

NORMAL INTEGRAL BASES FOR A_4 EXTENSIONS OF THE RATIONALS

JEAN COUGNARD

ABSTRACT. We give an algorithm for constructing normal integral bases of tame Galois extensions of the rationals with group A_4 . Using earlier works we can do the same until degree 15.

INTRODUCTION

It is known [11] that every rank one projective module over the alternated group A_4 is free. Consequently, if $\mathbb{Q} \subset N$ is a tame Galois extension with group A_4 (the ramification indices are prime to the residual characteristic), the ring of integers \mathcal{O}_N is free over $\mathbb{Z}[A_4]$, i.e., there exists $\theta \in \mathcal{O}_N$ which, together with its conjugates, gives a \mathbb{Z} -basis for \mathcal{O}_N . Then one says that \mathcal{O}_N has a normal integral basis. The aim of this work is to show how to construct such a basis.

The result in [11] is based on Swan theorems about induction properties in the projective class groups. Here we give a constructive version based on a fiber product which is more suited for our goal.

We recall well-known results about A_4 and $\mathbb{Z}[A_4]$ in the first part. The second section is devoted to the study of A_4 extensions of the rationals through Lagrange resolvents. In the third part, we use Lagrange resolvents to build maps reflecting the Galois-module structure. To compute some indices, we need a local study; this is done in the fourth part. This enables us to construct a normal integral basis and to give numerical exemples.

In combination with the earlier papers ([7], [3], [4], [5]), we can now construct normal integral basis, up to the degree 15, when they exist, and for some cases in degree 16 (the abelian cases are solved by Hilbert-Speiser Theorem independently of the degree).

1. $\mathbb{Z}[A_4]$ PROJECTIVE MODULES

The group A_4 is defined by generators and relations:

$$\{\sigma, \tau, \nu \mid \nu^3 = \sigma^2 = \tau^2 = e, \sigma\tau = \tau\sigma, \nu\sigma\nu^2 = \tau, \nu\tau\nu^2 = \sigma\tau\}.$$

It is an extension of a cyclic group of order 3 by the normal subgroup $H = \{e, \sigma, \tau, \sigma\tau\}$ (isomorphic to the Klein group V_4). It has four order 3 subgroups, namely $\{e, \nu, \nu^2\}$ and its conjugates by $\sigma, \tau, \sigma\tau$. The order 2 subgroups are generated by $\sigma, \tau, \sigma\tau$, and there is no other nontrivial subgroup but those listed above.

Received by the editor March 28, 2004 and, in revised form, October 28, 2004.

2000 *Mathematics Subject Classification*. Primary 11R04, 11Y40; Secondary 11R33.

Key words and phrases. Number theory, algorithm.

©2005 American Mathematical Society
Reverts to public domain 28 years from publication

There are three absolutely irreducible degree-1 representations of A_4 (inflated from the representations of A_4/H) and one, ρ , with degree 3 defined, up to conjugacy, by the images of σ and ν :

$$\sigma \mapsto \rho(\sigma) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \nu \mapsto \rho(\nu) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

A direct verification gives $\rho(e + \sigma + \tau + \sigma\tau) = 0$ and

$$\rho(e + \nu + \sigma\nu) = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \rho(e + \nu^2 + \sigma\nu^2) = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \rho(e + \nu + \sigma\tau\nu) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix},$$

while the images by ρ of $e + \nu^2 + \sigma\tau\nu^2$, $e + \nu + \tau\nu$, $e + \nu^2 + \tau\nu^2$ are transposed of the previous ones.

The morphism ρ from A_4 to $GL_3(\mathbb{Q})$ extends to a \mathbb{Q} -morphism of algebras from $\mathbb{Q}[A_4]$ to $M_3(\mathbb{Q})$. The image Λ of $\mathbb{Z}[A_4]$ is a \mathbb{Z} -order of $M_3(\mathbb{Q})$ included in the maximal order $M_3(\mathbb{Z})$. The relation $\rho(e + \sigma + \tau + \sigma\tau) = 0$ implies that Λ , as a \mathbb{Z} -module, has a basis given by ρ images of $\{e, \nu, \nu^2, \sigma, \sigma\nu, \sigma\nu^2, \tau, \tau\nu, \tau\nu^2\}$. Denote these elements by b_i ($1 \leq i \leq 9$). Then the discriminant $\det(\text{Tr}(b_i b_j))$ is 2^{12} . As the discriminant of a maximal order, for instance $M_3(\mathbb{Z})$, is 1, we have $[M_3(\mathbb{Z}) : \Lambda] = 2^6$, so Λ is locally maximal, except at 2. We can also give a basis of $M_3(\mathbb{Z})$ using ρ images of elements from $\mathbb{Q}[A_4]$: $\frac{\rho(e+\sigma)}{2}$, $\frac{\rho((e+\sigma)\nu)}{2}$, $\frac{\rho((e+\sigma)\nu^2)}{2}$, $\frac{\rho(e+\tau)}{2}$, $\frac{\rho((e+\tau)\nu)}{2}$, $\frac{\rho((e+\tau)\nu^2)}{2}$, $\frac{\rho(-\sigma-\tau)}{2} = \rho(e - \frac{e+\sigma}{2} - \frac{e+\tau}{2})$, $\frac{\rho((-\sigma-\tau)\nu)}{2}$, $\frac{\rho((-\sigma-\tau)\nu^2)}{2}$.

The order generated by $\mathbb{Z}[A_4]$, by the central idempotents $\frac{1}{12} \sum_{g \in A_4} g$, $\frac{1}{4} (\sum_{h \in H} h)$ and by $(\frac{e+\sigma}{2})$, $(\frac{e+\tau}{2})$, is a maximal order in $\mathbb{Q}[A_4]$ whose image under ρ is $M_3(\mathbb{Z})$.

Proposition 1.1. *Every rank one projective Λ -module is free.*

Proof. We use A. Fröhlich’s formula giving the projective class-group $\text{Cl}(\Lambda)$ of Λ ([6], Th. 49–23): $\text{Cl}(\Lambda) \simeq \frac{J(\mathbb{Q})}{\mathbb{Q}^* \text{Det}(J(\Lambda))}$, where $J(\mathbb{Q})$ denotes the idele group of \mathbb{Q} , \mathbb{Q}^* the image by the diagonal imbedding of the rationals, and $\text{Det}(J(\Lambda))$ denotes the group of reduced norms of Λ -ideles. We know that the reduced norm is locally surjective over \mathbb{Z}_p^* at p for $p \neq 2$ ([6] Th. 51–22). Locally at 2: Λ_2^* contains the elements uI_3 with $u \in \mathbb{Z}_2^*$, hence we find $\mathbb{Z}_2^* \supset \text{Det}(\Lambda_2^*) \supset (\mathbb{Z}_2^*)^3 = \mathbb{Z}_2^*$. So $\text{Cl}(\Lambda) \simeq \frac{J(\mathbb{Q})}{\mathbb{Q}^* J(\mathbb{Z})}$ is isomorphic to $\text{Cl}(\mathbb{Z}) = \{1\}$. \square

To compute $\text{Cl}(\mathbb{Z}[A_4])$ we use the order 3 quotient from A_4/H and the image Λ of $\mathbb{Z}[A_4]$ by ρ . We obtain a fiber product:

$$\begin{array}{ccc} \mathbb{Z}[A_4] & \longrightarrow & \Lambda \\ \downarrow & & \downarrow \\ \mathbb{Z}[C_3] & \longrightarrow & \mathbb{Z}/4\mathbb{Z}[C_3] \end{array}$$

It is well known ([10]) that $\text{Cl}(\mathbb{Z}[C_3]) = 1$. The projective class-group is then isomorphic to $\text{im}((\mathbb{Z}[C_3])^*) \setminus (\mathbb{Z}/4\mathbb{Z})[C_3]^* / \text{im}(\Lambda^*)$ (cf. [11]).

Lemma 1.2. *The morphism from Λ to $\mathbb{Z}/4\mathbb{Z}[C_3]$ gives a surjection from Λ^* to $(\mathbb{Z}/4\mathbb{Z})[C_3]^*$.*

Proof. We have a surjective morphism from $(\mathbb{Z}/4\mathbb{Z}[C_3])^*$ to $(\mathbb{Z}/2\mathbb{Z}[C_3])^*$ whose kernel is $1 + 2\mathbb{Z}/4\mathbb{Z}[C_3]$. The elements of $(\mathbb{Z}/4\mathbb{Z}[C_3])^*$ are the images of $\pm\nu^i$, $\nu^i(e + \nu + \sigma\nu)$, $\nu^i(e + \nu^2 + \sigma\nu^2)$ invertible in Λ as is easily verified. \square

Thus we have obtained a new proof of Reiner–Ullom result [11]:

Theorem 1.3. *Every finitely generated projective $\mathbb{Z}[A_4]$ -module is free.*

Corollary 1.4. *Let $\mathbb{Q} \subset N$ be a tame Galois extension with group A_4 . Then the ring of integers \mathcal{O}_N has a normal integral basis.*

2. LAGRANGE RESOLVENTS

From now on, we restrict ourselves to the extensions $\mathbb{Q} \subset N$ tamely ramified.

Let $\mathbb{Q} \subset N$ be a Galois extension with group A_4 . From Section 1, the field N contains the cyclic cubic field k of invariants under H . Inside N , there are four quartic conjugate subfields. Denote K the invariant field by $\{e, \nu, \nu^2\}$. The other quartic fields are K_σ , invariant under $\sigma\langle\nu\rangle\sigma$ and, similarly the fields $K_\tau, K_{\sigma\tau}$. The extension $k \subset N$ is biquadratic bicyclic, and the quadratic extensions of k in N are $k_\sigma, k_\tau, k_{\sigma\tau}$ respectively invariant by $\sigma, \tau, \sigma\tau$. Apart from \mathbb{Q} and N these are the only subfields of N .

The ring of integers \mathcal{O}_N is a free rank one $\mathbb{Z}[A_4]$ -module. The trace $\text{Tr}_{N/k}$ is a surjective map over the free $\mathbb{Z}[C_3]$ -module \mathcal{O}_k . We know how to construct a normal integral basis, either because k is a subfield of the cyclotomic field, with same conductor, or by using Châtelet’s technics [2]. The quotient $\mathcal{O}_N/\mathcal{O}_k$ is isomorphic to $\Lambda \otimes_{\mathbb{Z}[A_4]} \mathcal{O}_N$. It is Λ -projective, and therefore it is Λ -free. Given the fiber product

$$(2.1) \quad \begin{array}{ccc} \mathcal{O}_N & \longrightarrow & \mathcal{O}_N/\mathcal{O}_k \\ \downarrow \text{Tr}_{N/k} & & \downarrow \\ \mathcal{O}_k & \longrightarrow & \mathcal{O}_k/4\mathcal{O}_k \end{array}$$

let γ be a $\mathbb{Z}[C_3]$ -basis of \mathcal{O}_k and let x be an element in \mathcal{O}_N whose image in $\mathcal{O}_N/\mathcal{O}_k$ is a Λ -basis. We can multiply x by λ of $\mathbb{Z}[A_4]$ whose class is in Λ^* in such a way that γ and λx have the same image in $\mathcal{O}_k/4\mathcal{O}_k$. Then there exists $c \in \mathcal{O}_k$ such that $\text{Tr}_{N/k}(\lambda x) = \gamma + 4c$. It follows that $\theta = \lambda x - c$ is a $\mathbb{Z}[A_4]$ -basis for \mathcal{O}_N . To construct a normal integral basis of \mathcal{O}_N we are left with constructing $x \in \mathcal{O}_N$ whose image in $\mathcal{O}_N/\mathcal{O}_k$ is a Λ -basis.

Let \hat{H} be the dual group of H . The elements of \hat{H} are specified by their values:

	e	σ	τ	$\sigma\tau$
χ_0	1	1	1	1
χ_σ	1	1	-1	-1
χ_τ	1	-1	1	-1
$\chi_{\sigma\tau}$	1	-1	-1	1

For $\theta \in N$ and $\chi \in \hat{H}$ we define the Lagrange resolvent $\langle \theta, \chi \rangle$ of θ and χ by

$$\langle \theta, \chi \rangle = \sum_{h \in H} \chi(h^{-1})h(\theta) = \theta + \chi(\sigma)\sigma(\theta) + \chi(\tau)\tau(\theta) + \chi(\sigma\tau)\sigma\tau(\theta),$$

i.e.,

$$\begin{aligned} \langle \theta, \chi_0 \rangle &= \text{Tr}_{N/k}(\theta), & \langle \theta, \chi_\sigma \rangle &= \theta + \sigma(\theta) - \tau(\theta) - \sigma\tau(\theta), \\ \langle \theta, \chi_\tau \rangle &= \theta - \sigma(\theta) + \tau(\theta) - \sigma\tau(\theta), & \langle \theta, \chi_{\sigma\tau} \rangle &= \theta - \sigma(\theta) - \tau(\theta) + \sigma\tau(\theta). \end{aligned}$$

We list some straightforward properties of Lagrange resolvents below (further applications can be found in [9]).

Properties.

1. $4\theta = \langle \theta, \chi_0 \rangle + \langle \theta, \chi_\sigma \rangle + \langle \theta, \chi_\tau \rangle + \langle \theta, \chi_{\sigma\tau} \rangle$, so if $\langle \theta, \chi_\sigma \rangle = \langle \theta, \chi_\tau \rangle = \langle \theta, \chi_{\sigma\tau} \rangle = 0$, then θ belongs to k and conversely.

2. For $h \in H$, we have $\langle \theta, \chi \rangle^h := h(\langle \theta, \chi \rangle) = \chi(h)\langle \theta, \chi \rangle$ which gives: for every h in $H \setminus \{e\}$ the number $\langle \theta, \chi_h \rangle$ is in k_h and $\alpha_h = \langle \theta, \chi_h \rangle^2$ belongs to k .

3. If θ is such that $\langle \theta, \chi_h \rangle \neq 0$ for $h \in \{\sigma, \tau, \sigma\tau\}$, then for $\theta' \in N$ the quotient $\frac{\langle \theta', \chi_h \rangle}{\langle \theta, \chi_h \rangle}$ belongs to k . Replacing θ by θ' corresponds to multiplying α_h by a square of k^* .

4. The image of a Lagrange resolvent under ν is determined by

$$\begin{aligned} \langle \theta, \chi \rangle^\nu &:= \nu(\langle \theta, \chi \rangle) = \nu(\theta) + \nu(\sigma(\theta))\chi(\sigma) + \nu(\tau(\theta))\chi(\tau) + \nu(\sigma\tau(\theta))\chi(\sigma\tau) \\ &= \nu(\theta) + \tau(\nu(\theta))\chi(\sigma) + \sigma\tau(\nu(\theta))\chi(\tau) + \sigma(\nu(\theta))\chi(\sigma\tau). \end{aligned}$$

We deduce that

$$\begin{aligned} \langle \theta, \chi_0 \rangle^\nu &= \langle \nu(\theta), \chi_0 \rangle, & \langle \theta, \chi_\sigma \rangle^\nu &= \langle \nu(\theta), \chi_\tau \rangle, \\ \langle \theta, \chi_\tau \rangle^\nu &= \langle \nu(\theta), \chi_{\sigma\tau} \rangle, & \langle \theta, \chi_{\sigma\tau} \rangle^\nu &= \langle \nu(\theta), \chi_\sigma \rangle. \end{aligned}$$

For $\theta \in K$, these formulas become

$$\langle \theta, \chi_\sigma \rangle^\nu = \langle \theta, \chi_\tau \rangle, \quad \langle \theta, \chi_\tau \rangle^\nu = \langle \theta, \chi_{\sigma\tau} \rangle, \quad \langle \theta, \chi_{\sigma\tau} \rangle^\nu = \langle \theta, \chi_\sigma \rangle$$

Then we deduce:

Corollary 2.1. For $\theta \in K$, the $\langle \theta, \chi_h \rangle^2$ with h in $\{\sigma, \tau, \sigma\tau\}$ are conjugate in k .

Remark 2.2. If $\theta \in K \setminus \mathbb{Q}$ the elements $\langle \theta, \chi_h \rangle^2$ ($h \in \{\sigma, \tau, \sigma\tau\}$) are pairwise distinct in k . Otherwise they would be equal, as they are conjugate and, therefore they would belong to \mathbb{Q} . The same is true for the $\langle \theta, \chi_h \rangle$, as N contains no quadratic extension of \mathbb{Q} .

Corollary 2.3. For $\theta \in K \setminus \mathbb{Q}$, the product $\langle \theta, \chi_\sigma \rangle \langle \theta, \chi_\tau \rangle \langle \theta, \chi_{\sigma\tau} \rangle$ belongs to \mathbb{Q}^* .

Proof. The three numbers are conjugate under ν ; then ν fixes their product. By property 2, this product is also fixed by H . □

Remark 2.4. Under the same hypothesis the element $\langle \theta, \chi_h \rangle$ does not belong to k .

We mention, without proof, the following classical result.

Theorem 2.5. Assume that α is an element of $k^* \setminus k^{*2}$ whose norm over \mathbb{Q} is in \mathbb{Q}^{*2} and that s is an element in \mathbb{Q} . Denote $\alpha_1 = \alpha$, $\alpha_2 = \nu(\alpha)$, $\alpha_3 = \nu^2(\alpha)$. Then there exists a quartic extension $\mathbb{Q} \subset K$ such that the Galois closure of K has group A_4 , contains k , and there exists an element $\theta \in K$ such that $\text{Tr}_{K/\mathbb{Q}}(\theta) = s$, $\langle \theta, \chi_\sigma \rangle^2 = \alpha_1$, $\langle \theta, \chi_\tau \rangle^2 = \alpha_2$, $\langle \theta, \chi_{\sigma\tau} \rangle^2 = \alpha_3$.

Suppose α_1 is a root of $X^3 + aX^2 + bX - q^2 \in \mathbb{Q}[X]$. Then $z = 4\theta - s$ (where $\theta = \frac{1}{4}(s + \sqrt{\alpha_1} + \sqrt{\alpha_2} + \sqrt{\alpha_3})$) is a root of

$$\begin{aligned} & (X - z)(X - \sigma(z))(X - \tau(z))(X - \sigma\tau(z)) \\ &= (X - \sqrt{\alpha_1} - \sqrt{\alpha_2} - \sqrt{\alpha_3})(X - \sqrt{\alpha_1} + \sqrt{\alpha_2} + \sqrt{\alpha_3}) \\ &\quad \times (X + \sqrt{\alpha_1} - \sqrt{\alpha_2} + \sqrt{\alpha_3})(X + \sqrt{\alpha_1} + \sqrt{\alpha_2} - \sqrt{\alpha_3}) \\ &= (X^2 - 2\sqrt{\alpha_1}X + \alpha_1 - (\sqrt{\alpha_2} + \sqrt{\alpha_3})^2)(X^2 + 2\sqrt{\alpha_1}X + \alpha_1 - (\sqrt{\alpha_2} - \sqrt{\alpha_3})^2) \\ &= (X^2 - 2\sqrt{\alpha_1}X + \alpha_1 - \alpha_2 - \alpha_3 - 2\sqrt{\alpha_2}\sqrt{\alpha_3}) \\ &\quad \times (X^2 + 2\sqrt{\alpha_1}X + \alpha_1 - \alpha_2 - \alpha_3 + 2\sqrt{\alpha_2}\sqrt{\alpha_3}) \\ &= (X^2 + \alpha_1 - \alpha_2 - \alpha_3)^2 - 4(\sqrt{\alpha_1}X + \sqrt{\alpha_2}\sqrt{\alpha_3})^2 \\ &= X^4 + 2aX^2 - 8qX + a^2 - 4b. \end{aligned}$$

Remark 2.6. Given a fractional ideal \mathfrak{A} , we write it $\mathfrak{A} = \mathfrak{R}^2\mathfrak{J}_1$, with \mathfrak{R} a fractional ideal and \mathfrak{J}_1 a product of prime ideals pairwise distinct. Apply this decomposition to (α_1) ; as $N_{k/\mathbb{Q}}(\alpha_1)$ is a square, then so is $N_{k/\mathbb{Q}}(\mathfrak{J}_1)$. We can write $\mathfrak{J}_1 = \mathfrak{J}\nu(\mathfrak{J})$, where \mathfrak{J} is a product of pairwise distinct primes ideals in \mathcal{O}_k , split in $\mathbb{Q} \subset k$.

By property 3 we can assume that \mathfrak{R} is prime to a given ideal, in particular to $2\mathcal{O}_{\mathbb{Q}}$.

3. RINGS OF INTEGERS

We first state a property that actually remains true even if no tameness is assumed.

Theorem 3.1. *The ring \mathcal{O}_N is a free \mathcal{O}_k -module of rank 4.*

Proof. The discriminant of the extension $k \subset N$ is the product of the conductors of the extensions $k \subset k_h$. It is the square of a principal ideal in k . Let $\theta \in K$ whose conjugates give a k -normal basis of N (that is possible, see [9] where the classical proof is adapted. Another proof in this framework is in Section 5 below). Note that $\theta_0 = \theta$, $\theta_1 = \sigma(\theta)$, $\theta_2 = \tau(\theta)$, $\theta_3 = \sigma\tau(\theta)$. The discriminant of the free \mathcal{O}_k -lattice with this basis is

$$\begin{vmatrix} \theta_0 & \theta_1 & \theta_2 & \theta_3 \\ \theta_1 & \theta_0 & \theta_3 & \theta_2 \\ \theta_2 & \theta_3 & \theta_0 & \theta_1 \\ \theta_3 & \theta_2 & \theta_1 & \theta_0 \end{vmatrix}^2.$$

We compute this determinant classically:

$$\begin{aligned} & \begin{vmatrix} \theta_0 & \theta_1 & \theta_2 & \theta_3 \\ \theta_1 & \theta_0 & \theta_3 & \theta_2 \\ \theta_2 & \theta_3 & \theta_0 & \theta_1 \\ \theta_3 & \theta_2 & \theta_1 & \theta_0 \end{vmatrix} \times \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{vmatrix} \\ &= \begin{vmatrix} \langle \theta_0, \chi_0 \rangle & \langle \theta_0, \chi_\sigma \rangle & \langle \theta_0, \chi_\tau \rangle & \langle \theta_0, \chi_{\sigma\tau} \rangle \\ \langle \theta_1, \chi_0 \rangle & \langle \theta_1, \chi_\sigma \rangle & \langle \theta_1, \chi_\tau \rangle & \langle \theta_1, \chi_{\sigma\tau} \rangle \\ \langle \theta_2, \chi_0 \rangle & \langle \theta_2, \chi_\sigma \rangle & \langle \theta_2, \chi_\tau \rangle & \langle \theta_2, \chi_{\sigma\tau} \rangle \\ \langle \theta_3, \chi_0 \rangle & \langle \theta_3, \chi_\sigma \rangle & \langle \theta_3, \chi_\tau \rangle & \langle \theta_3, \chi_{\sigma\tau} \rangle \end{vmatrix}. \end{aligned}$$

Then we get $(\langle \theta_0, \chi_0 \rangle \langle \theta_0, \chi_\sigma \rangle \langle \theta_0, \chi_\tau \rangle \langle \theta_0, \chi_{\sigma\tau} \rangle)^2$ using properties of Lagrange resolvents. It is the square of an element in \mathbb{Q}^* , its quotient by the discriminant of the

extension $k \subset N$ is the square of a principal ideal in k , and the Artin criterion [1] ensures the existence of the relative basis. \square

Keep θ_0 as in the beginning of this section and $h \in \{\sigma, \tau, \sigma\tau\}$. Pick $\theta \in N$, such that $\langle \theta, \chi_h \rangle \neq 0$. Then the quotients $\frac{\langle \theta, \chi_h \rangle}{\langle \theta_0, \chi_h \rangle}$ belong to k . If we write $\alpha_h = \langle \theta, \chi_h \rangle^2 \in k$, we have $(\alpha_h) = \left(\frac{\langle \theta, \chi_h \rangle}{\langle \theta_0, \chi_h \rangle} \mathfrak{R}(\chi_h) \right)^2 \mathfrak{J}(\chi_h) \nu(\mathfrak{J}(\chi_h))$. Then the ideal $\mathfrak{J}(\chi_h)$ and the class of $\mathfrak{R}(\chi_h)$ are invariants connected to $\mathbb{Q} \subset N$.

We construct three \mathbb{Q} -linear maps from N to k by $f_h(\theta) = \frac{\langle \theta, \chi_h \rangle}{\langle \theta_0, \chi_h \rangle}$ for $h = \sigma, \tau, \sigma\tau$. We gather them as $f(\theta) = (f_\sigma(\theta), f_\tau(\theta), f_{\sigma\tau}(\theta))$, and obtain a \mathbb{Q} -linear map f from N to k^3 . Each of the f_h connects \mathcal{O}_K and $\mathfrak{R}(\chi_h)^{-1}$, and the map f is the key ingredient for the Galois structure of \mathcal{O}_N .

Proposition 3.2. *When restricted to K , the maps f_h are surjective with kernel \mathbb{Q} .*

Proof. If $\theta \in \ker f_h$, we have $\langle \theta, \chi_h \rangle = 0$, hence $\nu(\langle \theta, \chi_h \rangle) = \langle \theta, \chi_{h'} \rangle$ and $\nu^2(\langle \theta, \chi_h \rangle) = \langle \theta, \chi_{h''} \rangle$. Property 1 shows that $4\theta = \langle \theta, \chi_0 \rangle = \text{Tr}_{K/\mathbb{Q}}(\theta) \in \mathbb{Q}$. The kernel of f_h is included in \mathbb{Q} . The converse is immediate. The surjectivity of f_h follows from a consideration of the rank. \square

Proposition 3.3. *The map f is surjective with kernel k .*

Proof. It suffices to show the assertion regarding the kernel. By Property 1 in section 2 we have $4\theta = \langle \theta, \chi_0 \rangle + \langle \theta, \chi_\sigma \rangle + \langle \theta, \chi_\tau \rangle + \langle \theta, \chi_{\sigma\tau} \rangle$. As $\theta \in \ker(f)$, we get $4\theta = \langle \theta, \chi_0 \rangle \in k$. \square

Remark 3.4. It is important to observe that when we restrict f to \mathcal{O}_N , its image is just $\mathcal{O}_N/\mathcal{O}_k$, one of the terms of (2.1).

Proposition 3.5. *One has the inclusion $f_h(\mathcal{O}_N) \subset \mathfrak{R}(\chi_h)^{-1}$.*

Proof. Let θ in \mathcal{O}_N ; the number $\langle \theta, \chi_h \rangle^2$ is equal to $f_h(\theta)^2 \langle \theta_0, \chi_h \rangle^2$. Using remark 2.6, we write $(\langle \theta, \chi_h \rangle^2) = (f_h(\theta) \mathfrak{R}(\chi_h))^2 \mathfrak{J}(\chi_h) \nu(\mathfrak{J}(\chi_h))$. As θ is an integer, so is $\langle \theta, \chi_h \rangle^2$. But $\mathfrak{J}(\chi_h) \nu(\mathfrak{J}(\chi_h))$ is an integer ideal that is squarefree. It follows that $f_h(\theta) \mathfrak{R}(\chi_h)$ is an integer ideal, hence $f_h(\theta) \in \mathfrak{R}(\chi_h)^{-1}$ as expected. \square

Theorem 3.6. *One has $4\mathfrak{R}(\chi_h)^{-1} \subset f_h(\mathcal{O}_K) \subset \mathfrak{R}(\chi_h)^{-1}$.*

Proof. The right inclusion is true for every integer in N , hence in particular for those in K . For the left inclusion, let $\lambda_h \in 4\mathfrak{R}(\chi_h)^{-1}$. We set $\lambda_{h'} = \nu(\lambda_h)$, $\lambda_{h''} = \nu^2(\lambda_h)$ and we define

$$\theta = \frac{1}{4}[\lambda_h \langle \theta_0, \chi_h \rangle + \lambda_{h'} \langle \theta_0, \chi_{h'} \rangle + \lambda_{h''} \langle \theta_0, \chi_{h''} \rangle].$$

The action of ν on resolvents shows that θ is in K . As $\frac{\lambda_h}{4}$ is contained in $\mathfrak{R}(\chi_h)^{-1}$, the number $(\frac{\lambda_h}{4})^2 \langle \theta_0, \chi_h \rangle^2$ is in \mathcal{O}_k . Then $\frac{\lambda_h}{4} \langle \theta_0, \chi_h \rangle$ is an integer. The same is true for its conjugates and their sum θ . Orthogonality relations between characters implies $f_h(\theta) = \lambda_h$ and therefore $4\mathfrak{R}(\chi_h)^{-1} \subset f_h(\mathcal{O}_K)$. \square

Corollary 3.7. *Let x_1, x_2, x_3 be a \mathbb{Z} -basis of $f_h(\mathcal{O}_K)$, and let $\theta_1, \theta_2, \theta_3 \in \mathcal{O}_K$ such that $f_h(\theta_i) = x_i$. Then $\{1, \theta_1, \theta_2, \theta_3\}$ is a \mathbb{Z} -basis of \mathcal{O}_K .*

Proof. As $f_h(\mathcal{O}_K)$ is \mathbb{Z} -free, the exact sequence

$$0 \rightarrow \mathbb{Z} \rightarrow \mathcal{O}_K \rightarrow f_h(\mathcal{O}_K) \rightarrow 0$$

is split. Let g be a section and $\theta'_i = g(x_i)$. Then $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\theta'_1 \oplus \mathbb{Z}\theta'_2 \oplus \mathbb{Z}\theta'_3$. As θ_i and θ'_i are integers and $f_h(\theta_i - \theta'_i) = 0$, the differences $\theta_i - \theta'_i$ belong to \mathbb{Z} . \square

We now focus on f and \mathcal{O}_N . Set $M = \mathfrak{R}(\chi_\sigma)^{-1} \oplus \mathfrak{R}(\chi_\tau)^{-1} \oplus \mathfrak{R}(\chi_{\sigma\tau})^{-1}$.

Theorem 3.8. *We have $4M \subset f(\mathcal{O}_N) \subset M$.*

Proof. Analogous to the proof of Theorem 3.6, except that we use the relation

$$\theta = \frac{1}{4}[\lambda_\sigma \langle \theta_0, \chi_\sigma \rangle + \lambda_\tau \langle \theta_0, \chi_\tau \rangle + \lambda_{\sigma\tau} \langle \theta_0, \chi_{\sigma\tau} \rangle]$$

for a triple $\{\lambda_\sigma, \lambda_\tau, \lambda_{\sigma\tau}\} \in M$. \square

4. LOCALIZATION. INDEX COMPUTATIONS

This section is devoted to the structure of $f_\sigma(\mathcal{O}_K)/4\mathfrak{R}(\chi_\sigma)^{-1}$, $f(\mathcal{O}_N)/4M$ and $f(\mathcal{O}_N)$ as abelian groups. These quotients are finite 2-groups. We localize at 2 to study their structure. Denote by $A_{(2)}$ the localisation of a module A . The lattices $\mathfrak{R}(\chi_h)^{-1}$ and M are defined up to multiplication by a scalar. Localization allows us to choose θ_0 convenient for computations. Tameness implies the existence of normal integral basis of $\mathcal{O}_{k_h, (2)}$ as $\mathcal{O}_{k, (2)}[C_2]$ -modules and of $\mathcal{O}_{N, (2)}$ as $\mathcal{O}_{k, (2)}[H]$ - and $\mathbb{Z}_{(2)}[A_4]$ -module. We first construct these bases.

There exists $\alpha \in \mathcal{O}_k$ such that N is equal to $k(\sqrt{\alpha}, \sqrt{\nu(\alpha)})$. As the extension is tame, we can suppose $\alpha \in \mathcal{O}_{k, (2)}^*$ so $\alpha\nu(\alpha)\nu^2(\alpha) \in \mathbb{Z}_{(2)}^{*2}$. Tameness implies the existence for each prime \mathfrak{p} in $\mathcal{O}_{k, (2)}$ of $\xi_{\mathfrak{p}}$ such that $\alpha \equiv \xi_{\mathfrak{p}}^2 \pmod{(\mathfrak{p}^2)}$; by the Chinese Remainder Theorem, we can get the same ξ for all the \mathfrak{p} . As α is a unit, the same is true for ξ . We can change α by $\alpha\xi^{-2}$ and suppose $\alpha \equiv 1 \pmod{(4)}$.

It is now clear that, for $k_\sigma = k(\sqrt{\alpha})$, the ring of integers $\mathcal{O}_{k_\sigma, (2)}$ has a $\mathcal{O}_{k, (2)}$ normal integral basis generated by $\frac{1+\sqrt{\alpha}}{2}$. Acting on the latter by ν and ν^2 we get $\frac{1+\sqrt{\nu(\alpha)}}{2}$ (resp. $\frac{1+\sqrt{\nu^2(\alpha)}}{2}$) as normal integral basis for $\mathcal{O}_{k_\tau, (2)}$ (resp. $\mathcal{O}_{k_{\sigma\tau}, (2)}$).

We construct $t = \frac{1+\sqrt{\alpha}+\sqrt{\nu(\alpha)}+\sqrt{\nu^2(\alpha)}}{4}$ and its conjugates over k :

$$\begin{aligned} \sigma(t) &= \frac{1 + \sqrt{\alpha} - \sqrt{\nu(\alpha)} - \sqrt{\nu^2(\alpha)}}{4}, & \tau(t) &= \frac{1 - \sqrt{\alpha} + \sqrt{\nu(\alpha)} - \sqrt{\nu^2(\alpha)}}{4}, \\ \sigma\tau(t) &= \frac{1 - \sqrt{\alpha} - \sqrt{\nu(\alpha)} + \sqrt{\nu^2(\alpha)}}{4}, \end{aligned}$$

as $t \in \mathcal{O}_{K, (2)}$. The discriminant of the $\mathcal{O}_{k, (2)}$ -lattice generated by these elements can be computed as in Theorem 3.1. We get $\alpha\nu(\alpha)\nu^2(\alpha)$ which is a unit in $\mathcal{O}_{k, (2)}$. So t generates an $\mathcal{O}_{k, (2)}[H]$ normal integral basis for $\mathcal{O}_{N, (2)}$.

Let $\gamma \in \mathcal{O}_k$, with trace 1 over \mathbb{Q} , generating a normal integral basis for \mathcal{O}_k , hence a local normal integral basis for $\mathcal{O}_{k, (2)}$. Consider γt . On the one hand, as $t \in K$, it is invariant by ν . On the other hand, γ is fixed by H so $\nu^i h(\gamma t) = \nu^i(\gamma)h(t)$. It follows immediately that γt with its conjugates gives a $\mathbb{Z}_{(2)}$ normal basis of $\mathcal{O}_{N, (2)}$. One gets a $\mathbb{Z}_{(2)}$ -basis for $\mathcal{O}_{K, (2)}$: $\{\text{Tr}_{N/K}(\gamma t) = t, \text{Tr}_{N/K}(\gamma\sigma(t)), \text{Tr}_{N/K}(\gamma\tau(t)), 1\}$, this last element in place of $\text{Tr}_{N/K}(\sigma\tau(\gamma t))$ as $\text{Tr}_{N/K}(\gamma t + \sigma(\gamma t) + \tau(t) + \sigma\tau(\gamma t)) = \text{Tr}_{N/\mathbb{Q}}(\gamma t) = 1$.

Explicitly,

$$\begin{aligned} \mathrm{Tr}_{N/K}(\gamma t) &= t = \frac{1 + \sqrt{\alpha} + \sqrt{\nu(\alpha)} + \sqrt{\nu^2(\alpha)}}{4}, \\ \mathrm{Tr}_{N/K}(\gamma\sigma(t))\mathrm{Tr}_{N/K} &\left(\gamma \frac{1 + \sqrt{\alpha} - \sqrt{\nu(\alpha)} - \sqrt{\nu^2(\alpha)}}{4} \right) \\ &= \gamma \frac{1 + \sqrt{\alpha} - \sqrt{\nu(\alpha)} - \sqrt{\nu^2(\alpha)}}{4} + \nu(\gamma) \frac{1 + \sqrt{\nu(\alpha)} - \sqrt{\nu^2(\alpha)} - \sqrt{\alpha}}{4} \\ &\quad + \nu^2(\gamma) \frac{1 + \sqrt{\nu^2(\alpha)} - \sqrt{\alpha} - \sqrt{\nu(\alpha)}}{4} \\ &= \frac{1}{4} + \sqrt{\alpha} \frac{\gamma - \nu(\gamma) - \nu^2(\gamma)}{4} + \sqrt{\nu(\alpha)} \frac{-\gamma + \nu(\gamma) - \nu^2(\gamma)}{4} + \sqrt{\nu^2(\alpha)} \frac{-\gamma - \nu(\gamma) + \nu^2(\gamma)}{4}, \\ \mathrm{Tr}_{N/K}(\gamma\tau(t)) &= \mathrm{Tr}_{N/K} \left(\gamma \frac{1 - \sqrt{\alpha} + \sqrt{\nu(\alpha)} - \sqrt{\nu^2(\alpha)}}{4} \right) \\ &= \gamma \frac{1 - \sqrt{\alpha} + \sqrt{\nu(\alpha)} - \sqrt{\nu^2(\alpha)}}{4} + \nu(\gamma) \frac{1 - \sqrt{\nu(\alpha)} + \sqrt{\nu^2(\alpha)} - \sqrt{\alpha}}{4} \\ &\quad + \nu^2(\gamma) \frac{1 - \sqrt{\nu^2(\alpha)} + \sqrt{\alpha} - \sqrt{\nu(\alpha)}}{4} \\ &= \frac{1}{4} + \sqrt{\alpha} \frac{-\gamma - \nu(\gamma) + \nu^2(\gamma)}{4} + \sqrt{\nu(\alpha)} \frac{\gamma - \nu(\gamma) - \nu^2(\gamma)}{4} + \sqrt{\nu^2(\alpha)} \frac{-\gamma + \nu(\gamma) + \nu^2(\gamma)}{4}. \end{aligned}$$

To determine the index $f_\sigma(\mathcal{O}_K)$ in $\mathfrak{A}(\chi_\sigma)^{-1}$, choose $\theta_0 = t$ and compute the image $f_\sigma(\mathcal{O}_{K,(2)})$.

The Lagrange resolvents are

$$\langle t, \chi_\sigma \rangle = \sqrt{\alpha}.$$

The choice of θ_0 implies $\mathfrak{A}(\chi_\sigma)^{-1} = \mathcal{O}_{k,(2)}$. Also,

$$\begin{aligned} \langle \mathrm{Tr}_{N/K}(\gamma\sigma(t)), \chi_\sigma \rangle &= (2\gamma - 1)\sqrt{\alpha}, \\ \langle \mathrm{Tr}_{N/K}(\gamma\tau(t)), \chi_\sigma \rangle &= (2\nu^2(\gamma) - 1)\sqrt{\alpha}. \end{aligned}$$

Finally:

Theorem 4.1. *The image $f_\sigma(\mathcal{O}_{K,(2)})$ is generated by $f_\sigma(\mathrm{Tr}_{N/K}(\gamma\sigma(t))) = 2\gamma - 1$, $f_\sigma(\mathrm{Tr}_{N/K}(\gamma\tau(t))) = 2\nu^2(\gamma) - 1$ and 1. The quotient $\mathfrak{A}(\chi_\sigma)^{-1}/f_\sigma(\mathcal{O}_K)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

In the same way (or by conjugation) we have

$$\begin{aligned} \langle t, \chi_\tau \rangle &= \sqrt{\nu(\alpha)}, \\ \langle \mathrm{Tr}_{N/K}(\gamma\sigma(t)), \chi_\tau \rangle &= (2\nu(\gamma) - 1)\sqrt{\nu(\alpha)}, \\ \langle \mathrm{Tr}_{N/K}(\gamma\tau(t)), \chi_\tau \rangle &= (2\gamma - 1)\sqrt{\nu(\alpha)}, \end{aligned}$$

hence $f_\tau(t) = 1$, $f_\tau(\mathrm{Tr}_{N/K}(\gamma\sigma(t))) = 2\nu(\gamma) - 1$, $f_\tau(\mathrm{Tr}_{N/K}(\gamma\tau(t))) = 2\gamma - 1$, and

$$\begin{aligned} \langle t, \chi_{\sigma\tau} \rangle &= \sqrt{\nu^2(\alpha)}, \\ \langle \mathrm{Tr}_{N/K}(\gamma\sigma(t)), \chi_{\sigma\tau} \rangle &= (2\nu^2(\gamma) - 1)\sqrt{\nu^2(\alpha)}, \\ \langle \mathrm{Tr}_{N/K}(\gamma\tau(t)), \chi_{\sigma\tau} \rangle &= (2\nu(\gamma) - 1)\sqrt{\nu^2(\alpha)}. \end{aligned}$$

Finally we find $f_{\sigma\tau}(t) = 1$, $f_{\sigma\tau}(\text{Tr}_{N/K}(\gamma\sigma(t))) = 2\nu^2(\gamma) - 1$, $f_{\sigma\tau}(\text{Tr}_{N/K}(\gamma\tau(t))) = 2\nu(\gamma) - 1$. The quotients $\mathfrak{R}(\chi_\tau)^{-1}/f_\tau(\mathcal{O}_K)$ and $\mathfrak{R}(\chi_{\sigma\tau})^{-1}/f_\tau(\mathcal{O}_K)$ are isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Now we determine $f(\mathcal{O}_{N,(2)}) \simeq \mathcal{O}_{N,(2)}/\mathcal{O}_{k,(2)}$. We use the local normal integral basis in N/k , generated by t and its conjugates. Each element in $\mathcal{O}_{N,(2)}$ is uniquely written as $\sum_{h \in H} x_h h(t)$, $x_h \in \mathcal{O}_{k,(2)}$. That gives for Lagrange resolvents:

$$\begin{aligned} \langle x, \chi_\sigma \rangle &= \sum_{h \in H} x_h \langle h(t), \chi_\sigma \rangle = \sum_{h \in H} x_h \chi_\sigma(h) \langle t, \chi_\sigma \rangle, \\ \langle x, \chi_\tau \rangle &= \sum_{h \in H} x_h \langle h(t), \chi_\tau \rangle = \sum_{h \in H} x_h \chi_\tau(h) \langle t, \chi_\tau \rangle, \\ \langle x, \chi_{\sigma\tau} \rangle &= \sum_{h \in H} x_h \langle h(t), \chi_{\sigma\tau} \rangle = \sum_{h \in H} x_h \chi_{\sigma\tau}(h) \langle t, \chi_{\sigma\tau} \rangle. \end{aligned}$$

It follows that:

Proposition 4.2. *The image $f(\mathcal{O}_{N,(2)})$ is the set of all triples*

$$(x_e + x_\sigma - x_\tau - x_{\sigma\tau}, x_e - x_\sigma + x_\tau - x_{\sigma\tau}, x_e - x_\sigma - x_\tau + x_{\sigma\tau}),$$

with $x_e, x_\sigma, x_\tau, x_{\sigma\tau}$ in $\mathcal{O}_{k,(2)}$.

We can now prove

Theorem 4.3. *The image $f(\mathcal{O}_N)$ is the set of all triples*

$$(y_\sigma, y_\tau, y_{\sigma\tau}) \in M = \mathfrak{R}(\chi_\sigma)^{-1} \times \mathfrak{R}(\chi_\tau)^{-1} \times \mathfrak{R}(\chi_{\sigma\tau})^{-1}$$

such that $y_\sigma \equiv y_\tau \equiv y_{\sigma\tau} \pmod{(2)}$. The image $f_\sigma(\mathcal{O}_N)$ equals $\mathfrak{R}(\chi_\sigma)^{-1}$. Similarly for $f_\tau(\mathcal{O}_N)$, $f_{\sigma\tau}(\mathcal{O}_N)$.

Proof. Let

$$\begin{cases} x_e + x_\sigma - x_\tau - x_{\sigma\tau} = y_\sigma, \\ x_e - x_\sigma + x_\tau - x_{\sigma\tau} = y_\tau, \\ x_e - x_\sigma - x_\tau + x_{\sigma\tau} = y_{\sigma\tau}. \end{cases}$$

We have

$$\begin{aligned} 2x_\sigma - 2x_\tau &= y_\sigma - y_\tau, \\ 2x_\sigma - 2x_{\sigma\tau} &= y_\sigma - y_{\sigma\tau}, \end{aligned}$$

and deduce $y_\sigma \equiv y_\tau \equiv y_{\sigma\tau} \pmod{(2)}$.

Conversely, with the latter parity assumption, the elements $x_\sigma - x_\tau = \frac{y_\sigma - y_\tau}{2}$, $x_\sigma - x_{\sigma\tau} = \frac{y_\sigma - y_{\sigma\tau}}{2}$ are integers. Choose for instance x_σ . Then we deduce $x_\tau, x_{\sigma\tau}$, and we find x_e using the first equation. \square

5. AN ALGORITHM

By Remark 2.6 and Proposition 3.2, we can suppose $\mathfrak{R}(\chi_\sigma)^{-1}$ is prime to 2. It suffices to choose θ_0 satisfying the congruence $\theta_0 \equiv t \pmod{4}$.

We construct a convenient \mathbb{Z} -basis of \mathcal{O}_K . In fact $f_\sigma(\mathcal{O}_K)/4f_\sigma(\mathcal{O}_K)$ has for $\mathbb{Z}/4\mathbb{Z}$ -basis on the one hand the images of 1, $2\gamma - 1$, $2\nu^2(\gamma) - 1$ and on the other hand those of $f_\sigma(\theta_1)$, $f_\sigma(\theta_2)$, $f_\sigma(\theta_3)$. So there exists a matrix in $\text{Gl}_3(\mathbb{Z}/4\mathbb{Z})$ which sends the latter on the former. Such a matrix has determinant ± 1 . As there is a surjection from $\text{Sl}_3(\mathbb{Z})$ to $\text{Sl}_3(\mathbb{Z}/4\mathbb{Z})$, there exists a \mathbb{Z} -basis 1, φ , ψ , ρ such that $f_\sigma(\varphi) \equiv 1 \pmod{(4)}$, $f_\sigma(\psi) \equiv 2\gamma - 1 \pmod{(4)}$, $f_\sigma(\rho) \equiv 2\nu^2(\gamma) - 1 \pmod{(4)}$. We choose such a basis.

Remark 5.1. If the ideal $\mathfrak{R}(\chi_\sigma)$ is principal, one can change θ_0 such that $\mathfrak{R}(\chi_\sigma) = \mathcal{O}_k$; then, we can choose φ, ψ, ρ so as to have equalities rather than congruences.

We are now able to construct $x \in \mathcal{O}_N$ whose image in $\mathcal{O}_N/\mathcal{O}_k$ is a Λ -basis.

Consider the triple

$$\left(\frac{\langle \varphi, \chi_\sigma \rangle + \langle \psi, \chi_\sigma \rangle}{2\langle \theta_0, \chi_\sigma \rangle}, \frac{\langle \varphi, \chi_\tau \rangle + \langle \rho, \chi_\tau \rangle}{2\langle \theta_0, \chi_\tau \rangle}, -\frac{\langle \psi, \chi_{\sigma\tau} \rangle + \langle \rho, \chi_{\sigma\tau} \rangle}{2\langle \theta_0, \chi_{\sigma\tau} \rangle} \right).$$

The properties of ϕ, ψ, ρ imply first of all that it belongs to $\mathfrak{R}(\chi_\sigma)^{-1} \times \mathfrak{R}(\chi_\tau)^{-1} \times \mathfrak{R}(\chi_{\sigma\tau})^{-1}$. In addition, each of the components is congruent to $\gamma \pmod 2$, so they are pairwise congruent modulo 2, and we can deduce from the previous theorem:

Corollary 5.2. *There exists $x \in \mathcal{O}_N$ such that*

$$f(x) = \left(\frac{\langle \varphi, \chi_\sigma \rangle + \langle \psi, \chi_\sigma \rangle}{2\langle \theta_0, \chi_\sigma \rangle}, \frac{\langle \varphi, \chi_\tau \rangle + \langle \rho, \chi_\tau \rangle}{2\langle \theta_0, \chi_\tau \rangle}, -\frac{\langle \psi, \chi_{\sigma\tau} \rangle + \langle \rho, \chi_{\sigma\tau} \rangle}{2\langle \theta_0, \chi_{\sigma\tau} \rangle} \right).$$

So, there exists $a \in \mathcal{O}_k$ such that

$$x = \frac{1}{4} \left[a + \frac{\langle \varphi, \chi_\sigma \rangle + \langle \psi, \chi_\sigma \rangle}{2} + \frac{\langle \varphi, \chi_\tau \rangle + \langle \rho, \chi_\tau \rangle}{2} - \frac{\langle \psi, \chi_{\sigma\tau} \rangle + \langle \rho, \chi_{\sigma\tau} \rangle}{2} \right].$$

This a is determined mod 4. The previous congruences implies $a \equiv \gamma \pmod 2$, which leads to a finite number of tries.

Now consider the submodule $\mathbb{Z}[A_4]x$ of \mathcal{O}_N and its images under f_σ and f .

Lemma 5.3. *We have $f_\sigma(\mathbb{Z}[A_4]x) = \mathfrak{R}(\chi_\sigma)^{-1}$.*

Proof. As x is an integer, we have $f_\sigma(\mathbb{Z}[A_4]x) \subset \mathfrak{R}(\chi_\sigma)^{-1}$. By construction

$$f_\sigma(x) = \frac{\langle \varphi, \chi_\sigma \rangle + \langle \psi, \chi_\sigma \rangle}{2\langle \theta_0, \chi_\sigma \rangle},$$

$$f_\sigma(\nu(x)) = -\frac{\langle \psi, \chi_\sigma \rangle + \langle \rho, \chi_\sigma \rangle}{2\langle \theta_0, \chi_\sigma \rangle}, \quad f_\sigma(\nu^2(x)) = \frac{\langle \varphi, \chi_\sigma \rangle + \langle \rho, \chi_\sigma \rangle}{2\langle \theta_0, \chi_\sigma \rangle}$$

from which we deduce $f_\sigma(\mathbb{Z}[A_4]x) \supset \mathbb{Z}f_\sigma(\varphi) + \mathbb{Z}f_\sigma(\psi) + \mathbb{Z}f_\sigma(\rho) = f_\sigma(\mathcal{O}_K)$ and $[f_\sigma(\mathbb{Z}[A_4]x) : f_\sigma(\mathcal{O}_K)] = 4$. Comparing this with Theorem 4.1, we have the expected result. \square

Let \mathcal{M} be the maximal order described in Section 2.

Lemma 5.4. *We have $f(\mathcal{M}x) = \mathfrak{R}(\chi_\sigma)^{-1} \times \mathfrak{R}(\chi_\tau)^{-1} \times \mathfrak{R}(\chi_{\sigma\tau})^{-1}$.*

Proof. First consider $f_\sigma(\mathcal{M}x)$. It is generated by $f_\sigma(\mathbb{Z}[A_4]x)$ and the images by f_σ of $\frac{1}{12}(\sum_{g \in A_4} g)y, \frac{1}{4}(\sum_{h \in H} h)y$ and $(\frac{1+\sigma}{2})y, (\frac{1+\tau}{2})y, (\frac{1+\sigma\tau}{2})y$ with $y \in \mathbb{Z}[A_4]x$. The properties of the map f_σ give $f_\sigma(\mathcal{M}x) = f_\sigma(\mathbb{Z}[A_4]x)\mathfrak{R}(\chi_\sigma)^{-1}$.

As for $f(\mathcal{M}x)$, the properties of the maps f_h show that $f(\mathcal{M}x)$ is equal to $f((\frac{1+\sigma}{2})\mathbb{Z}[A_4]x) + f((\frac{1+\tau}{2})\mathbb{Z}[A_4]x) + f((\frac{1+\sigma\tau}{2})\mathbb{Z}[A_4]x)$. The orthogonality relations imply that $f(\mathcal{M}x)$ is equal to $\mathfrak{R}(\chi_\sigma)^{-1} \times \mathfrak{R}(\chi_\tau)^{-1} \times \mathfrak{R}(\chi_{\sigma\tau})^{-1}$, following the construction of x . \square

Theorem 5.5. *We have $f(\mathbb{Z}[A_4]x) = f(\mathcal{O}_N)$.*

Proof. One knows that

$$\mathfrak{R}(\chi_\sigma)^{-1} \times \mathfrak{R}(\chi_\tau)^{-1} \times \mathfrak{R}(\chi_{\sigma\tau})^{-1} = f(\mathcal{M}x) \supset f(\mathcal{O}_N) \supset f(\mathbb{Z}[A_4]x).$$

The properties of f concerning idempotents show that $[f(\mathcal{M}_x) : f(\mathbb{Z}[A_4]x)] = [M_3(\mathbb{Z}) : \Lambda] = 2^6$. By Theorem 4.3 this is equal to $[\mathfrak{R}(\chi_\sigma)^{-1} \times \mathfrak{R}(\chi_\tau)^{-1} \times \mathfrak{R}(\chi_{\sigma\tau})^{-1} : f(\mathcal{O}_N)]$. This proves the assertion. \square

The image of x in $\mathcal{O}_N/\mathcal{O}_k$ gives a basis of this Λ -module. The construction of the normal integral basis of \mathcal{O}_N is obtained using the fiber product (2.1).

6. A NUMERICAL EXAMPLE

The computations have been performed with the system PARI [8]. We give an example with $h_k \neq 1$ to avoid the simplifications due to $\mathfrak{R}(\chi)$ being principal. The smallest conductor for which there exists a cubic tame extension of \mathbb{Q} with ring of integers not principal is 91. There are two such fields (the construction can be done with the algorithm of [2]); we choose k to be the one where 11 is split. It is generated by a root of $X^3 - X^2 - 30X - 27$. The roots $\{\gamma, \nu(\gamma), \nu^2(\gamma)\}$ of this polynomial give a normal integral basis of \mathcal{O}_k . Another basis is given by $\{1, \gamma, (\gamma^2 - \gamma)/3\}$. Computing norms of elements with small coefficients in this basis shows that $3 + \gamma - \gamma^2$ has norm $27^2 = 729$ and minimal polynomial $X^3 + 51X^2 + 594X - 729$.

The construction of Section 2 gives the irreducible quartic polynomial $X^4 + 102X^2 + 216X + 225$. This polynomial generates a field with discriminant $3^2 7^2 13^2$. Its Galois closure is an extension of k with conductor 3. Among the polynomials generating the same field provided by the fonction *polred* in Pari we choose $P = X^4 - X^3 + 7X^2 + 9X + 24$. Let y be a root of P . The set $\{1, y, \frac{1}{2}(y^2 + y), \frac{1}{4}(y^3 - y)\}$ is a basis of the ring of integers \mathcal{O}_K . With *polroots* we get approximations of its roots and construct Lagrange resolvents for each character of H . We choose for θ_0 the root such that the square of the Lagrange resolvent has minimal polynomial $X^3 + 53X^2 - 1005X - 9801$.

From approximations of $\langle \theta_0, \chi_h \rangle^2$, we get $\langle \theta_0, \chi_\sigma \rangle^2 = -15 - 8\gamma$. The factorization of $\langle \theta_0, \chi_\sigma \rangle^2$ in prime ideals is $(11, -5 + \gamma)^2 (3, -1 + \gamma + (\gamma^2 - \gamma)/3)^3 (3, (\gamma^2 - \gamma)/3)$. We deduce that $\mathfrak{R}(\chi_\sigma)$ is the product

$$\mathfrak{R}(\chi_\sigma)(3, -1 + \gamma + (\gamma^2 - \gamma)/3)(11, -5 + \gamma).$$

The ideal $\mathfrak{R}(\chi_\sigma)^{-1}$ admits the \mathbb{Z} -basis $\{1, \gamma, \frac{5}{11} + \frac{20}{33}\gamma + \frac{1}{33}\frac{\gamma^2 - \gamma}{3}\}$. We can write $\{f_\sigma(\varphi), f_\sigma(\psi), f_\sigma(\rho)\}$ relative to $\{\gamma, \nu(\gamma), \nu^2(\gamma)\}$: $\{\gamma + \nu(\gamma) + \nu^2(\gamma), \frac{18}{11}\gamma + \frac{20}{11}\nu(\gamma) + \frac{4}{3}\nu^2(\gamma), -\frac{18}{11}\gamma - \frac{20}{11}\nu(\gamma) - 2\nu^2(\gamma)\}$. Then we express $\{1, 2\gamma - 1, 2\nu^2(\gamma) - 1\}$ according to $\{f_\sigma(\varphi), f_\sigma(\psi), f_\sigma(\rho)\}$ and get $\{2\gamma - 1 = 19f_\sigma(\varphi) - 3f_\sigma(\psi) + 8f_\sigma(\rho)\}$, $2\nu^2(\gamma) - 1 = -f_\sigma(\varphi) - 3f_\sigma(\psi) - 3f_\sigma(\rho)$. When reduced mod 4, the matrix of these vectors is the image of $\begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ in $\text{Sl}_3(\mathbb{Z})$. We change $\{1, \varphi, \psi, \rho\}$ in \mathcal{O}_K to $\{1, \varphi_1 = \varphi, \psi_1 = \psi - \varphi, \rho_1 = \rho + \psi - \varphi\}$.

We now have a new basis of $f_\sigma(\mathcal{O}_K)$ satisfying the expected congruences mod 4. We can construct $x \in N$ with formula (5) and $a = \gamma$. The minimal polynomial of x over k is $X^4 - \gamma X^3 - (3\nu(\gamma) - \nu^2(\gamma))X^2 + (20\gamma + 18\nu(\gamma) + 18\nu^2(\gamma))X + 100\gamma + 120\nu(\gamma) + 88\nu^2(\gamma)$, where x is an integer with trace over k equal to γ . The fiber product (2.1) shows that it gives a normal integral basis for \mathcal{O}_N .

The element x is a root of $X^{12} - X^{11} - 32X^{10} + 91X^9 + 656X^8 - 800X^7 - 5417X^6 + 3122X^5 + 56308X^4 + 133224X^3 + 157584X^2 + 98784X + 28224$. It is possible to compute all the conjugates of x , and the action of the Galois group on them. We can certify our assertion by computing the discriminant of the lattice

generated by the conjugates of x . A text file `conduc91*3.txt` giving the instructions for `gp` is available at <http://www.math.unicaen.fr/~cognard/preprint/>. Other examples are also available in `conduc7*13.txt`, which constructs a normal integral basis for N/\mathbb{Q} with conductor 13 over the cubic field of conductor 7 and in `conduc163*1.txt` for the Hilbert class field of the cubic field with conductor 163.

REFERENCES

- [1] E. ARTIN. *Questions de base minimale dans la théorie des nombres algébriques*, Colloque du C.N.R.S. Algèbre et Théorie des Nombres, Paris (1949) pp. 19–20. MR0042450 (13,113i)
- [2] A. CHÂTELET. *Arithmétique des corps abéliens du troisième degré*, Ann. Sci. E.N.S. **63** (1946), 121–160. MR0020598 (8:568a)
- [3] J. COUGNARD. *Anneau d'entiers stablement libre sur $\mathbb{Z}[H_8 \times C_2]$* , Journal de Théorie des Nombres de Bordeaux **10** (1998), 163–201. MR1827291 (2002a:11124)
- [4] J. COUGNARD. *Construction de base normale pour les extensions de \mathbb{Q} à groupe D_4* , Journal de Théorie des Nombres de Bordeaux **12** (2000), 399–409. MR1823192 (2002d:11128)
- [5] J. COUGNARD. and J. QUEYRUT. *Construction de bases normales pour les extensions galoisiennes absolues à groupe de Galois quaternionien d'ordre 12*, Journal de Théorie des Nombres de Bordeaux **14** fas. 1 (2002), 87–102. MR1925992 (2003k:11173)
- [6] C.W. CURTIS and I. REINER. *Methods of representation theory, with applications to finite groups and orders* Vol. II, John Wiley and Sons (1987). MR0892316 (88f:20002)
- [7] J. MARTINET. *Sur l'arithmétique d'une extension galoisienne à groupe de Galois diédral d'ordre $2p$* , Ann. Inst. Fourier **19** (1969), 1–80. MR0262210 (41:6820)
- [8] C. BATUT, K. BELABAS, D. BERNARDI, H. COHEN, and M. OLIVIER. *User's Guide to Pari-GP*, version 2.02.12 (1999).
- [9] J.-J. PAYAN. *Critère de décomposition d'une extension de Kummer sur un sous-corps du corps de base*, Ann. Sci. de l'E.N.S. 4e série **1** (1964), 445–458. MR0237472 (38:5754)
- [10] D.S. RIM. *Modules over finite groups* Ann. Math. (2) **69** (1959), 700–712. MR0104721 (21:3474)
- [11] I. REINER and S. ULLOM. *Remarks on class groups of integral group rings*, Symp. Math. Inst. Nazionale Alta Math. (Rome) **13** (1974), 501–506. MR0367043 (51:3285)

LMNO, UMR 6139 CNRS, UNIVERSITÉ DE CAEN, F 14032 CAEN CEDEX, FRANCE
E-mail address: `cognard@math.unicaen.fr`