ACTA ARITHMETICA
109.4 (2003)

Module structure of rings of integers in octahedral extensions

by

M. Godin and B. Sodaïgui (Valenciennes)

1. Introduction. For every number field K, O_K denotes its ring of integers and $\mathcal{C}l(K)$ its classgroup.

Let K/k be an extension of number fields of degree n. The ring O_K is a torsion free O_k-module of rank n, so there exists an ideal I of O_k such that $O_K \simeq O_k^{n-1} \oplus I$ as O_k-modules. The class of I in $\mathcal{C}l(k)$ is called the *Steinitz class* of K/k or of O_K, and is denoted by $\mathcal{C}l_k(O_K)$ (see [FT, Theorem 13, p. 95]). The structure of O_K as an O_k-module is determined up to isomorphism by its rank and its Steinitz class.

Now, let Γ be a finite group and Δ a normal subgroup of Γ. We have the following exact sequence:

$$\Sigma: \quad 1 \to \Delta \to \Gamma \to \Gamma/\Delta \to 1.$$

We fix a Galois extension E/k with Galois group isomorphic to Γ/Δ. We denote by $R(E/k,\Sigma)$ (resp. $R_t(E/k,\Sigma)$) the set of (realizable) classes $c \in \mathcal{C}l(k)$ such that there exists a Galois extension (resp. Galois extension which is at most tamely ramified, i.e. tame) N/k, containing E, with an isomorphism π from $\mathrm{Gal}(N/k)$ to Γ and with E being the subfield of N fixed by $\pi^{-1}(\Delta)$, and the Steinitz class of O_N equal to c.

For $\Delta = \Gamma$, $R(E/k,\Sigma)$ (resp. $R_t(E/k,\Sigma)$) is simply the set of the Steinitz classes of Galois extensions (resp. tame Galois extensions) of k whose Galois group is isomorphic to Γ; we write $R(k,\Gamma)$ and $R_t(k,\Gamma)$ instead of $R(E/k,\Sigma)$ and $R_t(E/k,\Sigma)$.

For previous work concerning the determination of $R(E/k,\Sigma)$ and $R_t(E/k,\Sigma)$ see [C1, C2, GS]. In [GS], we consider the case of $\Gamma = A_4$, the alternating group, and Δ its subgroup of order 3; under the hypothesis that the class number of k is odd, we determine $R(E/k,\Sigma)$ and $R_t(E/k,\Sigma)$ and prove that they are subgroups of $\mathcal{C}l(k)$ when O_E is a free O_k-module or the class number of k is not divisible by 3.

2000 *Mathematics Subject Classification*: 11R04, 11R29, 11R33.

When Γ is abelian, a consequence of McCulloh's work (see [Mc]) is that $R_t(k,\Gamma)$ is a subgroup of $\mathcal{C}l(k)$. In [C3], it is shown that $R_t(k,\Gamma)$ is a subgroup of $\mathcal{C}l(k)$ in the situation when Γ is a nonabelian group of order p^3, and k contains the mth roots of unity, where p is an odd prime number and m is the exponent of Γ. When Γ is the quaternion or dihedral group of order 8, or the alternating (tetrahedral) group A_4, it is respectively proven in [So1], [So2] and [GS] that $R_t(k,\Gamma) = \mathcal{C}l(k)$ (therefore equal to $R(k,\Gamma)$) if the class number of k is odd.

In this paper, we are interested in the case where Γ is the symmetric (octahedral) group S_4 on 4 letters which can be defined by the presentation:

$$S_4 = \langle \mu,\nu,\sigma,\tau : \mu^2 = \nu^2 = \sigma^3 = \tau^2 = 1,\ \mu\nu = \nu\mu,\ \tau\sigma\tau = \sigma^{-1},\\ \sigma\mu\sigma^{-1} = \nu,\ \tau\mu\tau = \nu\rangle,$$

and

$$\Delta = \langle \mu,\nu\rangle.$$

The group S_4 is a semidirect product of Δ and $\langle\sigma,\tau\rangle$, where $\Delta \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\langle\sigma,\tau\rangle \simeq D_3$ (or S_3), D_3 being the dihedral group of order 6. A Galois extension of k is called *octahedral* if its Galois group is isomorphic to S_4.

We have $\mathrm{Gal}(E/k) \simeq \langle\sigma,\tau\rangle$, therefore E/k is a dihedral extension of degree 6. In Section 2, we shall prove the following main result:

THEOREM 1.1. *Let k be a number field. Let E/k be a dihedral extension of degree* 6. *Assume that the class number of k is odd. Then*

(i) $R(E/k,\Sigma) = \mathcal{C}l_k(O_E)(\mathcal{C}l(k))^3$, *where $(\mathcal{C}l(k))^3$ is the subgroup of third powers of elements of $\mathcal{C}l(k)$. In addition, if E/k is tame then $R_t(E/k,\Sigma) = R(E/k,\Sigma)$.*

(ii) $R(k,S_4) = R_t(k,S_4) = \mathcal{C}l(k)$.

REMARK. The hypothesis that the class number of k is odd comes from an embedding problem.

If the class number of k is not divisible by 3 then $(\mathcal{C}l(k))^3 = \mathcal{C}l(k)$. According to the definition of the Steinitz class, O_E is a free O_k-module if and only if $\mathcal{C}l_k(O_E) = 1$. Therefore we have:

COROLLARY 1.2. *Under the hypotheses and notation of Theorem* 1.1 *we have the following assertions*:

(1) *If the class number of k is not divisible by* 3 *then* $R(E/k,\Sigma) = \mathcal{C}l(k)$ $(= R_t(E/k,\Sigma)$ *if E/k is tame*).

(2) *If O_E is a free O_k-module then $R(E/k,\Sigma)$ is the subgroup of $\mathcal{C}l(k)$ equal to* $(\mathcal{C}l(k))^3$ $(= R_t(E/k,\Sigma)$ *if E/k is tame*).

Now we point out our principal motivation for studying the set of Steinitz classes. Let $\mathcal{M}$ be a maximal O_k-order in $k[\Gamma]$ containing $O_k[\Gamma]$ and let $\mathcal{C}\ell(\mathcal{M})$ be its locally free classgroup. We denote by $\mathcal{R}(\mathcal{M})$ the set of realizable classes, that is, the set of classes $c \in \mathcal{C}\ell(\mathcal{M})$ such that there exists a Galois extension N/k, at most tamely ramified, and with Galois group isomorphic to Γ, for which the class of $\mathcal{M} \otimes_{O_k[\Gamma]} O_N$ is equal to c. An interesting problem is to determine the structure of $\mathcal{R}(\mathcal{M})$ in the case that Γ is nonabelian, the abelian case being solved by McCulloh (see [Mc]). For instance, in [So2, So3], a close link is shown between the determination of that structure and the problem of studying the Steinitz classes.

2. Proof of the main result. Let N/k be an octahedral extension. If π is an isomorphism from $\mathrm{Gal}(N/k)$ to S_4 and $\gamma \in S_4$, one identifies $\pi^{-1}(\gamma)$ with γ. Let E/k be the subextension of N fixed by Δ. Then E/k is a dihedral extension of degree 6. Let k'/k be the quadratic subextension of E/k. Then N/k' is a Galois extension with Galois group isomorphic to the alternating group A_4. The extension N/E is biquadratic, and contains three quadratic extensions of E; if L/E is one of these then the others are $\sigma(L)$ and $\sigma^2(L)$.

Proposition 2.1. *With the above notation we have*

$$\mathcal{C}l_k(O_N) = (\mathcal{C}l_k(O_E))^4 (N_{E/k}(\mathcal{C}l_E(O_L)))^3.$$

Proof (analogous to that in [GS, Proposition 2.1] because $\mathrm{Gal}(N/k') \simeq A_4$). By transitivity of the Steinitz class in a tower of number fields (see [F, Theorem 4.1]) we have

$$\mathcal{C}l_k(O_N) = (\mathcal{C}l_k(O_E))^4 N_{E/k}(\mathcal{C}l_E(O_N)).$$

We know ([GS, Lemme 2.2]) that the Steinitz class of a biquadratic extension is the product of the Steinitz classes of its three quadratic subextensions. Thus

$$\mathcal{C}l_E(O_N) = \mathcal{C}l_E(O_L)\mathcal{C}l_E(O_{\sigma(L)})\mathcal{C}l_E(O_{\sigma^2(L)}).$$

As we have seen in the proof of [GS, Proposition 2.1], if we write $L = E(\sqrt{m})$, then since $\sigma^i(L) = E(\sqrt{\sigma^i(m)})$ and $\sigma^i(\Delta(L/E)) = \Delta(\sigma^i(L)/E)$ (where $\Delta(L/E)$ and $\Delta(\sigma^i(L)/E)$ denote the discriminants), we have by Artin (see [A])

$$\mathcal{C}l_E(O_{\sigma^i(L)}) = \sigma^i(\mathcal{C}l_E(O_L)).$$

Hence

$$N_{E/k}(\mathcal{C}l_E(O_N)) = (N_{E/k}(\mathcal{C}l_E(O_L)))^3.$$

This completes the proof. ■

To prove Theorem 1.1, we need the following lemma which is a criterion for an embedding problem. This lemma is well known. Its origin lies in a statement in [Ma, p. 365, application for $n = 4$, (ii)] without proof. A part of it is Theorem I.2 of [J]. Here we complete the proof.

LEMMA 2.2. *Let k be a number field. Let E/k be a dihedral extension of degree* 6 *with Galois group $\langle\sigma,\tau\rangle$, and let K/k be its* (*cubic non-Galois*) *subextension fixed by τ. Let $a \in K$ be an element which is not a square in E, and let M be the quadratic extension $K(\sqrt{a})/K$. Then the following assertions are equivalent*:

(1) *E/k is embeddable in an octahedral extension N/k containing M and such that N/M is biquadratic.*

(2) *$N_{K/k}(a)$ is a square in k, where $N_{K/k}$ is the norm map in K/k.*

In addition if the embedding is possible, we can choose $N{=}E(\sqrt{a},\sqrt{\sigma(a)})$.

Proof. The implication (1)⇒(2) is Theorem I.2 of [J]. Now we prove (2)⇒(1). Since a is not a square in E, neither is $\sigma(a)$. By Kummer theory and the fact that $N_{K/k}(a)$ is a square, we have $E(\sqrt{a})/E \neq E(\sqrt{\sigma(a)})/E$. Let N/E be the biquadratic extension $E(\sqrt{a},\sqrt{\sigma(a)})/E$, and σ_1 and σ_2 the generators of $\mathrm{Gal}(N/E)$. We denote by $\overline{\sigma}$ (resp. $\overline{\tau}$) a k-embedding of N which extends σ (resp. τ). It is immediate that $\overline{\sigma}(\sqrt{a}) = \pm\sqrt{\sigma(a)}$. As $N_{K/k}(a) = a\sigma(a)\sigma^2(a)$ is a square in k, we deduce that $\sigma^2(a)$ has a square root in N. Hence $\overline{\sigma}(\sqrt{\sigma(a)}) = \pm\sqrt{\sigma^2(a)}$, and $\overline{\sigma}(N) \subset N$. We have $(\sqrt{a})^2 = a$, so $(\overline{\tau}(\sqrt{a}))^2 = \tau(a) = a$, and then $\overline{\tau}(\sqrt{a}) = \pm\sqrt{a}$. Similarly, $(\overline{\tau}(\sqrt{\sigma(a)}))^2 = \tau\sigma(a) = \sigma^2\tau(a) = \sigma^2(a)$, and therefore $\overline{\tau}(\sqrt{\sigma(a)}) = \pm\sqrt{\sigma^2(a)}$ and $\overline{\tau}(N) \subset N$. We conclude that N/k is Galois of degree 24 and $\mathrm{Gal}(N/k) = \langle\sigma_1,\sigma_2,\overline{\sigma},\overline{\tau}\rangle$. Now, choose (for instance) $\sigma_1,\sigma_2,\overline{\sigma},\overline{\tau}$ defined by:

$$\begin{array}{lll}
\sigma_1(\sqrt{a}) = -\sqrt{a}, & \sigma_1(\sqrt{\sigma(a)}) = \sqrt{\sigma(a)}, & \sigma_1(\sqrt{\sigma^2(a)}) = -\sqrt{\sigma^2(a)},\\
\sigma_2(\sqrt{a}) = -\sqrt{a}, & \sigma_2(\sqrt{\sigma(a)}) = -\sqrt{\sigma(a)}, & \sigma_2(\sqrt{\sigma^2(a)}) = \sqrt{\sigma^2(a)},\\
\overline{\sigma}(\sqrt{a}) = \sqrt{\sigma(a)}, & \overline{\sigma}(\sqrt{\sigma(a)}) = \sqrt{\sigma^2(a)}, & \overline{\sigma}(\sqrt{\sigma^2(a)}) = \sqrt{a},\\
\overline{\tau}(\sqrt{a}) = \sqrt{a}, & \overline{\tau}(\sqrt{\sigma(a)}) = \sqrt{\sigma^2(a)}, & \overline{\tau}(\sqrt{\sigma^2(a)}) = \sqrt{\sigma(a)}.
\end{array}$$

An easy calculation shows that $\mathrm{Gal}(N/k) \simeq S_4$, which completes the proof. ■

Proof of Theorem 1.1(i). Let k be a number field. Let E/k be a dihedral extension of degree 6. Assume that the class number of k is odd. We begin by proving the equalities

$$R(E/k,\Sigma) = (\mathcal{C}l_k(O_E))^4(N_{E/k}(\mathcal{C}l(E)))^3, \tag{2.1}$$

$$R_t(E/k,\Sigma) = R(E/k,\Sigma) \quad \text{if } E/k \text{ is tame.} \tag{2.2}$$

The inclusion (for any number field k)

$$R(E/k,\Sigma) \subset (\mathcal{C}l_k(O_E))^4(N_{E/k}(\mathcal{C}l(E)))^3 \tag{2.3}$$

is an immediate consequence of Proposition 2.1. Let us now show

$$(2.4)\qquad (\mathcal{C}l_k(O_E))^4(N_{E/k}(\mathcal{C}l(E)))^3 \subset R(E/k,\Sigma).$$

Let $c \in N_{E/k}(\mathcal{C}l(E))$. Since $N_{E/k}(\mathcal{C}l(E))$ is a subgroup of $\mathcal{C}l(k)$, its order is also odd. Hence there exists $c' \in N_{E/k}(\mathcal{C}l(E))$ such that $c = c'^4$. Let $C \in \mathcal{C}l(E)$ be such that $c' = N_{E/k}(C)$.

We denote by $\mathcal{C}l(E, 4O_E)$ the ray classgroup modulo $4O_E$. The canonical surjection from $\mathcal{C}l(E, 4O_E)$ onto $\mathcal{C}l(E)$ and the Chebotarev density theorem in ray classgroups (see [N, Chap. V, Theorem 6.4, p. 132]) allow us to assert that there exist $m \in E^\times$, a fractional ideal I of O_E, and a prime ideal $\mathfrak{P}$ of O_E such that $\mathfrak{P} \cap O_k$ splits completely in E/k and

$$mO_E = I^2\mathfrak{P}, \qquad m \equiv 1 \bmod^* 4O_E, \qquad \mathcal{C}l(I^{-1}) = C,$$

where mod* is the usual notion of congruence in class field theory (see [N]). We have

$$(m\sigma(m)\tau(m\sigma(m)))O_E = (I\sigma(I)\tau(I)\tau\sigma(I))^2\mathfrak{P}\sigma(\mathfrak{P})\tau(\mathfrak{P})\tau\sigma(\mathfrak{P}).$$

Put $a = m\sigma(m)\tau(m\sigma(m))$. It is obvious that a is not a square in E ($v_{\mathfrak{P}}(a) \equiv 1 \bmod 2$). Let K/k be the non-Galois cubic subextension of E/k fixed by τ. Since $\mathrm{Gal}(E/K) = \langle\tau\rangle$, we have $a = N_{E/K}(m\sigma(m)) \in K$. Let M be the quadratic extension $K(\sqrt{a})/K$. We have $N_{K/k}(a) = (N_{E/k}(m))^2$. By Lemma 2.2, E/k is embeddable in the octahedral extension $N = E(\sqrt{a}, \sqrt{\sigma(a)})$.

Let L be the quadratic extension $E(\sqrt{a})/E$. We deduce from $m \equiv 1 \bmod^* 4O_E$ that $\gamma(m) \equiv 1 \bmod^* 4O_E$ for $\gamma = \sigma$, τ or $\tau\sigma$, hence $a \equiv 1 \bmod^* 4O_E$. By Kummer theory (see [H, §39]) $\Delta(L/E) = \mathfrak{P}\sigma(\mathfrak{P})\tau(\mathfrak{P})\tau\sigma(\mathfrak{P})$. A result of Artin (see [A]) yields $\mathcal{C}l_E(O_L) = \mathcal{C}l(I\sigma(I)\tau(I)\tau\sigma(I))^{-1}$, whence

$$\mathcal{C}l_E(O_L) = C\sigma(C)\tau(C)\tau\sigma(C).$$

Using Proposition 2.1 we get

$$\mathcal{C}l_k(O_N) = (\mathcal{C}l_k(O_E))^4(N_{E/k}(C\sigma(C)\tau(C)\tau\sigma(C)))^3.$$

Therefore

$$\mathcal{C}l_k(O_N) = (\mathcal{C}l_k(O_E))^4(c'^4)^3 = (\mathcal{C}l_k(O_E))^4c^3.$$

We conclude that (2.4) holds, and then (2.1) follows thanks to (2.3) and (2.4).

Clearly $E(\sqrt{a})/E$ and $E(\sqrt{\sigma(a)})/E$ are tame. It follows that N/E is tame. If E/k is tame, so is N/k. Therefore

$$(\mathcal{C}l_k(O_E))^4(N_{E/k}(\mathcal{C}l(E)))^3 \subset R_t(E/k,\Sigma).$$

Hence $R(E/k,\Sigma) = R_t(E/k,\Sigma)$, which completes the proof of (2.2).

Now we complete the proof of (i). Let k'/k be the quadratic subextension of E/k. Because the class number of k is odd, k'/k is ramified. Since it is the unique nontrivial abelian subextension of E/k, we infer that $N_{E/k} : \mathcal{C}l(E) \to \mathcal{C}l(k)$ is surjective (see [W, Theorem 10.1, p. 400]). Therefore $N_{E/k}(\mathcal{C}l(E)) = \mathcal{C}l(k)$. Hence

$$R(E/k, \Sigma) = (\mathcal{C}l_k(O_E))^4(\mathcal{C}l(k))^3 = \mathcal{C}l_k(O_E)(\mathcal{C}l(k))^3.$$

Proof of Theorem 1.1(ii). Let D_3 be the dihedral group of order 6. For any number field k, it follows from [E, Chap. III, §3, 3.1, p. 59] that

$$R_t(k, D_3) = \mathcal{C}l(k).$$

Let $c \in \mathcal{C}l(k)$. There exists a tame dihedral extension E/k of degree 6 such that $c = \mathcal{C}l_k(O_E)$. On the other hand, by Theorem 1.1(i), $c \in R_t(E/k, \Sigma)$, thus $\mathcal{C}l(k) \subset R_t(k, S_4)$, whence $R_t(k, S_4) = \mathcal{C}l(k)$. Now, the equality $R(k, S_4) = R_t(k, S_4)$ is obvious.

References

[A] E. Artin, *Questions de base minimale dans la théorie des nombres algébriques*, in: Colloq. Internat. CNRS 24, Paris, 1950, 19–20.

[C1] J. E. Carter, *Steinitz classes of a nonabelian extension of degree p^3*, Colloq. Math. 71 (1996), 297–303.

[C2] —, *Module structure of integers in metacyclic extensions*, ibid. 76 (1998), 191–199.

[C3] —, *Steinitz classes of nonabelian extensions of degree p^3*, Acta Arith. 78 (1997), 297–303.

[E] L. P. Endo, *Steinitz classes of tamely ramified Galois extensions of algebraic number fields*, thesis, University of Illinois at Urbana-Champaign, 1975.

[F] A. Fröhlich, *The discriminant of relative extensions and the existence of integral bases*, Mathematika 7 (1960), 15–22.

[FT] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge Univ. Press, 1991.

[GS] M. Godin and B. Sodaïgui, *Classes de Steinitz d'extensions à groupe de Galois A_4*, J. Théor. Nombres Bordeaux 14 (2002), 241–248.

[H] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Grad. Texts in Math. 77, Springer, New York, 1981.

[J] A. Jehanne, *Sur les extensions de $\mathbb{Q}$ à groupe de Galois S_4 ou $\tilde{S}_4$*, Acta Arith. 69 (1995), 259–276.

[Ma] J. Martinet, *Discriminants and permutation groups*, in: Number Theory, R. A. Molin (ed.), de Gruyter, Berlin, 1990, 359–385.

[Mc] L. R. McCulloh, *Galois module structure of abelian extensions*, J. Reine Angew. Math. 375/376 (1987), 259–306.

[N] J. Neukirch, *Class Field Theory*, Springer, Berlin, 1986.

[So1] B. Sodaïgui, *Classes de Steinitz d'extensions galoisiennes relatives de degré une puissance de 2 et problème de plongement*, Illinois J. Math. 43 (1999), 47–60.

[So2] —, *Relative Galois module structure and Steinitz classes of dihedral extensions of degree* 8, J. Algebra 223 (1999), 367–378.

[So3] —, *Realizable classes of quaternion extensions of degree* $4l$, J. Number Theory 80 (2000), 304–315.

[W] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, Berlin, 1996.

Département de Mathématiques
Université de Valenciennes
Le Mont Houy
F-59313 Valenciennes Cedex 9, France
E-mail: marjory.godin@univ-valenciennes.fr
bouchaib.sodaigui@univ-valenciennes.fr

Received on 11.6.2001
and in revised form on 13.1.2003 (4050)