MATHEMATICS OF COMPUTATION
Volume 65, Number 213
January 1996, Pages 319 329

ON INTEGRAL BASES IN RELATIVE QUADRATIC EXTENSIONS

M. DABERKOW AND M. POHST

ABSTRACT. Let $\mathcal{F}$ be an algebraic number field and $\mathcal{E}$ a quadratic extension with $\mathcal{E} = \mathcal{F}(\sqrt{\mu})$. We describe a minimal set of elements for generating the integral elements $o_\mathcal{E}$ of $\mathcal{E}$ as an $o_\mathcal{F}$ module. A consequence of this theoretical result is an algorithm for constructing such a set. The construction yields a simple procedure for computing an integral basis of $\mathcal{E}$ as well. In the last section, we present examples of relative integral bases which were computed with the new algorithm and also give some running times.

1. PRELIMINARIES

The computation of integral bases of algebraic number fields is one of the basic tasks in computational algebraic number theory. Nonetheless, the existing algorithms for this problem tend to be very slow for fields of higher degree. In this paper, we therefore outline a new algorithm for the computation of an integral basis for those fields $\mathcal{E}$ which contain a subfield $\mathcal{F}$ of index 2.

Quadratic extensions have been extensively studied in the past [8, 6] and the main result of this paper is a generalization of a result of Sommer [10], who investigated biquadratic extensions.

In the sequel we consider number fields $\mathcal{F}$ with $[\mathcal{F} : \mathbb{Q}] = n$ and $\mathcal{E}$ subject to

$$\mathcal{E} = \mathcal{F}(\sqrt{\mu})$$

with an integral nonsquare element μ of $\mathcal{F}$. It is well known that the ring of integers $o_\mathcal{E}$ of $\mathcal{E}$ is not a free $o_\mathcal{F}$ module, in general. The following theorem gives a necessary and sufficient criterion for the existence of a relative integral basis [1].

Theorem 1.1. (i) *Let $f(t) = t^2 - \mu \in \mathcal{F}[t]$ be the minimal polynomial of $\sqrt{\mu}$ with polynomial discriminant $d(f)$, and let $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$ be the relative discriminant of $\mathcal{E}/\mathcal{F}$. A relative integral basis of $\mathcal{E}/\mathcal{F}$ exists if and only if the ideal Φ satisfying*

$$\Phi^2 = d(f)\mathfrak{d}_{\mathcal{E}/\mathcal{F}}^{-1}$$

is principal. We call the ideal Φ the ***index*** *of $o_\mathcal{F}[\sqrt{\mu}]$ in $o_\mathcal{E}$.*

(ii) *There are always elements $\xi_1, \xi_2, \xi_3 \in o_\mathcal{E}$ such that*

$$o_\mathcal{E} = \xi_1 o_\mathcal{F} + \xi_2 o_\mathcal{F} + \xi_3 o_\mathcal{F}.$$

Received by the editor June 17, 1994 and, in revised form, November 29, 1994.
1991 *Mathematics Subject Classification*. Primary 11R04, 11R20, 11Y40.

This criterion for the existence of a relative integral basis is easy to apply once we know the relative discriminant $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$. Thus, our first task is a complete description of $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$.

We cite the following theorem, which can be found in [7, Ch. 39], [6, Ch. 11].

Theorem 1.2. *Let $\wp$ be a prime ideal in $o_{\mathcal{F}}$ with $a := \nu_\wp(\mu)$ (i.e., $\mu \in \wp^a \setminus \wp^{a+1}$) and $e := \nu_\wp(2)$.*

(i) *If $e = 0$ and $a \equiv b \mod 2$ for $b \in \{0,1\}$, then*

$$\wp^b \| \mathfrak{d}_{\mathcal{E}/\mathcal{F}}.$$

(ii) *For $e \neq 0$*

$$\wp | \mathfrak{d}_{\mathcal{E}/\mathcal{F}} \Leftrightarrow \forall \gamma \in o_{\mathcal{F}} \ : \ \gamma^2 \not\equiv \mu \mod \wp^{2e+a}.$$

If $\wp \in \mathbb{P}_{\mathcal{F}}$ (where $\mathbb{P}_{\mathcal{F}}$ denotes the set of all prime ideals in $o_{\mathcal{F}}$) divides $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$, we additionally have [6]:

Theorem 1.3. *Let $a = \nu_\wp(\mu)$ and $e = \nu_\wp(2)$.*

(i) *If $a = 0$, then*

$$\wp^{v+1} \| \mathfrak{d}_{\mathcal{E}/\mathcal{F}}$$

for

$$v := 2e - \max\{\tilde{u} | \ 0 \leq \tilde{u} \leq 2e - 1 \text{ and } \exists \gamma \in o_{\mathcal{F}} \ : \ \gamma^2 \equiv \mu \mod \wp^{\tilde{u}}\}.$$

(ii) *If $a = 1$, then*

$$\wp^{2e+a} \| \mathfrak{d}_{\mathcal{E}/\mathcal{F}}.$$

If $\nu_\wp(\mu) \in \{0,1\}$ holds for all prime ideals mentioned above, Theorems 1.2 and 1.3 yield an easy algorithm for the computation of $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$. The assumption $\nu_\wp(\mu) \in \{0,1\}$ for all prime ideals above 2 is easily satisfied:

Proposition 1.4. *Let $\Pi \subset \mathbb{P}_{\mathcal{F}}$ with $|\Pi| < \infty$. Then there is an element $\mu^* \in o_{\mathcal{F}}$ satisfying*

$$\mathcal{F}(\sqrt{\mu^*}) = \mathcal{F}(\sqrt{\mu}) \ (= \mathcal{E})$$

and

$$\forall \wp \in \Pi \ : \quad \nu_\wp(\mu^*) \in \{0,1\}.$$

Proof. The proof is by an application of the Chinese Remainder Theorem. We set

$$\mu^* := \mu \prod_{\wp \in \Pi} \left(\frac{\delta_\wp}{\pi_\wp}\right)^{a_\wp}$$

subject to

- $\pi_\wp \in \wp \backslash \wp^2$ and $\pi_\wp \notin \mathfrak{q} \quad \forall \mathfrak{q} \in \Pi \setminus \{\wp\}$
- $a_\wp = 2k$, if $\nu_\wp(\mu) = 2k + i$ with $i \in \{0,1\}$
- $\delta_\wp \in \mathfrak{a}_\wp$ and $\delta_\wp \notin \mathfrak{b}$ for $\mathfrak{a}_\wp = (\pi_\wp)\wp^{-1}$ and $\mathfrak{b} := \prod_{\wp \in \Pi} \wp$.

Then one can easily verify that μ^* is a solution with the required properties. □

Consequently, we assume that if $\wp \in \mathbb{P}_{\mathcal{F}}$ and $\wp \mid 2$, then $\nu_\wp(\mu) \in \{0,1\}$ in the sequel. Before investigating quadratic extensions $\mathcal{E}/\mathcal{F}$ more intensively, we state the following lemma, which will be very important later on. It is an immediate consequence of the Chinese Remainder Theorem.

Lemma 1.5. *Let $\mathfrak{a}_1, \dots, \mathfrak{a}_m$ be comaximal (prime) ideals in $o_{\mathcal{F}}$, and let $\alpha, \alpha_1, \dots, \alpha_m$ be elements of $o_{\mathcal{F}}$ with*

$$\alpha \equiv \alpha_i^2 \mod \mathfrak{a}_i \qquad (1 \leq i \leq m).$$

Then there exists $\beta \in o_{\mathcal{F}}$ such that

$$\alpha \equiv \beta^2 \mod \prod_{i=1}^{m} \mathfrak{a}_i.$$

Theorem 1.2 and Theorem 1.3 provide a method for computing $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$. As already mentioned,

$$d(t^2 - \mu) = \mathfrak{d}_{\mathcal{E}/\mathcal{F}} \Phi^2,$$

where Φ is an ideal in $o_{\mathcal{F}}$. Since the index Φ is not prime to the ideal $\mu o_{\mathcal{F}}$ in general, we set

$$\begin{aligned} \Phi_2 &:= \gcd(2o_{\mathcal{F}}, \Phi), \\ \Phi_\mu &:= \Phi \cdot \Phi_2^{-1}. \end{aligned}$$

Hence, we have

$$\Phi = \Phi_2 \cdot \Phi_\mu. \tag{1.1}$$

This decomposition will play a key role in our subsequent considerations. We note that by construction

$$\Phi_2 \mid 2, \quad \Phi_\mu^2 \mid \mu \tag{1.2}$$

and since the generator μ satisfies

$$\nu_\wp(\mu) \in \{0, 1\} \quad \forall \wp \in \mathbb{P}_{\mathcal{F}} \; : \; \wp \mid 2,$$

we have $\gcd(\Phi_2, \Phi_\mu^2) = o_{\mathcal{F}}$. As a direct consequence of Theorem 1.3, Lemma 1.5 and (1.2), we obtain the following proposition:

Proposition 1.6. (i) *There is a $\tilde{\nu} \in o_{\mathcal{F}}$ such that*

$$\tilde{\nu}^2 \equiv \mu \mod \Phi_2^2. \tag{1.3}$$

(ii) *There is a $\nu \in o_{\mathcal{F}}$ solving the congruence $\nu^2 \equiv \mu \mod \Phi_2^2$ with*

$$\nu o_{\mathcal{F}} = \Phi_\mu \cdot \mathfrak{a}_\nu, \tag{1.4}$$

hence $(\nu^2 - \mu) o_{\mathcal{F}} = \Phi^2 \mathfrak{a}$.

2. Main theorem

Theorem 2.1. *Let $\mathfrak{b} = \beta_1 o_{\mathcal{F}} + \beta_2 o_{\mathcal{F}} = \sum_{i=1}^{n} \tilde{\beta}_i \mathbb{Z} \subset o_{\mathcal{F}}$ be a nonzero integral ideal such that there exists $\gamma \in o_{\mathcal{F}}$ with*

$$(\gamma) = \mathfrak{b}\Phi.$$

For any element $\nu \in o_{\mathcal{F}}$ satisfying Proposition 1.6, the following holds:

(i) *For all $\beta \in \mathfrak{b}$ we have $\beta \frac{\nu + \sqrt{\mu}}{\gamma} \in o_{\mathcal{E}}$.*

(ii) *With $\xi_i := \beta_i \frac{\nu + \sqrt{\mu}}{\gamma}$ $(i = 1, 2)$ we have $o_{\mathcal{E}} = o_{\mathcal{F}} + \xi_1 o_{\mathcal{F}} + \xi_2 o_{\mathcal{F}}$.*

(iii) *If $\omega_1, \dots, \omega_n$ is an integral basis of $o_{\mathcal{F}}$ and we set $\eta_i := \tilde{\beta}_i \frac{\nu + \sqrt{\mu}}{\gamma}$ for $1 \leq i \leq n$, then the elements $\omega_1, \dots, \omega_n, \eta_1, \dots, \eta_n$ are an integral basis of $o_{\mathcal{E}}$.*

The proof of this theorem is a bit lengthy. The first statement is easy to verify: For $\xi := \beta\frac{\nu+\sqrt{\mu}}{\gamma}$ and $\beta o_{\mathcal{F}} = \mathfrak{b}\cdot\tilde{\mathfrak{b}}$, we have

$$\begin{aligned}
\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\xi)o_{\mathcal{F}} &= (\frac{2\beta\nu}{\gamma})o_{\mathcal{F}}\\
&= 2o_{\mathcal{F}}\cdot\mathfrak{b}\cdot\tilde{\mathfrak{b}}\cdot\Phi_{\mu}\cdot\mathfrak{a}_{\nu}\cdot(\Phi\cdot\mathfrak{b})^{-1}\\
&= \frac{2o_{\mathcal{F}}}{\Phi_2}\cdot\tilde{\mathfrak{b}}\cdot\mathfrak{a}_{\nu}\subset o_{\mathcal{F}},\\
\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\xi)o_{\mathcal{F}} &= (\beta^2\frac{\nu^2-\mu}{\gamma^2})o_{\mathcal{F}}\\
&= (\mathfrak{b}\cdot\tilde{\mathfrak{b}})^2\cdot\Phi^2\cdot\mathfrak{a}\cdot(\Phi\cdot\mathfrak{b})^{-2}\subset o_{\mathcal{F}}.
\end{aligned}$$

Since the norm and the trace are both integral, ξ is integral, too. Thus, we have proved that η_i $(1\le i\le n)$ and ξ_1,ξ_2 are integral.

Next, we prove the last statement of the theorem, from which statement (ii) will follow easily.

We begin the proof with a lemma.

Lemma 2.2. *$o_{\mathcal{F}}[\sqrt{\mu}]$ is contained in $o_{\mathcal{F}}+\xi_1 o_{\mathcal{F}}+\xi_2 o_{\mathcal{F}}$.*

Proof. Because $\gamma\in\mathfrak{b}$, there exist $\alpha_1,\alpha_2\in o_{\mathcal{F}}$ with $\gamma=\alpha_1\beta_1+\alpha_2\beta_2$. Hence,

$$\sqrt{\mu} = -\nu+\alpha_1\xi_1+\alpha_2\xi_2. \quad \square$$

In the following we show that for all $p\in\mathbb{P}$ the set

$$\{\omega_1,\dots,\omega_n,\eta_1,\dots,\eta_n\}$$

is a $\mathbb{Z}(p) := \{x\in\mathbb{Q}|\ |x|_p\le 1\}$ basis for $o_{\mathcal{E}}(p) := \{x\in\mathcal{E}|\ |x|_{\mathfrak{P}}\le 1$ for all $\mathfrak{P}\in\mathbb{P}_{\mathcal{E}}\ :\ \mathfrak{P}|po_{\mathcal{E}}\}$. In other words, we need to describe all semilocal extensions $o_{\mathcal{E}}(\wp)/o_{\mathcal{F}}(\wp)$ for $\wp\in\mathbb{P}_{\mathcal{F}}$.

For prime ideals $\wp\in\mathbb{P}_{\mathcal{F}}$ there are three different cases possible:

(i) $\wp o_{\mathcal{E}}=\mathfrak{P}_1\cdot\mathfrak{P}_2$,
(ii) $\wp o_{\mathcal{E}}=\mathfrak{P}_1^2$,
(iii) $\wp o_{\mathcal{E}}=\mathfrak{P}_1$

with $\mathfrak{P}_1\ne\mathfrak{P}_2\in\mathbb{P}_{\mathcal{E}}$. We treat these three cases of prime ideals in two steps. In the first step, we look at prime ideals $\wp\in\mathbb{P}_{\mathcal{F}}$ which decompose into two different prime ideals $\mathfrak{P}_1,\mathfrak{P}_2\in\mathbb{P}_{\mathcal{E}}$. In the second step, we consider prime ideals $\wp\in\mathbb{P}_{\mathcal{F}}$ which do not completely split, e.g. the ideal $\wp o_{\mathcal{E}}$ does not decompose into two different prime ideals of $o_{\mathcal{E}}$. In each step we develop a description of $o_{\mathcal{E}}(\wp)$ as a free $o_{\mathcal{F}}(\wp)$ module.

For the first case the following lemma of [2, Lemma 3.3, p. 171] is crucial.

Lemma 2.3. *Let $\mathcal{K},\mathcal{M}$ be number fields with $\mathcal{M}=\mathcal{K}(\delta)$, where δ is a zero of a monic polynomial $f(t)\in o_{\mathcal{F}}(\wp)$ for $\wp\in\mathbb{P}_{\mathcal{K}}$. Moreover, let*

$$\wp o_{\mathcal{M}}=\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}$$

be the decomposition of $\wp$ in $o_{\mathcal{M}}$. If

$$|f'(\delta)|_{\mathfrak{P}_i}=1$$

for $1\le i\le g$, then $1,\delta,\dots,\delta^{[\mathcal{M}:\mathcal{K}]-1}$ is an $o_{\mathcal{K}}(\wp)$ basis of $o_{\mathcal{M}}(\wp)$.

Using this lemma, we are now able to prove the following statements, which completely solves the problem of an $o_{\mathcal{F}}(\wp)$ basis for $o_{\mathcal{E}}\,(\wp)$ for prime ideals $\wp \in \mathbb{P}_{\mathcal{F}}$ which split completely.

Lemma 2.4. *Let $\wp$ be a prime ideal in $o_{\mathcal{F}}$ which splits completely in $o_{\mathcal{E}}$, i.e.*

$$\wp o_{\mathcal{E}} = \mathfrak{P}_1 \cdot \mathfrak{P}_2$$

with $\mathfrak{P}_1 \neq \mathfrak{P}_2 \in \mathbb{P}_{\mathcal{E}}$. Let $a = \nu_{\wp}(\mu)$, $e = \nu_{\wp}(2)$ and $\pi \in \wp \setminus \wp^2$. Then an $o_{\mathcal{F}}(\wp)$ basis of $o_{\mathcal{E}}\,(\wp)$ is given by $1, \delta$ with:

(i) $\delta = \frac{1}{\pi^{a/2}}\sqrt{\mu}$ *if $a > 0$ and $e = 0$;*
(ii) $\delta = \frac{\nu+\sqrt{\mu}}{\pi^e}$ *if $a = 0$ and $e > 0$;*
(iii) $\delta = \sqrt{\mu}$ *if $a = 0$ and $e = 0$.*

Proof. Statements (i) and (iii) are straightforward, so we will only prove (ii). Obviously, $\mathcal{E} = \mathcal{F}(\delta)$, and δ is a zero of the polynomial

$$f(t) = t^2 - \frac{2\nu}{\pi^e}t + \frac{\nu^2 - \mu}{\pi^{2e}}.$$

Since ν satisfies equation (1.3) and $\pi^e | 2$, $f(t) \in o_{\mathcal{F}}(\wp)$.

We now look at $|f'(\delta)|_{\mathfrak{P}_i}$ $(i = 1, 2)$. Since $e = \nu_{\wp}(2)$, there is a unit $\alpha \in o_{\mathcal{F}}(\wp)$ with $2 = \alpha\pi^e$. Thus, $f'(\delta) = \alpha\sqrt{\mu}$ and $|f'(\delta)|_{\mathfrak{P}_i} = \left|\alpha\sqrt{\mu}\right|_{\mathfrak{P}_i} = |\alpha|_{\mathfrak{P}_i} \cdot \left|\sqrt{\mu}\right|_{\mathfrak{P}_i} = 1 \cdot 1 = 1$, and we apply Lemma 2.3 □

Remark 2.5. By the definition of ν, we have $(\nu) = \Phi_\mu \cdot \mathfrak{a}_\nu$ in $o_{\mathcal{F}}$. In the case $a > 0$ and $e = 0$, we have $\nu = \pi^{a/2}\alpha$ in $o_{\mathcal{F}}(\wp)$. Thus the elements $1, \frac{\nu+\sqrt{\mu}}{\pi^{a/2}}$ form an $o_{\mathcal{F}}(\wp)$ basis of $o_{\mathcal{E}}\,(\wp)$, too.

Lemma 2.6. *Let $\wp$ be a prime ideal in $o_{\mathcal{F}}$ which splits completely in $o_{\mathcal{E}}$ and let $1, \delta$ be an $o_{\mathcal{F}}(\wp)$ basis of $o_{\mathcal{E}}\,(\wp)$ with an element δ as in Lemma 2.4. Then there are $a_0, a_1, a_2 \in o_{\mathcal{F}}(\wp)$ such that*

$$\delta = a_0 + a_1\xi_1 + a_2\xi_2.$$

Proof. Without loss of generality let δ be of the form $\delta = \frac{\nu+\sqrt{\mu}}{\pi^r}$ with $r = |2|_{\wp}$ or $r = \frac{1}{2}\,|\mu|_{\wp}$ and $\pi \in \wp\setminus\wp^2$. Since $\wp$ splits completely, $\wp \nmid \mathfrak{d}_{\mathcal{E}/\mathcal{F}}$ and $(\gamma) = \Phi\mathfrak{b} = \wp^r\tilde{\Phi}\mathfrak{b}$. Hence the following decomposition holds in $o_{\mathcal{F}}$:

$$\gamma = \sum_{i=1}^{s} p_1^{(i)} \cdots p_r^{(i)} \cdot a^{(i)} \cdot \beta^{(i)}$$

with $s \in \mathbb{N}, p_j^{(i)} \in \wp$, $a^{(i)} \in \tilde{\Phi}$ and $\beta^{(i)} \in \mathfrak{b}$ $(1 \leq i \leq s, 1 \leq j \leq r)$.

In $o_{\mathcal{F}}(\wp)$ we have the decomposition $\gamma = \pi^r \cdot \lambda$ and the existence of $u^{(i)} \in o_{\mathcal{F}}(\wp)$ with $p_1^{(i)} \cdots p_r^{(i)} = \pi^r \cdot u^{(i)}$ for $1 \leq i \leq s$. Consequently,

$$\pi^r\lambda = \gamma = \sum_{i=1}^{s} p_1^{(i)} \cdots p_r^{(i)} \cdot a^{(i)} \cdot \beta^{(i)} = \pi^r \cdot \sum_{i=1}^{s} u^{(i)} \cdot a^{(i)} \cdot \beta^{(i)}.$$

Since $\beta^{(i)} \in \mathfrak{b}$, there are $\kappa_1^{(i)}, \kappa_2^{(i)} \in o_{\mathcal{F}}$ such that $a^{(i)} \cdot \beta^{(i)} = \kappa_1^{(i)}\beta_1 + \kappa_2^{(i)}\beta_2$ $(1 \leq i \leq s)$. Setting $\lambda_j^{(i)} := u^{(i)}\kappa_j^{(i)} \in o_{\mathcal{F}}(\wp)$ $(j = 1, 2;\ 1 \leq i \leq s)$, we rewrite λ as

$$\lambda = \sum_{i=1}^{s} \lambda_1^{(i)}\beta_1 + \lambda_2^{(i)}\beta_2$$

and obtain

$$\sum_{i=1}^{s} \lambda_1^{(i)} \xi_1 + \sum_{i=1}^{s} \lambda_2^{(i)} \xi_2 = \frac{\nu + \sqrt{\mu}}{\pi^r}. \quad \square$$

Next we describe $o_{\mathcal{E}}(\wp)$ as an $o_{\mathcal{F}}(\wp)$ module for prime ideals which do not completely split. For such prime ideals we study the local extension $\mathcal{E}_{\mathfrak{P}} \ /\mathcal{F}_{\wp}$ where $\mathfrak{P}$ is the only prime ideal in $o_{\mathcal{E}}$ above $\wp$. From local theory we know that $\mathcal{E}_{\mathfrak{P}} \ = \mathcal{F}_{\wp}(\sqrt{\mu})$, and we will apply the following theorem, due to Fröhlich [5], [9, Theorem 5.6, p. 221].

Theorem 2.7. *Let $\mathcal{F}_\wp$ be the $\wp$-adic completion of $\mathcal{F}$ with respect to $\wp$, and let τ be in $\mathfrak{R}_\wp = \{x \in \mathcal{F}_\wp | \ |x|_\wp \leq 1\}$ with $\tau \neq \alpha^2$ for all $\alpha \in \mathcal{F}_\wp$ and $\tau \notin \mathfrak{m}_\wp^2$, where $\mathfrak{m}_\wp := \{x \in \mathcal{F}_\wp | \ |x|_\wp < 1\}$ is the maximal ideal of $\mathfrak{R}_\wp$. Moreover, let π be an arbitrary element in $\mathfrak{m}_\wp \setminus \mathfrak{m}_\wp^2$. Then in the field $\mathcal{L} := F_\wp(\sqrt{\tau})$ the ring*

$$S = \{x \in \mathcal{L} | \ |x|_\wp \leq 1\}$$

is a free $\mathfrak{R}_\wp$ module. A basis is given by:

(i) $S = [1, \sqrt{\tau}]_{\mathfrak{R}_\wp}$ *if* $\pi \nmid 2\tau$;

(ii) $S = [1, \sqrt{\tau}]_{\mathfrak{R}_\wp}$ *if* $\pi | \tau$;

(iii) *If $\pi | 2$ and $\pi \nmid \tau$, let l be the largest number with*

$$\pi^l | 2 \text{ and } \exists \beta \in \mathfrak{R}_\wp \ : \ \beta^2 \equiv \tau \mod \mathfrak{m}_\wp^{2l}.$$

Then we have

$$S = [1, \frac{\beta + \sqrt{\tau}}{\pi^l}]_{\mathfrak{R}_\wp} .$$

Using this theorem, we can prove the following lemma, which is the second step in the description of $o_{\mathcal{E}}(\wp)$ as a free $o_{\mathcal{F}}(\wp)$ module.

Lemma 2.8. *Let $\wp$ be a prime ideal in $o_{\mathcal{F}}$ which does not completely split in $o_{\mathcal{E}}$, e.g. $\wp o_{\mathcal{E}} = \mathfrak{P}$ or $\wp o_{\mathcal{E}} = \mathfrak{P}^2$ with $\mathfrak{P} \in \mathbb{P}_{\mathcal{E}}$. We assume that π is an element in $\wp \setminus \wp^2$ and set $a := \nu_\wp(\mu)$ and $e := \nu_\wp(2)$. If we define $\delta \in o_{\mathcal{E}}(\wp)$ by*

(i) $\delta = \frac{\nu + \sqrt{\mu}}{\pi^k}$ *with* $k = \max\{0 \leq l \leq e | \exists \alpha \in o_{\mathcal{F}} \ : \ \alpha^2 \equiv \mu \textit{ mod } \wp^{2l}\}$ *if* $a = 0$ *and* $e > 0$;

(ii) $\delta = \frac{\nu + \sqrt{\mu}}{\pi^{\lfloor a/2 \rfloor}}$ *if* $a > 0$ *and* $e = 0$;

(iii) $\delta = \sqrt{\mu}$ *if* $e = 0$ *and* $a = 0$ *or* $e > 0$ *and* $a > 0$,

then the elements $1, \delta$ form a $o_{\mathcal{F}}(\wp)$ basis of $o_{\mathcal{E}}(\wp)$.

The proof is obtained by appropriate modifications of μ in order to satisfy the assumptions of Theorem 2.7. We note that in the second case of the lemma, the definition of δ strongly depends on the choice of ν since the element $\delta = \frac{1}{\pi^{\lfloor a/2 \rfloor}} \sqrt{\mu}$ is a proper choice for the second basis element, too.

As in the case of prime ideals which split completely, the following lemma can be proved similarly to Lemma 2.6.

Lemma 2.9. *Let $\wp$ be a prime ideal in $o_{\mathcal{F}}$ which does not completely split in $o_{\mathcal{E}}$ and let $1, \delta$ be a $o_{\mathcal{F}}(\wp)$ basis of $o_{\mathcal{E}}(\wp)$ with an element δ of Lemma 2.8. Then there are $a_0, a_1, a_2 \in o_{\mathcal{F}}(\wp)$ such that*

$$\delta = a_0 + a_1 \xi_1 + a_2 \xi_2.$$

We have shown that for every prime ideal $\wp \in \mathbb{P}_{\mathcal{F}}$ there is a $o_{\mathcal{F}}(\wp)$ basis $1, \delta_{\wp}$ of $o_{\mathcal{E}}\,(\wp)$ such that there exists $k \in \mathbb{N}$ and $\pi \in \wp \setminus \wp^2$ with

$$\delta_{\wp} = \frac{\nu + \sqrt{\mu}}{\pi^k}.$$

An important point for the upcoming steps in the proof is the fact that we can represent $\delta_{\wp}$ not only as a linear combination of $1, \xi_1, \xi_2$ with coefficients from $o_{\mathcal{F}}(\wp)$ (i.e. there are $a_0, a_1, a_2 \in o_{\mathcal{F}}(\wp)$ with $\delta_{\wp} = a_0 + a_1\xi_1 + a_2\xi_2$) but also as a linear combination of ξ_1, ξ_2. By the definition of γ we have a decomposition of γ in $o_{\mathcal{F}}$, such that

$$\gamma = \sum_{i=1}^{n} p_1^{(i)} \cdots p_k^{(i)} b^{(i)} a^{(i)}$$

with certain $p_1^{(i)}, \dots, p_k^{(i)} \in \wp$, $b^{(i)} \in \mathfrak{b}$ and $a^{(i)} \in \gamma o_{\mathcal{F}} \wp^{-k} \mathfrak{b}^{-1}$ $(1 \leq i \leq n)$. Since γ is an integral element, there are elements $u^{(i)} \in o_{\mathcal{F}}(\wp)$ and $b_1^{(i)}, b_2^{(i)} \in o_{\mathcal{F}}$ subject to

$$\begin{aligned}\gamma &= \pi^k \sum_{i=1}^{n} u^{(i)}(b_1^{(i)}\beta_1 + b_2^{(i)}\beta_2)a^{(i)} \\ &= \pi^k \left(\beta_1 \sum_{i=1}^{n} u^{(i)} b_1^{(i)} a^{(i)} + \beta_2 \sum_{i=1}^{n} u^{(i)} b_2^{(i)} a^{(i)}\right) \\ &=: \pi^k \left(\beta_1 a_1 + \beta_2 a_2\right).\end{aligned}$$

From $a_1, a_2 \in o_{\mathcal{F}}(\wp)$ we derive the predicted representation.

With this fact in mind, the next lemma is straightforward.

Lemma 2.10. *Let $\{\wp_1, \dots, \wp_s\} \subset \mathbb{P}_{\mathcal{F}}$ be a finite set of prime ideals. Then there is an element $\delta \in \mathcal{E}$ such that*

(i) $o_{\mathcal{E}}\,(\wp_i) = [1, \delta]_{o_{\mathcal{F}}(\wp_i)} \quad (1 \leq i \leq s)$,

(ii) $\delta = \alpha_1\xi_1 + \alpha_2\xi_2$ *for some* $\alpha_1, \alpha_2 \in \bigcap_{i=1}^{s} o_{\mathcal{F}}(\wp_i)$.

Lemma 2.10 enables us to complete the proof of Theorem 2.1 (iii).

Proof. We will prove the statement by showing that the set $\{\omega_1, \dots, \omega_n, \eta_1, \dots, \eta_n\}$ is a $\mathbb{Z}(p)$ basis of $o_{\mathcal{E}}\,(p)$ for all rational primes p.

Obviously, one has $[\omega_1, \dots, \omega_n, \eta_1, \dots, \eta_n]_{\mathbb{Z}(p)} \subseteq o_{\mathcal{E}}\,(p)$ since $\omega_i, \eta_i \in o_{\mathcal{E}}$ $(1 \leq i \leq n)$. Thus, it suffices to show

$$\text{(2.1)} \qquad o_{\mathcal{E}}\,(p) \subseteq [\omega_1, \dots, \omega_n, \eta_1, \dots, \eta_n]_{\mathbb{Z}(p)} \quad \forall p \in \mathbb{P}.$$

Let p be a rational prime. By the last lemma, we can find an element $\delta \in \mathcal{E}$ such that for all prime ideals $\wp \in \mathbb{P}_{\mathcal{F}}$ with $\wp | p o_{\mathcal{F}}$,

$$[1, \delta]_{o_{\mathcal{F}}(\wp)} = o_{\mathcal{E}}\,(\wp).$$

Therefore, the set $\{\omega_1, \dots, \omega_n, \delta\omega_1, \dots, \delta\omega_n\}$ is a $\mathbb{Z}(p)$ basis for $o_{\mathcal{E}}\,(\wp)$. Hence, it suffices to show

$$\text{(2.2)} \qquad \delta\omega_i \in [\omega_1, \dots, \omega_n, \eta_1, \dots, \eta_n]_{\mathbb{Z}(p)} \qquad (1 \leq i \leq n).$$

By the second statement of Lemma 2.10, there are $a_1, a_2 \in \bigcap_{i=1}^{s} o_{\mathcal{F}}(\wp_i) = o_{\mathcal{F}}(p)$ $(p o_{\mathcal{F}} = \wp_1^{g_1} \cdots \wp_s^{g_s})$ satisfying

$$\begin{aligned}\delta\omega_i &= (a_1\xi_1 + a_2\xi_2)\omega_i \\ &= a_1\omega_i\beta_1 \frac{\nu + \sqrt{\mu}}{\gamma} + a_2\omega_i\beta_2 \frac{\nu + \sqrt{\mu}}{\gamma}.\end{aligned}$$

Since ω_i is integral in $\mathcal{F}$ and β_1, β_2 are both elements of $\mathfrak{b}$, we can find $b_k^{(j)} \in \mathbb{Z}$ $(1 \leq k \leq n;\ j = 1,2)$ such that $\omega_i \beta_j = \sum_{k=1}^n b_k^{(j)} \tilde{\beta}_k$. We may also assume that a_j $(j = 1,2)$ has a representation as $a_j = \sum_{k=1}^n a_k^{(j)} \omega_k$ with certain $a_k^{(j)} \in \mathbb{Z}(p)$ $(j = 1,2;\ 1 \leq k \leq n)$. Thus we get

$$\delta\omega_i = \sum_{k=1}^n \sum_{l=1}^n a_k^{(1)} b_l^{(1)} \omega_k \eta_l + \sum_{k=1}^n \sum_{l=1}^n a_k^{(2)} b_l^{(2)} \omega_k \eta_l .$$

We now observe that $\omega_k \tilde{\beta}_l$ is an element of the ideal $\mathfrak{b}$, which means we can find $c_j^{(k.l)} \in \mathbb{Z}$ such that $\sum_{j=1}^n c_j^{(k.l)} \tilde{\beta}_l = \omega_k \tilde{\beta}_l$. Therefore we have $\omega_k \eta_l = \sum_{j=1}^n c_j^{(k.l)} \eta_j$, which yields

$$\delta\omega_i = \sum_{j=1}^n \sum_{k=1}^n \sum_{l=1}^n a_k^{(1)} b_l^{(1)} c_j^{(k.l)} \eta_j + \sum_{j=1}^n \sum_{k=1}^n \sum_{l=1}^n a_k^{(2)} b_l^{(2)} c_j^{(k.l)} \eta_j .$$

Since all coefficients $a_k^{(1)}, a_k^{(2)}, b_l^{(1)}, b_l^{(2)}, c_j^{(k.l)}$ are in $\mathbb{Z}$ or $\mathbb{Z}(p)$, we have proven (2.2), hence (2.1), and so Theorem 2.1 (iii). □

We can now prove statement (ii) of Theorem 2.1:

$$\mathfrak{o}_{\mathcal{E}} = [1, \xi_1, \xi_2]_{\mathfrak{o}_{\mathcal{F}}} .$$

Let α be in $\mathfrak{o}_{\mathcal{E}}$. By Theorem 2.1 (iii), there are $a_1, \dots, a_{2n} \in \mathbb{Z}$ such that $\alpha = \sum_{i=1}^n a_i \omega_i + \sum_{i=1}^n a_{n+i} \eta_i$. Therefore, we have $\alpha_0 := \sum_{i=1}^n a_i \omega_i \in \mathfrak{o}_{\mathcal{F}}$, and we can find $\alpha_1, \alpha_2 \in \mathfrak{o}_{\mathcal{F}}$ with $\alpha_1 \beta_1 + \alpha_2 \beta_2 = \sum_{i=1}^n a_{n+i} \tilde{\beta}_i$.

From the definition of $\eta_1, \dots, \eta_n$ and of ξ_1, ξ_2, we conclude

$$\alpha_1 \xi_1 + \alpha_2 \xi_2 = \sum_{i=1}^n a_{n+i} \eta_i ,$$

which finally gives

$$\alpha_0 + \alpha_1 \xi_1 + \alpha_2 \xi_2 = \sum_{i=1}^n a_i \omega_i + \sum_{i=1}^n a_{n+i} \eta_i = \alpha .$$

This finishes the proof of Theorem 2.1.

Remark 2.11. (i) In case the index Φ is a principal ideal (i.e. $\Phi = \gamma \mathfrak{o}_{\mathcal{F}}$), we can choose $\mathfrak{b} = \mathfrak{o}_{\mathcal{F}}$, leading to a relative integral basis $1, \xi = \frac{\nu + \sqrt{\mu}}{\gamma}$ of $\mathfrak{o}_{\mathcal{E}}$ over $\mathfrak{o}_{\mathcal{F}}$.

(ii) As all proofs are constructive, Theorem 2.1 yields an algorithm for the construction of a minimal set of $\mathfrak{o}_{\mathcal{F}}$ generators of $\mathfrak{o}_{\mathcal{E}}$.

(iii) Statement (iii) of Theorem 2.1 gives a simple algorithm for the computation of an integral basis of $\mathfrak{o}_{\mathcal{E}}$.

The algorithm is based on the fact that we can compute the relative discriminant $\mathfrak{d}_{\mathcal{E}/\mathcal{F}}$ easily by applying Theorem 1.2 and Theorem 1.3. The main problem is the computation of

$$\max\{\tilde{u} \mid 0 \leq \tilde{u} \leq 2e - 1 \text{ and } \exists \gamma \in \mathfrak{o}_{\mathcal{F}} \ :\ \gamma^2 \equiv \mu \mod \wp^{\tilde{u}}\}$$

for prime ideals $\wp \in \mathbb{P}_{\mathcal{F}}$ with $\nu_{\wp}(2) = e > 0$ and $\nu_{\wp}(\mu) = 0$. An efficient algorithm will be discussed by the first author in a forthcoming paper, although it is usually quite efficient to check all elements of $\mathfrak{o}_{\mathcal{F}} / \wp^{\tilde{u}}$.

If one is interested in a minimal set of $\mathfrak{o}_{\mathcal{F}}$ generators of $\mathfrak{o}_{\mathcal{E}}$, it is necessary to check whether or not the index Φ is a principal ideal. This can be very time consuming, since the check itself is difficult [4] and the principal ideal test algorithm requires an independent set of units for $o_{\mathcal{F}}$. On the other hand, the computation of an integral basis of $o_{\mathcal{E}}$ is relatively easy, and the only information we need about $\mathcal{F}$ is an integral basis of $o_{\mathcal{F}}$.

3. Examples

We present two explicit examples of relative extensions and also a short table of running times for quadratic extensions.

We first consider the number field $\mathcal{F}$ generated by a root of the polynomial

$$f(t) = t^6 - 2t^5 - 33t^4 + 46t^3 + 282t^2 - 184t - 559.$$

This field has class number 2, and an integral basis of $o_{\mathcal{F}}$ is given by

$$\begin{aligned}
\omega_1 &= 1, \\
\omega_2 &= (106262 + 40764\rho - 24704\rho^2 - 4428\rho^3 + 1021\rho^4 + 80\rho^5)/43511, \\
\omega_3 &= (32669 - 58594\rho - 8531\rho^2 + 8158\rho^3 + 379\rho^4 - 226\rho^5)/43511, \\
\omega_4 &= (-32669 + 102105\rho + 8531\rho^2 - 8158\rho^3 - 379\rho^4 + 226\rho^5)/43511, \\
\omega_5 &= (308776 - 8915\rho - 38373\rho^2 + 1865\rho^3 + 700\rho^4 - 73\rho^5)/43511, \\
\omega_6 &= (220545 - 86386\rho - 56577\rho^2 + 30249\rho^3 + 2488\rho^4 - 1254\rho^5)/43511.
\end{aligned}$$

We consider the two fields $\mathcal{E}_1 = \mathcal{F}(\sqrt{41})$ and $\mathcal{E}_2 = \mathcal{F}(\sqrt{47})$. In $o_{\mathcal{F}}$ the ideals $2o_{\mathcal{F}}, 41o_{\mathcal{F}}, 37o_{\mathcal{F}}$ decompose into prime ideals in the following way:

$$\begin{aligned}
2o_{\mathcal{F}} &= (2o_{\mathcal{F}} + (12\omega_1 + 2\omega_2 + 34\omega_3 + 16\omega_4 - 2\omega_5 - 3\omega_6)o_{\mathcal{F}})^2 \\
&=: \wp_2^2, \\
41o_{\mathcal{F}} &= (41o_{\mathcal{F}} + (5\omega_1 + \omega_3 + \omega_4)o_{\mathcal{F}}) \cdot (41o_{\mathcal{F}} + (12\omega_1 + \omega_3 + \omega_4)o_{\mathcal{F}}) \\
&\quad \cdot (41o_{\mathcal{F}} + (14\omega_1 + \omega_3 + \omega_4)o_{\mathcal{F}}) \cdot (41o_{\mathcal{F}} + (21\omega_1 + \omega_3 + \omega_4)o_{\mathcal{F}}) \\
&\quad \cdot (41o_{\mathcal{F}} + (30\omega_1 + \omega_3 + \omega_4)o_{\mathcal{F}}) \cdot (41o_{\mathcal{F}} + (39\omega_1 + \omega_3 + \omega_4)o_{\mathcal{F}}), \\
47o_{\mathcal{F}} &= 47o_{\mathcal{F}}.
\end{aligned}$$

In $\mathcal{E}_1$, 41 is a square modulo the ideal $\mathfrak{a} = \wp_2^4$ since $41 - \nu^2 \in \mathfrak{a}$ for $\nu := 1$. By Theorem 1.2 we know that $\wp_2$ does not divide $\mathfrak{d}_{\mathcal{E}_1/\mathcal{F}}$. Moreover, we know that $41o_{\mathcal{F}}$ divides the discriminant, since all prime ideals dividing $41o_{\mathcal{F}}$ are unramified. Therefore, the relative discriminant $\mathfrak{d}_{\mathcal{E}_1/\mathcal{F}}$ and the index Φ are:

$$\begin{aligned}
\mathfrak{d}_{\mathcal{E}_1/\mathcal{F}} &= 41o_{\mathcal{F}}, \\
\Phi &= \wp_2^2 = 2o_{\mathcal{F}}.
\end{aligned}$$

Since the index Φ is a principal ideal, we get a relative integral basis of $o_{\mathcal{F}}$ via

$$\begin{aligned}
\xi_1 &= 1, \\
\xi_2 &= \frac{1 + \sqrt{41}}{2}.
\end{aligned}$$

In $\mathcal{E}_2 = \mathcal{F}(\sqrt{47})$ the prime number 47 is a square modulo $\wp_2^3$, but not modulo $\wp_2^4$. For $\nu := -\omega_1 - \omega_4 - \omega_5 - \omega_6$ we have the relation $47 - \nu^2 \in \wp_2^3$. By Theorem 1.2

and Theorem 1.3 we know $\wp_2^2 | \mathfrak{d}_{\mathcal{E}_2/\mathcal{F}}$, and since $47 o_{\mathcal{F}}$ is a prime ideal, we conclude that $47 o_{\mathcal{F}} | \mathfrak{d}_{\mathcal{E}_2/\mathcal{F}}$. This results in

$$\begin{aligned} \mathfrak{d}_{\mathcal{E}_2/\mathcal{F}} &= \wp_2^2 \cdot 47 o_{\mathcal{F}} = 94 o_{\mathcal{F}}, \\ \Phi &= \wp_2. \end{aligned}$$

One can check with KANT V2 [3] that the index Φ is not a principal ideal. It follows that there is no integral basis for $o_{\mathcal{E}}$ over $o_{\mathcal{F}}$. However, a minimal set of generators for $o_{\mathcal{E}}$ over $o_{\mathcal{F}}$ is given by

$$\begin{aligned} \xi_1 &= 1, \\ \xi_2 &= -\omega_1 - \omega_4 - \omega_5 - \omega_6 + \sqrt{47}, \\ \xi_3 &= \frac{(62\omega_1 + 2\omega_2 - 8\omega_3 + \omega_4 + 7\omega_5 + 3\omega_6) - (2\omega_1 + 2\omega_2 + 2\omega_3 + \omega_4 + \omega_5 + \omega_6)\sqrt{47}}{2}. \end{aligned}$$

According to the definitions in Theorem 2.1 we chose $\mathfrak{b} = \wp$ and $\gamma o_{\mathcal{F}} = \wp_2^2 = 2 o_{\mathcal{F}}$.

Since an integral basis can also be computed by this algorithm, we will compare this method with the standard algorithm for the computation of an integral basis, the Round–2 algorithm of H. Zassenhaus [11].

For three different number fields $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3$ generated by a root of the polynomial $f_i(t) \in \mathbb{Z}[t]$ we consider several quadratic extensions and compare the running time of the Round–2 with the running time of the relative method. Let the polynomials $f_i(t)$ be defined as follows:

$$\begin{aligned} f_1(t) &= t^2 - 10, \\ f_2(t) &= t^4 - 72t^2 + 256, \\ f_3(t) &= t^6 - 2t^5 - 33t^4 + 46t^3 + 282t^2 - 184t - 559. \end{aligned}$$

For a quadratic extension of $\mathcal{F}_i$ $(i = 1, 2, 3)$, we consider fields $\mathcal{E}_{i,p} = \mathcal{F}_i(\sqrt{p})$ with $p \in \mathbb{P}$. In the following table we list running times of the Round–2 and the relative method.

Field	Round–2	relative method
	[sec]	[sec]
$\mathcal{F}_1(\sqrt{5})$	0.3	< 0.1
$\mathcal{F}_1(\sqrt{11})$	0.3	< 0.1
$\mathcal{F}_1(\sqrt{881})$	0.4	< 0.1
$\mathcal{F}_2(\sqrt{5})$	14.3	0.7
$\mathcal{F}_2(\sqrt{13})$	19.3	0.7
$\mathcal{F}_2(\sqrt{31})$	23.6	0.6
$\mathcal{F}_2(\sqrt{53})$	21.5	0.6
$\mathcal{F}_3(\sqrt{3})$	159	9.4
$\mathcal{F}_3(\sqrt{5})$	464	2.8
$\mathcal{F}_3(\sqrt{13})$	313	2.9
$\mathcal{F}_3(\sqrt{17})$	680	3.0

All computations were performed on a PC with a 486-33 CPU using software developed under KANT V2 [3] under the operating system Linux 0.95.

References

1. E. Artin, *Questions de base minimale dans la théorie des nombres algébriques*, The collected papers of Emil Artin, Addison–Wesley, Reading, MA, 1965, pp. 229–231. MR **31:**1159
2. J.W.S. Cassels, *Local fields*, Cambridge Univ. Press, Cambridge, 1986. MR **87i:**11172

3. Fachgruppe Computeralgebra der GI, *Computeralgebra in Deutschland*, Fachgruppe Computeralgebra der GI (1993), 212 – 218.
4. U. Fincke and M. Pohst, *A procedure for determining algebraic integers of given norm*, Proc. Eurosam 83, Springer Lecture Notes in Comput. Sci., vol. 162, 1983, pp. 194 – 202. MR **86k:**11078
5. A. Fröhlich, *Discriminants of algebraic number fields*, Math. Z. **74** (1960), 18 – 28. MR **22:**4707
6. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Jahresber. Deutsch. Math.-Verein. **35** (1926).
7. E. Hecke, *Lectures on the theory of algebraic numbers*, Springer-Verlag, New York, 1981. MR **83m:**12001
8. D. Hilbert, *Über die Theorie des relativquadratischen Zahlkörpers*, Math. Ann. **51** (1898).
9. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 2nd ed., Springer-Verlag, New York, 1990. MR **91h:**11107
10. J. Sommer, *Vorlesungen über Zahlentheorie*, Teubner, Leipzig, 1907.
11. H. Zassenhaus, *Ein Algorithmus zur Berechnung einer Minimalbasis über gegebener Ordnung*, Funktionalanalysis, Approximationstheorie, Numerische Mathematik (Oberwolfach, 1965), Birkhäuser, Basel, 1967, pp. 90–103. MR **37:**2720

Technische Universität Berlin, Fachbereich 3, Sekr. Ma8-1, Strasse des 17. Juni 136, 10623 Berlin, Germany

E-mail address, M. Daberkow: `daberkow@math.tu-berlin.de`

E-mail address, M. Pohst: `pohst@math.tu-berlin.de`