SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

BRUNO MARTEL

Base normale pour les unités principales

Séminaire de théorie des nombres de Grenoble, tome 4 (1974-1975), exp. n° 3, p. 1-12

<http://www.numdam.org/item?id=STNG_1974-1975__4__A3_0>

Séminaire de Théorie des Nombres
28 novembre 1974
Grenoble

BASE NORMALE POUR LES UNITES PRINCIPALES

par Bruno MARTEL

§ 0 - ENONCE DU PROBLEME.

Soit K un corps p-adique contenant les racines p^s-èmes de 1, mais non les racines p^{s+1}-èmes. K est dit régulier si $s = 0$, irrégulier sinon, et s s'appelle l'exposant d'irrégularité de K.

Le groupe E des unités principales de K (celles qui ont pour image 1 dans le corps résiduel) est un Z_p-module multiplicatif. On sait, depuis Hensel, qu'il est produit direct du groupe cyclique des racines p^s-èmes de 1 et d'un Z_p-module libre de rang N, le degré absolu de K.

On suppose désormais que K est une extension galoisienne finie de k, de groupe de Galois G. Comme G opère Z_p-linéairement sur E, E est un module sur l'algèbre de groupe $\Gamma = Z_p[G]$. Soit ζ une racine primitive p^s-ème de 1 dans K. On dit qu'il existe une base normale pour les unités principales de K/k si le Γ-module $E/\langle\zeta\rangle$ est libre. Son rang est alors égal à n, le degré absolu de k. Donc, n unités principales $(\theta_i)_{1\leq i\leq n}$ forment une base normale de E vis-à-vis de k si toute unité principale θ s'écrit, de manière unique :

$$\theta = \zeta^a \circ \prod_{i=1}^{n} \theta_i^{\gamma_i} \quad , \quad a \in Z/p^sZ \ , \quad \gamma_i \in \Gamma \ .$$

On montre facilement que si le groupe des unités principales de K a une base normale vis-à-vis de k, il en a une vis-à-vis de toute extension intermédiaire K_1, et que, si l'extension K_1/k est galoisienne, le groupe des unités principales de K_1 aussi en a une vis-à-vis de k.

§ 1 - LES PREMIERS RESULTATS.

Ils ont été obtenus par Krasner [K.]

(a) Si p ne divise pas le degré de l'extension, il existe une base normale.

(b) Si K est régulier et l'extension modérément ramifiée, il existe une base normale.

et Gilbarg [G.]

(c) Si K est régulier et s'il existe une base normale, l'extension est modérément ramifiée.

Nous allons montrer qu'il existe toujours un sous-groupe d'indice fini de E ayant une base normale, et donner une démonstration de a) et c).

LEMME 1. *Il existe un sous-groupe d'indice fini de* E *ayant une base normale.*

Soit α un entier de K engendrant une k-base normale de K. Soit $(\beta_i)_{1\leq i\leq n}$ une $\mathbb{Q}_p$-base de k formée d'entiers. Les entiers $(\sigma(\beta_i\alpha))_{\sigma\in G,\,1\leq i\leq n}$ forment une $\mathbb{Q}_p$-base de K, et en divisant chaque $\beta_i\alpha$ par le discriminant de cette base, on obtient une nouvelle base $(\sigma(a_i))$ telle que le Z_p-module $L = \sum_{\sigma,i} Z_p\sigma(a_i)$ contienne les entiers de K. Considérons l'application logarithme : $E \to \operatorname{Log} E$. En multipliant chaque a_i par une puissance convenable de p, on construit une $\mathbb{Q}_p$-base $(\sigma(b_i))$ telle que le Z_p-module $M = \sum_{\sigma,i} Z_p\sigma(b_i)$ soit contenu dans le domaine de convergence de l'exponentielle. Par construction M est d'indice fini dans L, et donc dans $\operatorname{Log} E$. On en déduit que le groupe multiplicatif $\exp M$ est d'indice fini dans E. Or M est un Γ-module libre de base $(b_i)_{1\leq i\leq n}$, donc $\exp M$ est un Γ-module libre de rang n.

COROLLAIRE. *Si* p *ne divise pas le degré de l'extension, il existe une base normale.*

Montrons d'abord que $Z_p[G]$ est un ordre maximal de Z_p dans $\Phi_p[G]$.

Soit $\mathcal{O}$ un ordre contenant $Z_p[G]$ et soit P la matrice de passage, à coefficients dans Z_p , d'une base $(\lambda_i)_{1\le i\le g}$ de $\mathcal{O}$ à la base $(\sigma)_{\sigma\in G}$ de $Z_p[G]$. On a, D désignant le discriminant vis-à-vis de la trace : $D(\sigma\ ;\ \sigma\in G) = (\det P)^2 \times D(\lambda_i\ ,\ i\le g)$. Or $D(\sigma\ ;\ \sigma\in G) = \pm g^g$ est une unité de Z_p puisque p ne divise pas g , l'ordre de G . On en déduit que P est inversible et que $\mathcal{O} = Z_p[G]$.

L'anneau $\Gamma = Z_p[G]$ est donc à idéaux principaux [D. ch.VI] . L est Γ-module libre de rang n , $\operatorname{Log} E$ en est un sous-module. On peut donc trouver n générateurs $(\operatorname{Log}\theta_i)_{1\le i\le n}$ de $\operatorname{Log} E$. Comme le noyau du logarithme est formé des racines p^s-èmes de 1 , on en déduit que toute unité principale θ s'écrit :

$$\theta = \zeta^a \prod_{i=1}^{n} \theta_i^{\gamma_i} \quad , \quad a \in Z/p^sZ \ , \ \gamma_i \in \Gamma \ .$$

Et l'écriture est unique, car les classes modulo $\langle\zeta\rangle$ des unités $(\theta_i^\sigma)_{\sigma\in G\ ,\ 1\le i\le n}$ forment une base du Z_p-module $E/\langle\zeta\rangle$.

LEMME 2. <u>On suppose qu'il existe une base normale pour les unités principales de</u> K/k . <u>Alors le groupe quotient</u> E_k/NE <u>est un groupe cyclique dont l'ordre divise</u> p^r (r <u>exposant d'irrégularité de</u> k).

Soit $(\theta_i)_{1\le i\le n}$ une base normale et $\varepsilon_i = N_{K/k}\theta_i = N\theta_i$.

Soit $\varepsilon \in E_k$, $\varepsilon = \zeta^a \prod_{i=1}^{n} \theta_i^{\gamma_i}$.

Soit $\sigma \in G$, $\varepsilon = \varepsilon^\sigma = \zeta^{\sigma a} \prod_{i=1}^{n} \theta_i^{\sigma\gamma_i}$.

Comme il y a unicité de l'écriture, $\forall i = 1,\dots,n$ et $\forall\sigma \in G$: $\sigma\gamma_i = \gamma_i$. On en déduit que $\gamma_i = a_i T$, où $T = \sum_{\tau\in G} \tau$, et que $\theta_i^{\gamma_i} = \varepsilon_i^{a_i}$.

Donc $\varepsilon = \zeta^a . \prod_{i=1}^{n} \varepsilon_i^{a_i} = \zeta_k^b . N(\prod_i \theta_i^{a_i})$, où ζ_k est une racine primitive p^r-ème de 1 dans k . Le Z_p-module E_k/NE est monogène, engendré par la classe de ζ_k . Il est donc cyclique, d'ordre un diviseur de p^r .

COROLLAIRE. Si K est régulier, et si l'extension K/k est sauvagement ramifiée, il n'existe pas de base normale.

Supposons qu'il existe une base normale. Comme K/k est sauvagement ramifiée, il existe un sous-groupe d'ordre p du groupe d'inertie, et donc une extension intermédiaire K_1 telle que K/K_1 soit totalement ramifiée de degré p . Il existe une base normale pour les unités principales de K/K_1 et, d'après le lemme 2, $E_{K_1} = N_{K/K_1} E$. D'après le corps de classe local, $(K_1^* : N_{K/K_1} K^*) = p$. Or, comme l'extension K/K_1 est totalement ramifiée de degré p , $(K_1^* : N_{K/K_1} K^*) = (E_{K_1} : N_{K/K_1} E)$. On arrive à une contradiction.

En résumé, lorsque K est régulier, il existe une base normale pour les unités principales de K/k si et seulement si K/k est modérément ramifiée. Lorsque K est irrégulier, le résultat précédent est en défaut. On peut montrer simplement qu'il n'existe pas de base normale pour les unités principales de l'extension non ramifiée $\mathbb{Q}_2(\sqrt{-3})/\mathbb{Q}_2$ [G.]. D'autre part, Borevic [B.] donne un exemple d'extension cyclique de degré p totalement ramifiée pour laquelle il existe une base normale. Dans un article ultérieur [B.S.], il caractérise les extensions K/k pour lesquelles il existe une base normale, lorsque K est irrégulier. C'est l'objet de la suite de l'exposé.

§ 2 - LE CAS MODEREMENT RAMIFIE.

On note r et $s \geq 1$ les exposants d'irrégularité de k et K, ζ une racine primitive p^s-ème de 1 dans K , e l'indice de ramification et f le degré résiduel de K/k .

THEOREME 1. Soit K/k une extension galoisienne modérément ramifiée. Si $p \neq 2$ ou si $p = 2$ et $r \geq 2$, il existe une base normale pour les unités principales de K/k si et seulement si p ne divise pas le degré de l'extension $K/k(\zeta)$.

Si $p = 2$ et $r = 1$, une condition nécessaire et suffisante est que le degré de $K/k(\zeta)$ soit impair et que $N_{K/k}(\zeta) = -1$.

Exemples :

1) Soit $p \neq 2$, k l'extension non ramifiée de degré p de $\mathbb{Q}_p$, ζ une racine primitive p-ème de 1, $K = k(\zeta)$.

L'extension $K/\mathbb{Q}_p(\zeta)$ est non ramifiée de degré p. Les exposants d'irrégularité de K et $\mathbb{Q}_p(\zeta)$ sont égaux à 1. Le groupe des unités principales de K n'a donc pas de base normale vis-à-vis de $\mathbb{Q}_p(\zeta)$; ni vis-à-vis de $\mathbb{Q}_p$. Remarquons qu'il existe pourtant une base normale pour les unités principales de $k/\mathbb{Q}_p$ (puisque k est régulier) et de K/k (puisque l'extension est de degré $p-1$). On obtient ainsi un contre-exemple à une éventuelle réciproque de la proposition citée à la fin du § 0.

2) Soit $k = \mathbb{Q}_2(i\sqrt{5}, i\sqrt{2})$ où $i = \sqrt{-1}$, $K = k(i)$.

L'extension K/k est non ramifiée. L'exposant d'irrégularité de k est 1, celui de K est 3 puisqu'il contient $\zeta = \frac{1+i}{\sqrt{2}}$, racine primitive 8-ème de 1. Comme $N_{K/k}(\zeta) = -1$, il existe une base normale.

La condition est suffisante (p impair).

(a) Rappels relatifs aux extensions galoisiennes modérément ramifiées décomposées.

Soit F le corps d'inertie d'une extension galoisienne modérément ramifiée K/k de degré ef. Soit q le cardinal du corps résiduel de k. Soit $G = \mathrm{Gal}(K/k)$ et $G_o = \mathrm{Gal}(K/F)$. On sait que G_o est un groupe cyclique dont l'ordre e divise q^f-1, qu'il est distingué dans G, et que le groupe quotient G/G_o est cyclique d'ordre f [S. ch.IV]. On dit que l'extension K/k est décomposée si G est une extension décomposée de G_o, c'est-à-dire si G est produit semi-direct de G_o par un

sous-groupe isomorphe à G/G_o .

LEMME 3. Les propositions suivantes sont équivalentes :

(i) K/k est décomposée.

(ii) Le Frobenius de F/k se prolonge en un automorphisme de K , d'ordre f .

(iii) Il existe une uniformisante π de K telle que π^e soit une uniformisante de k .

(i) $\Rightarrow$ (ii).

G est produit semi-direct de G_o par H . Soit L le corps fixe par H . Comme $Gal(K/L) \simeq G/G_o \simeq Gal(F/k)$, le résultat est acquis.

(ii) $\Rightarrow$ (iii).

Soit σ un prolongement du Frobénius de F/k en un automorphisme de K , d'ordre f . Soit L le corps fixe par $\langle\sigma\rangle$. L'extension L/k est à la fois totalement et modérément ramifiée, de degré e . Il existe donc une uniformisante π de L (et donc de K) telle que π^e soit une uniformisante de k [W-3-4-3].

(iii) $\Rightarrow$ (i).

Soit π une uniformisante de K telle que π^e soit une uniformisante de k . Soit ξ une racine primitive (q^f-1)-ème de 1 contenue dans K . On a : $F = k(\xi)$ et $K = k(\xi,\pi)$. Soit $L = k(\pi)$ et σ le Frobénius de l'extension non ramifiée K/L . Soit ι un générateur de G_o . Le groupe G est engendré par σ et ι , et l'on a :

$$\xi^\sigma = \xi^q \qquad \pi^\sigma = \pi$$

$$\xi^\iota = \xi \qquad \pi^\iota = \eta\pi \text{ où } \eta \text{ est une racine } e\text{-ème de 1 contenue dans } F .$$

On en déduit que $\sigma\iota\sigma^{-1} = \iota^q$, et que G est produit semi-direct de $\langle\iota\rangle$ par $\langle\sigma\rangle$.

(b) On suppose l'extension K/k décomposée.

On peut supposer que p divise f, sinon le résultat est acquis. Or, sous ces conditions, Iwasawa [I.] montre, en étudiant la structure de E/E^p comme $\mathbb{F}_p[G]$-module, qu'il existe dans le Γ-module E, un sous-module libre E' (de rang n) tel que le quotient E/E' soit cyclique d'ordre p^ℓ. (Remarquer que le lemme 1 démontre l'existence d'un sous-module libre tel que le quotient soit un p-groupe fini). L'homomorphisme canonique de $\langle\zeta\rangle$ dans E/E' est injectif, et donc $\ell \geq s$. Il suffit de montrer que $\ell = s$ pour obtenir le résultat.

Posons $f = g.p$, $\iota = \sigma^g$, où σ est un prolongement d'ordre f du Frobénius de F/k. Soit k' le corps fixe par le groupe d'ordre p engendré par ι. Comme, par hypothèse, p ne divise pas le degré de $K/k(\zeta)$, il ne divise pas celui de $K/k'(\zeta)$. On en déduit que $K = k'(\zeta)$ et que $\zeta^\iota \neq \zeta$ (1). Choisissons dans E une unité η dont la classe modulo E' engendre E/E'. Il existe un entier c, défini modulo p^ℓ, tel que $\eta^\sigma \equiv \eta^c \bmod E'$. Pour toute unité principale θ, $\theta^\sigma \equiv \theta^c \bmod E'$, et en particulier $\zeta^\sigma = \zeta^c$ (2). De $\eta = \eta^{\sigma^f} \equiv \eta^{c^f} \bmod E'$, résulte $c^f \equiv 1 \bmod p^\ell$. Si l'on suppose $\ell > s \geq 1$, de $c^{gp} \equiv 1 \bmod p^\ell$ résulte (car p est impair) $c^g \equiv 1 \bmod p^{\ell-1}$ donc $c^g \equiv 1 \bmod p^s$. Mais, en vertu de (2), $\zeta^\iota = \zeta^{c^g} = \zeta$ ce qui contredit (1).

(c) Il suffit désormais de montrer que toute extension modérément ramifiée K/k (qui satisfait à la condition du théorème 1) se plonge dans une extension modérément ramifiée K'/k décomposée (qui satisfait à la condition du théorème 1).

On prend pour K' l'extension non ramifiée de k de degré e. L'extension K'/k est galoisienne, modérément ramifiée. Comme K est irrégulier et que p ne divise pas e, K et K' ont même exposant d'irrégularité. L'extension K'/k satisfait à la condition du théorème 1.

Montrons que l'extension K'/k est décomposée. Soit ω une uniformisante de k. En adaptant le résultat de Weiss déjà cité, on met en évidence une uniformisante π de K telle que $\pi^e = \omega\xi$, où

ξ est une racine (q^f-1)-ème de 1 dans K . Comme $q^f \equiv 1 \bmod e$, $(q^f-1)e$ divise $q^{ef}-1$. On en déduit qu'il existe β , racine $(q^{ef}-1)$-ème de 1 dans K' telle que $\xi = \beta^e$. On considère alors l'uniformisante π' de K' définie par $\pi' = \pi\beta^{-1}$. Elle vérifie $\pi'^e = \pi^e\xi^{-1} = \omega$. Et l'on utilise le lemme 3.

La condition est nécessaire (p impair).

Soit $K_1 = k(\zeta)$, m le degré de K/K_1 , ν celui de $K_1/\mathbb{Q}_p$. On suppose qu'il existe une base normale pour les unités principales de K/k , donc de K/K_1 . Soit $(\theta_i)_{1\le i\le\nu}$ une telle base, et soit $\varepsilon_i = N_{K/K_1}\theta_i$. Utilisons le résultat du lemme ci-dessous : pour une extension galoisienne modérément ramifiée, la norme est surjective sur les unités principales. Puisque ζ est norme d'une unité principale, on a :

$$\zeta = N_{K/K_1}(\zeta^a \prod_{i=1}^{\nu} \theta_i^{\gamma_i}) = \zeta^{am} \prod_{i=1}^{\nu} \varepsilon_i^{a_i} \quad , \quad a_i \in \mathbb{Z}_p \ .$$

D'après l'unicité de l'écriture, $am \equiv 1 \bmod p^s$, et p ne divise pas m .

LEMME. <u>Soit</u> K/k <u>une extension galoisienne modérément ramifiée</u>. <u>Alors</u> $E_k = N_{K/k}E$.

Soit F le corps d'inertie de l'extension. Le résultat étant connu pour l'extension non ramifiée F/k , il suffit de le montrer pour l'extension K/F . D'après la théorie du corps de classe local, $(F^* : N_{K/F}K^*) = e$. Soit π une uniformisante de K , ω sa norme dans F (c'est une uniformisante de F , puisque K/F est totalement ramifiée), ξ une racine primitive (q^f-1)-ème de 1 dans F . En utilisant les décompositions : $K^* = \langle\pi\rangle \times \langle\xi\rangle \times E$, $F^* = \langle\omega\rangle \times \langle\xi\rangle \times E_F$, et le fait que e divise q^f-1 , on obtient le résultat.

§ 3 - LE CAS GENERAL.

On note K_1 le corps de ramification de l'extension K/k, s et s_1 les exposants d'irrégularité de K et K_1 (remarquer que $s \geq 1$, entraîne $s_1 \geq 1$), ζ_1 une racine primitive p^{s_1}-ème de 1 dans K_1.

THEOREME 2. Soit K/k une extension galoisienne finie.

Si $p \neq 2$ ou si $p = 2$ et $s_1 \geq 2$, il existe une base normale pour les unités principales de K/k si et seulement si :

(i) L'extension K_1/k satisfait à la condition du théorème 1 ;

(ii) $s = s_1$;

(iii) $K = K_1(\sqrt[p^m]{\pi_1})$, où m est un entier vérifiant $0 \leq m \leq s_1$ et π_1 une uniformisante de K_1 telle que ζ_1 ne soit pas une norme de l'extension $K_1(\sqrt[p]{\pi_1})/K_1$ (si $m \geq 1$).

Si $p = 2$ et $s_1 = 1$, et si la condition (i) est satisfaite, il existe une base normale si et seulement si :

(a) $K = K_1$ ou

(b) $K = K_1(\sqrt{-1})$ et $[K_1 : \mathbb{Q}_2]$ impair ou

(c) $K = K_1(\sqrt{\pi_1})$, où π_1 est une uniformisante de K_1 telle que -1 ne soit pas une norme de l'extension K/K_1.

La condition est nécessaire (p impair).

Supposons qu'il existe une base normale pour les unités principales de K/k. Il en existe alors une pour les unités principales de K/K_1 et de K_1/k. En particulier la condition du théorème 1 est vérifiée par l'extension K_1/k. Soit ν le degré absolu de K_1, $(\theta_i)_{1 \leq i \leq \nu}$ une base normale pour E vis-à-vis de K_1, $\varepsilon_i = N_{K/K_1}(\theta_i) = N\theta_i$. D'après le lemme 2, le Z_p-module E_1/NE est cyclique d'ordre p^m, avec $m \leq s_1$. Comme K/K_1 est une p-extension totalement ramifiée, les groupes quotients K_1^*/NK^* et E_1/NE sont isomorphes. D'après la théorie du corps de classe local, le

groupe E_1/NE est isomorphe au quotient du groupe de Galois G_1 de l'extension par son groupe dérivée. Comme ce quotient est cyclique, et que G_1 est un p-groupe, G_1 est cyclique [C.R. § 6, ex. 1]. Comme K_1 contient les racines p^m-èmes de 1, il existe $\alpha_1 \in K_1$ tel que $K = K_1(\sqrt[p^m]{\alpha_1})$. Supposons $m \geq 1$ et considérons le corps intermédiaire $\tilde{K} = K_1(\sqrt[p]{\alpha_1})$. Le groupe des normes des unités principales de $\tilde{K}$ dans K_1 coïncide avec le groupe $NE.E_1^p$, puisque $(E_1 : NE.E_1^p) = (E_1/NE : NE.E_1^p/NE) = p$. ζ_1 n'appartient pas à ce groupe, puisque sa classe modulo NE engendre E_1/NE. ζ_1 n'est donc pas une norme de $K_1(\sqrt[p]{\alpha_1})/K_1$.

Soit π'_1 une uniformisante de K_1 et soit $\alpha_1 = \pi_1'^{\ell}.u_1$, où u_1 est une unité de K_1. Supposons que p divise ℓ. Alors, modulo une puissance p-ème, α_1 est une unité principale de K_1. Il existe donc $\beta_1 \in K_1$ tel que (cf. dém. du lemme 2) :

$$\alpha_1\beta_1^p = \zeta_1^a \prod_{i=1}^{\nu} \varepsilon_i^{a_i} = \zeta_1^a \prod_{i=1}^{\nu} \theta_i^{Ta_i} \quad , \text{ où } \quad T = \sum_{\iota \in G_1} \iota \ .$$

Comme α_1 est une puissance p-ème dans K, $\alpha_1\beta_1^p$ est une puissance p-ème d'unité principale de K. On a donc :

$$\alpha_1\beta_1^p = \zeta^{pb} \prod_{i=1}^{\nu} \theta_i^{p\gamma_i} \quad , \quad \gamma_i \in \Gamma \ .$$

En vertu de l'unicité de l'écriture, pour tout $i = 1,\ldots,\nu$, $p\gamma_i = Ta_i$ et p divise a_i. Mais alors $\tilde{K} = K_1(\sqrt[p]{\zeta_1})$, et la norme de $\sqrt[p]{\zeta_1}$ dans l'extension $\tilde{K}/K_1$, ζ_1 en l'occurrence, appartient au groupe $NE.E_1^p$, ce qui est absurde. On a donc montré que $s = s_1$ et que p est premier à ℓ.

Soient alors g et h deux entiers tels que $gp^m + h\ell = 1$. Définissons l'uniformisante π_1 de K_1 par $\pi_1 = \pi'_1 u_1^h$. Elle vérifie $\pi_1 = \pi'_1\alpha_1^h\pi_1'^{-h\ell} = \alpha_1^h\pi_1'^{gp^m}$, et l'on a bien

$$K = K_1(\sqrt[p^m]{\pi_1}) \ .$$

La condition est suffisante (p impair).

Notons $N = N_{K/K_1}$. Le groupe des normes des unités principales de $K_1(\sqrt[p]{\pi_1})$ dans K_1 est le sous-groupe d'indice p de E_1 contenant NE . Comme ζ n'appartient pas à ce sous-groupe, par hypothèse, la classe de ζ modulo NE engendre le groupe E_1/NE .

Puisque l'extension K_1/k satisfait à la condition du théorème 1, il existe une base normale $\varepsilon_1,\dots,\varepsilon_n$ pour les unités principales de K_1/k . D'après ce qui précède, on peut supposer que $\varepsilon_j \in NE$, et l'on définit $\theta_j \in E$ par $\varepsilon_j = N\theta_j$.

Prolongeons chaque k-automorphisme de K_1 en un automorphisme de K (d'une manière quelconque), et notons $\sigma_1,\dots,\sigma_\mu$ ces prolongements, μ étant le degré de K_1/k . Soit ι un générateur de $G_1 = Gal(K/K_1)$. Les éléments du groupe de Galois G de K/k s'écrivent, de manière unique, sous la forme $(\sigma_i\iota^k)_{1\le i\le\mu\ ,\ 0\le k<p^m}$. Notons $T = T_{K/K_1} = \sum_{k=0}^{p^m-1} \iota^k$. Comme G_1 est distingué dans G , on a :

$$\forall i \le \mu : \ \sigma_i T = T\sigma_i \ ; \text{ et donc } \forall j \le n : \ \varepsilon_j^{\sigma_i} = \theta_j^{\sigma_i T} = N(\theta_j^{\sigma_i}) .$$

Considérons l'homomorphisme canonique : $E_1/E_1^p \to E/E^p$. Il est injectif. En effet, soit $\varepsilon \in E_1$ tel que $\varepsilon = \theta^p$, avec $\theta \in E$. Supposons que $\theta \notin E_1$. Alors $K_1(\theta)$ est l'extension de degré p de K_1 contenue dans K , c'est-à-dire $K_1(\sqrt[p]{\pi_1})$, ce qui est absurde. Les unités $(\zeta\ ,\ \varepsilon_j^{\sigma_i})_{1\le j\le n\ ,\ 1\le i\le\mu}$ sont donc $\mathbb{F}_p$-linéairement indépendantes dans E/E^p . On en déduit [B., lemme 3] que les unités $(\zeta\ ,\ \theta_j^{\sigma_i\iota^k})_{1\le j\le n\ ,\ 1\le i\le\mu\ ,\ 0\le k<p^m}$ sont $\mathbb{F}_p$-linéairement indépendantes dans E/E^p . Elles forment donc une $\mathbb{F}_p$-base de E/E^p puisque $\dim_{\mathbb{F}_p} E/E^p = N + 1 = n\mu p^m + 1$. On montre facilement que si des unités engendrent E/E^p comme $\mathbb{F}_p$-espace vectoriel, elles engendrent E comme Z_p-module. Il en résulte que les unités $(\theta_j)_{1\le j\le n}$ forment une base normale pour les unités principales de K vis-à-vis de k .

BIBLIOGRAPHIE

[B.] Z.I. Borevič - On the multiplicative group of cyclic p-extensions of a local field. Trudy Mat. Inst. Steklov 80 (1965), 15-30.

[B.S.] Z.I. Borevič and A.I. Skopin - Extensions of a local field with normal basis for principal units. Trudy Mat. Inst. Steklov 80 (1965), 48-55.

[C.R.] Curtis, Reiner - Representations theory of finite groups and associative algebras. Interscience Publishers 1962.

[D.] Deuring - Algebren. Springer-Verlag 1968.

[G.] D. Gilbarg - The structure of the groups of $\mathfrak{p}$-adic 1-units. Duke Math. J. 9 (1942), 262-271.

[I.] K. Iwasawa - On Galois groups of local fields. Trans. Amer. Math. Soc. 80 (1955), 448-469.

[K.] M. Krasner - Sur la représentation exponentielle dans les corps relativement galoisiens de nombres $\mathfrak{p}$-adique. Acta. Arith. 3 (1939), 133-173.

[S.] Serre - Corps locaux. Herman 1962.

[W.] Weiss - Algebraïc number theory. Mc Graw-Hill 1963.

-o-o-o-