$ est trivial si $s \equiv 0 \pmod p$, injectif si $s \not\equiv 0 \pmod p$. Dans ce dernier cas, $\operatorname{Im}\eta^0$ est le sous-groupe de $\bar{k}$ engendré par $\bar{\varepsilon}^{p-1}$*

(iii) *pour tout $m \in D(k) - \{0, pe'_k\}$:*

(a) *si $m + s < pe'_k$, $\eta^m: \Gamma_k^m \to \Gamma_K^{\delta(m)}$ est un isomorphisme défini par*

$$\eta^m(\bar{a}) = m\frac{\bar{\varepsilon}^{p-1}}{\bar{s}}\bar{a};$$

(b) *si $m + s > pe'_k$, $\eta^m: \Gamma_k^m \to \Gamma_K^{\delta(m)}$ est un isomorphisme défini par*

$$\eta^m(\bar{a}) = -\bar{A}\bar{a}^{1/p};$$

(c) *si $s + m = pe'_k$, $\eta^m: \Gamma_k^m \to \Gamma_K^{\delta(m)}$ est un homomorphisme défini par*

$$\eta^m(\bar{a}) = -(\bar{\varepsilon}^{p-1}\bar{a} + \bar{A}\bar{a}^{1/p}).$$

*Il est injectif si et seulement si $k$ ne contient pas les racines $p$-ièmes de l'unité. Si $k$ contient les racines $p$-ièmes de l'unité $\operatorname{Ker}\eta^m$ est cyclique d'ordre $p$, et $\operatorname{Coker}\eta^m \cong \bar{k}/P(\bar{k})$, où $P$ est le polynôme $P(X) = X^p - X$.*

Démonstration. Nous allons montrer simultanément les propositions 3.2.1 et 3.2.2. Pour alléger l'écriture, nous noterons $x \equiv 1 + a\pi^m$ au lieu de $x \equiv 1 + a\pi^m \pmod{U^{m+1}}$ chaque fois qu'il n'y aura pas de confusion possible.

(i) Si $e'_k$ est un entier et si $m = pe'_k$. Alors $\delta(m) = pe'_K$ et il est clair que $\eta(\Gamma_k^{pe'_k}) \subset \Gamma_K^{pe'_K}$. Comme $\Gamma_k^{pe'_k} = \Gamma_K^{pe'_k}$ et $\Gamma_K^{pe'_K} = \Gamma_K^{pe'_K}$, l'application $\eta^{pe'_k}$ n'est autre que la restriction de $\eta$ à $\Gamma_k^{pe'_k}$. Avec le choix des uniformisantes $\varpi$ et $\pi$, il est clair que $p/\varpi^{e_k}$ et $p/\pi^{e_K}$ ont même image dans $\bar{k}$, donc les application $\lambda_e$, introduites dans 2.2 (iii) coïncident. Si $x = 1 + b\varpi^{pe'_k} = 1 + B\pi^{pe'_K}$, il est clair que les images $\bar{b}$ et $\bar{B}$ de $b$ et $B$ dans $\bar{k}$ coïncident. Il en résulte, d'après 2.2 (iii), que $\eta^{pe'_k}$ est un isomorphisme de $\Gamma_k^{pe'_k}$ sur $\Gamma_K^{pe'_K}$.



(ii) Si $m = 0$. Soit $\bar{\lambda} \in \Gamma_k^0$ tel que $\operatorname{def}_k(\bar{\lambda}) = 0$. Alors $\bar{\lambda}$ admet un représentant $\lambda \in k^*$ tel que $\operatorname{ord}_k(\lambda) = i$, $0 < i < p$. Dans $K^*$ on peut mettre $\lambda$ sous la forme:

$$\lambda = \lambda_1^p\tilde{\lambda} \tag{1}$$

avec $\lambda_1 \in K^*$ et $\operatorname{ord}_K(\lambda_1) = i$, et $\tilde{\lambda} \in U_K^1$ et $d_K(\tilde{\lambda}) = \operatorname{def}_K(\tilde{\lambda}) = \operatorname{def}_K(\lambda) = \tilde{m} > pm$ (éventuellement infini). Montrons que $\tilde{m} \geqslant \delta(0) = ps - s$. Comme $\delta(0) < pe'_K$, on peut supposer $\tilde{m} < pe'_K$, d'où $\tilde{m} \not\equiv 0 \pmod p$ d'après 1.6.

Appliquons $\sigma$ à (1); il vient:

$$1 = \left(\frac{\sigma\lambda_1}{\lambda_1}\right)^p \frac{\sigma\tilde{\lambda}}{\tilde{\lambda}}. \tag{2}$$

Or d'après le lemme 3.1.3, $d_K\left(\frac{\sigma\tilde{\lambda}}{\tilde{\lambda}}\right) = s + \tilde{m}$. D'un autre côté, $d_K\left(\frac{\sigma\lambda_1}{\lambda_1}\right) = s$ et comme $s \leqslant pe'_k = e'_K$, $d_K\left(\frac{\sigma\lambda_1}{\lambda_1}\right)^p \geqslant ps$. Il résulte alors de (2) que $\tilde{m} + s \geqslant ps$ soit $\tilde{m} \geqslant \delta(0)$. Donc $\eta(\Gamma_k^0) \subset \Gamma_K^{\delta(0)}$. Nous montrerons dans (iii) que $\eta(\Gamma_k^1) \subset \Gamma_K^{\delta(1)}$. Déterminons l'homomorphisme $\eta^0: \Gamma_k^0 \to \Gamma_K^{\delta(0)}$.

Revenons à la décomposition (1), où $\tilde{m}$ est supposé quelconque

— si $s \equiv 0 \pmod p$: alors $s = pe'_k = e'_K$.

Si $\tilde{m} \geqslant pe'_K$, $\operatorname{def}_K\lambda = \tilde{m} > \delta(0)$ et $\bar{\lambda} \in \operatorname{Ker}\eta^0$.

Si $\tilde{m} < pe'_K$ alors $\tilde{m} \not\equiv 0 \pmod p$; (2) entraîne que $s + \tilde{m} \geqslant ps$, et en fait l'inégalité est stricte puisque $\tilde{m} \not\equiv 0 \pmod p$. Donc $\bar{\lambda}$ est encore dans $\operatorname{Ker}\eta^0$. Cela montre que $\eta^0$ est trivial.

— si $s \not\equiv 0 \pmod p$: alors $s < pe'_k = e'_K$ et $d_K\left(\frac{\sigma\lambda_1}{\lambda_1}\right)^p = ps$.

Si $\tilde{m} \geqslant pe'_K$, (2) entraînerait que $ps \geqslant s + \tilde{m}$ d'où $\delta(0) \geqslant pe'_K$: impossible. Donc $\tilde{m} < pe'_K$ et $\tilde{m} \not\equiv 0 \pmod p$. Dans ce cas, (2) donne: $\tilde{m} = ps - s = \delta(0)$, ce qui montre l'injectivité de $\eta^0$. Pour déterminer l'image de $\eta^0$, posons $\tilde{\lambda} = 1 + b\pi^{\tilde{m}}$. D'après le lemme 3.1.1, on a:

$$\frac{\sigma\tilde{\lambda}}{\tilde{\lambda}} \equiv 1 + \tilde{m}\varepsilon b\pi^{s+\tilde{m}}.$$

Or $\frac{\sigma\lambda_1}{\lambda_1} \equiv 1 + i\varepsilon\pi^s$ et d'après 1.2, $\frac{\sigma\lambda_1}{\lambda_1} \equiv 1 + i^p\varepsilon^p\pi^{ps}$.

On a alors, d'après (2): $\bar{\tilde{m}}\bar{\varepsilon}\bar{b} + i^{\bar{p}}\varepsilon^{\bar{p}} = 0$, soit puisque $\bar{\tilde{m}} = -\bar{s}$, $\bar{b} = i\frac{\bar{\varepsilon}^{p-1}}{\bar{s}}$, ce qui montre bien que l'image de $\eta^0$ est le sous-groupe de $\bar{k}$ engendré par $\bar{\varepsilon}^{p-1}$.

(iii) Si $m \in D(k) - \{0, pe'_k\}$. Soit $\bar{\lambda} \in \Gamma_k^m$ tel que $\mathrm{def}_k(\lambda) = m$, et soit $\lambda \in U_k^1$ un représentant de $\bar{\lambda}$ tel que $d_k(\lambda) = m$. Dans $K^*$, on peut écrire:

$$\lambda = \lambda_1^p \tilde{\lambda} \tag{3}$$

avec $\lambda_1 \in U_K^1$ et $d_K(\lambda_1) = m$, et $\tilde{\lambda} \in U_K^1$ et $d_K(\tilde{\lambda}) = \mathrm{def}_K(\tilde{\lambda}) = \mathrm{def}_K(\lambda) = \tilde{m} > pm$ (éventuellement infini). Montrons que $\tilde{m} \geqslant \delta(m)$. Comme $\delta(m) < pe'_K$, on peut supposer $\tilde{m} < pe'_K$ et $\tilde{m} \not\equiv 0 \pmod p$. En appliquant $\sigma$ à (3), on obtient:

$$1 = \left(\frac{\sigma\tilde{\lambda}_1}{\lambda_1}\right)^p \frac{\sigma\tilde{\lambda}}{\tilde{\lambda}}. \tag{4}$$

D'après le lemme 3.1.3, $d_K\left(\frac{\sigma\tilde{\lambda}}{\tilde{\lambda}}\right) = s + \tilde{m}$ et $d_K\left(\frac{\sigma\lambda_1}{\lambda_1}\right) = s + m$.

— si $s + m < pe'_k = e'_K$:

$d_K\left(\frac{\sigma\lambda_1}{\lambda_1}\right)^p = p(s+m)$ d'où, d'après (4), $s + \tilde{m} = ps + pm$, soit

$$\tilde{m} = pm + ps - s = \delta(m);$$

— si $s + m > pe'_k = e'_K$:

$$d_K\left(\frac{\sigma\lambda_1}{\lambda_1}\right)^p = s + m + e_K, \quad \text{d'où } s + \tilde{m} = s + m + e_K,$$

$$\text{soit } \tilde{m} = m + e_K = \delta(m);$$

— si $s + m = pe'_k = e'_K$:

$$d_K\left(\frac{\sigma\lambda_1}{\lambda_1}\right)^p \geqslant pe'_K, \quad \text{d'où } s + \tilde{m} > p(s+m) \text{ et } \tilde{m} \geqslant \delta(m).$$

Nous avons ainsi montré que $\eta(\Gamma_k^m) \subset \Gamma_K^{\delta(m)}$ pour tout $m \in D(k)$ (en tenant compte de (i) et (ii)). Comme $\delta$ est une fonction strictement croissante et $\delta(n)$ est entier si $n$ est entier, on en déduit que $\eta(\Gamma_k^{m+1}) \subset \Gamma_K^{\delta(m)+1}$ pour tout $m \in D(k)$.

Déterminons l'application $\eta^m$: $\Gamma_k^m \to \Gamma_K^{\delta(m)}$ pour $m \in D(k) - \{0, pe'_k\}$. Pour cela, revenons à la décomposition (3), où $\tilde{m}$ est quelconque.

(a) Si $s + m < pe'_k$.

Si $\tilde{m} \geqslant pe'_K$, on aurait d'après (4): $p(s+m) \geqslant s + \tilde{m}$ d'où $\delta(m) \geqslant pe'_K$; impossible. Donc $\tilde{m} < pe'_K$ et $\tilde{m} \not\equiv 0 \pmod p$, et d'après (4), $\tilde{m} = pm + ps - s$.

Posons:

$$\lambda = 1 + a\varpi^m, \quad a \in U_k,$$

$$\lambda_1 = 1 + a\pi^m, \quad a \in U_K, \quad \bar{a}^p = \bar{a},$$

$$\tilde{\lambda} = 1 + b\pi^{\tilde{m}}, \quad b \in U_K.$$



D'après le lemme 3.1.3, on a:

$$\frac{\sigma\lambda_1}{\lambda_1} \equiv 1 + ma\varepsilon\pi^{s+m} \quad \text{et} \quad \frac{\sigma\tilde{\lambda}}{\tilde{\lambda}} \equiv 1 + \tilde{m}b\varepsilon\pi^{s+\tilde{m}}.$$

D'après le théorème 1.2, comme $s + m < e'_K$, on a:

$$\left(\frac{\sigma\lambda_1}{\lambda_1}\right)^p \equiv 1 + m^p a^p \varepsilon^p \pi^{p(s+m)},$$

d'où, d'après (4):

$$\bar{m}^p \bar{a}^p \bar{\varepsilon}^p + \bar{\tilde{m}}\bar{b}\bar{\varepsilon} = 0$$

soit, puisque $\bar{\tilde{m}} = -\bar{s}$:

$$\bar{b} = m\frac{\bar{\varepsilon}^{p-1}}{\bar{s}}\bar{a}.$$

(b) Si $s + m > pe'_k = e'_K$.

Avec les même notations que dans (a), des calculs analogues donnent

$$\tilde{m} = m + e_K \quad \text{et} \quad \bar{b} = -\bar{A}\bar{a}^{1/p}.$$

(c) Si $s + m = pe'_k = e'_K$.

Avec les mêmes notations que précèdemment, d'après 1.2, on a:

$$\left(\frac{\sigma\lambda_1}{\lambda_1}\right)^p \equiv 1 + (m^p a^p \varepsilon^p + ma\varepsilon A)\pi^{p(s+m)}. \tag{5}$$

Soit $Q$ l'application de $\bar{k}$ dans $\bar{k}$ définie par:

$$Q(\bar{a}) = \bar{\varepsilon}^{p-1}\bar{a} + \bar{A}\bar{a}^{1/p}.$$

Montrons que $\mathrm{Ker}Q = \mathrm{Ker}\eta^m$:

— si $Q(\bar{a}) = 0$: alors $d_K\left(\frac{\sigma\lambda_1}{\lambda_1}\right)^p > p(s+m)$ d'après (5).

Si $\tilde{m} \geqslant pe'_K$, $\mathrm{def}_K\lambda = \tilde{m} > \delta(m)$ et $\bar{\lambda} \in \mathrm{Ker}\eta^m$. Si $\tilde{m} < pe'_K$, $\tilde{m} \not\equiv 0 \pmod p$ et d'après (4), on a: $s + \tilde{m} = d_K\left(\frac{\sigma\lambda_1}{\lambda_1}\right)^p$, d'où $\tilde{m} > \delta(m)$ et $\bar{\lambda} \in \mathrm{Ker}\eta^m$.

— si $Q(\bar{a}) \neq 0$: alors $d_K\left(\frac{\sigma\lambda_1}{\lambda_1}\right)^p = p(s+m)$ d'après (5).

Si $\tilde{m} \geqslant pe'_K$, on aurait, d'après (4): $d_K\left(\frac{\sigma\lambda_1}{\lambda_1}\right)^p \geqslant s + pe'_K$; contradiction.

Donc $\tilde{m} < pe'_K$ et $\tilde{m} \not\equiv 0 \pmod p$ d'où, toujours d'après (4): $s + \tilde{m} = p(s+m)$, soit $\tilde{m} = \delta(m)$ et $\bar{\lambda} \notin \mathrm{Ker}\eta^m$. Dans ce cas, (4) montre que: $\bar{\tilde{m}}\bar{b}\bar{\varepsilon} + \bar{m}^p\bar{a}^p\bar{\varepsilon}^p + \bar{m}\bar{a}\bar{\varepsilon}\bar{A} = 0$ soit, puisque $\bar{\tilde{m}} = -\bar{s} = \bar{m}$, $\bar{b} = \eta^m(\bar{\lambda}) = -Q(\bar{a})$.

Pour que $\mathrm{Ker}Q \neq (0)$, il faut et il suffit que $-\bar{A} \in \bar{k}^{*p-1}$, c'est-à-dire (lemme de Hensel) que $-\frac{p}{\pi(p-1)e'_K} \in k^{*p-1}$, ou encore $-p \in k^{*p-1}$, et

on sait que cette dernière condition équivaut à: „$k$ contient les racines $p$-ièmes de 1".

Si tel est le cas $\mathrm{Ker}\,\eta^m \neq (0)$, donc est cyclique d'ordre $p$. L'image de $\eta^m$ est celle de $Q$, donc $\mathrm{Coker}\,\eta^m \cong \bar{k}/Q(\bar{k})$. Si $\mathrm{Ker}\,Q \neq (0)$, soit $\bar{a}_0 \neq 0$ tel que $Q(\bar{a}_0) = 0$.

Alors $Q(\bar{a}) = \varepsilon^{p-1}\bar{a}_0\left(\dfrac{\bar{a}}{a_0} - \left(\dfrac{\bar{a}}{a_0}\right)^{1/p}\right)$, ce qui montre que $\mathrm{Coker}\,\eta^m = \bar{k}/P(\bar{k})$, où $P$ est le polynôme $P(X) = X^p - X$. ∎

**3.3. Cas d'une $p$ extension totalement ramifiée de $k$.** Soit $K$ une extension galoisienne de $k$, de degré $p^n$, totalement ramifiée ($n \geqslant 1$). Soient $\psi = \psi_{K/k}$ et $\eta = \eta_{K/k}$ et $\delta = \delta_{K/k}$.

**3.3.1.** Théorème. *Pour tout $m \in D(k)$, $\eta(\Gamma_k^m) \subset \Gamma_k^{\delta(m)}$ et $\eta(\Gamma_k^{m+1}) \subset \Gamma_k^{\delta(m)+1}$.*

Démonstration. C'est immédiat, par dévissage, en tenant compte de la transitivité de la fonction $\delta$. ∎

Le théorème précèdent permet de définir, par passage au quotient, des homomorphismes $\eta_{K/k}^m$: $\bar{\Gamma}_k^m \to \bar{\Gamma}_K^{\delta(m)}$, pour tout $m \in D(k)$. Ces homomorphismes peuvent être déterminés par dévissage à partir de la proposition 3.1.2. Nous avons par exemple les résultats suivants:

**3.3.2.** Proposition. *En conservant les hypothèses et les notations du théorème* 3.3.1, *désignons par $s_1 < s_2 < \ldots < s_r$ les sauts inférieurs de ramification de l'extension $K/k$ et par $G_{s_j}$, $1 \leqslant j \leqslant r$, les groupes de ramification. Alors*:

(i) *Si $e_k'$ est un entier $\eta^{pe_k'}$ est un isomorphisme.*

(ii) *$\eta^0$ est trivial si les sauts $s_j$ sont multiples de $p$, injectif sinon.*

(iii) *Si $k$ contient le groupe $E_p$ des racines $p$-ièmes de* 1, *pour tout $m \in D(k) - \{0, pe_k'\}$ tel que $\psi(pe_k' - m) = s_j$, $1 \leqslant j \leqslant r$, $\mathrm{Ker}\,\eta^m$ est d'ordre égal à $(G_{s_j} : G_{1+s_j})$.*

(iv) *Pour tout $m \in D(k) - \{0, pe_k'\}$, si $k$ ne contient pas $E_p$ ou si $\psi(pe_k' - m)$ est distinct de toutes les valeurs $s_j$, $\eta^m$ est un isomorphisme de $\bar{\Gamma}_k^m$ sur $\bar{\Gamma}_K^{\delta(m)}$.*

Démonstration. (i) et (ii) résultant immédiatement de 3.1.2, par dévissage. Nous allons démontrer les assertions (iii) et (iv) par récurrence, si $k$ contient $E_p$.

Si $K/k$ est de degré $p$, ces assertions sont vraies d'après 3.2.2.

Supposons $K/k$ de degré $p^n$, $n > 1$. Soit $G = \mathrm{Gal}(K/k)$. Soit $H$ un sous-groupe normal d'ordre $p$, contenu dans $G_{s_r}$. Soit $M$ le corps fixe de $H$. On sait que $H$ possède un seul saut de ramification, qui est $s_r$. D'après le théorème de Herbrand, il est immédiat que $(G/H)_{s_j} = G_{s_j}/H$ pour tout $1 \leqslant j \leqslant r$.



Posons

$$\psi = \psi_{K/k}, \quad \psi' = \psi_{M/k}, \quad \psi'' = \psi_{K/M},$$

$$\eta^m = \eta_{K/k}^m, \quad \eta' = \eta_{M/k}^m, \quad \eta'' = \eta_{K/M}^{m'}, \quad \text{où} \quad m' = \delta_{M/k}(m).$$

On a

$$\psi = \psi'' \circ \psi' \quad \text{et} \quad \eta^m = \eta'' \circ \eta'.$$

Si $\psi(pe_k' - m) = s_j$, distinguons trois cas:

— si $j < r$: alors par l'hypothèse de récurrence, $\mathrm{Ker}\,\eta'$ est d'ordre égal à $\left((G/H)_{s_j} : (G/H)_{1+s_j}\right) = (G_{s_j} : G_{1+s_j})$ et $\eta''$ est un isomorphisme, et (iii) est démontrée;

— si $j = r$ et $G_{s_r} = H$, $\mathrm{Ker}\,\eta''$ est d'ordre égal à $(H : 1) = (G_{s_r} : 1)$ et $\eta'$ est un isomorphisme, et (iii) est démontrée;

— si $j = r$ et $G_{s_r} \neq H$, $\mathrm{Ker}\,\eta''$ est d'ordre égal à $(H : 1)$ et $\mathrm{Ker}\,\eta'$ est d'ordre égal à $(G_{s_r}/H : 1) = (G_{s_r} : H)$, d'où on voit facilement que $\mathrm{Ker}\,\eta^m$ est d'ordre égal à $(G_{s_r} : 1)$, et (iii) est démontrée.

L'assertion (iv) se démontre de la même façon. ∎

Remarquons que, pour tout $m \in D(k) - \{pe_k', 0\}$, $\eta^m$ est représenté dans $\bar{k}$, modulo des élévations à la puissance $p$-ième (qui sont des automorphismes de $\bar{k}$), par un polynôme additif. Il en résulte que, si $\bar{k}$ est un corps quasi fini, $\mathrm{Ker}\,\eta^m$ et $\mathrm{Coker}\,\eta^m$ sont équipotents ([5], p. 231). Nous expliquerons cette propriété de façon plus canonique au § suivant.

**3.4. Relations avec la norme.** L'intervention de la fonction $\psi$, ainsi que la ressemblance des applications $\eta^m$ avec les applications déduites de la norme ([5], chap. 5) demandent à être expliquées. Pour éclaircir la situation, nous supposerons dans tout le § 3.4 que le corps résiduel $\bar{k}$ est *quasi-fini* et que $k$ contient $E_p$ des racines $p$-ièmes de l'unité. Nous avons alors notre disposition le symbole local $(\cdot, \cdot)_k$ de $k^* \times k^*$ dans $E_p$ ([5], chap. 14). Nous pouvons considérer $\Gamma_K$ comme espace vectoriel sur le corps premier $\boldsymbol{F}_p$. En identifiant $E_p$ à $\boldsymbol{F}_p$ par le choix d'une racine primitive, le symbole local devient, après passage au quotient mod $k^{*p}$, une forme binéaire non dégénérée $\Gamma_k \times \Gamma_k \to \boldsymbol{F}_p$, que nous continuerons à noter $(\cdot, \cdot)_k$.

**3.4.1.** La filtration orthogonale. Pour tout sous-ensemble $A$ de $\Gamma_k$, posons $A^\perp = \{a \in \Gamma_k;\ (a, \beta)_k = 0 \text{ pour tout } \beta \in A\}$.

**3.4.1.1.** Proposition. *Pour tout entier $0 \leqslant m \leqslant pe_k'$, $(\Gamma_k^m)^\perp = \Gamma_k^{M+1}$ où $M = pe_k' - m$.*

Démonstration. Pour tous $\bar{\lambda}$, $\bar{\mu} \in \Gamma_k$, soient $\lambda$ et $\mu$ respectivement deux représentants dans $k^*$. Pour $(\bar{\lambda}, \bar{\mu})_k = 0$, il faut et il suffit que $\mu$ soit une norme de $L = k(\lambda^{1/p})$ à $k$. Si $L/k$ est non ramifiée, on sait que $U_K \subset NL^*$.

De plus d'après une propriété de ramification que nous citerons plus loin (section 4), l'extension $L/k$ est totalement ramifiée si et seulement si $\mathrm{def}_k\lambda < pe'_k$, auquel cas l'unique saut de ramification de $L/k$ est égal à $pe'_k - \mathrm{def}_k\lambda$ et le conducteur de $L/k$ (i.e. le plus petit entier $f$ tel que $U'_k \subset NL^*$) est égal à $pe'_k - \mathrm{def}_k\lambda + 1$ ([5], p. 234, corol. 2).

La proposition en résulte. ■

Remarquons qu'une conséquence immédiate de cette proposition est que $\dim \Gamma_k^{pe'_k} = \mathrm{codim}\,\Gamma_k^1 = 1$, autrement dit, $\Gamma_k^{pe'_k}$ est un groupe d'ordre $p$.

**3.4.1.2.** Proposition. *Soit $K/k$ une $p$-extension totalement ramifiée, de groupe de Galois $G$. Soit $\psi = \psi_{K/k}$. Pour tout entier $m \in D(k) - \{0, pe'_k\}$, le dual de* $\mathrm{Coker}\,\eta^m$ *s'identifie à $G_{\psi(M)}/G_{\psi(M)+1}$, où $M = pe'_k - m$.*

Démonstration. Pour tout $\boldsymbol{F}_p$ — espace vectoriel $A$, on notera $\hat{A}$ l'espace dual.

Soit la suite exacte: $\Gamma_k^m \xrightarrow{\eta^m} \Gamma_K^{\delta(m)} \to C \to 0$, où $C = \mathrm{Coker}\,\eta^m$. On en tire, par dualité, la suite exacte:

$$0 \to \hat{C} \to \hat{\Gamma}_K^{\delta(m)} \to \hat{\Gamma}_k^m. \tag{1}$$

Or par orthogonalité et dualité, il est facile de voir que $\Gamma_k^M$ est isomorphe à $\hat{\Gamma}_k^m$, 'isomorphisme étant défini par:

$$\bar{\alpha} \in \Gamma_k^M \mapsto (\bar{\alpha}, \cdot)_k \in \hat{\Gamma}_k^m$$

avec $(\bar{\alpha}, \bar{\beta})_k = (\alpha, \beta)_k$, où $\alpha$ et $\beta$ représentent respectivement $\bar{\alpha}$ et $\bar{\beta}$ dans $\Gamma_k^M$ et $\Gamma_k^m$. De même, $\Gamma^{\psi(M)}$ est isomorphe à $\hat{\Gamma}^{\delta(m)}$ (en se rappelant que $\delta(m) = pe'_K - \psi(M)$). Par isomorphisme, la suite exacte (1) devient donc:

$$0 \to \hat{C} \to \Gamma_K^{\psi(M)} \xrightarrow{\nu} \Gamma_k^M, \tag{2}$$

la flèche $\nu$ étant définie de la façon suivante:

Pour tout $\bar{\alpha} \in \Gamma_K^{\psi(M)}$ et tout $\bar{\beta} \in \Gamma_k^M$, $(\nu\bar{\alpha}, \bar{\beta})_k = (\bar{\alpha}, \eta^m\bar{\beta})_K = (\alpha, \eta\beta)_K$, $\alpha$ et $\beta$ représentant respectivement $\bar{\alpha}$ et $\bar{\beta}$ dans $\Gamma_K^{\psi(M)}$ et $\Gamma_K^M$. D'après une propriété connue du symbole local, $(\alpha, \eta\beta)_K = (N\alpha, \beta)_k$ où $N$ désigne la norme de $K$ à $k$. Donc, en identifiant canoniquement $\Gamma_K^{\psi(M)}$ (resp. $\Gamma_k^M$) à $\overline{U}_K^{\psi(M)}$ (resp. $\overline{U}_k^M$), l'homomorphisme $\nu$ s'identifie à l'homomorphisme $N_M$ déduit de la norme. Il en résulte, d'après la suite exacte connue $0 \to G_{\psi(M)}/G_{\psi(M)+1} \to \overline{U}_K^{\psi(m)} \xrightarrow{N_m} \overline{U}_k^m$ ([5], p. 99), que $\hat{C}$ s'identifie à $G_{\psi(M)}/G_{\psi(M)+1}$. ■

**3.4.1.3.** Corollaire. *Pour tout $m \in D(k) - \{0, pe'_k\}$,* $\mathrm{Coker}\,\eta^m$ *et* $\mathrm{Ker}\,\eta^m$ *sont d'ordre égal à $(G_{\psi(M)} : G_{\psi(M)+1})$, $M = pe'_k - m$.*

C'est immédiat.

**3.4.2.** Le cas d'une $p$-extension cyclique. Pour clarifier les calculs de la section 4, nous aurons besoin de la proposition (strictement utilitaire) suivante:



Proposition. *Soit $K/k$ une $p$-extension cyclique totalement ramifiée, de groupe de Galois $G$, de sauts supérieurs de ramification $u_1 < u_2 < \ldots < u_n$. Alors:*

(i) *Pour tout $m \in D(k)$ tel que $0 < m < pe'_k - u_n$, $\eta^m_{K/k}$ est un isomorphisme.*

(ii) *Si $u_n < e'_k$, $\mathrm{Im}\,\eta^0_{K/k}$ est isomorphe à $(\Gamma_K^{\delta(0)})^G/(\Gamma_K^{\delta(0)+1})^G$.* (Si $G$ opère sur $A$, $A^G$ désigne l'ensemble des éléments de $A$ laissés fixes par $G$.)

Démonstration. (i) est un cas particulier de 3.3.2 (iv). Montrons (ii). Le groupe $G$ opère sur $\Gamma_K$ par passage au quotient, en laissant stable chaque sous-groupe $\Gamma_K^m$. Posons $h = \delta(0)$. Désignons par $s_i$ les sauts inférieurs. Il est clair que $\eta$ envoie $\Gamma_k^0/\Gamma_k^1$ dans $(\Gamma_K^h)^G/(\Gamma_K^{h+1})^G$. L'hypothèse $u_n < e'_k$ implique $s_n \not\equiv 0 \pmod p$, d'où la suite exacte:

$$0 \to \Gamma_k^0 \xrightarrow{\eta^0} (\Gamma_K^h)^G/(\Gamma_K^{h+1})^G.$$

Pour prouver l'isomorphisme, il faut et il suffit que $(\Gamma_K^h)^G/(\Gamma_K^{h+1})$ soit d'ordre $p$. Or $(\Gamma_K^h)^G = \Gamma_K^h \cap \Gamma_K^G$ et $(\Gamma_K^{h+1})^G = \Gamma_K^{h+1} \cap \Gamma_K^G$. Posons $H = pe'_K - h = \psi(pe'_k)$ et soit $I$ l'idéal d'augmentation de l'algèbre $\boldsymbol{F}_p[G]$ (i.e. l'idéal engendré par $\sigma - 1$, où $\sigma$ est un générateur de $G$). On a: $\Gamma_K^h = (\Gamma_K^{H+1})^\perp$ et $\Gamma_K^{h+1} = (\Gamma_K^H)^\perp$ (d'après 3.4.1.1) et $\Gamma_K^G = (I\Gamma_K)^\perp$ (d'après la propriété $(\sigma a, \sigma b)_K = (a, b)_K$ pour tous $a, b$, qui provient elle-même d'une propriété connue du symbole local). On en tire:

$$(\Gamma_K^h)^G = (\Gamma_K^{H+1} \cdot I\Gamma_K)^\perp \quad \text{et} \quad (\Gamma_K^{h+1})^G = (\Gamma_K^H \cdot I\Gamma_K)^\perp.$$

Or, par orthogonalité et dualité, on voit facilement que

$$(\Gamma_K^{H+1} \cdot I\Gamma_K)^\perp/(\Gamma_K^H \cdot I\Gamma_K)^\perp$$

s'identifie au dual de $\Gamma_K^H \cdot I\Gamma_K/\Gamma_K^{H+1} \cdot I\Gamma_K$, qui est lui même isomorphe (par application répétée des isomorphes standard) à $(\Gamma_K^H/\Gamma_K^{H+1})/(\Gamma_K^H \cap I\Gamma_K)/(\Gamma_K^{H+1} \cap I\Gamma_K)$. Or:

Lemme. *Si $H = \psi(pe'_k)$, la suite*

$$0 \to \Gamma_K^H \cap I\Gamma_K/\Gamma_K^{H+1} \cap I\Gamma_K \xrightarrow{j} \Gamma_K^H/\Gamma_K^{H+1} \xrightarrow{N} \Gamma_k^{pe'_k} \to 0$$

*(où $N$ est induite par la norme) est exacte.*

Démonstration du lemme. L'injection et la surjection sont évidentes. Montrons l'exactitude en $\overline{\Gamma}_K^H$. Il est clair que $\mathrm{Im}\,j \subset \mathrm{Ker}\,N$. Réciproquement, si $\bar{x} \in \mathrm{Ker}\,N$, cela veut dire que $\bar{x}$ est représenté par $x \in U_K^{\psi(pe')}$ tel que $Nx \in U_k^{pe'}$ est une puissance $p$-ième, donc $Nx = y^p$, $y \in U_k^{e'}$. Comme $u_n < e'$, la norme de $U_k^{\psi(e')}$ dans $U_k^{e'}$ est surjective ([5], p. 101), donc $y = Nz$ et $N(xz^{-p}) = 1$. D'après le théorème 90 de Hilbert, il s'ensuit que $\bar{x} \in \Gamma_K^H \cap I\Gamma_K$. ■

Il résulte du lemme que le groupe

$$(\Gamma_K^H/\Gamma_K^{H+1})/(\Gamma_K^H \cap I\Gamma_K)/(\Gamma_K^{H+1} \cap I\Gamma_K)$$

est d'ordre $p$. ■

**4. Ramification dans les $p$-extensions cycliques.** $L$ désignant une $p$-extension cyclique de $k$, on se propose de déterminer les conditions nécessaires et suffisantes que vérifient les sauts de ramification de $L/k$. Les condition nécessaires sont données par le théorème suivant:

**4.1.** THÉORÈME. *Soit $L$ une extension cyclique de degré $p^{n+1}$ de $k$, totalement ramifiée, de sauts supérieurs de ramification $u_1 < u_2 < \ldots < u_{n+1}$. Alors:*

(i) $u_1 \in D(k)$,

(ii) *si* $u_n \geqslant e'_k$, $u_{n+1} = u_n + e_k$,

(iii) *si* $u_n < e'_k$, $pu_n \leqslant u_{n+1} \leqslant pe'_k$, *avec* $u_{n+1} \not\equiv 0 \pmod p$ *si les inégalités sont strictes.*

(Pour la démonstration, cf. par exemple [1], propos. 4–3, qui se ramène au cas où le corps résiduel est algébriquement clos et utilise de classes „géométrique".)

La réciproque du théorème précèdent, dans le cas où $k$ ne contient pas le groupe $E_p$ des racines $p$-ièmes de l'unité et $\bar{k}$ est fini, a été entièrement résolu par E. Maus ([3], § 6). Nous nous proposons ici d'étudier le cas où $k$ contient $E_p$ et $\bar{k}$ est parfait. Nous supposerons donnée une extension $K/k$ cyclique de degré $p^n$, totalement ramifiée, de sauts supérieurs de ramification $u_1 < u_2 < \ldots < u_n$, et nous chercherons à construire les extensions $L/K$ cycliques de degré $p^{n+1}$ contenant $K$.

D'abord quelques lemmes techniques purement algébriques:

**4.2.** LEMME. *Soit $K/k$ une extension cyclique de degré $p^n$, et soit $\sigma$ un générateur de $\mathrm{Gal}(K/k)$. Soit $L = K(\alpha)$, $\alpha^p = a \in K^*$, une extension cyclique de degré $p$ de $K$. Alors $L/k$ est galoisienne de degré $p^{n+1}$ si et seulement si $\sigma a/a = x^p$, $x \in K^*$, et $L/k$ est cyclique si et seulement si, en plus, $N_{K/k}(x) \neq 1$.*

Démonstration. C'est un exercice facile de théorie de Galois (cf. [6], p. 146).

**4.3.** LEMME. *Soit $K/k$ cyclique de degré $p^n$. Soient $L_0 = K(\alpha)$, $\alpha^p = a \in K^*$, et $L_1 = K(\beta)$, $\beta^p = b \in K^*$, deux extensions cycliques de degré $p$ de $K$. Supposons que $L_0/k$ est cyclique de degré $p^{n+1}$. Alors, pour que $L_1/k$ soit cyclique de degré $p^{n+1}$, il faut et il suffit qu'il existe un entier $i \not\equiv 0 \pmod p$ et un élément $\lambda$ de $k^*$ tel que $a^{-1}(\lambda b^i) \in K^{*p}$.*

Démonstration. Soit $\sigma$ un générateur de $\mathrm{Gal}(K/k)$. D'après le lemme précèdent, on sait que $L_1/k$ est cyclique si et seulement si $\sigma b/b = y^p$, $y \in K^*$ et $N_{K/k}(y) = \xi$, une racine primitive $p$-ième de l'unité contenue dans $k^*$. De même, $L_0/k$ est cyclique si et seulement si $\sigma a/a = x^p$, $x \in K^*$ et $N_{K/k}(x) = \xi^i$, $i \not\equiv 0 \pmod p$. Mais $N_{K/k}(x) = \xi^i$ équivaut à $x = y^i \sigma c/c$, $c \in K^*$ et le lemme à démontrer s'ensuit immédiatement. ∎

Nous aurons également besoin du théorème suivant, qui relie la notion de défaut à celle de sauts de ramification:



**4.4.** THÉORÈME. *Soit $K = k(\alpha)$, $\alpha^p = a \in K^*$, une extension cyclique de degré $p$ de $k$. Alors $K/k$ est totalement ramifiée si et seulement si $\mathrm{def}_k(a) < pe'_k$. Dans ce cas, l'unique saut de ramification $s$ de $K/k$ est donné par $s = pe'_k - \mathrm{def}_k(a)$.*

Démonstration, cf. par exemple [6], p. 144.

Nous pouvons maintenant attaquer la réciproque du théorème 4.1 (ii).

**4.5.** THÉORÈME. *Soit $K/k$ cyclique de degré $p^n$, totalement ramifié, de sauts supérieurs de ramification $u_1 < u_2 < \ldots < u_n$. On suppose $u_n < e'_k$. Alors pour tout entier $u$ tel que $pu_n \leqslant u \leqslant pe'_k$ et $u \not\equiv 0 \pmod p$ si $pu_n < u < pe'_k$, il existe une extension $L$ de $k$, cyclique de degré $p^{n+1}$, contenant $K$, et dont le dernier saut supérieur de ramification est égal à $u$.*

Démonstration. Soit $G = \mathrm{Gal}(K/k)$ et soit $\sigma$ un générateur de $G$. Désignons par $s_1, s_2, \ldots, s_n$ les saut inférieurs de ramification de $K/k$ rangés par ordre croissant. Nous ferons la démonstration en trois étapes.

(i) Soit $\xi$ une racine primitive $p$-ième de 1 contenue dans $k^*$. On sait que $d_k(\xi) = e'_k$. Par hypothèse, $e'_k > u_n$, ce qui équivaut à $\psi_{K/k}(e'_k) > s_n$, donc ([5], chap. 5) il existe $x \in U_K^{v(e')}$ tel que $N_{K/k}(x) = \xi$.

D'après le théorème 90 de Hilbert, $x^p$ est de la forme $x^p = \sigma a/a$, $a \in K^*$, et d'après le lemme 4.2, l'extension $L = K(a^{1/p})$ est cyclique de degré $p^{n+1}$ sur $k$.

Soit $\mathscr{U}(K/k)$ l'ensemble de toutes les valeurs que peuvent prendre les derniers sauts supérieurs de ramification des surextensions cycliques $L/k$ de degré $p^{n+1}$ de $K/k$. Soit $u^0_{n+1}$ le plus petit élément de $\mathscr{U}$ et soit $L_0/k$ une extension cyclique de degré $p^{n+1}$ contenant $K$ et admettant $u^0_{n+1}$ pour dernier saut supérieur.

Montrons les trois assertions suivantes:

(a) $pe'_k \in \mathscr{U}$,

(b) si $\mathscr{U} \neq \{pe'_k\}$, $u^0_{n+1} = pu_n$,

(c) si $\mathscr{U} \neq \{pe'_k\}$, tout entier $u$ tel que $pu_n \leqslant u \leqslant pe'_k$ et $u \not\equiv 0 \pmod p$ si $pu_n < u < pe'_k$, appartient à $\mathscr{U}$.

(a) L'extension $L_0$ de $k$ que nous avons choisie est de la forme $L_0 = K(\alpha)$, $\alpha^p = a_0 \in K^*$. Soit $\lambda \in k^*$ tel que $\mathrm{def}_k(\lambda) = 0$, et soit $b = \lambda a_0$. Soit $L = K(\beta)$, $\beta^p = b$. Alors $L/k$ est cyclique de degré $p^{n+1}$ (lemme 4.3). Soient $s_{n+1}$ et $u_{n+1}$ les derniers sauts inférieurs de $L/K$. D'après le théorème 4.4, on a:

$$s_{n+1} = pe'_K - \mathrm{def}_K b \quad \text{et} \quad s^0_{n+1} = pe'_K - \mathrm{def}_K a_0.$$

— si $u^0_{n+1} = pe'_k$, on a, $pe'_k \in \mathscr{U}$ et il n'y a rien à montrer;

— si $u^0_{n+1} < pe'_k$, cela se traduit en termes de sauts inférieurs par:

$$s^0_{n+1} = pe'_K - \mathrm{def}_K a_0 < \psi(pe'_k),$$

d'où $\mathrm{def}_K a_0 > \delta(0) = \mathrm{def}_K \lambda$ et $\mathrm{def}_K b = \mathrm{def}_K \lambda$.

Il en résulte que

$$s_{n+1} = \psi(pe'_k) \quad \text{et} \quad u_{n+1} = pe'_k.$$

On a ainsi montré que $\mathscr{U}$ contient toujours l'entier $pe'_k$.

(b) Supposons $\mathscr{U} \neq \{pe'_k\}$. Alors $u^0_{n+1} < pe'_k$. D'après la partie directe, on sait que $u^0_{n+1} \geqslant pu_n$, avec $u^0_{n+1} \not\equiv 0 \pmod p$ si $u^0_{n+1} > pu_n$.

Si $u^0_{n+1} > pu_n$, on pourrait écrire $u_{n+1} = pe'_k - m$, $m \not\equiv 0 \pmod p$, $0 < m < p(e'_k - u_n)$, d'où

$$\mathrm{def}_K a_0 = pe'_K - \psi(pe'_k - m) = \delta(m).$$

D'après 3.4.2, $\eta^m$ est un isomorphisme, donc $a_0 = \lambda b c^p$, avec $\lambda \in k^*$, $b \in K^*$, $\mathrm{def}_K b > \mathrm{def}_K a_0$ et $\mathrm{def}_k \lambda = m$. L'extension $L = K(\beta)$, $\beta^p = b$, est cyclique de degré $p^{n+1}$ sur $k$ (lemme 4.3), et son dernier saut supérieur est

$$u_{n+1} = \varphi(pe'_k - \mathrm{def}_K b) < \varphi(pe'_K - \mathrm{def}_K a_0) = u^0_{n+1};$$

contradiction. Donc $u^0_{n+1} = pu_n$ si $\mathscr{U} \neq \{pe'_k\}$.

(c) Supposons $\mathscr{U} \neq \{pe'_k\}$. Tout entier $u$ tel que $pu_n < u < pe'_k$, $u \not\equiv 0 \pmod p$, peut s'écire $u = pe'_k - m$, avec $u < m < p(e'_k - u_n)$, $m \not\equiv 0 \pmod p$. Soit $\lambda \in k^*$ tel que $\mathrm{def}_k \lambda = m$ et soit $b = a_0 \lambda$. Comme $\eta^m$ est un isomorphisme (3.4.2 (i)), $\mathrm{def}_K \lambda = \delta(m)$, et comme $u^0_{n+1} = pu_n$ (d'après (b)), $\mathrm{def}_K a_0 = pe'_K - \psi(pu_n) > \delta(m)$, d'où $\mathrm{def}_K b = \mathrm{def}_K \lambda = \delta(m)$. L'extension $L = K(\beta)$, $\beta^p = b$, est cyclique de degré $p^{n+1}$ sur $k$, et son dernier saut supérieur est $u_{n+1} = \varphi(pe'_K - \delta(m)) = pe'_k - m = u$.

(iii) Pour terminer la démonstration du théorème, il reste à prouver que $\mathscr{U} \neq \{pe'_k\}$. On a vu dans (ii) qu'il existe $a_0 \in K^*$ tel que l'extension $K(a_0^{1/p})$ est cyclique de degré $p^{n+1}$ sur $k$, de dernier saut supérieur égal à $pe'_k$, ce qui correspond à $\mathrm{def}_K a_0 = \delta(0)$. Pour que $\mathscr{U} \neq \{pe'_k\}$, il faut et il suffit qu'il existe $\lambda \in k^*$ tel que $\mathrm{def}_k(\lambda a_0^j) > \delta(0)$, pour un certain entier $j \not\equiv 0 \pmod p$. Cela revient à prouver que l'image $\bar{a}_0$ de $a_0$ dans $\bar{I}_K^{\delta(0)}$ appartient à $\mathrm{Im}\,\eta^0$. Une condition clairement suffisante pour cela (et on voit facilement qu'elle est nécessaire) est que $\mathrm{Im}\,\eta^0 \cong (I_K^{\delta(0)})^G/(I_K^{\delta(0)+1})^G$

— si le corps résiduel $\bar{k}$ est quasi-fini, cette condition est réalisée (3.4.2 (ii));

— si $\bar{k}$ n'est pas quasi-fini, on peut appliquer une méthode de réduction due à Shankar Sen. Il existe un corps quasi-fini $\bar{k}_1$ et une extension $K_1/k_1$ tels que:

(a) $k_1$ est une extension totalement ramifiée finie du corps de Witt de $\bar{k}_1$,

(b) $K_1$ est une extension totalement ramifiée finie de $k_1$,

(c) $K$ (resp. $k$) est la complétion de l'extension maximale non ramifiée de $K_1$ (resp. $k_1$).



(Pour des détails, voir [4], lemme 2.0.)

Il s'ensuit que pour toute extension $L_1/k_1$, cyclique de degré $p^{n+1}$ contenant $K_1$, si l'on pose $L = L_1 \cdot K$, les groupes $\mathrm{Gal}(L/k)$ et $\mathrm{Gal}(L_1/k_1)$ sont isomorphes en tant que groupes filtrés par leurs groupes de ramification. Comme $\mathscr{U}(K_1/k_1) \neq \{pe'_{k_1}\}$, on aura $\mathscr{U}(K/k) \neq \{pe'_k\}$. ■

**4.6.** Remarque. L'assertion (ii) du théorème 4.1 admet-elle une réciproque? Avec les notations de la proposition 4.5, supposons $u_n > e'_k$. Alors il peut arriver que $K$ n'admet aucune surextension $L$ cyclique de degré $p^{n+1}$ sur $k$.

Prenons par exemple pour $k$ un corps p-adique contenant le groupe $E_p$ mais pas le groupe $E_{p^2}$ (groupe des racines $p^2$-ièmes de 1). Soit $K/k$ une extension cyclique de degré $p$. D'après le lemme 4.2, pour que $K/k$ soit contenue dans une extension $L/k$ cyclique de degré $p^2$, il faut et il suffit que $E_p \subset N_{K/k}K^*$. Si cela était vrai de toutes les extensions cycliques de degré $p$ de $k$, le groupe $E_p$ serait contenu dans l'intersection des groupes de normes de ces extensions. Or l'on sait, d'après le corps de classes local, que cette intersection et $k^{*p}$. Il en résulterait que $E_p \subset k^{*p}$, d'où $E_{p^2} \subset k^*$, contrairement à l'hypothèse.

On peut cependant donner la réciproque partielle suivante (dont on peut voir facilement qu'elle résulte aussi du théorème de Herbrand):

**4.7.** Proposition. *Soit $K/k$ une extension cyclique de degré $p^n$, totalement ramifiée, de sauts supérieurs de ramification $u_1 < u_2 < \ldots < u_n$. Soit $L/k$ une extension galoisienne de degré $p^{n+1}$, contenant $K$, de dernier saut supérieur $u_{n+1}$. Si $u_n > e'_k$ et $u_{n+1} > pe'_k$, alors $L/k$ est cyclique et $u_{n+1} = u_n + e_k$.*

Démonstration. Soit $L = K(\alpha)$, $\alpha^p = a \in K^*$. Soit $\sigma$ un générateur de $\mathrm{Gal}(K/k)$. D'après le lemme 4.3, $\sigma a/a = w^p$, $x \in K^*$. Si $L/k$ n'est pas cyclique, $N_{K/k}(x) = 1$ donc $x = b/\sigma b$, $b \in K^*$ (théorème 90 de Hilbert) et par suite $a = \lambda b^p$, $\lambda \in k^*$. Il en résulte que $\mathrm{def}_K a = \mathrm{def}_K \lambda \geqslant \delta(0)$. En désignant par $s_i$ les sauts inférieurs de $L/k$ on a alors $u_{n+1} = \varphi(s_{n+1}) = \varphi(pe'_k - \mathrm{def}_K a) \leqslant \varphi\psi(pe'_k) = pe'_k$, ce qui contredit l'hypothèse. Donc $L/k$ est cyclique, et $u_{n+1} = u_n + e_k$ d'après 4.1. ■

**4.8.** Corollaire (cf. aussi [6]; théorème 31). *Soit $K/k$ une extension galoisienne de degré $p^n$, totalement ramifiée, ayant $n$ sauts supérieurs $u_1 < u_2 < \ldots < u_n$ tels que $u_1 > e'_k$ et $u_{j+1} = u_j + e_k$ pour tout $1 \leqslant j \leqslant n-1$. Alors l'extension $L/k$ est cyclique.*

Démonstration. C'est clair, par récurrence à partir de la proposition précédente.

Acknowledgements. Nous tenons ici à remercier J. M. Fontaine pour son aide et ses encouragements.

**Bibliographie**

[1] J. M. Fontaine, *Groupes de ramification et représentations d'Artin*, Ann. Scient. Ec. Norm. Sup., t. 4, fac. 3, 1971, p. 337–392.
[2] H. Hasse, *Zahlentheorie*, Akademie Verlag, Berlin 1949.
[3] E. Maus, *Existenz p-adischer Zahlkörper zu vorgegebenem Verzweigungsverhalten*, Dissertation, Hamburg 1965.
[4] Shankar Sen, *Ramification in p-adic Lie extensions*, Inventiones Math. 50 (1972), p. 44–50.
[5] J. P. Serre, *Corps locaux*, Hermann, Paris 1968.
[6] B. Wyman, *Wildly ramified gamma extensions*, Amer. J. Math., Janv. 1969, p. 135–152.

*Reçu le 9. 12. 1974* (655)

---

ACTA ARITHMETICA
XXX (1976)

# On two conjectures of Kátai

by

P. D. T. A. Elliott (Boulder, Colo.)

**1.** An arithmetical function $f(n)$ is said to be additive if $f(ab) = f(a) + f(b)$ whenever $a$ and $b$ are coprime integers, and completely additive if this relation holds whether they are coprime or not.

In this paper I establish two conjectures of Kátai, the one a particular case of the other.

Let $f(n)$ be an additive arithmetic function. For each real number $x \geqslant 1$ define

$$M(x) = \max_{n \leqslant x} |f(n)|, \qquad E(x) = \max_{p \leqslant x} |f(p+1)|$$

where in the definition of $E(x)$, $p$ runs over prime numbers only.

Theorem. *There are positive absolute constants $A, B$ and $c$, so that*

$$M(x) \leqslant AE(x^B) + AM\big((\log x)^B\big) \qquad (x \geqslant c).$$

Corollary 1. *Let $f(n)$ be a completely additive arithmetic function. Then there are positive constants $A, B$ and $c$ (possibly different from those in the theorem) so that*

$$M(x) \leqslant AE(x^B) \qquad (x \geqslant c).$$

Corollary 2. *Let $f(n)$ be a completely additive arithmetic function and let*

$$|f(p+1)| \leqslant A \log(p+1)$$

*hold for every prime $p$. Then there is a positive absolute constant $B$ so that*

$$|f(n)| \leqslant AB \log n \qquad (n \geqslant 1).$$

Corollary 3. *Let $f(n)$ be completely additive and satisfy*

$$\lim_{p \to \infty} \frac{f(p+1)}{\log p} = 0 \qquad (p \text{ prime}).$$

*Then $f(n)$ is identically zero.*