THEORIE DES NOMBRES
BESANCON

Années 1986/87-1987/88
Fascicule 1

NON MONOGENEITE D'ANNEAUX D'ENTIERS

Georges GRAS

Non monogénéité d'anneaux d'entiers

Georges Gras

0. Introduction - Résultats. Nous mettons en évidence de nouvelles conditions nécessaires de monogénéité des anneaux d'entiers de corps de nombres, qui prolongent, dans un contexte très général, celles qui avaient été démontrées par M.-N. Gras, dans [G(MN)1, 2, 3], au moyen de considérations globales de théorie abélienne des entiers. Nous profitons de cette étude pour approfondir le point de vue local, soumis par H. Lenstra dans [L], et utilisé indépendamment par J. Cougnard, dans [C3, §2], qui a étendu les conditions nécessaires de [G(MN)1, 2, 3] au cas des extensions abéliennes des corps quadratiques imaginaires.

La théorie galoisienne des anneaux d'entiers conduit par nature à de telles généralisations (cf. par exemple [C1]) mais constitue un cadre inutilement fort comme le montre la méthode employée ici ; celle-ci renforce l'aspect local déjà évoqué ([L], [C3], ainsi que l'ancien résultat de J.-J. Payan [P] repris dans [G(MN)2, th.2] et dans [C3, §1]) en faisant intervenir un argument semi-local qui ne semble pas avoir été utilisé, et qui conduit à des non monogénéités nouvelles, même dans le cas abélien absolu.

Avant d'énoncer les résultats obtenus (constitués du théorème principal (0.4) et de ses conséquences, les théorèmes (0.6) et (0.9) et les corollaires (0.7), (0.7') et (0.10)), nous allons préciser le cadre général de cette étude ; celle-ci utilisera abondamment la théorie des

corps locaux pour laquelle nous renvoyons une fois pour toutes à J.-P. Serre [S].

Soit E un corps de nombres, et soit F un sous-corps de E tel que E/F soit une extension galoisienne ; on appelle n son degré et G son groupe de Galois. On utilisera constamment les notations suivantes :

(N) Notations. (i) Relativement à un idéal premier $\mathfrak{p}$ de E, on désigne par $(G_{\mathfrak{p},i})_{i \geq -1}$ la filtration des groupes de ramification associée à $\mathfrak{p}$ dans E/F ; le groupe $G_{\mathfrak{p},-1}$ (resp. $G_{\mathfrak{p},0}$) est le groupe de décomposition (resp. d'inertie) pour $\mathfrak{p}$ dans E/F ; il fixe le corps de décomposition $M(\mathfrak{p})$ (resp. d'inertie $N(\mathfrak{p})$). On pose :

$$e(\mathfrak{p}) = |G_{\mathfrak{p},0}| = [E : N(\mathfrak{p})] \text{ et } r(\mathfrak{p}) = [N(\mathfrak{p}) : M(\mathfrak{p})]$$

(i.e. $e(\mathfrak{p})$ est l'indice de ramification et $r(\mathfrak{p})$ le degré résiduel, de $\mathfrak{p}$ dans E/F).

(ii) On désigne par $S_{\mathfrak{p}}$ un système exact de représentants des classes à droite de G modulo $G_{\mathfrak{p},-1}$.

(iii) Pour tout sous-corps K de E contenant F , on désigne par Z_K (resp. Z_K^*) l'anneau des entiers de K (resp. son groupe des unités), par $\mathfrak{p}_K$ l'idéal premier $\mathfrak{p} \cap Z_K$ de K , et par $\overline{K}_{\mathfrak{p}}$ le corps résiduel $Z_K/\mathfrak{p}_K$.

Lorsque l'on considère des idéaux premiers $\mathfrak{p}, \mathfrak{l}, \ldots$ de E , on désigne par $p, \ell, \ldots$ les caractéristiques des corps résiduels correspondants.

(iv) Pour tout sous-corps K de E contenant F , on appelle $K_{\mathfrak{p}}$ la complétion de K en $\mathfrak{p}_K$; on désigne par $\mathcal{O}_{K_{\mathfrak{p}}}$ (resp. $\mathcal{O}_{K_{\mathfrak{p}}}^*$) l'anneau des entiers de $K_{\mathfrak{p}}$ (resp. son groupe des unités), et on note par $\mathfrak{p}_{K_{\mathfrak{p}}}$

l'idéal maximal de $\mathcal{O}_{K_\mathfrak{p}}$. On désigne par $\mu_{K_\mathfrak{p}}$ le groupe des racines de l'unité, d'ordre étranger à p, contenues dans $K_\mathfrak{p}$ (on a $\mu_{K_\mathfrak{p}} \simeq \overline{K}_\mathfrak{p}^\times$).

Pour $K = M(\mathfrak{p})$ et $N(\mathfrak{p})$, on désigne, par abus, par $M_\mathfrak{p}$ et $N_\mathfrak{p}$ les complétions correspondantes.

Enfin on désigne toujours par $(G_{\mathfrak{p},i})_{i \geq -1}$ la filtration des groupes de ramification associée à $E_\mathfrak{p}/F_\mathfrak{p}$ (on a donc $M_\mathfrak{p} = F_\mathfrak{p}$, $G_{\mathfrak{p},-1} = \mathrm{Gal}(E_\mathfrak{p}/F_\mathfrak{p})$, $G_{\mathfrak{p},0} = \mathrm{Gal}(E_\mathfrak{p}/N_\mathfrak{p})$).

(v) On désigne par $\eta_\mathfrak{p}^1$ le sous-groupe de $1 + \mathfrak{p}_{F_\mathfrak{p}}$ égal à $N_{E_\mathfrak{p}/F_\mathfrak{p}}(1 + \mathfrak{p}_{E_\mathfrak{p}})$; d'après le corps de classes local, $(1 + \mathfrak{p}_{F_\mathfrak{p}} : \eta_\mathfrak{p}^1)$ est égal à la p-partie de l'indice de ramification de la sous-extension abélienne maximale $E_\mathfrak{p}^{ab}$ de $F_\mathfrak{p}$ dans $E_\mathfrak{p}$ (par exemple, si E/F est abélienne, cet indice normique est égal à la p-partie de $e(\mathfrak{p})$).

(vi) On désigne par $\pi_\mathfrak{p}$ une uniformisante pour $\mathfrak{p}$ dans E, et par $v_\mathfrak{p} : E_\mathfrak{p}^\times \longrightarrow\!\!\!\!\rightarrow \mathbb{Z}$ la valuation $\mathfrak{p}$-adique sur $E_\mathfrak{p}^\times$, normalisée par la condition $v_\mathfrak{p}(\pi_\mathfrak{p}) = 1$.

(vii) Pour tout sous-corps strict K de E contenant F, on désigne par $\mathfrak{d}(E/K)$ l'idéal $\prod_I I^{n_I(E/K)}$ de E, où I parcourt l'ensemble des idéaux premiers de E totalement ramifiés dans E/K, et où $n_I(E/K) = k + 1$, $k \geq 0$ étant l'entier maximum tel que $\mathrm{Gal}(E/K) \subseteq G_{I,k}$: on a donc

$$k = \mathrm{Max}\{i \geq 0,\ \pi_I^{\sigma-1} \equiv 1 \bmod \pi_I^i \text{ pour tout } \sigma \in \mathrm{Gal}(E/K)\}.$$

Il en résulte que $n_I(E/K) = 1$ sauf si $[E:K]$ est une puissance de ℓ, auquel cas on a $n_I(E/K) \geq 2$.

(viii) Soit $\mathfrak{p}$ un idéal premier de E et soit h un diviseur de $e(\mathfrak{p}) = |G_{\mathfrak{p},0}|$. On sait que $G_{\mathfrak{p},1}$ est le p-Sylow de $G_{\mathfrak{p},0}$, que $G_{\mathfrak{p},0}/G_{\mathfrak{p},1}$ s'identifie à un sous-groupe de $\overline{N}_\mathfrak{p}^\times$, d'ordre égal au plus grand diviseur $e_\mathfrak{p}$ de $e(\mathfrak{p})$ étranger à p ; vu l'isomorphisme canonique $\mu_{N_\mathfrak{p}} \simeq \overline{N}_\mathfrak{p}^\times$,

il existe un élément $\xi_p \in \mu_{N_p}$ d'ordre h_p égal au plus grand diviseur étranger à p de h (h_p est donc un diviseur de e_p), dont l'image dans $\overline{N}_p^\times$ est notée $\overline{\xi}_p$.

On désigne alors par q_p le cardinal du corps fini $\mathbb{F}_p(\overline{\xi}_p)$.

Pour tout $a, b \in (\mathbb{Z}/h\mathbb{Z})^*$, on considère, dans $\overline{N}_p$,

$\overline{\eta}_{p,a,b} = \dfrac{1 - \overline{\xi}_p^a}{1 - \overline{\xi}_p^b}$, en remarquant que cette expression est non définie si

et seulement si h est puissance de p (i.e. $h_p = 1$, $\xi_p = 1$), auquel cas on pose $\overline{\eta}_{p,a,b} = \dfrac{\overline{a}}{\overline{b}}$ dans $\overline{N}_p$; on a une définition intrinsèque si l'on pose

$\overline{\eta}_{p,a,b} = \dfrac{\overline{1} + \overline{\xi}_p + \ldots + \overline{\xi}_p^{a'-1}}{\overline{1} + \overline{\xi}_p + \ldots + \overline{\xi}_p^{b'-1}}$, où a' et b' sont des représentants posi-

tifs de a et b $\in (\mathbb{Z}/h\mathbb{Z})^*$.

(ix) Soit X_p l'image dans $\overline{F}_p^\times$ de $N_{E/F} Z_E^*$ (ou à défaut celle du sous-groupe de Z_F^* formé des unités de F partout normes locales dans E/F) ; soit χ_p un caractère de G à valeurs dans $(\mathbb{Z}/h\mathbb{Z})^*$, et soit Y_p le sous-groupe de $\mathbb{F}_p(\overline{\xi}_p)^\times$ engendré par les produits

$$\prod_{s \in S_p} \prod_{i=1}^{r(p)} \left(\frac{1 - \overline{\xi}_p^{a \chi_p(s) f_p^i}}{1 - \overline{\xi}_p^{b \chi_p(s) f_p^i}} \right)^{e(p)}, \quad a, b \in (\mathbb{Z}/h\mathbb{Z})^*,$$

où $f_p = |\overline{F}_p|$. On pose alors

$$w_p = |X_p \cap Y_p|$$

(on remarque que w_p est un diviseur de $pgcd(f_p - 1, q_p - 1)$).

(x) Soit p une place à l'infini de E, ramifiée dans E/F ; on a $G_{p,-1} = G_{p,0} \simeq \mathbb{Z}/2\mathbb{Z}$. Par définition, la ramification d'une place à l'infini est modérée, auquel cas on peut poser $G_{p,i} = 1$ pour tout $i \geq 1$.

On désigne par $\tau_\mathfrak{p}$ le plongement $E \subsetneq \mathbb{C}$ associé à $\mathfrak{p}$; comme $\mathfrak{p}$ est ramifiée dans E/F, on a donc $\tau_\mathfrak{p}(F) \subseteq \tau_\mathfrak{p}(N(\mathfrak{p})) \subseteq \mathbf{R}$ et $\tau_\mathfrak{p}(E) \subseteq \mathbf{C}$, $\tau_\mathfrak{p}(E) \not\subseteq \mathbf{R}$ (i.e. $E_\mathfrak{p} = \mathbb{C}$ et $F_\mathfrak{p} = \mathbf{R}$).

(xi) On désigne une fois pour toutes par H un sous-groupe cyclique de G, d'ordre $h > 1$; pour tout $g \in G$, on appelle L_g le sous-corps de E fixe par gHg^{-1} et on pose $L_1 = L$.

On fera, le cas échéant, l'une des hypothèses suivantes, dans lesquelles $\mathfrak{p}$ désigne une place quelconque de E ramifiée dans E/F :

H0($\mathfrak{p}$) Tous les G-conjugués de H sont contenus dans $G_{\mathfrak{p},0}$.

H1($\mathfrak{p}$) On a $H \subseteq G_{\mathfrak{p},0}$, et tous les G-conjugués de H sont contenus dans $G_{\mathfrak{p},1}H$.

(0.1) Proposition. L'hypothèse H1($\mathfrak{p}$) est équivalente à la réunion des deux conditions suivantes :

(α) $H \subseteq G_{\mathfrak{p},0}$;

(β) il existe un unique caractère $\chi_\mathfrak{p} : G \to (\mathbb{Z}/h_\mathfrak{p}\mathbb{Z})^*$ tel que $g\sigma g^{-1}\sigma^{-\chi_\mathfrak{p}(g)} \in G_{\mathfrak{p},1}$, pour tout $\sigma \in H$ et tout $g \in G$.

Un sens étant évident, supposons H1($\mathfrak{p}$) et montrons l'existence de $\chi_\mathfrak{p}$. On a, pour un générateur σ_o de H et pour $g \in G$ fixé, $g\sigma_o g^{-1} = t\sigma_o'$, $t \in G_{\mathfrak{p},1}$, $\sigma_o' \in H$. Donc il existe $x \in \mathbb{Z}$ tel que $g\sigma_o g^{-1} = t\sigma_o^x$; on remarque que x est unique modulo $h_\mathfrak{p}$, car pour $t, t' \in G_{\mathfrak{p},1}$, $t\sigma_o^x = t'\sigma_o^{x'}$ implique $t'^{-1}t = \sigma_o^{x'-x} \in H \cap G_{\mathfrak{p},1}$, d'où $x' - x \equiv 0 \bmod h_\mathfrak{p}$.

Comme $G_{\mathfrak{p},1}$ est normal dans $G_{\mathfrak{p},0}$, pour tout $i \in \mathbb{Z}$ on a

$(t\,\sigma_o^x)^i = t_i\,\sigma_o^{xi}$, $t_i \in G_{\mathfrak{p},1}$, d'où $g\,\sigma_o^i\,g^{-1} = t_i\,\sigma_o^{xi}$, soit $g\sigma g^{-1} = t_\sigma \sigma^x$, $t_\sigma \in G_{\mathfrak{p},1}$, pour tout $\sigma \in H$; donc x ne dépend que de $g \in G$. On peut donc poser $x = \chi_{\mathfrak{p}}(g) \in (\mathbb{Z}/h_{\mathfrak{p}}\mathbb{Z})^*$.

En désignant par θ_g l'automorphisme intérieur de G associé à g , on a pour tout $\sigma \in H$ (en écrivant $\chi_{\mathfrak{p}} = \chi$) :

$$\theta_g(\sigma) = t_g\,\sigma^{\chi(g)} \text{ , } t_g \in G_{\mathfrak{p},1} \text{ ,}$$

$$\theta_{g'}(\sigma) = t_{g'}\,\sigma^{\chi(g')} \text{ , } t_{g'} \in G_{\mathfrak{p},1} \text{ ,}$$

$$\theta_{g'g}(\sigma) = t_{g'g}\,\sigma^{\chi(g'g)} \text{ , } t_{g'g} \in G_{\mathfrak{p},1} \text{ ;}$$

or $\theta_{g'g}(\sigma) = \theta_{g'}(t_g\,\sigma^{\chi(g)}) = \theta_{g'}(t_g)\,t'_{g'}\,\sigma^{\chi(g')\,\chi(g)}$, où $t'_{g'} \in G_{\mathfrak{p},1}$,

ce qui conduit à $t_{g'g}\,\sigma^{\chi(g'g)} = \theta_{g'}(t_g)\,t'_{g'}\,\sigma^{\chi(g')\,\chi(g)}$

soit $\quad t'^{-1}_{g'}\,\theta_{g'}(t_g)^{-1}\,t_{g'g} = \sigma^{\chi(g')\,\chi(g) - \chi(g'g)}$;

or $t'_{g'}$, $t_{g'g}$, $\sigma \in G_{\mathfrak{p},0}$, et l'égalité précédente implique $\theta_{g'}(t_g) \in G_{\mathfrak{p},0}$, et comme t_g est d'ordre puissance de p , $\theta_{g'}(t_g) \in G_{\mathfrak{p},1}$, d'où $\sigma^{\chi(g')\,\chi(g) - \chi(g'g)} \in G_{\mathfrak{p},1}$, ce qui donne $\chi(g'g) \equiv \chi(g')\,\chi(g) \bmod h_{\mathfrak{p}}$; d'où $\chi(g'g) = \chi(g')\,\chi(g)$ dans $(\mathbb{Z}/h_{\mathfrak{p}}\mathbb{Z})^*$, et $\chi_{\mathfrak{p}}$ est bien un caractère.

(R) Remarques. (i) On a évidemment $H1(\mathfrak{p}) \Rightarrow H0(\mathfrak{p})$.

(ii) Si $h_{\mathfrak{p}} = 1$ alors $H1(\mathfrak{p})$ et $H0(\mathfrak{p})$ sont équivalentes : en effet, dans ce cas, sous $H0(\mathfrak{p})$, tout G-conjugué de H est un p-sous-groupe de $G_{\mathfrak{p},0}$; il est donc contenu dans son unique p-Sylow $G_{\mathfrak{p},1}$. Enfin, si $h_{\mathfrak{p}} = 1$, on a $\chi_{\mathfrak{p}} = 1$.

Si $G_{\mathfrak{p},1} = 1$, $H1(\mathfrak{p})$ est équivalente à $H \subseteq G_{\mathfrak{p},0}$ et H normal dans G ; on a alors $g\sigma g^{-1} = \sigma^{\chi_{\mathfrak{p}}(g)}$, pour tout $\sigma \in H$ et tout $g \in G$.

(iii) Si G est abélien, les hypothèses $H0(\mathfrak{p})$ et $H1(\mathfrak{p})$ coïncident et sont équivalentes à la seule condition $H \subseteq G_{\mathfrak{p},0}$, et en outre on a $\chi_{\mathfrak{p}} = 1$.

(iv) Si $\mathfrak{p}$ est une place à l'infini telle que $H \subseteq G_{\mathfrak{p},0}$, alors nécessairement H est d'ordre 2 , $L = N(\mathfrak{p})$, les hypothèses $H0(\mathfrak{p})$ et $H1(\mathfrak{p})$

coïncident et sont équivalentes à la normalité de $H = G_{\mathfrak{p},0}$ dans G (auquel cas E est un corps à conjugaison complexe et $L = N(\mathfrak{p})$ est son sous-corps réel maximal). Dans ce cas, on a également $\chi_{\mathfrak{p}} = 1$.

(v) On a $G_{\mathfrak{p},0} \subseteq \mathrm{Ker}\ \chi_{\mathfrak{p}}$; en effet, comme $G_{\mathfrak{p},0}/G_{\mathfrak{p},1} \hookrightarrow \overline{N}_{\mathfrak{p}}^{\chi}$, si $g \in G_{\mathfrak{p},0}$, la relation $g\sigma g^{-1}\sigma^{-\chi_{\mathfrak{p}}(g)} \in G_{\mathfrak{p},1}$ conduit, dans ce quotient, à $\tilde{g}\tilde{\sigma}\tilde{g}^{-1}\tilde{\sigma}^{-\chi_{\mathfrak{p}}(g)} = \tilde{1}$, soit $\tilde{\sigma}^{1-\chi_{\mathfrak{p}}(g)} = \tilde{1}$, pour tout $\sigma \in H$, puisqu'alors $\tilde{g}$ et $\tilde{\sigma}$ commutent ; d'où $\chi_{\mathfrak{p}}(g) = 1$.

(vi) L'hypothèse $H0(\mathfrak{p})$ a lieu si et seulement si on a $sHs^{-1} \subseteq G_{\mathfrak{p},0}$ pour tout $s \in S_{\mathfrak{p}}$; de même, en utilisant la normalité de $G_{\mathfrak{p},0}$ et $G_{\mathfrak{p},1}$ dans $G_{\mathfrak{p},-1}$, et la cyclicité de $G_{\mathfrak{p},0}/G_{\mathfrak{p},1}$, on vérifie que $H1(\mathfrak{p})$ a lieu si et seulement si on a $H \subseteq G_{\mathfrak{p},0}$ et $sHs^{-1} \subseteq G_{\mathfrak{p},1}H$ pour tout $s \in S_{\mathfrak{p}}$.

L'ensemble des résultats obtenus est essentiellement résumé par les énoncés suivants, non indépendants, et dont (0.4) est le résultat central :

(0.2) Théorème. Soit H un sous-groupe cyclique non trivial de G, et soit L le corps qu'il fixe. Une condition nécessaire à la Z_F-monogénéité de Z_E est que $N_{E/F}\,\mathfrak{d}(E/L)$ (cf. (N, vii)) soit un idéal principal de F et qu'il en existe un générateur $\delta(E/L)$ vérifiant les propriétés suivantes :

(i) Pour tout idéal premier $\mathfrak{p}$ de E, ramifié dans E/F, l'image de $\delta(E/L)N_{E/M(\mathfrak{p})}\,\pi_{\mathfrak{p}}^{-\lambda_{\mathfrak{p}}}$ dans $\mathcal{O}_{F_{\mathfrak{p}}}^{*}/\mathcal{N}_{\mathfrak{p}}^{1}$ est une puissance $e(\mathfrak{p})$-ième, où l'on a posé $\lambda_{\mathfrak{p}} = \sum_{s \in S_{\mathfrak{p}}} n_{\mathfrak{p}}(E/L_s)$ (cf. (N, vii, xi)) ;

(ii) pour toute place à l'infini $\mathfrak{p}$ de E, ramifiée dans E/F, on a $\tau_{\mathfrak{p}}(\delta(E/L)) > 0$ (cf. (N, x)).

(0.3) Remarques. (i) Les points (i) et (ii) (qui ne font pas référence à $H0(\mathfrak{p})$ ou $H1(\mathfrak{p})$) ne font que traduire l'existence d'un générateur $\delta(E/L)$ de

$N_{E/F}\,\mathfrak{d}(E/L)$ partout norme locale dans E/F. Pour les idéaux premiers, $\mathcal{O}_{F_\mathfrak{p}}^*/\eta_\mathfrak{p}^1$ est isomorphe au produit direct de $\overline{F}_\mathfrak{p}^X$ (d'ordre $f_\mathfrak{p}-1$ étranger à p) par un p-groupe fini ; les conditions écrites en (i) sont donc équivalentes aux conditions suivantes :

$$(i')\quad \left(\delta(E/L)\, N_{E/M(\mathfrak{p})}\pi_\mathfrak{p}^{-\lambda_\mathfrak{p}}\right)^{(f_\mathfrak{p}-1)/e_\mathfrak{p}} \in \eta_\mathfrak{p}^1 ,$$

pour tout idéal premier $\mathfrak{p}$ de E, ramifié dans E/F ; ceci se traduit, dans $F_\mathfrak{p}$, par des congruences explicites.

Si $\eta_\mathfrak{p}^1 = 1 + \mathfrak{p}_{F_\mathfrak{p}}$ (cas où $E_\mathfrak{p}^{ab}/F_\mathfrak{p}$ est modérément ramifiée), (i') équivaut au fait que l'image dans $\overline{F}_\mathfrak{p}^X$ du membre de gauche est égale à 1 (cf.(N, v)).

Dans le cas où $F = \mathbb{Q}$ et où E/F est abélienne, nous donnons une caractérisation numérique très simple des conditions du théorème (0.2), qui provient du fait que dans ce cas le corps de classes est explicite (cf. (3.3)).

(ii) Nous n'envisageons ici que les aspects locaux, mais la condition de principalité de $N_{E/F}\,\mathfrak{d}(E/L)$ est déjà une condition essentielle qui conduit à de nombreuses obstructions (cf. [C3] pour un certain nombre d'exemples se basant aussi sur la principalité de $\mathfrak{d}(E/L)$).

(0.4) Théorème. Soit H un sous-groupe cyclique non trivial de G, et soit L le corps qu'il fixe. Une condition nécessaire à la Z_F-monogénéité de Z_E est que pour tout générateur σ de H, il existe un générateur $\delta_\sigma(E/L)$ de $N_{E/F}\,\mathfrak{d}(E/L)$ (cf.(N, vii)), partout norme locale dans E/F (i.e. vérifiant (0.2), (i), (ii)), qui vérifie la propriété semi-locale suivante :

Pour tout idéal premier $\mathfrak{I}$ de E vérifiant H0($\mathfrak{I}$), l'image de

$$\delta_\sigma(E/L)\, N_{E/M(\mathfrak{I})}\, \pi_\mathfrak{I}^{-|S_\mathfrak{I}|} \prod_{s\in S_\mathfrak{I}} N_{E/M(\mathfrak{I})}\,(1-\pi_\mathfrak{I}^{s\sigma s^{-1}-1})^{-1} \quad \text{dans}$$

$\mathcal{O}_{F_I}^{*}/\eta_I^1$, est la puissance e(I)-ième d'un élément indépendant de σ (cf.(N, i, iv, v)) .

(0.5) Remarques. (i) La condition nécessaire exprimée par (0.4) est plus forte que celle exprimée par (0.2) en raison de l'indépendance du résultat par rapport à σ . Cette indépendance, qui est l'argument essentiel, peut être précisée sous l'hypothèse H1, et conduit à des conditions nécessaires très fortes sur la valeur numérique des nombres $h_\mathfrak{p}$: on obtient des généralisations du type de conditions mis en évidence par M.-N. Gras dans [G(MN)1, 2, 3]. Enfin s'il existe, pour l'application de (0.4), des ensembles Σ d'idéaux I (vérifiant H0(I)), non réduits à un élément, il faut noter que le générateur $\delta_\sigma(E/L)$ doit être le même pour chaque $I \in \Sigma$. L'information optimale est donc obtenue lorsque l'on applique (0.4) pour chaque H avec l'ensemble Σ maximum par rapport à H , tout en exprimant, via (0.2), que pour toute place $\mathfrak{p} \notin \Sigma$, $\mathfrak{p}$ ramifiée dans E/F , $\delta_\sigma(E/L)$ est norme locale en $\mathfrak{p}$.

(ii) Si H est d'ordre 2 , il admet un unique générateur σ , auquel cas l'énoncé (0.4) est équivalent à (0.2) .
Ceci justifie le fait que l'énoncé de (0.4) ne considère que des idéaux premiers et non des places à l'infini.

(iii) Le théorème (0.4) doit être considéré comme le résultat le plus général, et est directement utilisable numériquement en dehors de toute hypothèse.

Les résultats suivants caractérisent (sous l'hypothèse H1) ces questions d'indépendance par rapport aux générateurs de H :

(0.6) Théorème. Une condition nécessaire à la Z_F-monogénéité de Z_E est que pour tout sous-groupe cyclique H de G , d'ordre $h > 1$, et tout idéal premier $\mathfrak{p}$ de E tel que H1($\mathfrak{p}$) soit vérifiée , on ait la propriété suivante :

$$\prod_{s \in S_{\mathfrak{p}}} \prod_{i=1}^{r(\mathfrak{p})} \left(\frac{1 - \zeta_{\mathfrak{p}}^{a \chi_{\mathfrak{p}}(s) f_{\mathfrak{p}}^{i}}}{1 - \zeta_{\mathfrak{p}}^{b \chi_{\mathfrak{p}}(s) f_{\mathfrak{p}}^{i}}} \right)^{e_{\mathfrak{p}} w_{\mathfrak{p}}} \equiv 1 \bmod p\mathbb{Z}[\zeta_{\mathfrak{p}}],$$

pour tout $a, b \in (\mathbb{Z}/h\mathbb{Z})^*$, où $\zeta_{\mathfrak{p}} = \exp(2i\pi/h_{\mathfrak{p}}) \in \mathbb{C}^{\times}$, cette congruence se lisant $(ab^{-1})^{n w_{\mathfrak{p}}} \equiv 1 \bmod p\mathbb{Z}$ si $h_{\mathfrak{p}} = 1$ (i.e. $\zeta_{\mathfrak{p}} = 1$) (cf.(N, i, viii, ix)).

(0.7) Corollaire. Une condition nécessaire à la Z_F-monogénéité de Z_E est que pour tout sous-groupe cyclique H de G, d'ordre $h > 1$, et tout idéal premier $\mathfrak{p}$ de E vérifiant H1($\mathfrak{p}$) et tel que $\chi_{\mathfrak{p}} = 1$, on ait la propriété suivante :

$$\left(\frac{1 - \zeta_{\mathfrak{p}}^{a}}{1 - \zeta_{\mathfrak{p}}^{b}} \right)^{e_{\mathfrak{p}} d_{\mathfrak{p}}} \equiv 1 \bmod p\mathbb{Z}[\zeta_{\mathfrak{p}}], \text{ pour tout } a, b \in (\mathbb{Z}/h\mathbb{Z})^*,$$

où $d_{\mathfrak{p}} = \text{p.g.c.d.} \left(\frac{q_{\mathfrak{p}} - 1}{e_{\mathfrak{p}}}, \frac{n}{e_{\mathfrak{p}}} w_{\mathfrak{p}} \right)$.

(0.8) Remarques. (i) Si $\mathfrak{p}$ est modérément ramifié dans E/L (i.e. $h_{\mathfrak{p}} = h$) et si $\chi_{\mathfrak{p}} = 1$, on retrouve, via (0.7), les conditions obtenues, dans [G(MN)1, 2, 3] et dans [C3], à partir de considérations d'extensions E/F abéliennes ; en particulier, les calculs binomiaux effectués en toute généralité dans [G(MN)3] s'appliquent aux extensions E/F étudiées ici, ce qui permet de démontrer la non monogénéité de Z_E sur Z_F dans de nombreux cas nouveaux.

(ii) Si $h_{\mathfrak{p}} = 2, 4, 6$, on a $1 - \left(\frac{1 - \zeta_{\mathfrak{p}}^{a}}{1 - \zeta_{\mathfrak{p}}^{b}} \right)^{h_{\mathfrak{p}} m} = 0$ pour tout $a, b \in (\mathbb{Z}/h_{\mathfrak{p}}\mathbb{Z})^*$ et tout $m \geq 1$; si $h_{\mathfrak{p}} = 3$, on a $1 - \left(\frac{1 - \zeta_{\mathfrak{p}}^{a}}{1 - \zeta_{\mathfrak{p}}^{b}} \right)^{3m} = 0$

(resp. 2) pour tout $a, b \in (\mathbb{Z}/3\mathbb{Z})^*$ si m est pair (resp. impair).

(iii) Si $h_\mathfrak{p} \neq 1$, on peut considérer a et b modulo $h_\mathfrak{p}$, et on peut même supposer $b = 1$.

(iv) Si $\mathfrak{p}$ est totalement sauvagement ramifié dans E/L (i.e. $e_\mathfrak{p} = h_\mathfrak{p} = 1$), on a nécessairement $\chi_\mathfrak{p} = 1$, auquel cas (0.7) s'applique : on a $q_\mathfrak{p} = p$, d'où $d_\mathfrak{p} = pgcd\,(p-1, nw_\mathfrak{p})$, or dans ce cas la condition nécessaire s'écrit $(ab^{-1})^{d_\mathfrak{p}} \equiv 1 \bmod p$, pour tout a, b étrangers à p, ce qui équivaut à $(\mathbf{F}_p^\times)^{d_\mathfrak{p}} = 1$, soit $d_\mathfrak{p} \equiv 0 \bmod (p-1)$, soit en fait $d_\mathfrak{p} = p-1$ et finalement $nw_\mathfrak{p} \equiv 0 \bmod (p-1)$. Or $w_\mathfrak{p}$ divise $p-1$ (car $Y_\mathfrak{p} = \mathbf{F}_p^\times$ ici) et la condition nécessaire peut s'énoncer de la façon suivante dans ce cas (compte tenu du fait qu'ici $H1(\mathfrak{p}) \Leftrightarrow H0(\mathfrak{p})$) :

(0.7') Corollaire. Une condition nécessaire à la Z_F-monogénéité de Z_E est que, pour tout idéal premier $\mathfrak{p}$ de E, sauvagement ramifié dans E/F, pour lequel il existe un sous-groupe non trivial H de $G_{\mathfrak{p},1}$ vérifiant $H0(\mathfrak{p})$, n soit multiple de $\dfrac{p-1}{w_\mathfrak{p}}$.

On a ainsi généralisé des conditions classiques (cf. [P], [G(MN)2, th.2], [C3, §1]). On remarque que la condition (0.7') est vide pour $p = 2$.

(0.9) Théorème. Une condition nécessaire à la Z_F-monogénéité de Z_E est que pour tout sous-groupe cyclique H de G, d'ordre $h > 1$, et tout $a, b \in (\mathbb{Z}/h\mathbb{Z})^*$, il existe une unité $\varepsilon_{a,b}$ de F, norme d'unité dans E/F (ou à défaut partout norme locale dans E/F), ayant la propriété semi-locale suivante :

pour tout idéal premier I de E vérifiant H1(I), l'image $\bar{\varepsilon}_{a,b}$ de $\varepsilon_{a,b}$ dans $\bar{F}_I^{\times}$ vérifie la relation :

$$\bar{\varepsilon}_{a,b} = \prod_{s \in S_I} \prod_{i=1}^{r(I)} \left(\frac{1 - \bar{\gamma}_I^{a \chi_I(s) f_I^i}}{1 - \bar{\gamma}_I^{b \chi_I(s) f_I^i}} \right)^{e(I)},$$

où $\bar{\gamma}_I$ est l'image dans $\bar{F}_I^{\times}$ de $\pi_I^{\sigma_o - 1}$, pour un générateur arbitraire σ_o de H fixé une fois pour toutes.

(0.10) Corollaire. Une condition nécessaire à la Z_F-monogénéité de Z_E est que pour tout sous-groupe cyclique H de G, d'ordre $h > 1$, et tout $a, b \in (\mathbb{Z}/h\mathbb{Z})^*$, il existe une unité $\varepsilon_{a,b}$, norme d'unité dans E/F (ou à défaut partout norme locale dans E/F), ayant la propriété semi-locale suivante : pour tout idéal premier I de E vérifiant H1(I) et tel que $\chi_I = 1$, l'image $\bar{\varepsilon}_{a,b}$ de $\varepsilon_{a,b}$ dans $\bar{F}_I^{\times}$ vérifie la relation :

$$\bar{\varepsilon}_{a,b} = \left(\frac{1 - \bar{\gamma}_I^a}{1 - \bar{\gamma}_I^b} \right)^n,$$

où $\bar{\gamma}_I$ est l'image dans $\bar{F}_I^{\times}$ de $\pi_I^{\sigma_o - 1}$, pour un générateur arbitraire σ_o de H fixé une fois pour toutes.

(0.11) Remarques. (i) On peut toujours supposer que $\bar{\gamma}_I = \bar{\xi}_I$ où $\xi_I \in \mu_{N_I}$ est d'ordre h_I. En outre, s'il existe un I vérifiant H1(I) tel que $h_I = 1$ (auquel cas h est une puissance de ℓ), on doit écrire que l'image dans $\bar{F}_I^{\times}$ de $\dfrac{1 - \gamma_I^a}{1 - \gamma_I^b}$ est ab^{-1} modulo ℓ.

(ii) Le calcul des $\pi_I^{\sigma_o - 1}$ est indispensable, car l'ensemble des ξ_I n'est pas n'importe quelle famille d'éléments d'ordres respectifs h_I des groupes μ_{N_I}.

(iii) Dans l'énoncé (0.9), la condition $\epsilon_{a,b}$ partout norme locale est également indispensable sinon il faut remplacer $\overline{F}_I^{\times}$ par $\mathcal{O}_{F_I}^{*}/\eta_I^1$; on a donc en particulier $\epsilon_{a,b} \equiv \xi_{a,b}^{e(\mathfrak{p})} \bmod^{\times} \eta_{\mathfrak{p}}^1$, pour tout idéal premier $\mathfrak{p}$ de E ramifié dans E/F , où $\xi_{a,b} \in \mu_{F_{\mathfrak{p}}}$ (cf. (1.2)), et $\tau_{\mathfrak{p}}(\epsilon_{a,b}) > 0$, pour toute place à l'infini $\mathfrak{p}$ de E ramifiée dans E/F .

(iv) La condition nécessaire exprimée par (0.9) est semi-locale en ce sens que, pour H , a , b fixés, l'unité $\epsilon_{a,b}$ doit satisfaire en général à plusieurs congruences simultanées ; cet aspect conduit effectivement à des non monogénéités nouvelles lorsque les conditions nécessaires des théorèmes (0.2), (0.4) sont vérifiées (cf. l'exemple numérique (ii) du §4) .

1. Etude locale générale. On commence par énoncer deux lemmes valables pour une extension galoisienne E/F quelconque, indépendamment de toute hypothèse :

(1.1) Lemme. S'il existe $\theta \in Z_E$ tel que $Z_E = Z_F[\theta]$, alors pour tout $g \in G$, $g \neq 1$, $(\theta - \theta^g) Z_E = \mathfrak{d}(E/K)$ (cf.(N, vii)), où K est le sous-corps de E fixe par $\langle g \rangle$. En particulier, si $\langle g \rangle = \langle g' \rangle$, pour $g, g' \in G$, on a $\dfrac{\theta - \theta^g}{\theta - \theta^{g'}} \in Z_E^*$.

Fixons $g \in G$. Soit $\mathfrak{p}$ un idéal premier de E ; si $\theta - \theta^g \equiv 0 \bmod \mathfrak{p}$, il en résulte facilement que $x - x^g \equiv 0 \bmod \mathfrak{p}$, pour tout $x \in Z_E$, ce qui signifie $g \in G_{\mathfrak{p},0}$; donc si $g \notin G_{\mathfrak{p},0}$, $\theta - \theta^g$ est étranger à $\mathfrak{p}$. Supposons maintenant que $g \in G_{\mathfrak{p},0}$; puisque $Z_E = Z_F[\theta]$, on a également $\mathcal{O}_{E_{\mathfrak{p}}} = \mathcal{O}_{F_{\mathfrak{p}}}[\theta]$ auquel cas on sait que $v_{\mathfrak{p}}(\theta - \theta^g) = 1 + \max\{i \geq 0 , g \in G_{\mathfrak{p},i}\} = n_{\mathfrak{p}}(E/K)$ (cf. (N, vii)) .
D'où le lemme.

(1.2) Lemme. Soit $\mathfrak{p}$ un idéal premier de E. Soit $x \in E^{\times}$, et soit $\lambda = v_{\mathfrak{p}}(x)$; alors il existe $\xi \in \mu_{F_{\mathfrak{p}}}$ tel que $N_{E_{\mathfrak{p}}/F_{\mathfrak{p}}} x \, N_{E_{\mathfrak{p}}/F_{\mathfrak{p}}} \pi_{\mathfrak{p}}^{-\lambda} \equiv \xi^{e(\mathfrak{p})} \bmod^{\times} \eta_{\mathfrak{p}}^{1}$ (cf.(N, i, iv, v, vi)).

On peut écrire, dans $E_{\mathfrak{p}}$,

$$x = \pi_{\mathfrak{p}}^{\lambda}(a_o + a\pi_{\mathfrak{p}}), \quad a_o \in \mathcal{O}_{N_{\mathfrak{p}}}^{*}, \quad a \in \mathcal{O}_{E_{\mathfrak{p}}}.$$

On sait que $\overline{N}_{\mathfrak{p}}^{\times}$ se relève dans $N_{\mathfrak{p}}$ en le groupe $\mu_{N_{\mathfrak{p}}}$ des racines $|\overline{N}_{\mathfrak{p}}^{\times}|$-ièmes de l'unité ; on peut donc supposer que $a_o = \xi_o \in \mu_{N_{\mathfrak{p}}}$. On a donc, dans $E_{\mathfrak{p}}$,

$$x = \pi_{\mathfrak{p}}^{\lambda} \xi_o \alpha, \quad \alpha \in 1 + \mathfrak{p}_{E_{\mathfrak{p}}} ;$$

d'où finalement, en posant $N_{N_{\mathfrak{p}}/F_{\mathfrak{p}}} \xi_o = \xi$:

$$N_{E_{\mathfrak{p}}/F_{\mathfrak{p}}} x \, N_{E_{\mathfrak{p}}/F_{\mathfrak{p}}} \pi_{\mathfrak{p}}^{-\lambda} \equiv \xi^{e(\mathfrak{p})} \bmod^{\times} \eta_{\mathfrak{p}}^{1}, \quad \xi \in \mu_{F_{\mathfrak{p}}}.$$

Ce résultat permet d'établir le théorème (0.2) :

En effet, d'après (1.1), si $Z_E = Z_F[\theta]$ et si σ est un générateur de H, $x = \theta - \theta^{\sigma}$ est un générateur de $\mathfrak{d}(E/L)$, auquel cas il suffit de poser $\delta(E/L) = N_{E/F} x$; on a alors $\delta(E/L) = N_{E/F} x = \prod_{s \in S_{\mathfrak{p}}} \prod_{t \in G_{\mathfrak{p},-1}} x^{ts} =$ $\prod_{s \in S_{\mathfrak{p}}} N_{E_{\mathfrak{p}}/F_{\mathfrak{p}}}(x^s)$ (cf.(N, ii)). D'après (1.2), on a $N_{E_{\mathfrak{p}}/F_{\mathfrak{p}}}(x^s) \equiv \xi_s^{e(\mathfrak{p})} N_{E_{\mathfrak{p}}/F_{\mathfrak{p}}} \pi_{\mathfrak{p}}^{v_{\mathfrak{p}}(x^s)} \bmod^{\times} \eta_{\mathfrak{p}}^{1}$, où $\xi_s \in \mu_{F_{\mathfrak{p}}}$; or $x^s = \theta^s - \theta^{s\sigma} = \theta^s - (\theta^s)^{s\sigma s^{-1}}$, et d'après (1.1) appliqué à θ^s (qui est aussi tel que $Z_E = Z_F[\theta^s]$), on a $v_{\mathfrak{p}}(x^s) = n_{\mathfrak{p}}(E/L_s)$ par définition.

D'où $\delta(E/L) \equiv \xi^{e(\mathfrak{p})} N_{E_{\mathfrak{p}}/F_{\mathfrak{p}}} \pi_{\mathfrak{p}}^{\lambda_{\mathfrak{p}}} \bmod^{\times} \eta_{\mathfrak{p}}^{1}$, où $\xi = \prod_{s \in S_{\mathfrak{p}}} \xi_s \in \mu_{F_{\mathfrak{p}}}$; d'où (i). Le cas d'une place à l'infini se traite de façon analogue à partir

de l'écriture $\tau_{\mathfrak{p}}(x^s) = a_s + \xi b_s$, a_s , $b_s \in \mathbf{R}$, $\xi^2 = -1$; si t engendre $\mathrm{Gal}(E/N(\mathfrak{p}))$, on a, pour tout $s \in S_{\mathfrak{p}}$:

$\tau_{\mathfrak{p}}(x^{tst}) = \tau_{\mathfrak{p}} \circ t \circ s(x) = \sigma_{-1} \circ \tau_{\mathfrak{p}} \circ s(x) = \sigma_{-1}(\tau_{\mathfrak{p}}(x^s))$, où σ_{-1} est la conjugaison complexe, d'où

$$\tau_{\mathfrak{p}}(x^{tst}) = a_s - \xi b_s$$

et

$$\tau_{\mathfrak{p}}\Big(\prod_{g \in G} x^g\Big) = \prod_{s \in S_{\mathfrak{p}}} (a_s + \xi b_s)(a_s - \xi b_s) = \prod_{s \in S_{\mathfrak{p}}} (a_s^2 + b_s^2) .$$

Faisons toujours l'hypothèse que $Z_E = Z_F[\theta]$, fixons un sous-groupe cyclique H de G , d'ordre $h > 1$, prenons-en un générateur σ , et considérons le nombre $\theta - \theta^{\sigma}$. Soit I un idéal premier de E vérifiant H0(I) ; pour tout $s \in S_I$ on peut écrire, dans E_I :

$$\theta^s = \sum_{i \geq 0} a_{i,s}\, \pi_I^i , \quad a_{i,s} \in \mathcal{O}_{N_I} . \tag{1.3}$$

Posons $\sigma_s = s\sigma s^{-1}$ pour tout $s \in S_I$ (d'après H0(I) , on a $\sigma_s \in G_{I,0}$) . On a

$$(\theta^{\sigma})^s = \theta^{s\sigma} = (\theta^s)^{\sigma_s} = \sum_{i \geq 0} a_{i,s}^{\sigma_s}\, \pi_I^{i\sigma_s} = \sum_{i \geq 0} a_{i,s}\, \pi_I^{i\sigma_s}$$

puisque $\sigma_s \in G_{I,0}$ et que $a_{i,s} \in \mathcal{O}_{N_I}$ pour tout s et tout i . On a donc

$$(\theta - \theta^{\sigma})^s = \theta^s - (\theta^s)^{\sigma_s} = \sum_{i \geq 1} a_{i,s}(\pi_I^i - \pi_I^{i\sigma_s}) ;$$

d'où

$$(\theta - \theta^{\sigma})^s = \sum_{i \geq 1} a_{i,s}\, \pi_I^i (1 - (\pi_I^{\sigma_s - 1})^i) . \tag{1.4}$$

(1.5) Lemme. On a $1 - (\pi_I^{\sigma_s - 1})^i \equiv 0 \bmod (1 - \pi_I^{\sigma_s - 1})\mathcal{O}_{E_I}$, pour tout $i \geq 1$ et tout $s \in S_I$.

(1.6) Lemme. On peut supposer que $a_{1,s} = \xi_s \in \mu_{N_I}$; en outre c'est un élément indépendant du choix de σ.

Si $a_{1,s} \equiv 0 \bmod I$ dans E_I, il en résulte que si l'on pose $v_I(1 - \pi_I^{\sigma_s - 1}) = k_s \geq 0$, on obtient $\theta^s - (\theta^s)^{\sigma_s} \equiv 0 \bmod \pi_I^{2+k_s}$. Or $\mathcal{O}_{E_I} = \mathcal{O}_{F_I}[\theta^s]$ puisque $Z_E = Z_F[\theta] = Z_F[\theta^s]$; on aurait donc $\sigma_s \in G_{I,k_s+1}$ ce qui est absurde puisque $v_I(1 - \pi_I^{\sigma_s - 1}) = k_s \geq 0$ équivaut à $\sigma_s \in G_{I,k_s} - G_{I,k_s+1}$. On peut donc supposer que $a_{1,s} = \xi_s \in \mu_{N_I}$. L'indépendance de ξ_s par rapport au choix de σ est claire, les $a_{i,s}$ étant définis par l'égalité (1.3).

Il vient donc, à partir de (1.4) :

$$(\theta - \theta^\sigma)^s = \xi_s \pi_I (1 - \pi_I^{\sigma_s - 1}) \alpha_{\sigma_s}, \quad \xi_s \in \mu_{N_I}, \quad \alpha_{\sigma_s} \in 1 + \pi_I \mathcal{O}_{E_I}.$$

Soit $t \in G_{I,-1}$; il vient

$$(\theta - \theta^\sigma)^{ts} = \xi_s^t \pi_I^t (1 - \pi_I^{\sigma_s - 1})^t \alpha_{\sigma_s}^t,$$

d'où, en décomposant tout $g \in G$ sous la forme $g = ts$, $t \in G_{I,-1}$, $s \in S_I$, on obtient, dans E_I :

$$\frac{N_{E/F}(\theta - \theta^\sigma)}{\prod_{s \in S_I} N_{E/M(I)}(\pi_I(1 - \pi_I^{\sigma_s - 1}))} \equiv \Big(\prod_{s \in S_I} N_{N_I/F_I} \xi_s \Big)^{e(I)} \bmod^\times \eta_I^1$$

$$\equiv \xi_I^{e(I)} \bmod^\times \eta_I^1,$$

où $\xi_I \in \mu_{F_I}$ est indépendant de σ.

Posons $\delta_\sigma(E/L) = N_{E/F}(\theta - \theta^\sigma)$; c'est un générateur de l'idéal $N_{E/F}\,\mathfrak{d}(E/L)$; il est norme d'entier (donc partout norme locale), et pour tout I vérifiant $H0(I)$, il vérifie la congruence suivante :

$$(1.7)\qquad \delta_\sigma(E/L) \prod_{s \in S_I} N_{E/M(I)}\left(\pi_I(1 - \pi_I^{\sigma_s - 1})\right)^{-1} \equiv \xi_I^{e(I)} \bmod^{\times} \eta_I^1 ,$$

où $\xi_I \in \mu_{F_I}$ est indépendante de σ ; ceci n'est autre que le théorème (0.4), puisque $\prod_{s \in S_I} N_{E/M(I)}\,\pi_I^{-1} = N_{E/M(I)}\,\pi_I^{-|S_I|}$.

(1.8) Remarques. (i) Une fois les uniformisantes π_I choisies numériquement, la vérification des conditions nécessaires données par les théorèmes (0.2) et (0.4) ne pose aucun problème pratique ; en ce qui concerne (0.4), on peut procéder comme suit :

Si $\delta_o(E/L) \in Z_F$ est un générateur quelconque de $N_{E/F}\,\mathfrak{d}(E/L)$, on cherche si, pour tout générateur σ de H, il existe une unité $\varepsilon_\sigma \in Z_F^*$ telle que les deux conditions suivantes aient lieu :

(α) $\varepsilon_\sigma\,\delta_o(E/L)$ est partout norme locale (on utilise par exemple (0.2)) ;

(β) pour tout idéal premier I vérifiant $H0(I)$, les images de $\varepsilon_\sigma\,\delta_o(E/L) \prod_{s \in S_I} N_{E/M(I)}(\pi_I(1 - \pi_I^{\sigma_s - 1}))^{-1}$ dans $\mathcal{O}_{F_I}^*/\eta_I^1$ sont des puissances $e(I)$-ièmes d'éléments indépendants de σ.

(ii) Si les groupes η_I^1 ne sont pas connus, on peut affaiblir la condition nécessaire en remplaçant (α), (β) par :

(α') pour tout idéal premier $\mathfrak{p}$ de E, ramifié dans E/F, l'image de $\varepsilon_\sigma\,\delta_o(E/L)$ dans $\overline{F}_{\mathfrak{p}}^{\times}$ est une puissance $e_{\mathfrak{p}}$-ième (cf.(N, viii)), et pour toute place à l'infini $\mathfrak{p}$ de E, ramifiée dans E/F, on a $\tau_{\mathfrak{p}}(\varepsilon_\sigma\,\delta_o(E/L)) > 0$ (cf.(N, x)).

(β') pour tout idéal premier vérifiant H0(I), les images de

$$\varepsilon_\sigma\, \delta_o(E/L) \prod_{s \in S_I} N_{E/M(I)} (\pi_I (1 - \pi_I^{\sigma_s - 1}))^{-1} \text{ dans } \overline{F}_I^{\chi},$$

sont des puissances e_I-ièmes d'éléments indépendants de σ.

L'algorithme précédent est à utiliser si l'on ne dispose pas, d'une manière générale, de l'hypothèse H1 ; dans le cas contraire, on peut élaborer considérablement les vérifications précédentes (c'est le but du §2 suivant).

2. Démonstration des théorèmes (0.6) et (0.9). Supposons donc que $Z_E = Z_F[\theta]$. Soit H un sous-groupe cyclique de G, d'ordre $h > 1$; on peut donc utiliser (0.4) qui affirme que pour tout générateur σ de H, il existe $\delta_\sigma(E/L)$, générateur de $N_{E/F}\, \mathfrak{d}(E/L)$, tel que pour tout idéal premier $\mathfrak{p}$ de E vérifiant H0($\mathfrak{p}$), on ait :

(2.1) $$\delta_\sigma(E/L) \prod_{s \in S_\mathfrak{p}} N_{E/M(\mathfrak{p})} \left(\pi_\mathfrak{p} (1 - \pi_\mathfrak{p}^{\sigma_s - 1})\right)^{-1} \equiv \xi_\mathfrak{p}^{e(\mathfrak{p})} \bmod^{\chi} \eta_\mathfrak{p}^1,$$

où $\xi_\mathfrak{p} \in \mu_{F_\mathfrak{p}}$ est indépendant de σ.

(2.2) Lemme. Soit σ un générateur de H ; si l'hypothèse H1($\mathfrak{p}$) est vérifiée, on a les résultats suivants :

(i) pour tout $g \in G$, on a $\pi_\mathfrak{p}^{g\sigma g^{-1} - 1} \equiv u^{\chi_\mathfrak{p}(g)} \bmod \pi_\mathfrak{p}$, où $u = \pi_\mathfrak{p}^{\sigma - 1} \in \mathcal{O}_{E_\mathfrak{p}}^*$ (cf. (0.1)) ;

(ii) pour tout $t \in G_{\mathfrak{p}, -1}$, l'image $\overline{u}$ de u dans $\overline{N}_\mathfrak{p}^{\chi}$ vérifie $\overline{u}^t = \overline{u}^{\chi_\mathfrak{p}(t)}$; en particulier, $\overline{u}$ est dans le sous-corps de $\overline{N}_\mathfrak{p}$ fixe par l'image, dans $G_{\mathfrak{p}, -1}/G_{\mathfrak{p}, 0} \simeq \mathrm{Gal}(\overline{N}_\mathfrak{p}/\overline{F}_\mathfrak{p})$, du noyau de $\chi_\mathfrak{p}$ dans $G_{\mathfrak{p}, -1}$.

Puisque $\sigma \in G_{\mathfrak{p},0}$, on a $u \in \mathcal{O}_{E_\mathfrak{p}}^*$ (i.e. $\bar{u} \in \bar{N}_\mathfrak{p}^{\chi}$). Soit $g \in G$; d'après H1($\mathfrak{p}$), on a $\sigma_g = g\sigma g^{-1} = t_1 \sigma^{\chi_\mathfrak{p}(g)}$, $t_1 \in G_{\mathfrak{p},1}$, d'où $\pi_\mathfrak{p}^{\sigma_g - 1} = \pi_\mathfrak{p}^{t_1 \sigma^{\chi_\mathfrak{p}(g)} - 1} = \left(\pi_\mathfrak{p}^{\sigma^{\chi_\mathfrak{p}(g)}}\right)^{t_1} \pi_\mathfrak{p}^{-1} \equiv u^{\chi_\mathfrak{p}(g)} \pi_\mathfrak{p}^{t_1 - 1} \equiv u^{\chi_\mathfrak{p}(g)} \bmod \pi_\mathfrak{p}$,

car $\pi_\mathfrak{p}^{t_1 - 1} \equiv 1 \bmod \pi_\mathfrak{p}$, $u^\sigma \equiv u$, et $u^{t_1} \equiv u \bmod \pi_\mathfrak{p}$ (ce qui établit (i)).

Soit $t \in G_{\mathfrak{p},-1}$; on a $u^t = (\pi_\mathfrak{p}^{\sigma - 1})^t = \pi_\mathfrak{p}^{t\sigma}\, \pi_\mathfrak{p}^{-t} = \pi_\mathfrak{p}^{\sigma_t t}\, \pi_\mathfrak{p}^{-t} = (\pi_\mathfrak{p}^t)^{\sigma_t - 1}$, où $\sigma_t = t\sigma t^{-1}$. Posons $\pi_\mathfrak{p}^t = w_t \pi_\mathfrak{p}$, $w_t \in \mathcal{O}_{E_\mathfrak{p}}^*$; il vient $u^t = (w_t \pi_\mathfrak{p})^{\sigma_t - 1} = w_t^{\sigma_t - 1}\, \pi_\mathfrak{p}^{\sigma_t - 1}$, mais, par normalité de $G_{\mathfrak{p},0}$ dans $G_{\mathfrak{p},-1}$, on a $\sigma_t \in G_{\mathfrak{p},0}$ et $w_t^{\sigma_t - 1} \equiv 1 \bmod \pi_\mathfrak{p}$, d'où $u^t \equiv \pi_\mathfrak{p}^{\sigma_t - 1} \bmod \pi_\mathfrak{p}$, soit, d'après (i), $u^t \equiv u^{\chi_\mathfrak{p}(t)} \bmod \pi_\mathfrak{p}$ (d'où (ii)).

Considérons maintenant (2.1) pour deux générateurs σ, σ' de H et pour tout $\mathfrak{p}$ vérifiant cette fois H1($\mathfrak{p}$) ; il vient :

$$\frac{\delta_\sigma(E/L)}{\delta_{\sigma'}(E/L)} \equiv \prod_{s \in S_\mathfrak{p}} N_{E/M(\mathfrak{p})} \left(\frac{1 - \pi_\mathfrak{p}^{\sigma_s - 1}}{1 - \pi_\mathfrak{p}^{\sigma'_s - 1}} \right) \bmod^{\times} \eta_\mathfrak{p}^1 . \tag{2.3}$$

Ecrivons, à partir d'un générateur σ_o fixé de H, $\sigma = \sigma_o^a$, $\sigma' = \sigma_o^b$, $a, b \in (\mathbb{Z}/h\mathbb{Z})^*$; on a, pour tout $s \in S_\mathfrak{p}$, $\sigma_s = \sigma_{0,s}^a$ et $\sigma'_s = \sigma_{0,s}^b$. Posons alors $\pi_\mathfrak{p}^{\sigma_o - 1} = u$, et soit $\xi_\mathfrak{p} \in \mu_{N_\mathfrak{p}}$ tel que $\bar{u} = \bar{\xi}_\mathfrak{p}$ dans $\bar{N}_\mathfrak{p}^{\chi}$; d'après (2.2), l'image de $u_s = \pi_\mathfrak{p}^{\sigma_{0,s} - 1}$ dans $\bar{N}_\mathfrak{p}^{\chi}$ est $\bar{\xi}_\mathfrak{p}^{\chi_\mathfrak{p}(s)}$. Deux cas se présentent, selon que $h_\mathfrak{p} > 1$ ou $h_\mathfrak{p} = 1$:

a) <u>H d'ordre non puissance de p</u> (i.e. $h_\mathfrak{p} \neq 1$). On sait que l'application qui à $t \in G_{\mathfrak{p},0}$ associe $\pi_\mathfrak{p}^{t-1} \bmod \mathfrak{p}$ induit un isomorphisme de

$G_{\mathfrak{p},0}/G_{\mathfrak{p},1}$ sur un sous-groupe de $\overline{N}_{\mathfrak{p}}^{\times}$; donc d'une part $\xi_{\mathfrak{p}}$ est d'ordre $h_{\mathfrak{p}} \neq 1$ et d'autre part on a :

$$\frac{1 - \pi_{\mathfrak{p}}^{\sigma_{0,s}^{a} - 1}}{1 - \pi_{\mathfrak{p}}^{\sigma_{0,s}^{b} - 1}} \equiv \frac{1 - \xi_{\mathfrak{p}}^{a\chi_{\mathfrak{p}}(s)}}{1 - \xi_{\mathfrak{p}}^{b\chi_{\mathfrak{p}}(s)}} \mod^{\times} (1 + \mathfrak{p}_{E_{\mathfrak{p}}})$$

d'où

$$\frac{\delta_{\sigma}(E/L)}{\delta_{\sigma'}(E/L)} \equiv \prod_{s \in S_{\mathfrak{p}}} N_{E/M(\mathfrak{p})} \left(\frac{1 - \xi_{\mathfrak{p}}^{a\chi_{\mathfrak{p}}(s)}}{1 - \xi_{\mathfrak{p}}^{b\chi_{\mathfrak{p}}(s)}} \right)$$

$$\equiv \prod_{s \in S_{\mathfrak{p}}} N_{N(\mathfrak{p})/M(\mathfrak{p})} \left(\frac{1 - \xi_{\mathfrak{p}}^{a\chi_{\mathfrak{p}}(s)}}{1 - \xi_{\mathfrak{p}}^{b\chi_{\mathfrak{p}}(s)}} \right)^{e(\mathfrak{p})} \mod^{\times} \eta_{\mathfrak{p}}^{1} .$$

Comme $\delta_{\sigma}(E/L)$ et $\delta_{\sigma'}(E/L)$ sont les normes dans E/F de générateurs du même idéal $\mathfrak{d}(E/L)$, $\dfrac{\delta_{\sigma}(E/L)}{\delta_{\sigma'}(E/L)}$ est la norme, dans E/F, d'une unité de Z_E^* ; posons

$$\varepsilon_{a,b} = \frac{\delta_{\sigma}(E/L)}{\delta_{\sigma'}(E/L)} \text{ , où } \sigma = \sigma_o^a \text{ , } \sigma' = \sigma_o^b \text{ , } \sigma_o \text{ fixé ;}$$

il vient alors, pour tout idéal premier $\mathfrak{p}$ vérifiant H1($\mathfrak{p}$) :

(2.4) $$\varepsilon_{a,b} \equiv \prod_{s \in S_{\mathfrak{p}}} N_{N(\mathfrak{p})/M(\mathfrak{p})} \left(\frac{1 - \xi_{\mathfrak{p}}^{a\chi_{\mathfrak{p}}(s)}}{1 - \xi_{\mathfrak{p}}^{b\chi_{\mathfrak{p}}(s)}} \right)^{e(\mathfrak{p})} \mod^{\times} \eta_{\mathfrak{p}}^{1} .$$

Cette relation induit, au niveau des images dans $\overline{F}_{\mathfrak{p}}^{\times}$, la relation

(2.5) $$\bar{\varepsilon}_{a,b} = \prod_{s \in S_{\mathfrak{p}}} N_{\overline{N}_{\mathfrak{p}}/\overline{F}_{\mathfrak{p}}} \left(\frac{1 - \bar{\xi}_{\mathfrak{p}}^{a\chi_{\mathfrak{p}}(s)}}{1 - \bar{\xi}_{\mathfrak{p}}^{b\chi_{\mathfrak{p}}(s)}} \right)^{e(\mathfrak{p})}$$

$$= \prod_{s \in S_{\mathfrak{p}}} \prod_{i=1}^{r(\mathfrak{p})} \left(\frac{1 - \bar{\xi}_{\mathfrak{p}}^{a\chi_{\mathfrak{p}}(s) f_{\mathfrak{p}}^{i}}}{1 - \bar{\xi}_{\mathfrak{p}}^{b\chi_{\mathfrak{p}}(s) f_{\mathfrak{p}}^{i}}} \right)^{e(\mathfrak{p})} .$$

On a alors $\bar{\varepsilon}_{a,b} \in X_{\mathfrak{p}} \cap Y_{\mathfrak{p}}$ (cf.(N, ix)), ce qui implique

$$\prod_{s \in S_{\mathfrak{p}}} N_{\overline{N}_{\mathfrak{p}}/\overline{F}_{\mathfrak{p}}} \left(\frac{1 - \bar{\xi}_{\mathfrak{p}}^{a\chi_{\mathfrak{p}}(s)}}{1 - \bar{\xi}_{\mathfrak{p}}^{b\chi_{\mathfrak{p}}(s)}} \right)^{e_{\mathfrak{p}} w_{\mathfrak{p}}} = \bar{1} \text{ , pour tout } a, b \in (\mathbb{Z}/h\mathbb{Z})^{*}$$

(on a pu remplacer $e(\mathfrak{p})$ par $e_{\mathfrak{p}}$ car $\overline{F}_{\mathfrak{p}}$ est de caractéristique p) .

Remarque. Le fait de ne considérer (2.4) que modulo $\mathfrak{p}$ (cf.(2.5)) et non modulo $^{\times}\eta_{\mathfrak{p}}^{1}$ n'est pas restrictif ; en effet, posons $e(\mathfrak{p}) = p^{r} e_{\mathfrak{p}}$, et $\eta = \prod_{s \in S_{\mathfrak{p}}} N_{N(\mathfrak{p})/M(\mathfrak{p})} \left(\frac{1 - \xi_{\mathfrak{p}}^{a\chi_{\mathfrak{p}}(s)}}{1 - \xi_{\mathfrak{p}}^{b\chi_{\mathfrak{p}}(s)}} \right)$; la relation (2.5) conduit à

$\bar{\varepsilon}_{a,b}^{p^{R}} = \bar{\eta}^{e_{\mathfrak{p}}}$, où $R \geq 0$ est un entier convenable tel que $r + R$ soit l'ordre du frobenius dans $\mathrm{Gal}(\overline{F}_{\mathfrak{p}}/\mathbb{F}_{p})$; il vient alors

$$\varepsilon_{a,b}^{p^{R}} \equiv \eta^{e_{\mathfrak{p}}} \mod^{\times} (1 + \mathfrak{p}_{F_{\mathfrak{p}}}) ,$$

soit

$$\varepsilon_{a,b}^{p^{r+R}} \equiv \eta^{e(\mathfrak{p})} \mod^{\times} (1 + \mathfrak{p}_{F_{\mathfrak{p}}})^{p^{r}} ;$$

or on a $(1 + \mathfrak{p}_{F_{\mathfrak{p}}})^{p^{r}} \subseteq \eta_{\mathfrak{p}}^{1}$, et par hypothèse $\varepsilon_{a,b}$ est norme locale en $\mathfrak{p}$ dans E/F , et il existe donc $\xi_{a,b} \in \mu_{F_{\mathfrak{p}}}$ telle que

$\varepsilon_{a,b} \equiv \xi_{a,b} \mod^{\times} \eta_{\mathfrak{p}}^{1}$, d'où

$$\epsilon_{a,b}^{p^{r+R}} \equiv \xi_{a,b}^{p^{r+R}} \equiv \xi_{a,b} \equiv \epsilon_{a,b} \bmod^{\times} \eta_{\mathfrak{p}}^{1} ,$$

soit

$$\epsilon_{a,b} \equiv \eta^{e(\mathfrak{p})} \bmod^{\times} \eta_{\mathfrak{p}}^{1} ,$$

ce qui redonne bien (2.4).

Ceci étant, la démonstration de (0.6) résulte alors de l'application du lemme suivant au polynome

$$f(X,Y) = \prod_{s \in S_{\mathfrak{p}}} \prod_{i=1}^{r(\mathfrak{p})} \left(1 - X^{a\chi_{\mathfrak{p}}(s) f_{\mathfrak{p}}^{i}}\right)^{e_{\mathfrak{p}} w_{\mathfrak{p}}}$$

$$- \prod_{s \in S_{\mathfrak{p}}} \prod_{i=1}^{r(\mathfrak{p})} \left(1 - Y^{b\chi_{\mathfrak{p}}(s) f_{\mathfrak{p}}^{i}}\right)^{e_{\mathfrak{p}} w_{\mathfrak{p}}}$$

où, par abus, les exposants a, b, $\chi_{\mathfrak{p}}(s)$ sont ici des relèvements arbitraires dans $\mathbb{N}$ des éléments de $(\mathbb{Z}/h\mathbb{Z})^{*}$ qu'ils désignent :

(2.6) Lemme. Soit p un nombre premier et soit c un entier étranger à p. Soit μ_c (resp. $\tilde{\mu}_c$) le groupe des racines c-ièmes de l'unité dans $\mathbb{C}$ (resp. dans une clôture algébrique $\tilde{\mathbb{F}}_p$ de $\mathbb{F}_p$). Soit $f \in \mathbb{Z}[X,Y]$; alors les conditions suivantes sont équivalentes :

(i) $f(\tilde{\zeta}, \tilde{\zeta}') = 0$ dans $\tilde{\mathbb{F}}_p$, pour tous générateurs $\tilde{\zeta}$, $\tilde{\zeta}'$ de $\tilde{\mu}_c$;

(ii) $f(\zeta, \zeta') \equiv 0 \bmod p\mathbb{Z}[\mu_c]$, pour tous générateurs ζ, ζ' de μ_c.

Soit $\mathfrak{P}$ un idéal premier de $\mathbb{Z}[\mu_c]$ divisant p, et considérons l'homomorphisme de $\mathbb{Z}[\mu_c]$ dans $\tilde{\mathbb{F}}_p$, de noyau $\mathfrak{P}$, qui identifie μ_c à $\tilde{\mu}_c$. Le point (i) équivaut alors à l'écriture $f(\zeta, \zeta') \equiv 0 \bmod \mathfrak{P}$ pour tous ζ, ζ' engendrant μ_c. En conjuguant cette relation par les

éléments τ de $\mathrm{Gal}(\mathbb{Q}(\mu_c)/\mathbb{Q})$, il vient $f(\zeta, \zeta') \equiv 0 \bmod \mathfrak{p}^{\tau}$, pour tous ζ, ζ' engendrant μ_c ; d'où (ii) puisque $\bigcap_{\tau} \mathfrak{p}^{\tau} = p\mathbb{Z}[\mu_c]$. L'implication inverse est triviale .

b) <u>H d'ordre puissance de p</u> (i.e. $h_{\mathfrak{p}} = 1$) . Dans ce cas, on rappelle que, d'après (R, ii), les hypothèses H1($\mathfrak{p}$) et H0($\mathfrak{p}$) coïncident, que l'on a $H \subseteq G_{\mathfrak{p},1}$ et que $\chi_{\mathfrak{p}} = 1$ (cf.(0.1)). Pour tout $s \in S_{\mathfrak{p}}$ posons

$$\pi_{\mathfrak{p}}^{\sigma_{0,s}-1} = 1 + \pi_{\mathfrak{p}}^{k_s} v_s \ , \ k_s \geq 1 \ , \ v_s \in \mathcal{O}_{E_{\mathfrak{p}}}^{*} \ .$$

Ici, l'application qui à $t \in G_{\mathfrak{p},i}$, $i \geq 1$, associe la classe de $(\pi_{\mathfrak{p}}^{t-1} - 1)\pi_{\mathfrak{p}}^{-i}$ modulo $\pi_{\mathfrak{p}}$ est un homomorphisme de $G_{\mathfrak{p},i}$ dans le groupe additif $\overline{N}_{\mathfrak{p}}$; donc, puisque $\sigma_s = \sigma_{0,s}^{a}$, $\sigma_s' = \sigma_{0,s}^{b}$, il vient :

$$\pi_{\mathfrak{p}}^{\sigma_s - 1} \equiv 1 + \pi_{\mathfrak{p}}^{k_s} a v_s \bmod \pi_{\mathfrak{p}}^{k_s+1} \ ,$$

$$\pi_{\mathfrak{p}}^{\sigma_s' - 1} \equiv 1 + \pi_{\mathfrak{p}}^{k_s} b v_s \bmod \pi_{\mathfrak{p}}^{k_s+1} \ ,$$

d'où

$$\frac{1 - \pi_{\mathfrak{p}}^{\sigma_s - 1}}{1 - \pi_{\mathfrak{p}}^{\sigma_s' - 1}} \equiv \frac{a}{b} \bmod^{\times} (1 + \mathfrak{p}_{E_{\mathfrak{p}}}) \ .$$

D'où, d'après (2.3), et pour tout idéal premier $\mathfrak{p}$ vérifiant H1($\mathfrak{p}$) :

$$\frac{\delta_{\sigma}(E/L)}{\delta_{\sigma'}(E/L)} \equiv \prod_{s \in S_{\mathfrak{p}}} N_{E/M(\mathfrak{p})}\left(\frac{a}{b}\right) \equiv \left(\frac{a}{b}\right)^{n} \bmod^{\times} \eta_{\mathfrak{p}}^{1} \ ;$$

c'est-à-dire que pour tout $a, b \in (\mathbb{Z}/h\mathbb{Z})^{*}$, il existe une unité $\epsilon_{a,b} \in N_{E/F} Z_E^{*}$ telle que

$$\epsilon_{a,b} \equiv (ab^{-1})^{n} \bmod^{\times} \eta_{\mathfrak{p}}^{1} \ ,$$

ce qui conduit en particulier à

(2.7) $$\bar{\varepsilon}_{a,b} = (\bar{a}\,\bar{b}^{-1})^{n} \text{ dans } \bar{F}_{\mathfrak{p}}^{\times} .$$

On a donc de même $\bar{\varepsilon}_{a,b} \in X_{\mathfrak{p}} \cap Y_{\mathfrak{p}}$ (avec $Y_{\mathfrak{p}} = \mathbf{F}_{p}$), d'où $(\bar{a}\,\bar{b}^{-1})^{nw_{\mathfrak{p}}} = \bar{1}$ pour tout $a,b \in (\mathbf{Z}/h\mathbf{Z})^{*}$, donc en fait pour tout $a,b \in \mathbf{F}_{p}^{\times}$. On peut aussi remplacer l'exposant $nw_{\mathfrak{p}}$ par l'exposant $\operatorname{pgcd}(p-1, nw_{\mathfrak{p}})$; or ici $\xi_{\mathfrak{p}} = 1$, auquel cas $q_{\mathfrak{p}} = p$ et $h_{\mathfrak{p}} = 1$, et (0.6) est démontré dans ce cas puisqu'alors $\dfrac{1-\zeta_{\mathfrak{p}}^{a}}{1-\zeta_{\mathfrak{p}}^{b}}$ s'interprète comme étant ab^{-1} modulo p (cf.(N, viii)).

Remarque. Comme dans le cas (i), la relation (2.7) n'est pas moins forte que la relation $\varepsilon_{a,b} \equiv (ab^{-1})^{n} \bmod^{\times} \eta_{\mathfrak{p}}^{1}$, comme on le vérifie facilement.

Le théorème (0.9) résulte simplement du fait que pour tout $a,b \in (\mathbf{Z}/h\mathbf{Z})^{*}$, il existe une unité $\varepsilon_{a,b}$ de F, partout norme locale dans E/F, telle que pour tout idéal premier $\mathfrak{p}$ de E vérifiant H1($\mathfrak{p}$), on ait la relation (2.5) (resp.(2.7)) dans le cas $h_{\mathfrak{p}} \neq 1$ (resp. $h_{\mathfrak{p}} = 1$).

Le corollaire (0.7) résulte du fait que, lorsque $\chi_{\mathfrak{p}} = 1$, on a $\bar{\xi}_{\mathfrak{p}} \in \bar{F}_{\mathfrak{p}}$ (cf.(2.2, ii)), auquel cas $\bar{\xi}_{\mathfrak{p}}^{f_{\mathfrak{p}}} = \bar{\xi}_{\mathfrak{p}}$, et la relation (2.5) (comme (2.7)) s'écrit alors :

$$\bar{\varepsilon}_{a,b} = \Big(\frac{1-\bar{\xi}_{\mathfrak{p}}^{a}}{1-\bar{\xi}_{\mathfrak{p}}^{b}}\Big)^{n}, \text{ pour tout } a,b \in (\mathbf{Z}/h\mathbf{Z})^{*} ;$$

d'où la congruence correspondante dans $\mathbf{Z}[\zeta_{\mathfrak{p}}]$, après avoir remplacé l'exposant $nw_{\mathfrak{p}}$ par l'exposant $e_{\mathfrak{p}} d_{\mathfrak{p}}$. D'où également le corollaire (0.10).

3. Application aux extensions absolument abéliennes. On suppose donc que $F = \mathbb{Q}$ et que E est une extension abélienne de $\mathbb{Q}$ de degré n et de groupe de Galois G. On désigne par R l'ensemble des nombres premiers ramifiés dans $E/\mathbb{Q}$; dans le cas abélien, les idéaux premiers $\mathfrak{p}$ de E, ramifiés dans $E/\mathbb{Q}$, n'interviennent que par le nombre premier $p \in R$ correspondant, aussi suffit-il de tout indexer via les éléments de R.

On désigne par f le conducteur de E, par f_p (resp. f'_p), pour $p \in R$, la p-partie de f (resp. f/f_p), et par $\mathbb{Q}(f)$ (resp. $\mathbb{Q}(f_p)$, $\mathbb{Q}(f'_p)$) le corps cyclotomique des racines f-ièmes (resp. f_p, f'_p-ièmes) de l'unité dans $\mathbb{C}$. On désigne par ω_p un générateur du groupe des racines f_p-ièmes de l'unité.

On sait que $\mathbb{Q}(f)$ est composé direct sur $\mathbb{Q}$ des corps $\mathbb{Q}(f_p)$, $p \in R$, et que les groupes d'inertie des $p \in R$ sont les groupes $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q}(f'_p))$ qui constituent la décomposition en somme directe de $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})$ correspondante. On identifie $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q})$ et $(\mathbb{Z}/f\mathbb{Z})^*$ au moyen de l'application d'Artin qui à $\bar{a} \in (\mathbb{Z}/f\mathbb{Z})^*$ associe l'automorphisme σ_a défini par $\omega^{\sigma_a} = \omega^a$ pour toute racine f-ième de l'unité ω.

On désigne alors par $A \subseteq (\mathbb{Z}/f\mathbb{Z})^*$ le groupe d'Artin

$$A = \mathrm{Gal}(\mathbb{Q}(f)/E),$$

et on pose :

$$A' = \{ a \in \mathbb{Z},\ (a,f) = 1,\ \sigma_a \in A \}.$$

Pour $p \in R$, notons $M(p)$ (resp. $N(p)$) le corps de décomposition (resp. d'inertie) de p dans $E/\mathbb{Q}$; on a donc ici $N(p) = E \cap \mathbb{Q}(f'_p)$.

On pose également $E'(p) = E\,\mathbb{Q}(f'_p)$ et $E(p) = E'(p) \cap \mathbb{Q}(f_p)$.

Soit H un sous-groupe cyclique non trivial de G dont on fixe un générateur σ_o, et soit L le sous-corps de E fixe par H. Désignons par $R(E/L)$ le sous-ensemble de R formé des p totalement

ramifiés dans E/L , et par $\delta(E/L)$ le générateur positif de l'idéal $N_{E/\mathbb{Q}}\,\mathfrak{d}(E/L)$; c'est, d'après (N, vii), l'entier défini par

$$N_{E/\mathbb{Q}}\,\mathfrak{d}(E/L) = \prod_{p \in R(E/L)} p^{n_p(E/L)\,n/e(p)} \quad , \text{ où } e(p) = [E : N(p)] .$$

La valeur de $n_p(E/L)$ (égale à $n_{\mathfrak{p}}(E/L)$ pour tout $\mathfrak{p}|p$) se trouve facilement dans le cadre abélien, et est donnée par le résultat suivant :

(3.1) Lemme. Si $h = |H|$ n'est pas une puissance de p , alors $n_p(E/L) = 1$.

Si $h = p^{j_p}$, $j_p \geq 1$, et si $p \neq 2$, on a $n_p(E/L) = \dfrac{f_p\, p^{-j_p} - 1}{p - 1}\, e_p + 1$.

Enfin si $p = 2$, nécessairement $h = 2^{j_2}$, $j_2 \geq 1$, et $n_2(E/L)$ a la valeur suivante :

(i) si $E(2) = \mathbb{Q}(\omega_2 + \omega_2^{-1})$ ou $\mathbb{Q}(\omega_2 - \omega_2^{-1})$, on a

$n_2(E/L) = f_2\, 2^{-j_2 - 1} + 1$;

(ii) si $E(2) = \mathbb{Q}(\omega_2)$, on a $n_2(E/L) = 2$ sauf si

$(L\,\mathbb{Q}(f_2')) \cap \mathbb{Q}(f_2) = \mathbb{Q}(f_2\, 2^{-j_2})$, auquel cas $n_2(E/L) = f_2\, 2^{-j_2}$.

Si $h_p \neq 1$, on a $H \subseteq G_{p,0}$, $H \not\subseteq G_{p,1}$, d'où $n_p(E/L) = 1$.

Supposons que $h = p^{j_p}$. On a $n_p(E/L) = k + 1$, où k est défini par l'égalité $\pi_p^{\sigma_o - 1} = 1 + \alpha\, \pi_p^k$, α étranger à π_p , où σ_o engendre H .

Posons $\pi = N_{\mathbb{Q}(f)/E'(p)}(1 - \omega_p)$; comme $\mathbb{Q}(f)/E'(p)$ est totalement ramifiée et $E'(p)/E$ non ramifiée en p , π est une uniformisante dans $E'(p)$ et il existe $u \in E'(p)$ étranger à π tel que $u\,\pi = \pi_p$ (cf.(3.5)) .

En relevant σ_o dans $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q}(f_p'))$ en σ_a , a convenable, on a

$$\pi_p^{\sigma_o - 1} = u^{\sigma_a - 1}\, \pi^{\sigma_a - 1} = 1 + \alpha\, \pi_p^k = 1 + \alpha'\, \pi^k \quad , \quad \alpha' \in E'(p)$$

étranger à π ; comme $u^{\sigma_a - 1} \equiv 1 \bmod \pi(\pi^{\sigma_a - 1} - 1)$, il suffit donc de calculer la π-valuation de $\pi^{\sigma_a - 1} - 1$ dans $E'(p)$, ou, ce qui revient au même, dans $E(p)/\mathbb{Q}$ puisque $\pi \in E(p)$.

a) Cas $p \neq 2$. Posons $d = [\mathbb{Q}(f_p) : E(p)]$; on a $(d, p) = 1$ sinon le conducteur de E diviserait $f p^{-1}$, d'où en fait :

$$d = \frac{p - 1}{e_p} .$$

On peut prendre $a = 1 + f_p p^{-j_p}$ car c'est un élément d'ordre p^{j_p} dans $(\mathbb{Z}/f_p\mathbb{Z})^*$ qui est ici cyclique. Posons $f_p p^{-j_p} = p^r$, $r \geq 1$. On a alors

$$\pi^{\sigma_a - 1} = N_{\mathbb{Q}(f_p)/E(p)} \left(\frac{1 - \omega_p^a}{1 - \omega_p} \right) ;$$

or

$$\frac{1 - \omega_p^a}{1 - \omega_p} = \frac{1 - \omega_p + \omega_p(1 - \omega_p^{p^r})}{1 - \omega_p} = 1 + \omega_p \frac{1 - \omega_p^{p^r}}{1 - \omega_p}$$

$$\equiv 1 + (1 - \omega_p)^{p^r - 1} \bmod (1 - \omega_p)^{p^r} ,$$

car $\mathbb{Q}(\omega_p)/\mathbb{Q}$ est totalement ramifiée en p et de degré multiple de p^r puisqu'on a supposé $j_p \geq 1$.

Si $(i, p) = 1$, on a $(1 - \omega_p^i)^{p^r - 1} = (1 - \omega_p)^{p^r - 1} \left(\frac{1 - \omega_p^i}{1 - \omega_p} \right)^{p^r - 1}$;

or $\left(\frac{1 - \omega_p^i}{1 - \omega_p} \right)^{p^r - 1} \equiv i^{p^r - 1} \equiv 1 \bmod (1 - \omega_p)$, d'où

$(1 - \omega_p^i)^{p^r - 1} \equiv (1 - \omega_p)^{p^r - 1} \bmod (1 - \omega_p)^{p^r}$, et on obtient

$$\pi^{\sigma_a - 1} \equiv 1 + d(1 - \omega_p)^{p^r - 1} \mod (1 - \omega_p)^{p^r} .$$

Finalement, on obtient pour $p \neq 2$:

$$n_p(E/L) = \frac{p^r - 1}{d} + 1 = e_p \frac{p^r - 1}{p - 1} + 1 = e_p \frac{f_p p^{-j_p} - 1}{p - 1} + 1 .$$

b) Cas $p = 2$. Le corps $E(2)$ est l'un des 3 corps

$$\mathbb{Q}(\omega_2) = \mathbb{Q}(f_2) , \quad \mathbb{Q}(\omega_2 + \omega_2^{-1}) , \quad \mathbb{Q}(\omega_2 - \omega_2^{-1}) ,$$

les 2 derniers cas supposant $f_2 \equiv 0 \mod 8$.

(i) $E(2) = \mathbb{Q}(\omega_2)$. Si $f_2 = 4$, on a $\pi = 1 - i$ et dans ce cas

$$\pi^{\sigma_a - 1} - 1 = \frac{1 + i}{1 - i} - 1 = -\pi , \text{ d'où}$$

$$n_2(E/L) = 2 \text{ dans ce cas.}$$

Supposons maintenant $f_2 \equiv 0 \mod 8$; on a $\pi = 1 - \omega_2$, et

$$a = 1 + f_2 2^{-j_2} , \text{ ou } a = -1 - f_2 2^{-j_2} , \text{ ou } a = -1 \text{ (et } j_2 = 1) .$$

Posons $f_2 2^{-j_2} = 2^r$. On a, avec $a = 1 + 2^r$:

$$\pi^{\sigma_a - 1} = (1 - \omega_2)^{\sigma_a - 1} = \frac{1 - \omega_2 + \omega_2(1 - \omega_2^{2^r})}{1 - \omega_2}$$

$$= 1 + \omega_2 \frac{1 - \omega_2^{2^r}}{1 - \omega_2}$$

$$\equiv 1 + (1 - \omega_2)^{2^r} - 1 \mod (1 - \omega_2)^{2^r} ,$$

d'où $n_2(E/L) = f_2 2^{-j_2}$.

Avec $a = -1 - 2^r$, on a :

$$\pi^{\sigma_a - 1} = \frac{1 - \omega_2^{-1-2^r}}{1 - \omega_2} = \frac{1 - \omega_2^{-1} + \omega_2^{-1}(1 - \omega_2^{-2^r})}{1 - \omega_2}$$

$$= \frac{1 - \omega_2^{-1}}{1 - \omega_2} + \omega_2^{-1} \frac{1 - \omega_2^{-2^r}}{1 - \omega_2} ;$$

or dans ce cas, on a $r \geq 2$ (car $2^{j_2} \leq f_2/4$), et on a

$\frac{1 - \omega_2^{-1}}{1 - \omega_2} = 1 - \omega_2^{-1} \frac{1 - \omega_2^2}{1 - \omega_2}$, d'où $\pi^{\sigma_a - 1} \equiv 1 + \frac{1 - \omega_2^2}{1 - \omega_2} \mod (1 - \omega_2)^2$.

On a donc ici $k = 1$ et $n_2(E/L) = 2$.

Si $a = -1$, on a $\pi^{\sigma_a - 1} = \frac{1 - \omega_2^{-1}}{1 - \omega_2} = -\omega_2^{-1} \equiv 1 - \pi \mod \pi^2$; d'où

$n_2(E/L) = 2$ encore.

(ii) $E(2) = \mathbb{Q}(\omega_2 + \omega_2^{-1})$. On a dans ce cas

$a = 1 + 2^r$, où l'on a posé $2^r = f_2 2^{-j_2}$.

On a $\pi = (1 - \omega_2)(1 - \omega_2^{-1}) = -\omega_2^{-1}(1 - \omega_2)^2$; d'où

$$\pi^{\sigma_a - 1} = \omega_2^{-2^r} \left(1 + \omega_2 \frac{1 - \omega_2^{2^r}}{1 - \omega_2}\right)^2$$

$$= \omega_2^{-2^r} \left(1 + \omega_2^2 \left(\frac{1 - \omega_2^{2^r}}{1 - \omega_2}\right)^2 + 2\omega_2 \frac{1 - \omega_2^{2^r}}{1 - \omega_2}\right) ;$$

or $2 \equiv 0 \mod (1 - \omega_2)^{f_2 2^{-1}}$ et $f_2 2^{-1} + 2^r - 1 > 2(2^r - 1)$

d'où, puisqu'on a aussi $r \geq 2$,

$$\pi^{\sigma_a - 1} - 1 \equiv -1 + \omega_2^{-2^r} + (1 - \omega_2)^{2(2^r - 1)} \mod (1 - \omega_2)^{2^{r+1} - 1}$$

$$\equiv -1 + \omega_2^{-2^r} \mod (1 - \omega_2)^{2^r + 1} ,$$

d'où $n_2(E/L) = 2^{r-1} + 1 = f_2 2^{-j_2 - 1} + 1$.

(iii) $E(2) = \mathbb{Q}(\omega_2 - \omega_2^{-1})$. On a encore $a = 1 + 2^r$, où $2^r = f_2 2^{-j_2}$. On a $\pi = (1 - \omega_2)(1 + \omega_2^{-1}) = 1 - \omega_2 + \omega_2^{-1} - 1 = \omega_2^{-1}(1 - \omega_2^2)$:

d'où

$$\pi^{\sigma_a - 1} = \omega_2^{-2^r} \frac{1 - \omega_2^{2 + 2^{r+1}}}{1 - \omega_2^2} = \omega_2^{-2^r} \frac{1 - \omega_2^2 + \omega_2^2(1 - \omega_2^{2^{r+1}})}{1 - \omega_2^2}$$

$$= \omega_2^{-2^r} \left(1 + \omega_2^2 \frac{1 - \omega_2^{2^{r+1}}}{1 - \omega_2^2}\right)$$

$$= \omega_2^{-2^r} + \omega_2^{2 - 2^r} \frac{1 - \omega_2^{2^{r+1}}}{1 - \omega_2^2}$$

et

$$\pi^{\sigma_a - 1} - 1 = \omega_2^{-2^r} - 1 + \omega_2^{2 - 2^r} \frac{1 - \omega_2^{2^{r+1}}}{1 - \omega_2^2} ;$$

comme $r \geq 2$, il vient

$$\pi^{\sigma_a - 1} - 1 \equiv (\omega_2 - 1)^{2^r} \mod (1 - \omega_2)^{2^r + 1}$$

et ici

$$n_2(E/L) = 2^{r-1} + 1 = f_2 2^{-j_2 - 1} + 1 .$$

Ce qui achève la démonstration du lemme.

(3.2) Conditions nécessaires de monogénéité (algorithme pratique).

Pour analyser en pratique l'éventuelle non monogénéité de Z_E, il suffit d'effectuer les étapes suivantes (ceci pour tous les choix de H possibles) :

(i) On vérifie que pour tout $p \in R$ tel que $H \subseteq G_{p,0}$, H d'ordre h non puissance de p, on a

$$\left(\frac{1-\zeta_p^a}{1-\zeta_p^b}\right)^{e_p d_p} \equiv 1 \bmod p\mathbb{Z}[\zeta_p], \text{ pour tout } a,b \in (\mathbb{Z}/h\mathbb{Z})^*,$$

où e_p est le plus grand diviseur étranger à p de $e(p) = |G_{p,0}|$, $\zeta_p = \exp(2i\pi/h_p)$, $h_p = pgcd(e_p, h)$, $d_p = pgcd(\frac{p-1}{e_p}, \frac{n}{e_p} w_p)$, $w_p = 1$ ou 2 est égal à 1 si -1 n'est pas partout norme locale dans $E/\mathbb{Q}$, $w_p = |\{\pm\overline{1}\} \cap \mathbb{F}_p^{\times n}|$ sinon (cf. corol.(0.7)) ; ceci constitue la partie " calculs binomiaux" qui ont été faits dans [G(MN), 3] et qui éliminent une majorité de valeurs pour l'exposant $e_p d_p$. Enfin on vérifie que pour tout $p \in R$ sauvagement ramifié, n est multiple de $(p-1)/w_p$ (cf. corol.(0.7')).

(ii) On vérifie ensuite que pour tout $a,b \in (\mathbb{Z}/h\mathbb{Z})^*$ il existe $\varepsilon_{a,b} \in \{\pm 1\}$, $\varepsilon_{a,b}$ partout norme locale dans $E/\mathbb{Q}$, telle que pour tout $\ell \in R$ tel que $H \subseteq G_{\ell,0}$, on ait :

$$\overline{\varepsilon}_{a,b} = \left(\frac{1-\overline{\gamma}_\ell^a}{1-\overline{\gamma}_\ell^b}\right)^n \left(\text{resp.} \left(\frac{\overline{a}}{\overline{b}}\right)^n \text{ si } \overline{\gamma}_\ell = \overline{1}\right) \text{ dans } \mathbb{F}_\ell^\times,$$

où $\overline{\gamma}_\ell$ est l'image de $\pi_\ell^{\sigma_o - 1}$ dans $\mathbb{F}_\ell^\times$ (cf. corol.(0.10)) ; ceci suppose le calcul numérique des γ_ℓ modulo ℓ (voir la méthode en (3.7)).

(iii) Enfin on vérifie qu'il existe un signe $\varepsilon \in \{\pm 1\}$ tel que $\varepsilon\delta(E/L)$ soit partout norme locale dans $E/\mathbb{Q}$ (cf. th. (0.2)) .

Donnons précisément un critère simple de reste normique en $p \in R$, à partir de la connaissance du groupe d'Artin A de E (i.e. en pratique de A') ; ce critère étant destiné à être appliqué soit aux $\delta(E/L)$ soit à -1 , il suffit d'étudier les conditions de reste normique en tout $p \in R$, et en ∞ si E n'est pas réel (en toute autre place, $\delta(E/L)$ et -1 sont normes locales). Posons

$$\delta(E/L) = p^{\lambda_p} m_p \text{ , pour tout } p \in R(E/L) ,$$

où $\lambda_p = n_p(E/L)n / e(p)$, $m_p = \prod_{q \in R(E/L) - \{p\}} q^{\lambda_q}$ (cf. (3.1)) .

(3.3) Théorème. (i) Pour $\varepsilon \in \{\pm 1\}$, $\varepsilon\delta(E/L)$ est norme locale en $p \in R$ si et seulement si l'entier a défini, modulo f, par

$$a \equiv \varepsilon m_p \mod f_p$$

$$a \equiv p^{-\lambda_p} \mod f'_p$$

$$a > 0$$

est un élément de A' .

(ii) Le nombre -1 est partout norme locale dans $E/\mathbb{Q}$ si et seulement si les conditions suivantes sont réalisées :

(α) E est un corps réel,

(β) pour tout $p \in R$, $p \neq 2$, e_p est un diviseur de $\frac{p-1}{2}$.

En effet, d'après le corps de classes, le symbole de reste normique de Hasse en $p \in R$ pour $x \in \mathbb{Q}^\times$, $\left(\frac{x\,,\,E/\mathbb{Q}}{(p)}\right)$, est donné

par le symbole d'Artin $\left(\frac{E/\mathbb{Q}}{(a)}\right)$, $a = b\,p^{-v_p(x)}$, où b est un p-associé de x (i.e. tel que $\frac{b}{x} \equiv 1 \bmod f_p$ et $b \equiv 1 \bmod f'_p\infty$). Quant à $\left(\frac{E/\mathbb{Q}}{(a)}\right)$, on sait que c'est $\sigma_{|a|} = \sigma_a$ puisque b (donc a) est positif. D'où le résultat pour $x = \varepsilon\,\delta(E/L) = p^{\lambda_p}\,\varepsilon\,m_p$.

Pour que -1 soit norme locale en $p \neq 2$ dans $E/\mathbb{Q}$, il faut et il suffit qu'il existe $\sigma_a \in A$ tel que

$$a \equiv -1 \bmod f_p$$
$$a \equiv 1 \bmod f'_p\infty ;$$

ceci équivaut au fait que $A \cap \mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q}(f'_p))$ contient le relèvement canonique de la conjugaison complexe de $\mathrm{Gal}(\mathbb{Q}(f_p)/\mathbb{Q})$; comme ce groupe est cyclique pour $p \neq 2$, ceci équivaut facilement à la condition $e_p \mid \frac{p-1}{2}$.

On remarque que, grâce à la formule du produit, le calcul du symbole de Hasse en 2 est inutile (on l'obtient cependant par le même raisonnement, et -1 est norme locale en 2 si et seulement si le corps $E(2)$ est le sous-corps réel maximal de $\mathbb{Q}(f_2)$). De même, on peut utiliser le point (i) pour toutes les places de R (resp. $R \cup \{\infty\}$) sauf une ; on voit en particulier que si $R = \{p\}$ (resp. $R = \{p, \infty\}$), $\delta(E/L)$ est partout norme locale. Enfin, dans le cas (i), si l'on détermine u, v tels que $uf_p + vf'_p = 1$, on obtient a en prenant le plus petit résidu modulo f de $\varepsilon\,m_p\,vf'_p + p^{-\lambda_p}\,uf_p$.

(3.4) Remarques. (i) Il peut être utile de déterminer explicitement le groupe des normes locales $N_{E_p/F_p}\,E_p^{\times} = \overline{N_{E/M(p)}\,E}^{\times}$; il suffit pour cela de connaître $N_{E/M(p)}\,\pi_p$, pour une uniformisante π_p quelconque de

E en p , puisque $\overline{N_{E/M(p)} E^{\times}} = (p^{r(p)} u_p)^{\mathbb{Z}} \times U$, où le sous-groupe U de $\mathbb{Z}_p^*$, d'indice e(p) , est donné par

$$U = A'(1 + f_p \mathbb{Z}_p) ,$$

et où l'on a posé $N_{E_p/\mathbb{Q}_p} \pi_p = p^{r(p)} u_p$, $u_p \in \mathbb{Z}_p^*$, $r(p) = [N(p) : M(p)]$.

Or $p^{r(p)} u_p$ est norme locale en p dans $E/\mathbb{Q}$ si et seulement si il existe $a \in A'$ tel que $a \equiv u_p \bmod f_p$ et $a \equiv p^{-r(p)} \bmod f'_\infty$; il suffit donc de déterminer, dans $(\mathbb{Z}/f\mathbb{Z})^*$, le relèvement $\bar{c}_p$ de frobenius de p dans $\mathbb{Q}(f'_p)/\mathbb{Q}$ qui est tel que $c_p^{r(p)} \in A'$, ceci en partant directement de $p^{r(p)}$ modulo f ; on peut prendre $u_p = c_p^{-r(p)}$ dans $\mathbb{Z}_p^*$.

(ii) Le groupe η_p^1 est égal à $1 + p e(p) \mathbb{Z}_p$ pour $p \neq 2$; η_2^1 est l'un des 3 groupes :

$$(1 + 2e(2))^{\mathbb{Z}_2} , \quad \{\pm 1\} \times (1 + 4e(2))^{\mathbb{Z}_2} , \quad (-1 - 2e(2))^{\mathbb{Z}_2}$$

correspondant respectivement au cas où E(2) est l'un des 3 corps $\mathbb{Q}(f_2) = \mathbb{Q}(\omega_2)$, $\mathbb{Q}(\omega_2 + \omega_2^{-1})$, $\mathbb{Q}(\omega_2 - \omega_2^{-1})$.

(iii) Sous la forme énoncée en (0.2) , le critère de reste normique pour $\varepsilon\delta(E/L)$ s'énonce alors comme suit, à partir de la connaissance des c_p et η_p^1 :

L'entier $\varepsilon\delta(E/L)$ est partout norme locale dans $E/\mathbb{Q}$ si et seulement si les conditions suivantes sont réalisées :

(α) $\varepsilon = 1$ si E n'est pas réel,

(β) pour tout $p \in R$, $p \neq 2$, $\varepsilon m_p c_p^{n_p(E/L) n / e(p)}$ est puissance e(p)-ième dans $\mathbb{Z}_p^*/\eta_p^1$, ce qui est encore équivalent à

$$(\varepsilon m_p c_p^{n_p(E/L) n / e(p)})^{(p-1)/e_p} \equiv 1 \bmod p^{e(p)} .$$

Les conditions normiques en 2 sont donc inutiles ; elles seraient cependant :

$$\varepsilon\, m_2\, c_2^{\,n_2(E/L)\,n/e(2)} \equiv 1 \bmod 2e(2) \text{ si } E(2) = \mathbb{Q}(\omega_2),$$

$$\equiv \pm 1 \bmod 4e(2) \text{ si } E(2) = \mathbb{Q}(\omega_2 + \omega_2^{-1}),$$

$$\equiv 1\,,\ -1 + 2e(2) \bmod 4e(2) \text{ si } E(2) = \mathbb{Q}(\omega_2 - \omega_2^{-1}).$$

Venons-en maintenant à l'application du corollaire (0.10) (cf.(3.2, ii)) pour lequel il faut connaître $\pi_\ell^{\sigma_o - 1}$ pour tout $\ell \in R(E/L)$.

(3.5) Lemme. Soit $\ell \in R(E/L)$. Il existe $u_\ell \in E'(\ell)$, u_ℓ étranger à ℓ, tel que $\pi_\ell = u_\ell\, N_{\mathbb{Q}(f)/E'(\ell)}(1 - \omega_\ell)$ soit une uniformisante en ℓ dans E.

En effet, $\mathbb{Q}(f)/\mathbb{Q}(f'_\ell)$ est totalement ramifiée en ℓ, $\mathbb{Q}(f'_\ell)/\mathbb{Q}$ est non ramifiée en ℓ, et $1 - \omega_\ell$ est une uniformisante en ℓ dans $\mathbb{Q}(f)$; donc $N_{\mathbb{Q}(f)/E'(\ell)}(1 - \omega_\ell)$ est une telle uniformisante dans $E'(\ell)$, et comme $E'(\ell)/E$ est non ramifiée en ℓ, il existe bien $u_\ell \in E'(\ell)$, u_ℓ étranger à ℓ, tel que π_ℓ soit une uniformisante en ℓ dans E.

Fixons $g_o \in \mathbb{Z}$ tel que la restriction de σ_{g_o} à E soit égale au générateur σ_o de H, et considérons

$$\gamma_\ell = \pi_\ell^{\sigma_{g_o} - 1}\,, \quad \ell \in R(E/L).$$

(3.6) Remarque. Si $\ell = 2$, alors h est une puissance de 2, auquel cas la composante sur $\mathbb{F}_2^\times = \{1\}$ de $\dfrac{1 - \gamma_2^a}{1 - \gamma_2^b}$ est par définition $ab^{-1} \equiv 1 \bmod 2$, puisqu'alors $\gamma_2 \equiv 1 \bmod 2$; par ailleurs $\varepsilon_{a,b} = \pm 1 \equiv 1 \bmod 2$. On peut donc supposer $\ell \neq 2$; tous les $G_{\ell,0}$ considérés sont alors cycliques.

Soit σ_{g_ℓ} un générateur de $\mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q}(f'_\ell))$; sa restriction à E engendre $G_{\ell,0}$. Il existe donc un entier α_ℓ et un élément $a_\ell \in A'$, tels que :

$$\sigma_{g_o} = \sigma_{g_\ell}^{\alpha_\ell} \sigma_{a_\ell}.$$

On a $\gamma_\ell = \pi_\ell^{\sigma_{g_o}-1} = u_\ell^{\sigma_{g_o}-1} N_{\mathbb{Q}(f)/E'(\ell)}(1-\omega_\ell)^{\sigma_{g_o}-1}$; comme σ_{g_ℓ} est dans le groupe d'inertie de ℓ dans $\mathbb{Q}(f)/\mathbb{Q}$, on a

$u_\ell^{\sigma_{g_\ell}-1} \equiv 1 \bmod (1-\omega_\ell)$, d'où

$$u_\ell^{\sigma_{g_o}-1} = u_\ell^{\sigma_{g_\ell}^{\alpha_\ell}\sigma_{a_\ell}-1} = u_\ell^{(\sigma_{g_\ell}^{\alpha_\ell}-1)\sigma_{a_\ell}} u_\ell^{\sigma_{a_\ell}-1}$$

$$\equiv u_\ell^{\sigma_{a_\ell}-1} \bmod (1-\omega_\ell) ;$$

mais $\pi_I \in E$, donc pour tout $b \in A'$, $\pi_I^{\sigma_b-1} = 1$ soit

$u_\ell^{\sigma_b-1} N_{\mathbb{Q}(f)/E'(\ell)}(1-\omega_\ell)^{\sigma_b-1} = 1$; d'où

$u_\ell^{\sigma_b-1} N_{\mathbb{Q}(f)/E'(\ell)}\left(\frac{1-\omega_\ell^b}{1-\omega_\ell}\right) = 1$, ce qui conduit à

$u_\ell^{\sigma_b-1}{}^{b^{[\mathbb{Q}(f):E'(\ell)]}} \equiv 1 \bmod (1-\omega_\ell)$. En particulier, on a

$u_\ell^{\sigma_{a_\ell}-1} \equiv a_\ell^{-[\mathbb{Q}(f):E'(\ell)]} \bmod (1-\omega_\ell)$. On a alors

$$\gamma_\ell \equiv a_\ell^{-[\mathbb{Q}(f):E'(\ell)]}{}^{g_o^{[\mathbb{Q}(f):E'(\ell)]}}$$

$$\equiv (a_\ell^{-1} a_\ell g_\ell^{\alpha_\ell})^{[\mathbb{Q}(f):E'(\ell)]} \equiv g_\ell^{\alpha_\ell[\mathbb{Q}(f):E'(\ell)]} \bmod (1-\omega_\ell),$$

congruence qui est donc valable modulo π_ℓ puisque $\gamma_\ell \in E$, $g_\ell \in \mathbb{Z}$. On a $\alpha_\ell = [L : N(\ell)]\beta_\ell$, β_ℓ étranger à h ; d'où finalement :

$$\overline{\gamma}_\ell = \overline{g}_\ell^{\beta_\ell [\mathbb{Q}(f_\ell) : \mathbb{Q}]/h} = \overline{g}_\ell^{\beta_\ell \varphi(f_\ell)/h},$$

en désignant par φ l'indicateur d'Euler.

(3.7) Théorème. Une condition nécessaire à la $\mathbb{Z}$-monogénéité de Z_E est que pour tout sous-groupe cyclique H de G, d'ordre $h > 1$, on ait la propriété suivante : Pour tout $a, b \in (\mathbb{Z}/h\mathbb{Z})^*$, il existe $\epsilon_{a,b} \in \{\pm 1\}$, $\epsilon_{a,b}$ partout norme locale dans $E/\mathbb{Q}$ (cf.(3.3, ii)), tel que pour tout $\ell \neq 2$ dont le groupe d'inertie contient H, on ait :

$$\epsilon_{a,b} \equiv \left(\frac{1 - \gamma_\ell^a}{1 - \gamma_\ell^b}\right)^n \left(\text{resp. } \left(\frac{a}{b}\right)^n \text{ si } \gamma_\ell \equiv 1 \bmod \ell\right) \bmod \ell,$$

avec les données suivantes :

on fixe d'abord un générateur σ_o de H et un entier g_o tel que la restriction de σ_{g_o} à E coïncide avec σ_o ; on pose

$\gamma_\ell = g_\ell^{\beta_\ell \varphi(f_\ell)/h}$, où g_ℓ est un générateur de $(\mathbb{Z}/f_\ell\mathbb{Z})^*$ congru à 1 modulo f/f_ℓ, où β_ℓ est défini modulo h par la condition $g_o g_\ell^{-\beta_\ell e(\ell)/h} \in A'$, où $e(\ell)$ est l'indice de ramification de ℓ dans $E/\mathbb{Q}$.

Remarque. On rappelle que le programme " GALCYCL ", détaillé dans [G(G)], permet précisément d'effectuer les vérifications numériques nécessaires aux théorèmes (3.3) et (3.7), lorsque l'extension $E/\mathbb{Q}$ est cyclique de degré quelconque.

4. Exemples numériques. (i) Dans [G(MN)3], le premier exemple (dans le cas abélien absolu, et pour h = 5) pour lequel le théorème (0.6) (ou le corollaire (0.7), cf.(3.2),(i)) ne permet pas nécessairement de conclure est le cas n = 15 pour lequel on a :

$$\left(\frac{1-\zeta_5^a}{1-\zeta_5^b}\right)^{30} \equiv 1 \mod (11 \times 31),$$

pour tout $a, b \in (\mathbb{Z}/5\mathbb{Z})^*$.

On est donc amené à étudier les extensions abéliennes $E/\mathbb{Q}$ de degré 15 pour lesquelles $R = \{11, 31\}$ ou $\{5, 11, 31\}$.

a) Etude du cas $R = \{11, 31\}$. Nécessairement $e(11) = 5$ et $e(31) = 15$, ce qui est réalisé par 4 corps réels E_i, $1 \leq i \leq 4$, de conducteur $11 \times 31 = 341$, que l'on peut caractériser par les ensembles A_i' représentant les groupes d'Artin $\mathrm{Gal}(\mathbb{Q}(341)/E_i)$; le programme GALCYCL fournit les données suivantes :

$A_1' = \{ 1, 32, 147, 271, 281, 126, 108, 46, 283, 190,$
$309, 340, 70, 194, 215, 60, 295, 233, 151, 58\}$;

$A_2' = \{ 1, 32, 240, 178, 312, 95, 294, 201, 314, 159,$
$309, 340, 163, 101, 246, 29, 140, 47, 182, 27\}$;

$A_3' = \{ 1, 32, 116, 302, 250, 157, 15, 139, 97, 35,$
$309, 340, 39, 225, 184, 91, 202, 326, 306, 244\}$;

$A_4' = \{ 1, 32, 85, 333, 64, 2, 325, 170, 4, 128,$
$309, 340, 8, 256, 339, 277, 171, 16, 213, 337\}$.

On appelle désormais H le sous-groupe d'ordre 5 de G ; il fixe le sous-corps cubique L de E.

D'après (3.1), on a $\delta(E/L) = 11^3 \times 31$. Puisque -1 est norme, une condition nécessaire de monogénéité est que $11^3 \times 31$ soit norme locale en 11 et 31 (cf.(3.3)) ; modulo 11, il faut résoudre les congruences simultanées :

$$a \equiv 31 \mod 11$$

$$a \equiv 11^{-3} \mod 31 ,$$

soit

$$a \equiv -2 \mod 11$$

$$a \equiv 15 \mod 31 ,$$

ce qui conduit à $a \equiv 108 \mod 341$.

Or $108 \in A_1^!$ et $108 \notin A_i^!$ pour $2 \leq i \leq 4$; ainsi pour les corps $E = E_2$, E_3 et E_4 , Z_E n'est pas monogène.

On est donc ramené à étudier E_1 .

Le théorème (3.7) s'applique en utilisant les éléments numériques suivants (donnés par GALCYCL) :

Un générateur de G est représenté par $g = 12$; d'où $g_o = 12^3 \equiv 23 \mod (341)$ représente par exemple le générateur σ_o de H ; on a ensuite le tableau suivant :

ℓ	g_ℓ	β_ℓ	γ_ℓ
11	63	1	218
31	12	1	188

On vérifie alors que pour tout $a, b \in (\mathbb{Z}/5\mathbb{Z})^*$, il existe bien $\epsilon_{a,b} \in \{\pm 1\}$ tel que

$$\left(\frac{1 - \gamma_{11}^a}{1 - \gamma_{11}^b}\right)^{15} \equiv \epsilon_{a,b} \mod 11$$

et

$$\left(\frac{1 - \gamma_{31}^a}{1 - \gamma_{31}^b}\right)^{15} \equiv \epsilon_{a,b} \mod 31 .$$