Module structure of rings of integers in octahedral extensions

by

M. Godin and B. Sodàgui (Valenciennes)

1. Introduction. For every number field $K$, $O_K$ denotes its ring of integers and $\text{Cl}(K)$ 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 $O_K \cong O_k^{n-1} \oplus I$ as $O_k$-modules. The class of $I$ in $\text{Cl}(k)$ is called the Steinitz class of $K/k$ or of $O_K$, and is denoted by $\text{Cl}_k(O_K)$ (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 $\Gamma$ be a finite group and $\Delta$ a normal subgroup of $\Gamma$. We have the following exact sequence:

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

We fix a Galois extension $E/k$ with Galois group isomorphic to $\Gamma/\Delta$. We denote by $R(E/k, \Sigma)$ (resp. $R_t(E/k, \Sigma)$) the set of (realizable) classes $c \in \text{Cl}(k)$ 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 $\pi$ from $\text{Gal}(N/k)$ to $\Gamma$ 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 $\Gamma$; 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 $\Delta$ 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 $\text{Cl}(k)$ 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.

[321]
When $\Gamma$ is abelian, a consequence of McCulloh’s work (see [Mc]) is that $R_t(k, \Gamma)$ is a subgroup of $Cl(k)$. In [C3], it is shown that $R_t(k, \Gamma)$ is a subgroup of $Cl(k)$ in the situation when $\Gamma$ is a nonabelian group of order $p^3$, and $k$ contains the $m$th roots of unity, where $p$ is an odd prime number and $m$ is the exponent of $\Gamma$. When $\Gamma$ 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 $R_t(k, \Gamma) = Cl(k)$ (therefore equal to $R(k, \Gamma)$) if the class number of $k$ is odd.

In this paper, we are interested in the case where $\Gamma$ 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 $\Delta$ 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 $\text{Gal}(E/k) \simeq \langle \sigma, \tau \rangle$, 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) $R(E/k, \Sigma) = Cl_k(O_E)(Cl(k))^3$, where $(Cl(k))^3$ is the subgroup of third powers of elements of $Cl(k)$. In addition, if $E/k$ is tame then $R_t(E/k, \Sigma) = R(E/k, \Sigma)$.

(ii) $R(k, S_4) = R_t(k, S_4) = Cl(k)$.

**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 $(Cl(k))^3 = Cl(k)$. According to the definition of the Steinitz class, $O_E$ is a free $O_k$-module if and only if $Cl_k(O_E) = 1$. 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 $R(E/k, \Sigma) = Cl(k)$ ($= R_t(E/k, \Sigma)$ if $E/k$ is tame).

2. If $O_E$ is a free $O_k$-module then $R(E/k, \Sigma)$ is the subgroup of $Cl(k)$ equal to $(Cl(k))^3$ ($= R_t(E/k, \Sigma)$ 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 $\text{Cl}(\mathcal{M})$ be its locally free classgroup. We denote by $\mathcal{R}(\mathcal{M})$ the set of realizable classes, that is, the set of classes $c \in \mathcal{Cl}(\mathcal{M})$ such that there exists a Galois extension $N/k$, at most tamely ramified, and with Galois group isomorphic to $\Gamma$, 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 $\Gamma$ 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 $\pi$ is an isomorphism from $\text{Gal}(N/k)$ to $S_4$ and $\gamma \in S_4$, one identifies $\pi^{-1}(\gamma)$ with $\gamma$. Let $E/k$ be the subextension of $N$ fixed by $\Delta$. 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

$$\text{Cl}_k(O_N) = (\text{Cl}_k(O_E))^4(N_{E/k}(\text{Cl}_E(O_L)))^3.$$

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

$$\text{Cl}_k(O_N) = (\text{Cl}_k(O_E))^4N_{E/k}(\text{Cl}_E(O_N)).$$

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

$$\text{Cl}_E(O_N) = \text{Cl}_E(O_L)\text{Cl}_E(O_{\sigma(L)})\text{Cl}_E(O_{\sigma^2(L)}).$$

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])

$$\text{Cl}_E(O_{\sigma^i(L)}) = \sigma^i(\text{Cl}_E(O_L)).$$

Hence

$$N_{E/k}(\text{Cl}_E(O_N)) = (N_{E/k}(\text{Cl}_E(O_L)))^3.$$

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 \( \tau \). 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 \((1) \Rightarrow (2)\) is Theorem I.2 of [J]. Now we prove \((2) \Rightarrow (1)\). 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 \( \sigma_1 \) and \( \sigma_2 \) the generators of \( \text{Gal}(N/E) \). We denote by \( \bar{\sigma} \) (resp. \( \bar{\tau} \)) a \( k \)-embedding of \( N \) which extends \( \sigma \) (resp. \( \tau \)). It is immediate that \( \bar{\sigma}(\sqrt{a}) = \pm \sqrt{\sigma(a)} \). 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 \( \bar{\sigma}(\sqrt{\sigma(a)}) = \pm \sqrt{\sigma^2(a)} \), and \( \bar{\sigma}(N) \subset N \). We have \((\sqrt{a})^2 = a \), so \( (\bar{\tau}(\sqrt{a}))^2 = \bar{\tau}(a) = a \), and then \( \bar{\tau}(\sqrt{a}) = \pm \sqrt{a} \). Similarly, \( (\bar{\tau}(\sqrt{\sigma(a)}))^2 = \tau \sigma(a) = \sigma^2 \tau(a) = \sigma^2(a) \), and therefore \( \bar{\tau}(\sqrt{\sigma(a)}) = \pm \sqrt{\sigma^2(a)} \) and \( \bar{\tau}(N) \subset N \). We conclude that \( N/k \) is Galois of degree 24 and \( \text{Gal}(N/k) = \langle \sigma_1, \sigma_2, \bar{\sigma}, \bar{\tau} \rangle \). Now, choose (for instance) \( \sigma_1, \sigma_2, \bar{\sigma}, \bar{\tau} \) defined by:

\[
\begin{align*}
\sigma_1(\sqrt{a}) &= -\sqrt{a}, & \sigma_1(\sqrt{\sigma(a)}) &= \sqrt{\sigma(a)}, & \sigma_1(\sqrt{\sigma^2(a)}) &= -\sqrt{\sigma^2(a)}, \\
\sigma_2(\sqrt{a}) &= -\sqrt{a}, & \sigma_2(\sqrt{\sigma(a)}) &= -\sqrt{\sigma(a)}, & \sigma_2(\sqrt{\sigma^2(a)}) &= \sqrt{\sigma^2(a)}, \\
\bar{\sigma}(\sqrt{a}) &= \sqrt{\sigma(a)}, & \bar{\sigma}(\sqrt{\sigma(a)}) &= \sqrt{\sigma^2(a)}, & \bar{\sigma}(\sqrt{\sigma^2(a)}) &= \sqrt{\sigma(a)}, \\
\bar{\tau}(\sqrt{a}) &= \sqrt{a}, & \bar{\tau}(\sqrt{\sigma(a)}) &= \sqrt{\sigma^2(a)}, & \bar{\tau}(\sqrt{\sigma^2(a)}) &= \sqrt{\sigma(a)}.
\end{align*}
\]

An easy calculation shows that \( \text{Gal}(N/k) \simeq S_4 \), 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

\[
\begin{align*}
(2.1) & \quad R(E/k, \Sigma) = (\text{Cl}_k(O_E))^4(N_{E/k}(\text{Cl}(E)))^3, \\
(2.2) & \quad R_t(E/k, \Sigma) = R(E/k, \Sigma) \quad \text{if } E/k \text{ is tame.}
\end{align*}
\]

The inclusion (for any number field \( k \))

\[
(2.3) \quad R(E/k, \Sigma) \subset (\text{Cl}_k(O_E))^4(N_{E/k}(\text{Cl}(E)))^3
\]
is an immediate consequence of Proposition 2.1. Let us now show
\[(2.4) \quad (\text{Cl}_k(O_E))^4(N_{E/k}(\text{Cl}(E)))^3 \subset R(E/k, \Sigma).\]
Let \(c \in N_{E/k}(\text{Cl}(E)).\) Since \(N_{E/k}(\text{Cl}(E))\) is a subgroup of \(\text{Cl}(k),\) its order is also odd. Hence there exists \(c' \in N_{E/k}(\text{Cl}(E))\) such that \(c = c'^4.\) Let \(C \in \text{Cl}(E)\) be such that \(c' = N_{E/k}(C).\)

We denote by \(\text{Cl}(E, 4O_E)\) the ray classgroup modulo \(4O_E.\) The canonical surjection from \(\text{Cl}(E, 4O_E)\) onto \(\text{Cl}(E)\) 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
\[mO_E = I^2\mathfrak{P}, \quad m \equiv 1 \mod^* 4O_E, \quad \text{Cl}(I^{-1}) = C,\]
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 \(E\) \((\nu_E(a) \equiv 1 \mod 2).\) Let \(K/k\) be the non-Galois cubic subextension of \(E/k\) fixed by \(\tau.\) Since \(\text{Gal}(E/K) = \langle \tau \rangle,\) 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 \(m \equiv 1 \mod^* 4O_E\) that \(\gamma(m) \equiv 1 \mod^* 4O_E\) for \(\gamma = \sigma, \tau\) or \(\tau\sigma,\) hence \(a \equiv 1 \mod^* 4O_E.\) 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 \(\text{Cl}_E(O_L) = \text{Cl}(I\sigma(I)\tau(I)\tau\sigma(I))^{-1},\) whence \(\text{Cl}_E(O_L) = C\sigma(C)\tau(C)\tau\sigma(C).\)

Using Proposition 2.1 we get
\[
\text{Cl}_k(O_N) = (\text{Cl}_k(O_E))^4(N_{E/k}(C\sigma(C)\tau(C)\tau\sigma(C)))^3.
\]
Therefore
\[
\text{Cl}_k(O_N) = (\text{Cl}_k(O_E))^4(c'^4)^3 = (\text{Cl}_k(O_E))^4c^3.
\]
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
\[(\text{Cl}_k(O_E))^4(N_{E/k}(\text{Cl}(E)))^3 \subset R_t(E/k, \Sigma).\]
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 $N_{E/k} : Cl(E) \to Cl(k)$ is surjective (see [W, Theorem 10.1, p. 400]). Therefore $N_{E/k}(Cl(E)) = Cl(k)$. Hence

$$R(E/k, \Sigma) = (Cl_k(O_E))^4(Cl(k))^3 = Cl_k(O_E)(Cl(k))^3.$$ 

**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

$$R_t(k, D_3) = Cl(k).$$

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

**References**


Module structure of rings of integers


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