ACTA ARITHMETICA
119.2 (2005)

Galois module structure in weakly ramified 3-extensions

by

Stéphane Vinatier (Limoges)

1. Introduction. Let p be an odd prime number, N a finite Galois p-extension of $\mathbb{Q}$, $\mathcal{O}$ its ring of integers, $\mathcal{D}$ its different and G its Galois group. Since G is of odd order, there exists a unique fractional ideal $\mathcal{A}$ of $\mathcal{O}$ such that

$$\mathcal{A}^2 = \mathcal{D}^{-1};$$

$\mathcal{A}$ is called the *square root of the inverse different*. It has the structure of a $\mathbb{Z}[G]$-module, which Erez has shown to be locally free if and only if the extension is *weakly ramified*, that is, if the second ramification groups are trivial at all places. We assume this condition is fulfilled (it is only relevant for places above p here) and we denote by $(\mathcal{A})$ the class of $\mathcal{A}$ in the class group $\mathrm{Cl}(\mathbb{Z}[G])$ of locally free $\mathbb{Z}[G]$-modules. The main result of this paper focusses on the case $p = 3$.

Theorem 1. *Let $N/\mathbb{Q}$ be a weakly ramified 3-extension. Then $(\mathcal{A})^3 = 1$ in $\mathrm{Cl}(\mathbb{Z}[G])$.*

This is an improvement, in the case $p = 3$ considered here, of [V3, Theorem 1], which states that $(\mathcal{A})^e = 1$ (for any odd p, e standing for the ramification index of p in $N/\mathbb{Q}$). In other situations, the class $(\mathcal{A})$ is known to be trivial (and then $\mathcal{A}$ is a free $\mathbb{Z}[G]$-module) when $N/\mathbb{Q}$ is a tame extension of odd degree (see [E], which deals more generally with relative extensions) and when $N/\mathbb{Q}$ is a weakly ramified extension of odd degree with abelian decomposition groups at wild places [V1].

The majorization of the order of $(\mathcal{A})$ obtained here for the non-locally abelian and non-tame case does not depend on the weakly ramified

2000 *Mathematics Subject Classification*: Primary 11R33; Secondary 05E05.

Key words and phrases: Galois module structure, weakly ramified extensions, resolvents, symmetric polynomials.

Large part of this work has been completed while the author held a GTEM postdoctoral position at the "Chaire de Structures Algébriques et Géométriques" of Prof. Bayer, EPFL, Switzerland.

3-extension under consideration (examples of these are constructed in [V2]); further it is as close as possible to the expected result that $(\mathcal{A})$ is trivial. There are at least two technical reasons, to be given below, that make $(\mathcal{A})^3$ much easier to handle than $(\mathcal{A})$ itself. Dealing with the general p case is another problem to solve. The importance of $p = 3$ will appear in the combinatorial computations of Section 3, which we are currently able to make only under this assumption.

The proof of Theorem 1 builds on results of [V3], namely those preceding Lemma 2.9 there, which is our starting point. In the next section we recall useful notations and results from that paper and from the literature; we also establish useful preliminary results, especially an integrality criterion. This is done for all p. Eventually, in Section 3, we restrict to the case $p = 3$, reformulate our main result in terms of the former integrality criterion (Theorem 3.1) and give its proof, which makes a crucial use of the symmetries in the sum of pth powers of resolvents appearing in the criterion.

Let us fix some notations before going any further: if K is a finite extension of $\mathbb{Q}_p$ contained in a fixed algebraic closure $\mathbb{Q}_p^c$ of $\mathbb{Q}_p$, we let Ω_K denote its absolute Galois group $\mathrm{Gal}(\mathbb{Q}_p^c/K)$, v_K its discrete valuation from $K^\times$ onto $\mathbb{Z}$, $\mathcal{O}_K$ its valuation ring, π_K a uniformizing parameter, and $\wp_K = \pi_K\mathcal{O}_K$ its valuation ideal. If L is a finite Galois p-extension of K, we denote by $\mathcal{D}_{L/K}$ and $\mathcal{A}_{L/K}$ the different of the extension and the square root of its inverse. The order of a finite group Λ is denoted by $|\Lambda|$, the subgroup generated by some $\lambda \in \Lambda$ by $\langle\lambda\rangle$ and the set of irreducible characters of Λ with values in $\mathbb{Q}_p^c$ by $\widehat{\Lambda}$.

2. Preliminaries

2.1. *Prerequisites.* We need some tools first developed by Fröhlich and Taylor to study the class of the ring of integers $(\mathcal{O})$ in $\mathrm{Cl}(\mathbb{Z}[G])$ when the extension $N/\mathbb{Q}$ is tamely ramified, and adjusted by Erez to the study of our class $(\mathcal{A})$. Details may be found in [F], [T] and [E]. The most important tool is Fröhlich's Hom-description of the class group, which is the following explicit isomorphism of groups:

$$\mathrm{Cl}(\mathbb{Z}[G]) \simeq \frac{\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, J(E))}{\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_G, E^\times)\,\mathrm{Det}(\mathcal{U}(\mathbb{Z}[G]))},$$

where R_G is the additive group of virtual characters of G with values in an algebraic closure $\mathbb{Q}^c$ of $\mathbb{Q}$, $E \subset \mathbb{Q}^c$ is a "big enough" number field, $J(E)$ its idèle group, $\Omega_\mathbb{Q} = \mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})$ and $\mathcal{U}(\mathbb{Z}[G]) = \mathbb{R}[G]^\times \times \prod_l \mathbb{Z}_l[G]^\times$, l running over all prime numbers. We shall define the Det morphism at the finite components of $\mathcal{U}(\mathbb{Z}[G])$ below in formula (1).

The class $(\mathcal{A})$ is represented by an $\Omega_\mathbb{Q}$-equivariant morphism f (namely $f(\chi^\omega) = f(\chi)^\omega$ for all $\chi \in R_G, \omega \in \Omega_\mathbb{Q}$), which can be explicitly expressed

in terms of resolvents and twisted Galois Gauss sums [E, Theorem 3.6]. For each prime number l, we denote by f_l the semi-local component of f in $J_l(E) = \prod_{\mathcal{L}|l} E_{\mathcal{L}}^{\times}$, where $\mathcal{L}$ runs through the prime ideals of $\mathcal{O}_E$ above l and $E_{\mathcal{L}}$ is the completion of E with respect to its $\mathcal{L}$-adic valuation. Our ultimate goal is to show that, up to multiplication of f by a suitable global $\Omega_{\mathbb{Q}}$-equivariant morphism (namely in $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, E^{\times})$), f_l lies in $\mathrm{Det}(\mathbb{Z}_l[G]^{\times})$ for every prime number l. In this paper we shall content ourselves with proving it for the pth power of f_l when $p = 3$.

There are several simplifications due to former results at this stage: by [E, Theorem 2], we know that f_l belongs to $\mathrm{Det}(\mathbb{Z}_l[G]^{\times})$ for $l \neq p$, so we only have to deal with f_p. Further, f_p can be written as a product [V3, Prop. 2.2]: $f_p = f_{(p),p} \prod_{l \neq p} f^*_{(l),p}$, in which the factors indexed by $l \neq p$ only involve tame ramification, so they are dealt with by adapting [T, Theorem 3] (see [V1, Lemma 4.4]). Since the absolute Galois group $\Omega_{\mathbb{Q}}$ acts transitively on the prime ideals $\wp$ above p in E, it is sufficient to look at what happens for one of them. We thus fix an embedding $j_p : \mathbb{Q}^{\mathrm{c}} \hookrightarrow \mathbb{Q}_p^{\mathrm{c}}$ and we denote by M_p the closure in $\mathbb{Q}_p^{\mathrm{c}}$ of the image $j_p(M)$ of a number field $M \subset \mathbb{Q}^{\mathrm{c}}$; it yields a surjective morphism that we also denote by $j_p : J_p(E) \twoheadrightarrow E_p$, and an isomorphism between R_G and $R_{G,p}$, the group of virtual characters of G with values in $\mathbb{Q}_p^{\mathrm{c}}$. We also get an embedding $j_p^* : \Omega_{\mathbb{Q}_p} \hookrightarrow \Omega_{\mathbb{Q}}$, $\omega \mapsto j_p^{-1} \circ \omega \circ j_p$, which yields the following isomorphism (see [CNT] for details):

$$j_p^* : \frac{\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_G, J_p(E))}{\mathrm{Det}(\mathbb{Z}_p[G]^{\times})} \xrightarrow{\sim} \frac{\mathrm{Hom}_{\Omega_{\mathbb{Q}_p}}(R_{G,p}, E_p^{\times})}{\mathrm{Det}(\mathbb{Z}_p[G]^{\times})},$$

such that $j_p^*(f_{(p),p}) = j_p \circ f_{(p),p} \circ j_p^{-1}$. In fact, $j_p^*(f_{(p),p})$ is easily seen [V1, §3.4] to be induced from a morphism g_p on the group of virtual characters of $G(p)$, the decomposition group at the place of N above p corresponding to j_p, which we identify through j_p^* with $\Gamma = \mathrm{Gal}(N_p/\mathbb{Q}_p)$. In other words,

$$j_p^*(f_{(p),p})(\theta) = \mathrm{Ind}_G^{\Gamma}(g_p)(\theta) = g_p(\mathrm{Res}\,\theta),$$

where $\mathrm{Res}\,\theta$ is the restriction of a character θ of G to Γ. Showing that $(\mathcal{A})$ is trivial is now equivalent to showing that, up to multiplication of f by a suitable global $\Omega_{\mathbb{Q}}$-equivariant morphism, the resulting morphism g_p belongs to $\mathrm{Det}(\mathbb{Z}_p[\Gamma]^{\times})$, that is, there exists $u = \sum_{\Gamma} u_\gamma \gamma \in \mathbb{Z}_p[\Gamma]^{\times}$ such that $g_p = \mathrm{Det}(u)$. By definition, $\mathrm{Det}(u)$ is the $\Omega_{\mathbb{Q}_p}$-equivariant morphism from $R_{\Gamma,p}$ to $E_p^{\times}$ such that, for any irreducible character θ of Γ,

$$\mathrm{Det}_\theta(u) = \det\Big(\sum_{\gamma \in \Gamma} u_\gamma \Theta(\gamma)\Big), \tag{1}$$

where Θ is a matrix representation of Γ of character θ.

Now we take advantage of studying the pth power of $(\mathcal{A})$, instead of $(\mathcal{A})$ itself. The class $(\mathcal{A})^p$ is represented in Fröhlich's Hom-description by f^p so,

by the same arguments as above, we are reduced to showing that g_p^p belongs to $\mathrm{Det}(\mathbb{Z}_p[\Gamma]^\times)$. By [V3, Prop. 2.5], we can get rid of the pth power of the twisted Galois Gauss sum involved in g_p^p, hence we only have to deal with the pth power of the resolvent function $h_p \in \mathrm{Hom}(R_{\Gamma,p}, \mathcal{O}_{E_p}^\times)$, defined by

$$h_p(\theta) = (\alpha_p \,|\, \theta) = \mathrm{Det}_\theta\Big(\sum_{\gamma\in\Gamma} \gamma(\alpha_p)\gamma^{-1}\Big), \tag{2}$$

where α_p denotes a basis of $\mathcal{A}_{N_p/\mathbb{Q}_p}$ as a $\mathbb{Z}_p[\Gamma]$-module. Further, if we denote by Γ_0 the inertia group of the extension $N_p/\mathbb{Q}_p$, by N_0 the fixed subfield and by β a basis of $\mathcal{A}_{N_p/N_0}$ as a $\mathcal{O}_{N_0}[\Gamma_0]$-module (it was denoted by β_p in [V3], but we wish to keep the notation β_i for another purpose in Section 3), we know by [E, (6.3)] that there exists $\lambda \in \mathcal{O}_{N_0}[\Gamma]^\times$ such that, for every $\theta \in R_{\Gamma,p}$,

$$(\alpha_p \,|\, \theta) = (\beta \,|\, \mathrm{Res}\,\theta)\,\mathrm{Det}_\theta(\lambda),$$

where Res is now the restriction of the characters of Γ to the inertia group. We shall characterize bases of $\mathcal{A}_{N_p/N_0}$ over $\mathcal{O}_{N_0}[\Gamma_0]$ in Subsection 2.3. Let $k_p \in \mathrm{Hom}(R_{\Gamma_0,p}, E_p^\times)$ be defined by $k_p(\chi) = (\beta \,|\, \chi)$ for every $\chi \in R_{\Gamma_0,p}$. We deduce that, for some $\lambda \in \mathcal{O}_{N_0}[\Gamma]^\times$,

$$h_p = \mathrm{Ind}_\Gamma^{\Gamma_0}(k_p)\,\mathrm{Det}(\lambda).$$

[V3, Lemma 2.9] states that the pth power of k_p is Ω_{N_0}-equivariant and takes values in the unit group, namely

$$k_p^p \in \mathrm{Hom}_{\Omega_{N_0}}(R_{\Gamma_0,p}, \mathcal{O}_{E_p}^\times) = \mathrm{Det}(\mathcal{M}_0^\times),$$

where $\mathcal{M}_0$ is the maximal order of $N_0[\Gamma_0]$. By arguments similar to those used at the end of [V3, §2.2], we obtain:

Proposition 2.1. *If* $k_p^p \in \mathrm{Det}(\mathcal{O}_{N_0}[\Gamma_0]^\times)$, *then* $(\mathcal{A})^p = 1$.

We are thus reduced to studying a function on the characters of Γ_0 instead of a function on the characters of Γ. We will see in the next subsection that Γ_0 is a very convenient group to work in (to begin with, it is abelian in our situation). Further in Subsection 2.4, we give an integrality criterion in order to establish the hypothesis of Proposition 2.1.

2.2. *"Linear duality" of* Γ_0. Since the second ramification group Γ_2 of N_p/N_0 is trivial, we know by [S1, IV2, Cor. 3 and 4] that $\Gamma_0 = \Gamma_1$ is abelian of exponent p, namely isomorphic, as an abelian group, to the product of say $m \geq 1$ copies of the field $\mathbb{F}_p$ with p elements. This gives Γ_0 the structure of an $\mathbb{F}_p$-vector space of dimension m. Notice that a subgroup of index p of Γ_0 becomes a hyperplane for this structure, whereas a subgroup of order p becomes a line. Further, fixing a group isomorphism from μ_p, the group of pth roots of unity in $\mathbb{Q}_p^c$, to $\mathbb{F}_p$, enables identifying a character χ of Γ_0

with a linear form, so that the group of irreducible characters $\widehat{\Gamma_0}$ becomes the dual of Γ_0 as an $\mathbb{F}_p$-vector space, namely the "linear dual" of Γ_0.

One easily checks that Γ_0 has

$$r = \frac{p^m - 1}{p - 1} = 1 + p + \cdots + p^{m-1}$$

subgroups of order p, just by considering the elements of order p. By duality we get:

LEMMA 2.2. *The number of subgroups of index p of Γ_0 equals r.*

The following result, as well as analogous ones, will be used repeatedly in Section 3.

LEMMA 2.3. (i) *If $\gamma \in \Gamma_0 \setminus \{1\}$, then the number of characters $\chi \in \widehat{\Gamma_0}$ such that $\chi(\gamma) = 1$ equals p^{m-1}.*

(ii) *If $m \geq 2$, $\gamma \in \Gamma_0 \setminus \{1\}$ and $\gamma' \in \Gamma_0 \setminus \langle\gamma\rangle$, then the number of characters $\chi \in \widehat{\Gamma_0}$ such that $\chi(\gamma) = \chi(\gamma') = 1$ equals p^{m-2}.*

Proof. The map $\widehat{\gamma} : \widehat{\Gamma_0} \to \mu_p$, $\chi \mapsto \chi(\gamma)$, is a linear form with the previous identifications, so its kernel is a hyperplane of $\widehat{\Gamma_0}$ (since $\gamma \neq 1$), thus of cardinality p^{m-1}. The conditions on γ and γ' ensure that they are linearly independent, so the set of characters which are trivial on both of them is the intersection of two distinct hyperplanes, hence of dimension $m - 2$ and of cardinality p^{m-2}. ∎

2.3. *Normal basis for the square root of the inverse different.* Here we consider a slightly more general situation: we let K denote any finite extension of $\mathbb{Q}_p$, L/K a finite abelian totally and weakly ramified p-extension, and we set $\Lambda = \mathrm{Gal}(L/K)$. We characterize bases of $\mathcal{A}_{L/K}$ over $\mathcal{O}_K[\Lambda]$ and, for every extension K' of K contained in L, we find a particular basis of $\mathcal{A}_{K'/K}$ over $\mathcal{O}_K[\mathrm{Gal}(K'/K)]$.

By [B, Lemma 4.2], there exists a uniformizing parameter π of K such that L is contained in the second Lubin–Tate division field $K_\pi^{(2)}$ of K corresponding to π. This implies in particular that for K' as above, K'/K is also weakly ramified. Further, by [B, Theorem 2], any uniformizing parameter π_L of L generates $\mathcal{O}_L$ as a module over its associated order in the group algebra $K[\Lambda]$ (see (3) below). We deduce the following.

PROPOSITION 2.4. *Any uniformizing parameter π_L of L is a basis of $\wp_L$ over $\mathcal{O}_K[\Lambda]$.*

By Ullom's results [U, Theorem 2], we know that $\wp_L$ is a free $\mathcal{O}_K[\Lambda]$-module; it is clear that any generator is of valuation 1. Byott's work implies that the converse is true.

Proof. By [B, Lemma 3.1], the order associated to $\mathcal{O}_L$ satisfies:

$$\{x \in K[\Lambda] \mid x\mathcal{O}_L \subseteq \mathcal{O}_L\} = \mathcal{O}_K[\Lambda] + \mathcal{O}_K(\pi_K^{-1}T_\Lambda), \tag{3}$$

where $T_\Lambda = \sum_{\lambda\in\Lambda}\lambda$. Thus by [B, Theorem 2], any $x \in \wp_L \subset \mathcal{O}_L$ may be expressed as

$$x = \sum_{\lambda\in\Lambda} n_\lambda\lambda(\pi_L) + y\pi_K^{-1}T_\Lambda(\pi_L),$$

where $y \in \mathcal{O}_K$ and $n_\lambda \in \mathcal{O}_K$ for every $\lambda \in \Lambda$. Notice that $\sum_\Lambda n_\lambda\lambda(\pi_L) \in \wp_L$, and thus $y\pi_K^{-1}T_\Lambda(\pi_L) \in \wp_L \cap \mathcal{O}_K = \wp_K$. We deduce that $y \in \wp_K$: indeed, since L/K is weakly ramified, [S1, III, Prop. 7] shows that $\mathrm{Tr}_{L/K}(\wp_L) = \wp_K$ and $\mathrm{Tr}_{L/K}(\wp_L^2) = \wp_K^2$. This yields the following surjective additive morphism:

$$\mathrm{Tr}_{L/K} : \frac{\wp_L}{\wp_L^2} \twoheadrightarrow \frac{\wp_K}{\wp_K^2},$$

where the quotients involved are both isomorphic to the residue field of K, so the map is a 1-to-1 correspondence. Thus $T_\Lambda(\pi_L) = \mathrm{Tr}_{L/K}(\pi_L) \in \wp_K \setminus \wp_K^2$ and $y \in \wp_K$. Writing $y = \pi_K z$ with $z \in \mathcal{O}_K$ yields $x = \sum_\Lambda(n_\lambda + z)\lambda(\pi_L)$, so $\wp_L \subseteq \mathcal{O}_K[\Lambda]\,\pi_L$, which implies the proposition. ∎

Let $e = |\Lambda|$ denote the ramification index in L/K.

Corollary 2.5. (i) *If $\beta \in L$, then β is a basis of $\mathcal{A}_{L/K}$ over $\mathcal{O}_K[\Lambda]$ if and only if $v_L(\beta) = 1 - e$.*

(ii) *Assume the previous condition is fulfilled and let K' be any intermediate extension of L/K. Then $\mathrm{Tr}_{L/K'}(\mathcal{A}_{L/K}) = \mathcal{A}_{K'/K} = \mathcal{O}_K[\mathrm{Gal}(K'/K)]\beta'$, where $\beta' = \mathrm{Tr}_{L/K'}(\beta)$.*

Proof. By Hilbert's formula for the valuation of the different [S1, IV2, Prop. 4], $\mathcal{A}_{L/K} = \wp_L^{1-e} = \pi_K^{-1}\wp_L$; thus $\mathcal{A}_{L/K} = \mathcal{O}_K[\Lambda]\beta \Leftrightarrow \wp_L = \mathcal{O}_K[\Lambda](\pi_K\beta)$, and (i) is implied by Proposition 2.4. Set $e' = [K' : K]$. By [S1, III, Prop. 7], one has

$$\mathrm{Tr}_{L/K'}(\mathcal{A}_{L/K}) = \mathrm{Tr}_{L/K'}(\wp_L^{1-e}) = \wp_{K'}^{1-e'} = \mathcal{A}_{K'/K},$$

so $v_{K'}(\beta') \geq 1 - e'$. Further, any $x \in \mathcal{A}_{L/K}$ can be written $x = \sum_\Lambda x_\lambda\lambda(\beta)$ with $x_\lambda \in \mathcal{O}_K$, hence $\mathrm{Tr}_{L/K'}(x) = \sum_\Lambda x_\lambda\lambda(\beta')$, which implies $v_{K'}(\beta') \leq 1 - e'$, and (i) yields (ii). ∎

2.4. *An integrality criterion.* Let again K be a finite extension of $\mathbb{Q}_p$ contained in $\mathbb{Q}_p^c$ and let Λ be any finite abelian group. We denote by $\mathcal{M}_\Lambda$ the maximal order of $K[\Lambda]$. Wedderburn's isomorphism of $\mathbb{Q}_p^c$-algebras reads [S2, Prop. 10]:

$$\mathbb{Q}_p^c[\Lambda] \simeq \bigoplus_{\chi\in\widehat{\Lambda}} \mathbb{Q}_p^c, \qquad u = \sum_{\lambda\in\Lambda} u_\lambda\lambda \mapsto \Big(\sum_{\lambda\in\Lambda} u_\lambda\chi(\lambda)\Big)_{\chi\in\widehat{\Lambda}}.$$

Notice that $\sum_\Lambda u_\lambda \chi(\lambda) = \mathrm{Det}_\chi(u)$ by (1). This morphism yields

$$\mathcal{M}_\Lambda \simeq \bigoplus_{\chi \in \widehat{\Lambda}} \mathcal{O}_{K(\chi)},$$

where $K(\chi)$ is the extension of K generated by the values of χ. Fourier's inversion formula [S2, Prop. 11] links the coordinates u_λ of u to its image by the former isomorphism:

$$u_\lambda = \frac{1}{|\Lambda|} \sum_{\chi \in \widehat{\Lambda}} \chi(\lambda^{-1}) \, \mathrm{Det}_\chi(u).$$

We deduce the integrality criterion we are looking for.

PROPOSITION 2.6. *If $\psi \in \mathrm{Det}(\mathcal{M}_\Lambda^\times)$, then $\psi \in \mathrm{Det}(\mathcal{O}_K[\Lambda]^\times)$ if and only if, for every $\lambda \in \Lambda$, the sum*

$$S_\psi(\lambda) = \sum_{\chi \in \widehat{\Lambda}} \chi(\lambda^{-1}) \psi(\chi)$$

belongs to $|\Lambda| \mathcal{O}_K$.

Proof. Let $u \in \mathcal{M}_\Lambda^\times$ be such that $\psi = \mathrm{Det}(u)$. Write $u = \sum_\Lambda u_\lambda \lambda$ with $u_\lambda \in K$. Then $u \in \mathcal{O}_K[\Lambda]^\times$ if and only if $u_\lambda \in \mathcal{O}_K$ for every $\lambda \in \Lambda$, since $\mathcal{O}_K[\Lambda] \cap \mathcal{M}_\Lambda^\times = \mathcal{O}_K[\Lambda]^\times$. So we are done thanks to the above formula. ∎

3. The $p = 3$ case. We now suppose $p = 3$, so our weakly ramified extension $N/\mathbb{Q}$ is a 3-extension. We still denote by N_3 the closure in $\mathbb{Q}_3^c$ of $j_3(N)$, by Γ the Galois group of the local extension $N_3/\mathbb{Q}_3$, by Γ_0 its inertia group, by N_0 the fixed subfield of N_3 under Γ_0 and by β a basis of $\mathcal{A}_{N_3/N_0}$ over $\mathcal{O}_{N_0}[\Gamma_0]$. The 3-extension N_3/N_0 is abelian, totally and weakly ramified, so we may apply the results of Subsection 2.3. In order to prove Theorem 1, thanks to Propositions 2.1 and 2.6, we are reduced to showing:

THEOREM 3.1. *For every $\gamma \in \Gamma_0$, $S(\gamma) = \sum_{\chi \in \widehat{\Gamma_0}} \chi(\gamma^{-1})(\beta \,|\, \chi)^3$ belongs to $|\Gamma_0| \mathcal{O}_{N_0}$.*

Let m be such that $|\Gamma_0| = 3^m$. We suppose $m \geq 2$ in the following, since [V3, Theorem 1] implies Theorem 1 when $m = 1$. By Lemma 2.2, Γ_0 has $r = (3^m - 1)/2$ subgroups of index 3; to each of them, we attach an irreducible character $\chi_i \in \widehat{\Gamma_0}$, $1 \leq i \leq r$, which has this subgroup as kernel. We denote by χ_0 the trivial character of Γ_0; then the set $\{\chi_i \mid 0 \leq i \leq r\}$ represents the orbits of $\widehat{\Gamma_0}$ under the action of Ω_{N_0}. Indeed, two characters χ and χ' are conjugate under the action of Ω_{N_0} if and only if $\ker(\chi) = \ker(\chi')$; one then has $\chi' = \chi$ or $\chi' = \chi^2$.

For each $1 \leq i \leq r$, we let K_i denote the fixed subfield of N_3 under $\ker(\chi_i)$, we set $\Delta_i = \mathrm{Gal}(K_i/N_0)$ and $\beta_i = \mathrm{Tr}_{N_3/K_i}(\beta)$. Then, by Corollary 2.5, β_i is a basis of $\mathcal{A}_{K_i/N_0}$ over $\mathcal{O}_{N_0}[\Delta_i]$. Further we set $\beta_0 = \mathrm{Tr}_{N_3/N_0}(\beta)$.

The following diagram sums up the notations for the local extension.

$$\begin{array}{ccccc} & & N_3 & \ni & \beta \\ & \ker(\chi_i)\big(& \big| 3^{m-1} & & \\ & & K_i & \ni & \beta_i, \qquad 1 \le i \le r. \\ & \Delta_i\big(& \big| 3 & & \\ & & N_0 & \ni & \beta_0 \\ & & \big| & & \\ & & \mathbb{Q}_3 & & \end{array}$$

From the definition (2) of the resolvent, one easily sees that $(\beta \,|\, \chi_0) = \beta_0$. Further, if χ is a non-trivial character of Γ_0, there exists $1 \le i \le r$ such that $\ker(\chi) = \ker(\chi_i)$, and one has

$$(\beta \,|\, \chi)_{\Gamma_0} = (\beta_i \,|\, \chi)_{\Delta_i},$$

where the subscripts mean that χ is viewed as a character of Γ_0 (inflated from Δ_i) on the left side and as a character of Δ_i on the right side. We shall omit such subscripts in the following. We set, for $1 \le i \le r$,

$$T_i(\gamma) = \chi_i(\gamma^{-1})(\beta_i \,|\, \chi_i)^3 + \chi_i^2(\gamma^{-1})(\beta_i \,|\, \chi_i^2)^3;$$

we then get

$$S(\gamma) = \beta_0^3 + \sum_{i=1}^{r} T_i(\gamma). \tag{4}$$

3.1. *Computation of* $S(1)$. We let ζ be a primitive 3rd root of unity and for each $1 \le i \le r$, we choose δ_i in Γ_0 such that $\chi_i(\delta_i) = \zeta$; consequently, $\Gamma_0 = \langle \delta_i \rangle \times \ker(\chi_i)$ and $\Delta_i = \langle \delta_{i|K_i} \rangle$. For $k \in \{1,2,3\}$, we denote by $\sigma_{k,i}$ the sum of all products of k distinct conjugates of β_i in K_i/N_0 and by $\tau_{k,i}$ the sum of the kth powers of all these conjugates. We compute:

$$\begin{aligned} T_i(1) &= (\beta_i \,|\, \chi_i)^3 + (\beta_i \,|\, \chi_i^2)^3 \\ &= (\beta_i + \zeta^2\delta_i(\beta_i) + \zeta\delta_i^2(\beta_i))^3 + (\beta_i + \zeta\delta_i(\beta_i) + \zeta^2\delta_i^2(\beta_i))^3 \\ &= 2\tau_{3,i} + 12\sigma_{3,i} + 3\,\mathrm{Tr}_{K_i/N_0}(\beta_i^2(-\delta_i(\beta_i) - \delta_i^2(\beta_i))) \\ &= 2\tau_{3,i} + 12\sigma_{3,i} + 3(\tau_{3,i} - \beta_0\tau_{2,i}). \end{aligned}$$

Using the relations between σ's and τ's [vW, Exercise 5.18] yields

$$T_i(1) = 2\beta_0^3 - 9\beta_0\sigma_{2,i} + 27\sigma_{3,i},$$

so that

$$S(1) = (2r+1)\beta_0^3 - 9\beta_0 \sum_{i=1}^{r} \sigma_{2,i} + 27 \sum_{i=1}^{r} \sigma_{3,i}. \tag{5}$$

Since $\beta_0 = \mathrm{Tr}_{N_3/N_0}(\beta)$ and $\mathcal{A}_{N_0/N_0} = \mathcal{O}_{N_0}$, β_0 is a unit by Corollary 2.5; further, $2r+1 = 3^m$, so we only have to deal with $9\sum_{i=1}^{r}\sigma_{2,i}$ and $27\sum_{i=1}^{r}\sigma_{3,i}$.

We first notice that the $\sigma_{k,i}$ are evaluations at the $\gamma(\beta)$'s, $\gamma \in \Gamma_0$, of polynomials in indeterminates X_γ's, $\gamma \in \Gamma_0$. As an abuse of language, we shall say that a property is *formally* satisfied by the evaluation at the $\gamma(\beta)$'s of such a polynomial when we mean that it is satisfied by this polynomial. Notice that Γ_0 acts on polynomials in the X_γ's by permutation of the indeterminates.

LEMMA 3.2. *Each $\sigma_{k,i}$, $1 \le i \le r$ and $1 \le k \le 3$, is formally invariant under the action of Γ_0.*

Since $\sigma_{k,i}$ lies in N_0, this is of course stronger than stating that $\sigma_{k,i}$ is invariant under Γ_0. It means for instance that the polynomial $\sum_{\gamma\in\Gamma_0} X_\gamma$, whose evaluation at the $\gamma(\beta)$'s is $\beta_0 = \mathrm{Tr}_{K_i/N_0}(\beta_i) = \sigma_{1,i}$ for any i, is invariant under the action of Γ_0. In other words, each $\sigma_{k,i}$ is a symmetric function of the conjugates of β over N_0 with respect to the action of Γ_0.

Proof. By definition, $\sigma_{k,i}$ is a symmetric function of the conjugates of β_i with respect to the action of $\langle\delta_i\rangle$; further $\beta_i = \mathrm{Tr}_{N_3/K_i}(\beta)$ is formally invariant under the action of $\ker(\chi_i)$, as are its conjugates under $\langle\delta_i\rangle$, so the same holds for $\sigma_{k,i}$, and the result follows since $\Gamma_0 = \ker(\chi_i)\times\langle\delta_i\rangle$. ∎

We denote by σ_2 the second elementary symmetric function of the conjugates of β over N_0.

LEMMA 3.3. $9\sum_{i=1}^{r}\sigma_{2,i} = 3^{m+1}\sigma_2$ *belongs to* $3^{m+1}\mathcal{O}_{N_0}$.

Proof. By definition,

$$\sigma_{2,i} = \beta_i\delta_i(\beta_i) + \delta_i(\beta_i)\delta_i^2(\beta_i) + \delta_i^2(\beta_i)\beta_i,$$

so a product $\beta\delta(\beta)$ with $\delta \in \Gamma_0 \setminus \{1\}$ may formally appear in $\sigma_{2,i}$ only in the first or in the third product, that is, in

$$\beta_i(\delta_i(\beta_i) + \delta_i^2(\beta_i)) = \Big(\sum_{\gamma\in\ker(\chi_i)}\gamma(\beta)\Big)\Big(\sum_{\gamma'\in\ker(\chi_i)}(\delta_i\gamma'(\beta) + \delta_i^2\gamma'(\beta))\Big),$$

and we see that $\beta\delta(\beta)$ formally appears in $\sigma_{2,i}$ if and only if $\delta \notin \ker(\chi_i)$. We deduce from Lemma 2.3 that

$$\#\{i \in \{1,\dots,r\} \mid \delta \notin \ker(\chi_i)\} = 3^{m-1},$$

so for each $\delta \in \Gamma_0 \setminus \{1\}$, the product $\beta\delta(\beta)$ formally appears 3^{m-1} times in $\sum_{i=1}^{r}\sigma_{2,i}$. Thanks to Lemma 3.2, the same happens for its conjugates under Γ_0. It is easy to check that all these conjugates are formally different, that $\beta\delta(\beta)$ and $\beta\delta^2(\beta)$ give rise to the same set of conjugates and that no other formal coincidence occurs. Hence there are $3^m\frac{3^m-1}{2}$ formally different products $\gamma_1(\beta)\gamma_2(\beta)$ occurring 3^{m-1} times each in $\sum_{i=1}^{r}\sigma_{2,i}$; but σ_2 is precisely the sum of these $\binom{3^m}{2}$ products, so the equality of the lemma holds.

It remains to write $\sigma_2 = \frac{1}{2}\operatorname{Tr}_{N_3/N_0}(\sum_{\gamma\in\Gamma_0\setminus\{1\}}\beta\gamma(\beta))$ and to notice that $\beta\gamma(\beta)\in\mathcal{A}_{N_3}^2=\mathcal{D}_{N_3}^{-1}$ to get $\sigma_2\in\mathcal{O}_{N_0}$, hence the result. ∎

LEMMA 3.4. *$27\sum_{i=1}^r\sigma_{3,i}$ belongs to $3^m\mathcal{O}_{N_0}$.*

Proof. We follow the same path as in the former proof:

$$\sigma_{3,i}=\Big(\sum_{\gamma_1\in\ker(\chi_i)}\gamma_1(\beta)\Big)\Big(\sum_{\gamma_2\in\ker(\chi_i)}\delta_i\gamma_2(\beta)\Big)\Big(\sum_{\gamma_3\in\ker(\chi_i)}\delta_i^2\gamma_3(\beta)\Big),$$

so a product $\beta\delta(\beta)\delta'(\beta)$, with $\delta,\delta'\in\Gamma_0$ and $\#\{1,\delta,\delta'\}=3$, formally appears in $\sigma_{3,i}$ if and only if $\Gamma_0=\ker(\chi_i)\amalg\delta\ker(\chi_i)\amalg\delta'\ker(\chi_i)$, which is also equivalent to

$$\delta\notin\ker(\chi_i),\quad \delta\delta'\in\ker(\chi_i).$$

We now have to consider two cases:

• if $\delta'=\delta^2$, the two conditions above amount to $\delta\notin\ker(\chi_i)$, which happens for 3^{m-1} values of i, so $\beta\delta(\beta)\delta^2(\beta)$ formally appears 3^{m-1} times in $\sum_i\sigma_{3,i}$;

• if $\delta'\neq\delta^2$, that is, $\delta'\notin\langle\delta\rangle$, there are 3^{m-1} characters χ of Γ_0 such that $\delta\delta'\in\ker(\chi)$, among which 3^{m-2} are such that δ belongs to $\ker(\chi)$ (indeed $\delta\delta'\notin\langle\delta\rangle$, so Lemma 2.3(ii) applies). This gives $3^{m-1}-3^{m-2}=2\cdot3^{m-2}$ characters of Γ_0 whose kernels contain $\delta\delta'$ but not δ, hence there are 3^{m-2} values of i such that $\beta\delta(\beta)\delta'(\beta)$ formally appears in $\sigma_{3,i}$ (recall χ_i and χ_i^2 share the same kernel). We infer that $\beta\delta(\beta)\delta'(\beta)$ formally appears 3^{m-2} times in $\sum_i\sigma_{3,i}$.

By Lemma 3.2, each $\beta\delta(\beta)\delta^2(\beta)$ ($\delta\neq1$) formally appears with its 3^{m-1} formally distinct conjugates under Γ_0 (this product is fixed under $\langle\delta\rangle$), so that the sum of these conjugates equals one third of the trace of $\beta\delta(\beta)\delta^2(\beta)$, whereas a product $\beta\delta(\beta)\delta'(\beta)$ satisfying the previous conditions has 3^m formally distinct conjugates under Γ_0. This implies

$$\sum_{i=1}^r\sigma_{3,i}=\frac{3^{m-1}}{3}\operatorname{Tr}_{N_3/N_0}\Big(\frac{1}{2}\sum_{\delta\neq1}\beta\delta(\beta)\delta^2(\beta)\Big)+3^{m-2}\operatorname{Tr}_{N_3/N_0}\Big(\frac{1}{2}\sum_{\delta,\delta'}\beta\delta(\beta)\delta'(\beta)\Big),$$

where the last sum runs over the $\delta\in\Gamma_0\setminus\{1\}$ and $\delta'\in\Gamma_0\setminus\langle\delta\rangle$, and the $\frac{1}{2}$'s correspond to the fact that each given product formally appears twice in the sums. We eventually get

$$27\sum_{i=1}^r\sigma_{3,i}\in3^{m+1}\operatorname{Tr}_{N_3/N_0}(\mathcal{A}_{N_3/N_0}^3)=3^{m+1}\cdot\frac{1}{3}\,\mathcal{O}_{N_0}=3^m\mathcal{O}_{N_0}.\ ∎$$

Notice that, unlike $\sum_i \sigma_{2,i}$, $\sum_i \sigma_{3,i}$ is not a symmetric function of the conjugates of β over N_0 with respect to the whole permutation group $\mathfrak{S}_{3^m}$ of these conjugates, since the products of the first kind formally appear three times more often in $\sum_i \sigma_{3,i}$ than those of the second kind.

Lemmas 3.3 and 3.4 together with formula (5) yield

$$S(1) \in 3^m \mathcal{O}_{N_0}. \tag{6}$$

Before dealing with $S(\gamma)$ in the case $\gamma \neq 1$, we have the following interlude.

3.2. *The square root of the discriminant of* $\mathcal{A}_{K_i/N_0}$. Let $i \in \{1, \dots, r\}$ and δ_i as above; the set $\{\beta_i, \delta_i(\beta_i), \delta_i^2(\beta_i)\}$ is a basis of $\mathcal{A}_{K_i/N_0}$ over $\mathcal{O}_{N_0}$, so the discriminant of $\mathcal{A}_{K_i/N_0}$ over $\mathcal{O}_{N_0}$ is the principal fractional ideal generated by

$$(\beta_i - \delta_i(\beta_i))^2 (\delta_i(\beta_i) - \delta_i^2(\beta_i))^2 (\delta_i^2(\beta_i) - \beta_i)^2.$$

We define R_i to be the following square root of this generator:

$$R_i = (\beta_i - \delta_i(\beta_i))(\delta_i(\beta_i) - \delta_i^2(\beta_i))(\delta_i^2(\beta_i) - \beta_i);$$

then $R_i \in N_0$, since R_i is in K_i, $R_i^2 \in N_0$ and $[K_i : N_0]$ is odd. Of course R_i is not formally invariant under the action of the whole permutation group $\mathfrak{S}_{3^m}$. Yet one has:

LEMMA 3.5. *R_i is formally invariant under the action of Γ_0 and*

$$\begin{aligned} R_i &= \mathrm{Tr}_{K_i/N_0}(\beta_i^2(\delta_i^2(\beta_i) - \delta_i(\beta_i))) \\ &= \mathrm{Tr}_{N_3/N_0}\Big(\beta \sum_{(\gamma_1,\gamma_2)} \gamma_1(\beta)\gamma_2(\delta_i^2(\beta) - \delta_i(\beta))\Big), \end{aligned}$$

where the sum runs over $\ker(\chi_i) \times \ker(\chi_i)$.

Proof. The first equality is straightforward, it proves the assertion and yields the second one immediately. ∎

In fact, the formal invariance property of R_i will not be needed, since we shall make use of the second trace formula instead. We are now ready to finish the proof of Theorem 3.1.

3.3. *Computation of* $S(\gamma)$ *for* $\gamma \neq 1$. We fix $\gamma \in \Gamma_0$ with $\gamma \neq 1$ and we define the partition $I_\gamma \amalg J_\gamma$ of $\{1, \dots, r\}$ by

$$I_\gamma = \{1 \leq i \leq r \mid \gamma \notin \ker(\chi_i)\}, \qquad J_\gamma = \{1 \leq j \leq r \mid \gamma \in \ker(\chi_j)\}.$$

One easily deduces from Lemma 2.3 that $\#I_\gamma = 3^{m-1}$ and $\#J_\gamma = (3^{m-1} - 1)/2$. For each $i \in I_\gamma$, we ensure $\chi_i(\gamma) = \zeta$ (the primitive 3rd root of unity introduced at the beginning of this section), replacing χ_i by its square if necessary, and we choose $\delta_i \in \Gamma_0 \setminus \ker(\chi_i)$ such that $\chi_i(\delta_i) = \zeta$.

We wish to compute (4):

$$S(\gamma) = \beta_0^3 + \sum_{i=1}^{r} T_i(\gamma),$$

where $T_i(\gamma) = \chi_i(\gamma^{-1})(\beta_i \,|\, \chi_i)^3 + \chi_i^2(\gamma^{-1})(\beta_i \,|\, \chi_i^2)^3$. For $j \in J_\gamma$, we know from Subsection 3.1 that

$$T_j(\gamma) = T_j(1) = 2\beta_0^3 - 9\beta_0\sigma_{2,j} + 27\sigma_{3,j}.$$

We compute $T_i(\gamma)$ for $i \in I_\gamma$:

$$\begin{aligned} T_i(\gamma) &= \zeta^2(\beta_i \,|\, \chi_i)^3 + \zeta(\beta_i \,|\, \chi_i^2)^3 \\ &= \zeta^2(\beta_i + \zeta^2\delta_i(\beta_i) + \zeta\delta_i^2(\beta_i))^3 + \zeta(\beta_i + \zeta\delta_i(\beta_i) + \zeta^2\delta_i^2(\beta_i))^3 \\ &= -\tau_{3,i} - 6\sigma_{3,i} + 3\,\mathrm{Tr}_{K_i/N_0}(\beta_i^2(2\delta_i^2(\beta_i) - \delta_i(\beta_i))) \\ &= -\beta_0^3 + 3\beta_0\sigma_{2,i} - 9\sigma_{3,i} + 3\,\mathrm{Tr}_{K_i/N_0}(\beta_i^2(2\delta_i^2(\beta_i) - \delta_i(\beta_i))), \end{aligned}$$

whereas $T_i(\gamma^2) = -\beta_0^3 + 3\beta_0\sigma_{2,i} - 9\sigma_{3,i} + 3\,\mathrm{Tr}_{K_i/N_0}(\beta_i^2(2\delta_i(\beta_i) - \delta_i^2(\beta_i)))$, so that

$$T_i(\gamma) - T_i(\gamma^2) = 9R_i,$$

where R_i is the square root of the discriminant of $\mathcal{A}_{K_i/N_0}$ introduced in the previous subsection. On the other hand, $T_i(1) + T_i(\gamma) + T_i(\gamma^2) = 0$, so $T_i(\gamma) + T_i(\gamma^2) = -2\beta_0^3 + 9\beta_0\sigma_{2,i} - 27\sigma_{3,i}$ and we get

$$T_i(\gamma) = -\beta_0^3 + \frac{9}{2}\,\beta_0\sigma_{2,i} - \frac{27}{2}\,\sigma_{3,i} + \frac{9}{2}\,R_i,$$

which yields

$$S(\gamma) = \frac{9}{2}\,\beta_0 \sum_{i=1}^{r} \sigma_{2,i} - \frac{27}{2} \sum_{i=1}^{r} \sigma_{3,i} - \frac{27}{2}\,\beta_0 \sum_{j\in J_\gamma} \sigma_{2,j} + \frac{81}{2} \sum_{j\in J_\gamma} \sigma_{3,j} + \frac{9}{2} \sum_{i\in I_\gamma} R_i.$$

The first two terms have already been dealt with in Lemmas 3.3 and 3.4, whose proofs we may now adjust in order to deal with the third and fourth terms.

LEMMA 3.6. *$-\frac{27}{2}\beta_0 \sum_{J_\gamma} \sigma_{2,j}$ belongs to $3^{m+1}\mathcal{O}_{N_0}$.*

Proof. Recall from the proof of Lemma 3.3 that a product $\beta\delta(\beta)$ formally appears in $\sigma_{2,j}$ if and only if $\delta \notin \ker(\chi_j)$. This implies that the products $\beta\gamma(\beta)$ and $\beta\gamma^2(\beta)$ do not formally appear in $\sum_{J_\gamma} \sigma_{2,j}$, and that any product $\beta\delta(\beta)$ with $\delta \in \Gamma_0 \setminus \langle\gamma\rangle$ formally appears in $\sigma_{2,j}$ for some $j \in J_\gamma$, since $\langle\gamma\rangle = \bigcap_{J_\gamma} \ker(\chi_j)$.

Let $\delta \in \Gamma_0 \setminus \langle\gamma\rangle$. Then $\delta \in \ker(\chi_j)$ with $j \in J_\gamma$ if and only if $\chi_j \in \ker(\widehat{\delta}) \cap \ker(\widehat{\gamma})$, where $\widehat{\delta}$ denotes the linear form $\widehat{\Gamma_0} \to \mu_3$, $\chi \mapsto \chi(\delta)$ (see Subsection 2.2). This intersection of two distinct hyperplanes of $\widehat{\Gamma_0}$ is of codimension 2 and of cardinality 3^{m-2}, so δ happens to be in $\ker(\chi_j)$ for $(3^{m-2}-1)/2$ values of $j \in J_\gamma$. Hence $\delta \notin \ker(\chi_j)$ is true for $(3^{m-1}-1)/2 - (3^{m-2}-1)/2 =$

3^{m-2} values of $j \in J_\gamma$ and $\beta\delta(\beta)$ formally appears 3^{m-2} times in $\sum_{J_\gamma} \sigma_{2,j}$, together with its distinct conjugates under Γ_0 by Lemma 3.2. All of them being formally different but generated by both products $\beta\delta(\beta)$ and $\beta\delta^2(\beta)$, we get

$$\sum_{j\in J_\gamma} \sigma_{2,j} = 3^{m-2}\,\mathrm{Tr}_{N_3/N_0}\left(\frac{1}{2}\sum_{\delta\notin\langle\gamma\rangle}\beta\delta(\beta)\right) \in 3^{m-2}\mathcal{O}_{N_0},$$

which gives the result. ∎

LEMMA 3.7. $\frac{81}{2}\sum_{J_\gamma}\sigma_{3,j}$ *belongs to* $3^m\mathcal{O}_{N_0}$.

Proof. We deduce from the proof of Lemma 3.4 that a product $\beta\delta(\beta)\delta'(\beta)$ with $\#\{1,\delta,\delta'\}=3$ formally appears in $\sigma_{3,j}$ with $j\in J_\gamma$ if and only if

$$\delta \notin \ker(\chi_j), \quad \delta\delta' \in \ker(\chi_j) \quad \text{and} \quad \gamma \in \ker(\chi_j).$$

These conditions imply as before that δ and δ' do not belong to $\langle\gamma\rangle$, but also that $\delta' \notin \delta\langle\gamma\rangle$ (otherwise $\delta\delta' \in \ker(\chi_j)$ would never be possible for $j \in J_\gamma$).

We now fix δ and δ' in Γ_0 such that $\delta \notin \langle\gamma\rangle$ and $\delta' \notin \langle\gamma\rangle \amalg \delta\langle\gamma\rangle$. Observe first that $\delta \notin \langle\gamma, \delta\delta'\rangle$, because otherwise $\delta\delta'$ would belong to $\delta\langle\gamma\rangle \amalg \delta^2\langle\gamma\rangle$, which contradicts our hypothesis. We have to consider two cases:

• if $\delta' \in \delta^2\langle\gamma\rangle$, the three preceding conditions amount to $\gamma \in \ker(\chi_j)$ and $\delta \notin \ker(\chi_j)$, so each of the three terms: $\beta\delta(\beta)\delta^2(\beta)$, $\beta\delta(\beta)\delta^2\gamma(\beta)$ and $\beta\delta(\beta)\delta^2\gamma^2(\beta)$, formally appears in $\sigma_{3,j}$ for 3^{m-2} values of j in J_γ;

• if $\delta' \notin \delta^2\langle\gamma\rangle$, then $\delta\delta' \notin \langle\gamma\rangle$. If $m = 2$, this yields $\Gamma_0 = \langle\gamma, \delta\delta'\rangle$, which contradicts $\delta \notin \langle\gamma, \delta\delta'\rangle$, so that no such product occurs in $\sum_{J_\gamma}\sigma_{3,j}$. If $m \geq 3$, the two conditions: $\gamma \in \ker(\chi)$ and $\delta\delta' \in \ker(\chi)$, define a codimension 2 subspace of $\widehat{\Gamma_0}$, in which the additional condition $\delta \in \ker(\chi)$ defines a hyperplane, since $\delta \notin \langle\gamma, \delta\delta'\rangle$. Thus there are $2\cdot 3^{m-3}$ characters χ of Γ_0 such that $\gamma \in \ker(\chi)$, $\delta\delta' \in \ker(\chi)$ and $\delta \notin \ker(\chi)$, and our product $\beta\delta(\beta)\delta'(\beta)$ formally appears in $\sigma_{3,j}$ for 3^{m-3} values of $j \in J_\gamma$.

Using Lemma 3.2 we obtain

$$\begin{aligned}\sum_{J_\gamma}\sigma_{3,j} = {} & 3^{m-3}\,\mathrm{Tr}_{N_3/N_0}\left(\frac{1}{2}\sum_{\delta\notin\langle\gamma\rangle}\beta\delta(\beta)\delta^2(\beta)\right)\\ & + 3^{m-2}\,\mathrm{Tr}_{N_3/N_0}\left(\frac{1}{2}\sum_{\delta\notin\langle\gamma\rangle}(\beta\delta(\beta)\delta^2\gamma(\beta) + \beta\delta(\beta)\delta^2\gamma^2(\beta))\right)\\ & + 3^{m-3}\,\mathrm{Tr}_{N_3/N_0}\left(\frac{1}{2}\sum_{\delta\notin\langle\gamma\rangle}\beta\delta(\beta)\sum_{\delta'\notin\langle\gamma,\delta\rangle}\delta'(\beta)\right)\end{aligned}$$

(the last term vanishes if $m = 2$) and we conclude as in the proof of Lemma 3.4, taking advantage of the fact that the gain in the valuation of $81 = 3\cdot 27$ balances the loss in the valuation of $3^{m-3} = \frac{1}{3}\cdot 3^{m-2}$. ∎

LEMMA 3.8. *$\frac{9}{2}\sum_{I_\gamma} R_i$ belongs to $3^m\mathcal{O}_{N_0}$.*

Proof. We start with the second expression of R_i given in Lemma 3.5, and we note that the only constraint on δ_i for $i \in I_\gamma$ is that $\chi_i(\delta_i) = \zeta$, so we may choose $\delta_i = \gamma$ for any $i \in I_\gamma$. We get

$$R_i = \mathrm{Tr}_{N_3/N_0}\Big(\sum_{\gamma_1,\gamma_2} \beta\gamma_1(\beta)\gamma_2(\beta')\Big),$$

where γ_1 and γ_2 both run through $\ker(\chi_i)$ and $\beta' = \gamma^2(\beta) - \gamma(\beta)$. We have the following decomposition of the sum inside brackets:

$$\beta^2\beta' + \beta^2\sum_{\gamma_2\neq 1}\gamma_2(\beta') + \beta\sum_{\gamma_1\neq 1}\gamma_1(\beta)(\beta' + \gamma_1(\beta') + \gamma_1^2(\beta')) + \beta\sum_{\gamma_1\neq 1}\gamma_1(\beta)\sum_{\gamma_2\notin\langle\gamma_1\rangle}\gamma_2(\beta').$$

Clearly $\beta^2\beta'$ formally appears in each R_i, so its trace comes with a factor 3^{m-1} in $\sum_{I_\gamma} R_i$. The products involving only one parameter $\delta \in \Gamma_0 \setminus \{1\}$, that is, $\beta^2\delta(\beta')$, $\beta\delta(\beta)\beta'$, $\beta\delta(\beta)\delta(\beta')$ and $\beta\delta(\beta)\delta^2(\beta')$, formally appear in R_i if and only if $\delta \in \ker(\chi_i)$, so δ may be any element of $\Gamma_0 \setminus \langle\gamma\rangle$. If this is the case, each of the former products formally appears in R_i for 3^{m-2} values of $i \in I_\gamma$ (there are 3^{m-1} characters χ of Γ_0 such that $\delta \in \ker(\chi)$, among which $2\cdot 3^{m-2}$ are not trivial on γ), and their traces come with a factor 3^{m-2} in $\sum_{I_\gamma} R_i$.

The last term contains products of the shape $\beta\delta(\beta)\delta'(\beta')$ with $\delta \in \Gamma_0\setminus\{1\}$ and $\delta' \in \Gamma_0 \setminus \langle\delta\rangle$. Clearly, δ and δ' cannot lie in $\langle\gamma\rangle$. Further γ cannot belong to $\langle\delta,\delta'\rangle$, in other words $\delta' \notin \langle\delta,\gamma\rangle$. Consequently, this term vanishes when $m = 2$. Suppose $m \geq 3$, $\delta \in \Gamma_0 \setminus \langle\gamma\rangle$ and $\delta' \in \Gamma_0 \setminus \langle\delta,\gamma\rangle$. The characters χ of Γ_0 such that $\chi(\delta) = \chi(\delta') = 1$ form a codimension 2 subspace of $\widehat{\Gamma_0}$, in which the additional condition $\chi(\gamma) = 1$ defines a hyperplane; thus there are 3^{m-3} values of $i \in I_\gamma$ such that $\beta\delta(\beta)\delta'(\beta')$ formally appears in R_i, and its trace comes with a factor 3^{m-3} in $\sum_{I_\gamma} R_i$.

Eventually we get

$$\sum_{I_\gamma} R_i = 3^{m-1}\,\mathrm{Tr}_{N_3/N_0}(\beta^2\beta') + 3^{m-2}\,\mathrm{Tr}_{N_3/N_0}\Big(\beta^2\sum_{\delta\notin\langle\gamma\rangle}\delta(\beta')\Big) + 3^{m-2}\,\mathrm{Tr}_{N_3/N_0}\Big(\beta\sum_{\delta\notin\langle\gamma\rangle}\delta(\beta)(\beta' + \delta(\beta') + \delta^2(\beta'))\Big) + 3^{m-3}\,\mathrm{Tr}_{N_3/N_0}\Big(\sum_{\delta\notin\langle\gamma\rangle}\beta\delta(\beta)\sum_{\delta'\notin\langle\delta,\gamma\rangle}\delta'(\beta')\Big),$$

keeping in mind that the last term vanishes when $m = 2$. In fact, it also

vanishes if $m \geq 3$: fix $\delta \in \Gamma_0 \setminus \langle\gamma\rangle$; then

$$\sum_{\delta' \notin \langle\delta,\gamma\rangle} \delta'(\beta') = \sum_{\delta' \notin \langle\delta,\gamma\rangle} \delta'\gamma^2(\beta) - \sum_{\delta' \notin \langle\delta,\gamma\rangle} \delta'\gamma(\beta) = 0$$

since $\gamma^2\langle\delta,\gamma\rangle = \langle\delta,\gamma\rangle = \gamma\langle\delta,\gamma\rangle$. Let us now have a look at the other sums involved:

$$\beta^2 \sum_{\delta \notin \langle\gamma\rangle} \delta(\beta') = \beta^2\Big(\sum_{\delta \notin \langle\gamma\rangle} \delta\gamma^2(\beta) - \sum_{\delta \notin \langle\gamma\rangle} \delta\gamma(\beta)\Big) = 0,$$

$$\begin{aligned}\beta \sum_{\delta \notin \langle\gamma\rangle} \delta(\beta)\beta' &= \beta\beta_0\beta' - \beta(\beta + \gamma(\beta) + \gamma^2(\beta))\beta' \\ &= \beta_0\beta\beta' - (\beta^2\gamma^2(\beta) + \beta\gamma^2(\beta^2)) + \gamma(\beta^2\gamma^2(\beta) + \beta\gamma^2(\beta^2)),\end{aligned}$$

so that

$$\operatorname{Tr}_{N_3/N_0}\Big(\beta \sum_{\delta \notin \langle\gamma\rangle} \delta(\beta)\beta'\Big) = \beta_0 \operatorname{Tr}_{N_3/N_0}(\beta\beta');$$

and

$$\beta \sum_{\delta \notin \langle\gamma\rangle} \delta(\beta)\delta(\beta') = \beta\Big(\sum_{\delta \notin \langle\gamma\rangle} \delta(\beta)\delta\gamma^2(\beta) - \sum_{\delta \notin \langle\gamma\rangle} \delta(\beta)\delta\gamma(\beta)\Big) = 0.$$

In order to study the only remaining sum $\beta\sum_{\delta\notin\langle\gamma\rangle}\delta(\beta)\delta^2(\beta')$, we introduce the binary relation $\overset{\gamma}{\sim}$ on $\Gamma_0 \setminus \langle\gamma\rangle$, defined by

$$\delta \overset{\gamma}{\sim} \delta' \quad \text{if} \quad \delta' \in \langle\delta,\gamma\rangle \setminus \langle\gamma\rangle.$$

It is easily verified that $\overset{\gamma}{\sim}$ is an equivalence relation, and that each class of $\Gamma_0\setminus\langle\gamma\rangle$ under $\overset{\gamma}{\sim}$ contains 6 elements. Further, one checks that $\beta\delta(\beta)\delta'^2\gamma^2(\beta)$ and $\beta\delta(\beta)\delta^2\gamma^2(\beta)$ (respectively $\beta\delta(\beta)\delta'^2\gamma(\beta)$ and $\beta\delta(\beta)\delta^2\gamma(\beta)$) are conjugate if $\delta \overset{\gamma}{\sim} \delta'$, hence

$$\operatorname{Tr}_{N_3/N_0}\Big(\beta \sum_{\delta \notin \langle\gamma\rangle} \delta(\beta)\delta^2(\beta')\Big) = 6 \operatorname{Tr}_{N_3/N_0}\Big(\beta \sum_{\delta \in \Gamma_\gamma} \delta(\beta)\delta^2(\beta')\Big),$$

where Γ_γ denotes a set of coset representatives of $\overset{\gamma}{\sim}$ in $\Gamma_0 \setminus \langle\gamma\rangle$.

Collecting the results yields

$$\begin{aligned}\sum_{\Gamma_\gamma} R_i &= 3^{m-1} \operatorname{Tr}_{N_3/N_0}(\beta^2\beta') + 3^{m-2}\beta_0 \operatorname{Tr}_{N_3/N_0}(\beta\beta') \\ &\quad + 2 \cdot 3^{m-1} \operatorname{Tr}_{N_3/N_0}\Big(\beta \sum_{\delta \in \Gamma_\gamma} \delta(\beta)\delta^2(\beta')\Big),\end{aligned}$$

which clearly belongs to $3^{m-2}\mathcal{O}_{N_0}$. ∎

Putting everything together with (6), we obtain

$$\forall\gamma \in \Gamma_0, \quad S(\gamma) \in 3^m\mathcal{O}_{N_0},$$

which is Theorem 3.1 and implies Theorem 1.

REMARK. One may compute $\sum_{I_\gamma} \sigma_{k,i}$ for $k \in \{2,3\}$ in order to check the coherence of the results for the analogous sums over J_γ with the expressions of $\sum_{i=1}^{r} \sigma_{k,i}$ given in Subsection 3.1. These computations turn out to be more complicated than the ones presented above.

Acknowledgments. The author wishes to thank Prof. Jean Cougnard for his careful reading of the manuscript, and the copy editor for language corrections.

References

[B] N. P. Byott, *Integral Galois module structure of some Lubin–Tate extensions*, J. Number Theory 77 (1999), 252–273.

[CNT] Ph. Cassou-Noguès and M. J. Taylor, *Galois module structure for wild extensions*, in: Algebraic Number Theory and Diophantine Analysis (Graz, 1998), F. Halter-Koch and R. F. Tichy (eds.), de Gruyter, New York, 2000, 69–91.

[E] B. Erez, *The Galois structure of the square root of the inverse different*, Math. Z. 208 (1991), 239–255.

[F] A. Fröhlich, *Galois Module Structure of Algebraic Integers*, Ergeb. Math. Grenzgeb. (3) 1, Springer, Berlin, 1983.

[S1] J.-P. Serre, *Corps locaux*, 3e éd., Hermann, Paris, 1968.

[S2] —, *Représentations linéaires des groupes finis*, 3e éd., Hermann, Paris, 1978.

[T] M. J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. 63 (1981), 41–79.

[U] S. Ullom, *Integral normal bases in Galois extensions of local fields*, Nagoya Math. J. 39 (1970), 141–148.

[V1] S. Vinatier, *Structure galoisienne dans les extensions faiblement ramifiées de* $\mathbb{Q}$, J. Number Theory 91 (2001), 126–152.

[V2] —, *Une famille infinie d'extensions faiblement ramifiées*, Math. Nachr. 243 (2002), 165–187.

[V3] —, *Sur la racine carrée de la codifférente*, J. Théor. Nombres Bordeaux 15 (2003), 393–410.

[vW] B. L. van der Waerden, *Algebra*, Vol. I, Springer, New York, 1991.

LACO Université de Limoges
123 avenue Albert Thomas
F-87060 Limoges Cedex, France
E-mail: stephane.vinatier@unilim.fr

Received on 18.6.2004
and in revised form on 29.4.2005 (4791)