# ERRATA: *IDENTIFYING THE MATRIX RING*

JOHN VOIGHT

This note gives errata for the article *Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms* [2]. Thanks to Travis Morrison and Daniel Smertnig.

(1) Algorithm 3.22 is incorrect: in the final step, the element $j$ indeed has $\operatorname{trd}(j) = 0$, but it is not necessarily true that $\operatorname{trd}(ij) = 0$, for example with $F = \mathbb{Q} \subseteq K = \mathbb{Q}(i) \subseteq B = (-1, -1 \,|\, \mathbb{Q})$ and the Hurwitz order $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$ where $k = (-1+i+j+k)/2$: we can write $\mathcal{O} = \mathbb{Z}_K + \mathfrak{b}j$ as in Step 3, with $\mathbb{Z}_K = \mathbb{Z}[i]$, but we could not have $\operatorname{trd}(j) = \operatorname{trd}(ij) = 0$, since then $\operatorname{trd}(\mathcal{O}) = 2\mathbb{Z}$, whereas $\operatorname{trd}(k) = 1$. It should be replaced by the following.

**Algorithm 3.22.** Let $\mathcal{O} \subset B$ be a quaternion order over $\mathbb{Z}_F$. Let $\iota : K \to B$ be an embedding of $F$-algebras with $K$ a field such that $[K : F] = 2$ and let $\iota(K) \cap \mathcal{O} = \mathbb{Z}_K$ is maximal. This algorithm returns $\mathsf{true}$ and a fractional ideal $\mathfrak{b}$ of $K$, an element $j \in \mathcal{O}$ such that $\mathcal{O} = \iota(\mathbb{Z}_K) \oplus \iota(\mathfrak{b})j \cong \left(\dfrac{\mathbb{Z}_K, \mathfrak{b}, b}{\mathbb{Z}_F}\right)$ if $\mathcal{O}$ can be written in this way, otherwise $\mathsf{false}$.

1. Identify $K$ with $\iota(K)$. Let $K = F \oplus Fi$ with $i \in B$.
2. By linear algebra over $R$, compute the orthogonal complement $(\mathbb{Z}_K)^\perp := K^\perp \cap \mathcal{O}$ of $\mathbb{Z}_K$ in $\mathcal{O}$. If $\mathcal{O} \neq \mathbb{Z}_K \oplus (\mathbb{Z}_K)^\perp$, return $\mathsf{false}$.
3. Using an HNF, write $(\mathbb{Z}_K)^\perp = \mathfrak{b}j$; return $\mathsf{true}$, $\mathfrak{b}$, and $j$.

*Proof of correctness.* In Step 2, we could choose generators $x_1, \dots, x_m$ of $\mathcal{O}$ as an $R$-module (or $\mathbb{Z}$-module); then $\sum_k a_k x_k \in (\mathbb{Z}_K)^\perp$ if and only if

$$\sum_{k=1}^{m} a_k \operatorname{trd}(x_k) = \sum_{k=1}^{m} a_k \operatorname{trd}(i x_k) = 0$$

so this describes generators for $(\mathbb{Z}_K)^\perp$ as the kernel of a matrix. We correctly return $\mathsf{false}$ in that step if $\mathcal{O} \neq \mathbb{Z}_K + (\mathbb{Z}_K)^\perp$, since this is true for $\left(\dfrac{\mathbb{Z}_K, \mathfrak{b}, b}{R}\right)$. ∎

For a more general discussion of crossed products, see Voight [1, Proposition 4.12].

## References

[1] John Voight, *Characterizing quaternion rings over an arbitrary base*, J. Reine Angew. Math. **657** (2011), 113–134.

*Date*: May 21, 2019.

[2] *Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms*, Quadratic and higher degree forms, eds. K. Alladi, M. Bhargava, D. Savitt, and P.H. Tiep, Developments in Math., vol. 31, Springer, New York, 2013, 255–298.