Computing Square Roots in Quaternion Algebras

Przemysław Koprowski[*]

Institute of Mathematics

University of Silesia in Katowice

ul. Bankowa 14, 40-007 Katowice, Poland

przemyslaw.koprowski@us.edu.pl

Abstract. We present an explicit algorithmic method for computing square roots in quaternion algebras over global fields of characteristic different from 2.

1. Introduction

The computation of square roots is one of the most basic operations in mathematics. Effective methods for computing square roots are among the oldest algorithms in the realm of computational mathematics. In fact, Heron's method for a numerical approximation of a square root of a real number is two thousand years old and preceded by the Euclidean algorithm (wildly believed to be the oldest mathematical algorithm) by only about three to four centuries (for an in-depth discussion on the chronology see [1]). Although numerous methods for computing square roots in various algebraic structures are known nowadays, some important omissions prevail. Among them are general quaternion algebras. Computation of square roots in the algebra of Hamilton quaternions $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$ is well-known (see [2]) and very simple as for every quaternion $q \in \mathbb{H}$ there is a subfield $K \cong \mathbb{C}$ of $\mathbb{H}$ containing q, and so the computation of the square root in $\mathbb{H}$ can be reduced to the computation of the square root in $\mathbb{C}$. It is no longer so in a general quaternion algebra $\mathcal{Q} = \left(\frac{\alpha,\beta}{K}\right)$ for an arbitrary field K and two

---

[*]Address for correspondence: Institute of Mathematics, University of Silesia, ul. Bankowa 14, 40-007 Katowice, Poland.

elements $\alpha, \beta \in K^{\times}$. To the best of our knowledge, no algorithm for computing quaternionic square roots exists in the literature. One possible explanation for this (quite surprising) fact is that in the commutative case when one considers a field extension L/K, a typical way to compute a square root of an element $a \in L$ is to factor the polynomial $x^2 - a$ in $L[x]$. However, for quaternion algebras, there are no known polynomial factorization algorithms.

The sole purpose of this paper is to correct this evident omission and present an explicit algorithm for computing square roots in quaternion algebras over arbitrary global fields of characteristic different from 2.

2.   Notation

Throughout this paper, K will denote an arbitrary global field of characteristic $\operatorname{char} K \neq 2$. Hence, K is either a number field, i.e. a finite extension of $\mathbb{Q}$ (then its characteristic is just 0) or a global function field, that is, a finite extension of a rational function field over a finite field $\mathbb{F}_q$, where q is a power of an odd prime. The set of nonzero elements of K is denoted $K^{\times}$.

Recall that a quaternion algebra $\mathcal{Q} = \left(\frac{\alpha, \beta}{K}\right)$ over q K is a 4-dimensional K-algebra with a basis $\{1, i, j, \hbar\}$ and a multiplication gathered by the rules:

$$i^2 = \alpha, \quad j^2 = \beta, \quad ij = \hbar = -ji.$$

As usual, we shall identify the field K with the subfield $K \cdot 1$ of $\mathcal{Q}$, which is known to coincide with the center $Z(\mathcal{Q})$ of $\mathcal{Q}$. We refer the reader to [3, 4] for a comprehensive presentation of the theory of quaternion algebras.

A quaternion q is called *pure* (see e.g., [4, Definition 5.2.1]) if $q \in \operatorname{span}_K\{i, j, \hbar\}$. Every quaternion $q \in \mathcal{Q}$ can be uniquely expressed as a sum $q = a + q_0$ of a scalar $a \in K$ and a pure quaternion q_0. We write $\overline{q} := a - q_0$ for the *conjugate* of q. The map that sends a quaternion to its conjugate is an involution.

If x is an element of either a quadratic field extension $L = K\left(\sqrt{\alpha}\right)$ of K or a quaternion algebra $\mathcal{Q} = \left(\frac{\alpha, \beta}{K}\right)$ over K, we write $N(x) := x\overline{x}$ and call it the *norm* of x. If the domain is not clear from the context, we write $N_{L/K}$ or $N_{\mathcal{Q}/K}$.

Remark 2.1. When $\mathcal{Q}$ is a quaternion algebra, the norm of q in the above sense should not be confused with the determinant of the endomorphism of $\mathcal{Q}$ defined by the multiplication by q, which is often also called the norm. For this reason, in [3, 4] the map $q \mapsto q\overline{q}$ is called the *reduced norm* and denoted nrd. In that manner, our terminology in the present paper agrees with the one used by Lam in [5] but not with the one used by Vigneras in [3] and Voight in [4].

Equivalence classes of valuations on K are called *places*. Throughout this paper, places are denoted using fraktur letters $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$. Every place of a global field is either *archimedean*, when it extends the standard absolute value on $\mathbb{Q}$ (then the field K is necessarily a number field) or *non-archimedean*. Over a global function field, every place is non-archimedean. To avoid monotonous repetitions, non-archimedean places will also be called *primes* (or *finite primes* when we want to emphasize the fact

that they are non-archimedean). The completion of K with respect to a place $\mathfrak{p}$ is denoted $K_\mathfrak{p}$. If $\mathfrak{p}$ is a finite prime, we write $\mathrm{ord}_\mathfrak{p} : K \to \mathbb{Z}$ to denote the corresponding (normalized) discrete valuation on K. The prime $\mathfrak{p}$ is called dyadic if $\mathrm{ord}_\mathfrak{p} 2 \neq 0$. The map $\mathrm{ord}_\mathfrak{p}$ induces a natural map $K^\times/K^{\times 2} \to \mathbb{Z}/2\mathbb{Z}$ on the group of square classes of K that is again denoted $\mathrm{ord}_\mathfrak{p}$.

If $\mathfrak{p}$ is an archimedean place, then the completion $K_\mathfrak{p}$ is isomorphic either to $\mathbb{C}$ or to $\mathbb{R}$. The places of the second kind are called *real*. The field K is *formally real* if -1 is not a sum of squares in K. Otherwise, it is called *non-real*. It is well known that a global field is formally real if and only if it contains at least one real place. We write $\mathrm{sgn}_\mathfrak{r} a$ for the sign of $a \in K$ with respect to the unique ordering of K induced by a real place $\mathfrak{r}$.

Given some nonzero elements $a_1, \ldots, a_n \in K$ we denote by $\langle a_1, \ldots, a_n \rangle$ the quadratic form $a_1 x_1^2 + \cdots + a_n x_n^2$. Further, if $\mathfrak{p}$ is a place and $a, b \in K^\times$ we write $(a, b)_\mathfrak{p}$ for the Hilbert symbol of a and b at $\mathfrak{p}$, that is

$$(a, b)_\mathfrak{p} := \begin{cases} 1 & \text{if } \left(\frac{a,b}{K_\mathfrak{p}}\right) \cong M_2 K_\mathfrak{p}, \\ -1 & \text{otherwise.} \end{cases}$$

Here, $M_2 K_\mathfrak{p}$ denotes the ring of 2×2 matrices with entries in $K_\mathfrak{p}$. The Hilbert symbol is symmetric, bi-multiplicative and for every $a, b \in K^\times$ and every place $\mathfrak{p}$ one has $(a, b)_\mathfrak{p} \cdot (a, b)_\mathfrak{p} = 1$. These three properties of the Hilbert symbol will be extensively used in the paper.

For a quadratic form $\xi = \langle a_1, \ldots, a_n \rangle$ we define its Hasse invariant $s_\mathfrak{p}\xi$ at $\mathfrak{p}$ by the formula (see e.g., [5, Definition V.3.17]):

$$s_\mathfrak{p}\xi := \prod_{i<j}(a_i, a_j)_\mathfrak{p}.$$

Given a quadratic form $\xi = \langle a_1, \ldots, a_n \rangle$ over K and a place $\mathfrak{p}$, we write $\xi \otimes K_\mathfrak{p}$ for the form over $K_\mathfrak{p}$ with the same entries as ξ. If $\mathfrak{r}$ is a real place, the form $\xi \otimes K_\mathfrak{r}$ is called *definite* if all its entries $a_1, \ldots, a_n$ have the same sign. Otherwise, it is called *indefinite*.

Finally, abusing the notation harmlessly, by $\log_{-1}$ we will denote the (unique) isomorphism from the multiplicative group $\{\pm 1\}$ to the additive group $\{0, 1\}$ with addition modulo 2.

3. Square roots of non-central elements

Let us begin by writing down the explicit formula for a square in quaternion algebra so that we can easily reference it in the discussion that follows.

Observation 3.1. If $q = q_0 + q_1 i + q_2 j + q_3 k \in \mathcal{Q}$ is a quaternion, then

$$\begin{aligned} q^2 &= (q_0^2 + q_1^2\alpha + q_2^2\beta - q_3^2\alpha\beta) + 2q_0 q_1 i + 2q_0 q_2 j + 2q_0 q_3 k \\ &= (2q_0^2 - N(q)) + 2q_0 \cdot (q_1 i + q_2 j + q_3 k). \end{aligned} \tag{1}$$

An immediate consequence of the previous observation is the following rather well-known fact.

Corollary 3.2. If $q \in \mathcal{Q}$ is a pure quaternion, then $q^2 \in Z(\mathcal{Q}) = K$.

Another direct consequence of Eq. (1) is the following observation that may be treated as a partial converse of Corollary 3.2.

Observation 3.3. Let $q \in \mathcal{Q}$ be a square root of some element $a \in K$. Then q is either pure or $q \in K$.

Proof:
Let $q = q_0 + q_1 i + q_2 j + q_3 k$. If $q^2 = a \in K$ then by Eq. (1) we have
$$2q_0 q_1 = 2q_0 q_2 = 2q_0 q_3 = 0.$$
Therefore, if q is not pure, that is if $q_0 \neq 0$, then $q_1 = q_2 = q_3 = 0$, hence $q \in K$. $\square$

Combining Corollary 3.2 with Observation 3.3 we see that for computing the square roots in quaternion algebras it is crucial to distinguish between the case when one computes a quaternionic square root of an element in K (i.e., in the center of $\mathcal{Q}$) and the case when the argument comes from $\mathcal{Q} \setminus Z(\mathcal{Q})$. It turns out that the latter case is, in fact, trivial and requires nothing more than high-school mathematics.

Algorithm 1. Let $\mathcal{Q} = \left(\frac{\alpha, \beta}{K} \right)$ be a quaternion algebra over a field K of characteristic $\operatorname{char} K \neq 2$. Given a quaternion $q = q_0 + q_1 i + q_2 j + q_3 k \in \mathcal{Q} \setminus Z(\mathcal{Q})$, this algorithm outputs its square root or reports a failure when q is not a square.

1. Check if the norm $N(q)$ of q is a square in K.

   (a) If it is not, then report a failure and quit.
   (b) If it is, let d be an element of K such that $d^2 = N(q)$.

2. Check if any of the following two elements is a square in K:
$$a_+ := \frac{q_0 + d}{2}, \qquad a_- := \frac{q_0 - d}{2}.$$

3. If neither of them is a square, then report a failure and quit.

4. Otherwise, fix r_0 such that either $r_0^2 = a_+$ or $r_0^2 = a_-$.

5. Set
$$r_1 := \frac{q_1}{2r_0}, \quad r_2 := \frac{q_2}{2r_0}, \quad r_3 := \frac{q_3}{2r_0}.$$

6. Output $z = r_0 + r_1 i + r_2 j + r_3 k$.

Proof of correctness:
Since the norm $N : \mathcal{Q} \to K$ is multiplicative, it is obvious that if $N(q) \notin K^2$, then q cannot be a square in $\mathcal{Q}$. This fact justifies the early exit in step (1a) of the algorithm. Assume that $N(q) = d^2$ and let $z = r_0 + r_1 i + r_2 j + r_3 k$ be the sought square root of q, if it exists. By Eq. (1) we have
$$q_1 = 2r_0 r_1, \qquad q_2 = 2r_0 r_2, \qquad q_3 = 2r_0 r_3.$$
It is, thus, clear that it suffices to find r_0. Again by Eq. (1) we may write
$$q_0 = r_0^2 + r_1^2 \alpha + r_2^2 \beta - r_3^2 \alpha\beta = r_0^2 + \left(\frac{q_1}{2r_0} \right)^2 \alpha + \left(\frac{q_2}{2r_0} \right)^2 \beta - \left(\frac{q_3}{2r_0} \right)^2 \alpha\beta.$$

The above formula can be rewritten in the form of a bi-quadratic equation:

$$4r_0^4 - 4q_0 r_0^2 + \left(q_1^2 \alpha + q_2^2 \beta - q_3^2 \alpha\beta\right) = 0.$$

If we treat the left-hand-side as a quadratic equation in r_0^2, then its discriminant equals $16 \cdot N(q) = (4d)^2$, hence

$$r_0^2 = \frac{q_0 \pm d}{2} = a_\pm.$$

It follows that the sought quaternion z exists if and only if either a_+ or a_- is a square in K. This proves the correctness of the algorithm. $\qquad\square$

Remark 3.4. In the above proof, we constructed the square root z of a quaternion $q \in \mathcal{Q} \setminus Z(\mathcal{Q})$ by solving a bi-quadratic equation. Such equations in general, may have four roots. Hence, one may suspect that there are four distinct quaternions z such that $z^2 = q$. It is not the case. It is clear from the above proof that $q \in \mathcal{Q} \setminus Z(\mathcal{Q})$ has only finitely many square roots in $\mathcal{Q}$. Now, if $z^2 \in \mathbb{Q}$, then z is a root of a quaternionic polynomial $x^2 - q$. But [6, Theorem 5] asserts that a quadratic polynomial over $\mathcal{Q}$ which has more than two zeros must have infinitely many of them. This way, we conclude that q has just two square roots. Notice that for hamiltonian quaternions this fact has been observed already 80 years ago by Niven in [2].

4. Square roots of central elements. Split case

It is evident from the preceding section that the only non-trivial case that must be considered is how to compute a quaternionic square root of an element of the base field K, which is not a square in K. In contrast to the previous case (cf. Remark 3.4), in general, an element $a \in K = Z(\mathcal{Q})$ may have infinitely many square roots in $\mathcal{Q}$. Once again, for hamiltonian quaternions it has been observed already by Niven.

First, we need, however, to introduce an auxiliary algorithm that is not specific to quaternions, as it deals with an arbitrary quadratic form. Recall that a quadratic form is called *isotropic* (see e.g., [5, Definition I.3.1]) if it represents zero non-trivially. It is well known (see, e.g., [5, Theorem I.3.4]) that every isotropic form represents all elements of K.

Algorithm 2. Let ξ be an isotropic quadratic form of dimension n over a field K of characteristic char $K \neq 2$. Given an element $a \in K$ and a vector $V \in K^n$ such that $\xi(V) = 0$, this algorithm outputs a vector $W \in K^n$ satisfying the condition $\xi(W) = a$.

1. Find a vector $U \in K^n$ such that U and V are linearly independent.

2. Set $b := \xi(U)$ and $c := \frac{1}{2} \cdot \left(\xi(U + V) - \xi(U)\right)$.

3. Output

$$W := U + \frac{a - b}{2c} \cdot V.$$

Proof of correctness:
Just compute:

$$
\begin{aligned}
\xi(W) &= \xi\left(U + \frac{a-b}{2c} \cdot V\right) \\
&= \xi(U) + \frac{a-b}{2c} \cdot \big(\xi(U+V) - \xi(U) - \xi(V)\big) + \frac{(a-b)^2}{4c^2}\xi(V) \\
&= b + \frac{a-b}{2c} \cdot 2c + 0 = a \qquad\qquad \square
\end{aligned}
$$

Recall that a quaternion algebra $\mathcal{Q} = \left(\frac{\alpha,\beta}{K}\right)$ is said to *split* (see e.g., [4, Definition 5.4.5]) if $\mathcal{Q}$ is isomorphic to the matrix ring $M_2 K$. It is well known (see e.g., [4, Theorem 5.4.4] or [5, Theorem III.2.7]) that $\mathcal{Q}$ is split if and only if the quadratic form $\langle -\alpha, -\beta, \alpha\beta \rangle$ is isotropic. If it is the case, the preceding algorithm combined with Eq. (1) lets us compute the quaternionic square root of any element of the base field. In particular, when K is a global field, $\operatorname{char} K \neq 2$, then the computation of the square root of $a \in K$ in a split quaternion algebra boils down to solving a norm equation in a quadratic extension of K. Algorithms for the latter task are well known. They can be found in [7, 8, 9, 10, 11].

Algorithm 3. Let $\mathcal{Q} = \left(\frac{\alpha,\beta}{K}\right)$ be a split quaternion algebra over a global field K of characteristic $\operatorname{char} K \neq 2$. Given a nonzero element $a \in K$, this algorithm outputs a pure quaternion $\mathfrak{q} \in \mathcal{Q}$ such that $\mathfrak{q}^2 = a$.

1. Check if α is a square in K. If there is $c \in K^\times$ such that $c^2 = \alpha$, then set $V := (0, c, 1)$.

2. Otherwise, if $\alpha \notin K^{\times 2}$, then:

   (a) Construct a quadratic field extension $L = K\left(\sqrt{\alpha}\right)$ of K.

   (b) Solve the norm equation
   $$
   N_{L/K}(x) = -\frac{\alpha}{\beta}
   $$
   and denote the solution by $\lambda = b + c\sqrt{\alpha}$.

   (c) Set $V := (1, b, c)$.

3. Let $\xi := \langle -\alpha, -\beta, \alpha\beta \rangle$ be the pure subform of the norm form of $\mathcal{Q}$. Execute Algorithm 2 with the input $(-a, V, \xi)$ to construct a vector $W = (w_1, w_2, w_3)$ such that $\xi(W) = -a$.

4. Output $\mathfrak{q} = 0 + w_1 i + w_2 j + w_3 k$.

Proof of correctness:
We claim that the vector V constructed either in step (1) or in step (2) of the algorithm is an isotropic vector for ξ. First, suppose that α is a square in K. Say $\alpha = c^2$ for some $c \in K^\times$. Then

$$
-\alpha \cdot 0^2 - \beta \cdot c^2 + \alpha\beta \cdot 1^2 = 0.
$$

Conversely, assume that $\alpha \notin K^{\times 2}$ and so $L = K\left(\sqrt{\alpha}\right)$ is a proper extension of K. Let $\lambda = b + c\sqrt{\alpha}$ be an element of L such that $N(\lambda) = -\alpha/\beta$. Then

$$-\frac{\alpha}{\beta} = \lambda\overline{\lambda} = b^2 - \alpha c^2.$$

It follows that

$$-\alpha \cdot 1^2 - \beta \cdot b^2 + \alpha\beta \cdot c^2 = 0.$$

Hence, in both cases V is an isotropic vector of ξ, as claimed. Consequently, executing Algorithm 2 in step (3) we obtain a vector W satisfying the condition $\xi(W) = -a$. Now, by Eq. (1) the square of the quaternion q outputted by the algorithm equals

$$q^2 = -N(q) = -\xi(W) = a.$$

Thus, to conclude the proof, we only need to show that the norm equation in step (2b) is solvable. But this follows immediately from the fact that $\mathfrak{Q}$ is split. Hence ξ is isotropic. Indeed, if $V = (v_1, v_2, v_3)$ is an isotropic vector of ξ, then

$$-\alpha \cdot v_1^2 - \beta \cdot v_2^2 + \alpha\beta \cdot v_3^2 = 0.$$

Observe that v_1 must be nonzero since otherwise, α would be a square. It follows that

$$-\frac{\alpha}{\beta} = \left(\frac{v_2}{v_1}\right)^2 - \alpha\left(\frac{v_3}{v_1}\right)^2 = N_{L/K}\left(\frac{v_2}{v_1} + \frac{v_3}{v_1}\sqrt{\alpha}\right).$$

Therefore, the norm equation is solvable, as claimed. $\square$

Remark 4.1. The construction of the isotropic vector V in steps (1–2) of Algorithm 3 is equivalent to establishing an explicit isomorphism $\mathfrak{Q} \cong M_2 K$. For details, see [5, Chapter III]. Of course, if the quaternion algebra $\mathfrak{Q}$ is fixed, the vector V should be computed only once and cached between successive computations of square roots.

Remark 4.2. If the isomorphism $\mathfrak{Q} \cong M_2 K$ is a priori known explicitly, then the computation of the quaternionic square root of any $a \in K^\times$ trivializes, as we have the identity

$$\begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

5. Square roots of central elements. Non-split case

Now the only case left to be dealt with is when $a \in K^\times$ but $\mathfrak{Q}$ is not split. Here we have to solve not one but two norm equations (see Algorithm 5 below). First, however, we need to introduce the following auxiliary algorithm that constructs an element simultaneously represented by two binary

forms. Recall (see e.g., [5, Definition I.2.1]) that for a given quadratic form ξ of dimension d, we denote the set of nonzero elements of K represented by ξ by the symbol

$$D_K(\xi) := \big\{ \xi(V) \mid V \in K^d \text{ and } \xi(V) \neq 0 \big\}.$$

Let $\mathfrak{P}$ be any finite set of primes of K. Recall that an element $a \in K^\times$ is called $\mathfrak{P}$-*singular* if $\mathrm{ord}_\mathfrak{p} \, a \equiv 0 \pmod 2$ for all finite primes $\mathfrak{p} \notin \mathfrak{P}$. The set of all $\mathfrak{P}$-singular elements forms a subgroup of the group $K^\times$ containing $K^{\times 2}$. Thus, the notion of $\mathfrak{P}$-singularity generalizes naturally to the square classes. Define the set

$$\mathbb{E}_\mathfrak{P} := \big\{ aK^{\times 2} \mid a \text{ is } \mathfrak{P}\text{-singular} \big\}$$

of $\mathfrak{P}$-singular square classes. It is a subgroup of the group $K^\times/K^{\times 2}$ of square classes of K, hence a vector space over $\mathbb{F}_2$. It is known that the dimension of this vector space is finite. In fact it equals (see e.g., [12, p. 607])

$$\dim_{\mathbb{F}_2} \mathbb{E}_\mathfrak{P} = |\mathfrak{P}| + \dim_{\mathbb{F}_2} C_\mathfrak{P}/C_\mathfrak{P}^2,$$

where $C_\mathfrak{P}$ is the $\mathfrak{P}$-class group of K. There is a number of known algorithms to construct a basis of this vector space. For details see e.g., [13, 14, 15].

Before we present the next algorithm it is crucial to point out that the set of non-archimedean places of a global field K is countable. All the places of K can be arranged into an infinite sequence $\mathfrak{q}_1, \mathfrak{q}_2, \dots$. One possible way to do that is the following one. If K is a number field, let $p_1, p_2, p_3, \dots = 2, 3, 5, \dots$ be the (strictly increasing) sequence of all prime numbers. On the other hand, if K is a global function field, i.e., a finite extension of a rational function field $\mathbb{F}_q(x)$, let $p_1 = 1/x$ and $p_2, p_3, p_4, \dots$ be a sequence of all the irreducible polynomials from $\mathbb{F}_q[x]$ ordered in such a way that $\deg p_j \leq \deg p_{j+1}$ for every j. Now, we can first take the places of K that extend p_1, then the ones that extend p_2, then p_3, and so on. Consequently, it is possible to iterate over the set of primes of K. This observation will be indispensable for the rigorous proof of correctness of the algorithm that follows.

Algorithm 4. Let K be a global field of characteristic $\mathrm{char}\, K \neq 2$. Given two binary quadratic forms $\xi = \langle x_0, x_1 \rangle$ and $\zeta = \langle z_0, z_1 \rangle$ over K with $x_0, x_1, z_0, z_1 \neq 0$, this algorithm outputs a nonzero element $d \in K^\times$ such that $d \in D_K(\xi) \cap D_K(\zeta)$ or reports a failure if there is no such d.

1. If $-x_0 x_1$ is a square in K, then output z_0 and quit.

2. Likewise, if $-z_0 z_1$ is a square in K, then output x_0 and quit.

3. Check (using e.g., [16, Algorithm 5]) whether the form

$$\xi \perp (-\zeta) = \langle x_0, x_1, -z_0, -z_1 \rangle$$

   is isotropic. If it is not, then report a failure and quit.

4. Construct a set $\mathfrak{P}$ consisting of all dyadic places of K (if there are any) and of all these non-dyadic primes of K where at least one of the elements x_0, x_1, z_0, z_1 has an odd valuation.

5. If K is a formally real number field, then:

(a) Construct the set $\mathfrak{R}$ of all the real places of K, where either ξ or ζ is definite and denote its cardinality by r, i.e.

$$\mathfrak{R} = \{\mathfrak{r} \mid \mathrm{sgn}_{\mathfrak{r}}\, x_0 x_1 = 1 \text{ or } \mathrm{sgn}_{\mathfrak{r}}\, z_0 z_1 = 1\}, \qquad r = |\mathfrak{R}|.$$

(b) [Notation only] Let $\mathfrak{r}_1, \ldots, \mathfrak{r}_r$ be all the elements of $\mathfrak{R}$.

(c) Construct a vector $W = (w_1, \ldots, w_r) \in \{0, 1\}^r$ setting

$$w_i = \begin{cases} \log_{-1} \mathrm{sgn}_{\mathfrak{r}_i}\, x_0 & \text{if } \mathrm{sgn}_{\mathfrak{r}_i}\, x_0 x_1 = 1, \\ \log_{-1} \mathrm{sgn}_{\mathfrak{r}_i}\, z_0 & \text{if } \mathrm{sgn}_{\mathfrak{r}_i}\, x_0 x_1 = -1. \end{cases}$$

Otherwise, if the field K is non-real, set $\mathfrak{R} := \emptyset$, $r = 0$ and $W := ()$.

6. Repeat the following steps until the sought element d is found:

   (a) [Notation only] Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be all the elements of $\mathfrak{P}$.

   (b) Construct a basis $\mathscr{B} = \{\beta_1, \ldots, \beta_k\}$ of the group $\mathbb{E}_{\mathfrak{P}}$ of $\mathfrak{P}$-singular square classes.

   (c) Construct vectors $U = (u_1, \ldots, u_s)$ and $V = (v_1, \ldots, v_s)$ setting

   $$u_i = \log_{-1}(x_0, x_1)_{\mathfrak{p}_i} \qquad \text{and} \qquad v_i = \log_{-1}(z_0, z_1)_{\mathfrak{p}_i}.$$

   (d) Construct matrices $A = (a_{ij})$ and $B = (b_{ij})$, with $k = |\mathscr{B}|$ columns and $s = |\mathfrak{P}|$ rows, setting

   $$a_{ij} = \log_{-1}(-x_0 x_1, \beta_j)_{\mathfrak{p}_i} \qquad \text{and} \qquad b_{ij} = \log_{-1}(-z_0 z_1, \beta_j)_{\mathfrak{p}_i}.$$

   (e) If $\mathfrak{R} \neq \emptyset$ construct a matrix $C = (c_{ij})$ with k columns and $r = |\mathfrak{R}|$ rows, setting

   $$c_{ij} = \log_{-1} \mathrm{sgn}_{r_i}\, \beta_j.$$

   Otherwise, when $\mathfrak{R} = \emptyset$, set $C = ()$.

   (f) Check if the following system of $\mathbb{F}_2$-linear equations has a solution

   $$\left(\frac{\frac{A}{B}}{C} \right) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} U \\ \hline V \\ \hline W \end{pmatrix} \qquad (\mathfrak{Y})$$

   (g) If it does, denote the solution by $(\varepsilon_1, \ldots, \varepsilon_k) \in \{0, 1\}^k$. Output $d = \beta_1^{\varepsilon_1} \cdots \beta_k^{\varepsilon_k}$ and quit.

   (h) If the system $(\mathfrak{Y})$ has no solution, then append to $\mathfrak{P}$ the first prime $\mathfrak{q}_j$ of K that is not yet in $\mathfrak{P}$ (see the comment preceding the algorithm) and reiterate the loop.

Proof of correctness:

First, suppose that $-x_0 x_1$ is a square in K. This means that the form ξ is isotropic (see, e.g., [5, Theorem I.3.2]). Hence, by [5, Theorem I.3.4] it represents every element of K. In particular, it represents z_0. Since ζ also represents z_0 (trivially), step (1) of the algorithm outputs the correct result. The same argument also applies to step (2), when it is the form ζ that is isotropic. It is also clear that the sets $D_K(\xi)$ and $D_K(\zeta)$ of elements represented by ξ and ζ, intersect if and only if $\xi \perp (-\zeta)$ is isotropic. This justifies the test in step (3). Therefore, without loss of generality, for the remainder of the proof, we may assume that $\xi \perp (-\zeta)$ is isotropic while both forms ξ and ζ are anisotropic.

We will first show that the algorithm terminates. Let $W = (w_0, w_1, w_2, w_3) \in K^4$ be an isotropic vector of $\xi \perp (-\zeta)$. Denote $e := \xi(w_0, w_1) = \zeta(w_2, w_3)$. Further, let $\mathfrak{R}$ and $\mathfrak{P}$ be the sets of places (real and non-archimedean, respectively) constructed in steps (4–5) of the algorithm. We shall now apply [17, Lemma 2.1]. In the notation of [17] we take S to be the union of $\mathfrak{P}$ and the set of all non-archimedean places of K. In particular, S contains $\mathfrak{R}$. For every prime $\mathfrak{p} \in \mathfrak{P}$ we set $n(\mathfrak{p}) := 1 + \mathrm{ord}_{\mathfrak{p}} 4$. For real places $\mathfrak{r} \in \mathfrak{R}$, take $n(\mathfrak{r}) := 1$. For non-archimedean places $\mathfrak{p} \notin \mathfrak{R}$, the choice of $n(\mathfrak{p})$ is irrelevant. As in [17], let $\mathfrak{m} = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{n(\mathfrak{p})}$ be a modulus. Next, take $b_{\mathfrak{p}} := e$ for every $\mathfrak{p} \in S$. Moreover, if K is a global function field, pick one more prime not in S and denote[1] it $\mathfrak{p}_*$ and set the corresponding exponent to be 2. Then [17, Lemma 2.1] asserts that there exists a finite prime $\mathfrak{p}_0$ of K (denoted q in [17]) and an element $d \in K^\times$ (denoted b ibid) such that:

i. $\mathrm{ord}_{\mathfrak{p}} d = 0$ for every finite prime $\mathfrak{p} \notin \mathfrak{P} \cup \{\mathfrak{p}_0\}$, except that if K is a global function field, at the singled out prime $\mathfrak{p}_*$ the valuation $\mathrm{ord}_{\mathfrak{p}_*} d$ is even but possibly nonzero;

ii. $d \equiv e \pmod{\mathfrak{p}^{1 + \mathrm{ord}_{\mathfrak{p}} 4}}$ for every $\mathfrak{p} \in \mathfrak{P}$;

iii. $\mathrm{ord}_{\mathfrak{p}_0} d = 1$;

iv. $\mathrm{sgn}_{\mathfrak{r}} d = \mathrm{sgn}_{\mathfrak{r}} e$ for every real places $\mathfrak{r}$ of K.

Let $\mathscr{B} = \{\beta_1, \ldots, \beta_k\}$ be a basis of the group $\mathbb{E}_{\mathfrak{P} \cup \{\mathfrak{p}_0\}}$ of $(\mathfrak{P} \cup \{\mathfrak{p}_0\})$-singular square classes. The element d is $(\mathfrak{P} \cup \{\mathfrak{p}_0\})$-singular, hence it can be expressed in the form

$$d = \beta_1^{\varepsilon_1} \cdots \beta_k^{\varepsilon_k},$$

where $\varepsilon_1, \ldots, \varepsilon_k \in \mathbb{F}_2$ are the coordinates of d with respect to $\mathscr{B}$.

Fix a real place $\mathfrak{r}_i \in \mathfrak{R}$. First, suppose that $\mathrm{sgn}_{\mathfrak{r}_i} x_0 x_1 = 1$, so the form $\xi \otimes K_{\mathfrak{r}_i}$ is definite. Then $\mathrm{sgn}_{\mathfrak{r}_i}(-d) = \mathrm{sgn}_{\mathfrak{r}_i}(-e) = \mathrm{sgn}_{\mathfrak{r}_i} x_0$ since $\langle -e, x_0, x_1 \rangle$ is isotropic. But this implies that

$$\prod_{j=1}^{k} (-1)^{c_{ij} \varepsilon_j} = \prod_{j=1}^{k} \mathrm{sgn}_{\mathfrak{r}_i} \beta_j^{\varepsilon_j} = \mathrm{sgn}_{\mathfrak{r}_i} d = \mathrm{sgn}_{\mathfrak{r}_i} x_0 = (-1)^{w_i}.$$

Consequently

$$c_{i1} \varepsilon_1 + \cdots + c_{ik} \varepsilon_k = w_i. \tag{2}$$

Conversely, assume that $\xi \otimes K_{\mathfrak{r}_i}$ is indefinite, hence $\zeta \otimes K_{\mathfrak{r}_i}$ must be definite. Applying the same arguments to the form ζ instead of ξ, we show that Eq. (2) also holds in this case.

---

[1] This prime is denotes p_0 in [17], but we will not use this symbol as it would contradict the notation in the rest of the proof.

Now fix a finite prime $\mathfrak{p}_i \in \mathfrak{P}$. Observe that by the local square theorem (see, e.g., [5, Theorem VI.2.19]) condition (ii) implies that the local squares classes $dK_{\mathfrak{p}_i}^{\times 2}$ and $eK_{\mathfrak{p}_i}^{\times 2}$ coincide. It follows that the form

$$\langle -d, x_0, x_1 \rangle \otimes K_{\mathfrak{p}_i} \cong \langle -e, x_0, x_1 \rangle \otimes K_{\mathfrak{p}_i}$$

is isotropic. Now, [5, Proposition V.3.22] asserts that the Hasse invariant of $\langle -d, x_0, x_1 \rangle \otimes K_{\mathfrak{p}_i}$ equals

$$s_{\mathfrak{p}_i}\langle -d, x_0, x_1 \rangle = (-1, x_0 x_1 \cdot d)_{\mathfrak{p}_i}. \tag{3}$$

Using the definition of the Hasse invariant and properties of the Hilbert symbol we can rewrite the above condition as follows

$$\begin{aligned}
1 &= s_{\mathfrak{p}_i}\langle -d, x_0, x_1 \rangle \cdot (-1, x_0 x_1 \cdot d)_{\mathfrak{p}_i} \\
&= (-d, x_0)_{\mathfrak{p}_i}(-d, x_1)_{\mathfrak{p}_i}(x_0, x_1)_{\mathfrak{p}_i}(-1, x_0 x_1)_{\mathfrak{p}_i}(-1, d)_{\mathfrak{p}_i} \\
&= (-d, x_0 x_1)_{\mathfrak{p}_i}(-1, x_0 x_1)_{\mathfrak{p}_i}(-1, d)_{\mathfrak{p}_i}(x_0, x_1)_{\mathfrak{p}_i} \\
&= (d, x_0 x_1)_{\mathfrak{p}_i}(-1, d)_{\mathfrak{p}_i}(x_0, x_1)_{\mathfrak{p}_i} \\
&= (-x_0 x_1, d)_{\mathfrak{p}_i}(x_0, x_1)_{\mathfrak{p}_i}.
\end{aligned}$$

Therefore, formula (3) is equivalent to the following one:

$$(-x_0 x_1, d)_{\mathfrak{p}_i} = (x_0, x_1)_{\mathfrak{p}_i}.$$

Substituting $\beta_1^{\varepsilon_1} \cdots \beta_k^{\varepsilon_k}$ for d we obtain

$$\prod_{j=1}^{k} (-x_0 x_1, \beta_j)_{\mathfrak{p}_i}^{\varepsilon_j} = (x_0, x_1)_{\mathfrak{p}_i}.$$

Now, $(x_0, x_1)_{\mathfrak{p}_i} = (-1)^{u_i}$ and $(-x_0 x_1, \beta_j)_{\mathfrak{p}_i} = (-1)^{a_{ij}}$, where $u_i, a_{ij} \in \{0, 1\}$ are the elements constructed in steps (6c–6d). Therefore, the last condition can be expressed as a linear equation over $\mathbb{F}_2$:

$$a_{i1}\varepsilon_1 + \cdots + a_{ik}\varepsilon_k = u_i. \tag{4}$$

Finally, we will show that the above equation also holds for the index $i = 0$, that is for the prime $\mathfrak{p}_0$ appended to $\mathfrak{P}$. This fact follows from Hilbert reciprocity law (see, e.g., [5, Theorem VI.5.5]). We already know that for every $i \in \{1, \ldots, s\}$ we have

$$(-x_0 x_1, d)_{\mathfrak{p}_i} = (x_0, x_1)_{\mathfrak{p}_i}.$$

The same also holds for primes not in $\mathfrak{P}$. Indeed, if $\mathfrak{q} \notin \mathfrak{P} \cup \{\mathfrak{p}_0\}$ then $\mathfrak{q}$ is non-dyadic and all three elements x_0, x_1 and d have even valuations at $\mathfrak{q}$. Consequently, by [5, Corollary VI.2.5] one obtains

$$(-x_0 x_1, d)_{\mathfrak{q}} = (x_0, x_1)_{\mathfrak{q}} = 1.$$

Now, by Hilbert reciprocity law, we can write

$$
\begin{aligned}
1 &= \prod_{\mathfrak{p}}(-x_0 x_1, d)_{\mathfrak{p}} \cdot \prod_{\mathfrak{p}}(x_0, x_1)_{\mathfrak{p}} \\
&= (-x_0 x_1, d)_{\mathfrak{p}_0}(x_0, x_1)_{\mathfrak{p}_0} \cdot \prod_{\mathfrak{p} \in \mathfrak{P}}\Big((-x_0 x_1, d)_{\mathfrak{p}}(x_0, x_1)_{\mathfrak{p}}\Big) \cdot \prod_{\mathfrak{q} \notin \mathfrak{P} \cup \{\mathfrak{p}_0\}}\Big((-x_0 x_1, d)_{\mathfrak{q}}(x_0, x_1)_{\mathfrak{q}}\Big) \\
&= (-x_0 x_1, d)_{\mathfrak{p}_0}(x_0, x_1)_{\mathfrak{p}_0}.
\end{aligned}
$$

Hence, in the same way as above, we show that Eq. (4) also holds for $i = 0$. Applying the same arguments to the form ζ, we obtain

$$
b_{i1}\varepsilon_1 + \cdots + b_{ik}\varepsilon_k = v_i, \tag{5}
$$

for all $i \in \{0, 1, \ldots, s\}$.

All in all, we have proved that Eq. ($\wp$) has a solution in $\mathbb{E}_{\mathfrak{P} \cup \{\mathfrak{p}_0\}}$. Now, for every $\mathfrak{P}' \supseteq \mathfrak{P} \cup \{\mathfrak{p}_0\}$ we have $\mathbb{E}_{\mathfrak{P} \cup \{\mathfrak{p}_0\}} \subseteq \mathbb{E}_{\mathfrak{P}'}$, hence once the prime $\mathfrak{p}_0$ is appended to $\mathfrak{P}$ the algorithm terminates (see also Remark 5.1 w below).

Now, when we have proved that the algorithm stops, we must show that it outputs a correct result. To this end, we will show that the forms $\langle -d, x_0, x_1 \rangle$ and $\langle -d, z_0, z_1 \rangle$ are locally isotropic in every completion of K. The assumptions are symmetric with respect to both forms, except in real places. Hence it generally suffices to prove the isotropy of one of them.

Both forms are trivially isotropic in all complex completions of K (provided that there are any) and in all real completions $K_\mathfrak{r}$ for $\mathfrak{r} \notin \mathfrak{R}$. Fix now a real place $\mathfrak{r}_i \in \mathfrak{R}$. First, assume that the form $\langle x_0, x_1 \rangle \otimes K_{\mathfrak{r}_i}$ is definite. From the preceding part we know that the element $d = \beta_1^{\varepsilon_1} \cdots \beta_k^{\varepsilon_k}$, constructed by the algorithm, satisfies the condition $\mathrm{sgn}_{\mathfrak{r}_i} d = \mathrm{sgn}_{\mathfrak{r}_i} x_0$. Therefore the form $\langle -d, x_0, x_1 \rangle \otimes K_{\mathfrak{r}_i}$ is isotropic. Now, the form $\xi \perp (-\zeta)$ is isotropic because otherwise, the execution of the algorithm would have been interrupted already in step (3). Thus, either $\mathrm{sgn}_{\mathfrak{r}_i} z_0 = \mathrm{sgn}_{\mathfrak{r}_i} x_0 = \mathrm{sgn}_{\mathfrak{r}_i} d$ or $\mathrm{sgn}_{\mathfrak{r}_i} z_1 = \mathrm{sgn}_{\mathfrak{r}_i} x_0 = \mathrm{sgn}_{\mathfrak{r}_i} d$. In both cases, we have that the form $\langle -d, z_0, z_1 \rangle \otimes K_{\mathfrak{r}_i}$ is isotropic, as well. Conversely, assume that $\xi \otimes K_{\mathfrak{r}_i}$ is indefinite, and so it is $\zeta \otimes K_{\mathfrak{r}_i}$ that must be definite. Then, $\langle -d, x_0, x_1 \rangle \otimes K_{\mathfrak{r}_i}$ is trivially isotropic and to the form $\langle -d, z_0, z_1 \rangle \otimes K_{\mathfrak{r}_i}$ we apply the some argument as to the form $\langle -d, x_0, x_1 \rangle \otimes K_{\mathfrak{r}_i}$ in the previous case.

We may now concentrate on finite primes. Fix a prime $\mathfrak{p}$. Suppose $\mathfrak{p}$ is not among the primes constituting $\mathfrak{P}$ (here, we allow $\mathfrak{P}$ to have been already enlarged during the execution of the algorithm). In that case, $\mathfrak{p}$ is certainly non-dyadic, and all three elements x_0, x_1, and d have even valuations at $\mathfrak{p}$. Hence, [5, Corollary VI.2.5] asserts that $\langle -d, x_0, x_1 \rangle \otimes K_\mathfrak{p}$ is isotropic. On the other hand, we know from the first part of the proof that if $\mathfrak{p} = \mathfrak{p}_i \in \mathfrak{P}$, then d satisfies the condition $(-x_0 x_1, d)_\mathfrak{p} = (x_0, x_1)_\mathfrak{p}$, which is equivalent to $s_\mathfrak{p}\langle -d, x_0, x_1 \rangle = (-1, x_0 x_1 \cdot d)_\mathfrak{p}$. The later condition implies that $\langle -d, x_0, x_1 \rangle \otimes K_\mathfrak{p}$ is isotropic, again by [5, Proposition V.3.22]. The very same arguments may be applied to the form $\langle -d, z_0, z_1 \rangle \otimes K_\mathfrak{p}$.

All in all, we have shown that the forms $\langle -d, x_0, x_1 \rangle$ and $\langle -d, z_0, z_1 \rangle$ are locally isotropic in every completion of K. Thus, they are isotropic over K by the Hasse–Minkowski principle (see e.g., [5, Theorem VI.3.1]). This means that the forms ξ and ζ represent d over K by [5, Corollary I.3.5]. □

Remark 5.1. To rigorously prove that Algorithm 4 terminates, we used the fact that it is possible to iterate over the primes of K arranging all of them into a sequence. Hence, after finitely many steps the prime $\mathfrak{p}_0$, specified in the proof of correctness, is appended to $\mathfrak{P}$ and so the algorithm stops. However, it does not present a complete picture. We proved that the corresponding prime $\mathfrak{p}_0$ exists using [17, Lemma 2.1]. If one analyzes the proof of this lemma, one will realize that the authors rely on Chebotarev's density theorem to show that the set of primes satisfying the assertions of the lemma has positive density (hence is non-empty, consequently the corresponding prime exists). This means that in a practical implementation, in step (6h) of the algorithm it is possible to actually add primes to $\mathfrak{P}$ at random. If the density of the set mentioned above is $d \in (0, 1]$, then the probability that the system (2) fails to be solvable after n steps is $(1 - d)^n$, for sufficiently large n. Hence, it diminishes expotentially with the number of iterations.

We are now in a position to present an algorithm that computes a square root of a scalar in a non-split quaternion algebra.

Algorithm 5. Let $\mathcal{Q} = \left(\frac{\alpha, \beta}{K}\right)$ be a non-split quaternion algebra over a global field of characteristic char $K \neq 2$. Given a nonzero element $a \in K$ this algorithm outputs a quaternion $q \in \mathcal{Q}$ such that $q^2 = a$ or reports a failure if a is not a square in $\mathcal{Q}$.

1. Check if a is a square in K. If there is $c \in K^\times$ such that $a = c^2$, then output $q = c + 0i + 0j + 0k$ and quit.

2. Check if $a\alpha$ is a square in K. If there is $c \in K^\times$ such that $a\alpha = c^2$, then output $q = 0 + (c/\alpha)i + 0j + 0k$ and quit.

3. Check if $a\beta$ is a square in K. If there is $c \in K^\times$ such that $a\beta = c^2$, then output $q = 0 + 0i + (c/\beta)j + 0k$ and quit.

4. Execute Algorithm 4 with input $\xi = \langle a, -\alpha \rangle$ and $\zeta = \langle \beta, -\alpha\beta \rangle$. If it fails, then report a failure and quit. Otherwise, let $d \in K^\times$ denote the outputted element represented by these two binary forms.

5. Construct two quadratic extensions of K:

$$L := K\left(\sqrt{\alpha}\right) \qquad \text{and} \qquad M := K\left(\sqrt{a\alpha}\right).$$

6. Solve the following two norm equations:

$$\frac{d}{\beta} = N_{L/K}(x) \qquad \text{and} \qquad \frac{d}{a} = N_{M/K}(y).$$

Denote the solutions by

$$\lambda = l_0 + l_1\sqrt{\alpha} \qquad \text{and} \qquad \mu = m_0 + m_1\sqrt{a\alpha},$$

respectively.

7. Output $q = 0 + a \cdot \frac{m_1}{m_0}i + \frac{l_0}{m_0}j + \frac{l_1}{m_0}k.$

Proof of correctness:

The correctness of the results outputted in step (1) is obvious as is the correctness of output of steps (2–3). Indeed, if $a\alpha = c^2$ for some $c \in K^\times$ and $q = (c/\alpha)i$, then $q^2 = \alpha \cdot c^2/\alpha^2 = a$. In the remainder of the proof, we can, thus, assume that neither a nor $a\alpha$ is a square in K. Likewise, α is not a square, either, since otherwise, the quaternion algebra $\mathcal{Q}$ would split. Therefore, L and M are proper quadratic extensions of K. It follows from Observation 3.3 that a is a square of some pure quaternion $q = q_1 i + q_2 j + q_3 k$ if and only if

$$a \cdot 1^2 - \alpha \cdot q_1^2 = \beta \cdot q_2^2 - \alpha\beta \cdot q_3^2.$$

This equality is equivalent to the condition that the sets of elements of K represented by the binary forms $\xi = \langle a, -\alpha \rangle$ and $\zeta = \langle \beta, -\alpha\beta \rangle$ have a non-empty intersection. Thus, if Algorithm 4 executed in step (4) reports a failure, then a is not a square in $\mathcal{Q}$. Now, assume that Algorithm 4 returned some element $d \in D_K(\xi) \cap D_K(\zeta)$. Then there are $l_0, l_1, m_0, m_1 \in K$ such that

$$\begin{cases} d = am_0^2 - \alpha(am_1)^2 = a \cdot N_{M/K}\left(m_0 + m_1\sqrt{a\alpha}\right) \\ d = \beta l_0^2 - \alpha\beta l_1^2 = \beta \cdot N_{L/K}\left(l_0 + l_1\sqrt{\alpha}\right). \end{cases}$$

Rearranging the terms we have

$$a = \alpha\left(\frac{am_1}{m_0}\right)^2 + \beta\left(\frac{l_0}{m_0}\right)^2 - \alpha\beta\left(\frac{l_1}{m_0}\right)^2.$$

Now, the right-hand-side is nothing else but the square of the quaternion q constructed in step (7). This proves that the algorithm is correct. $\square$

References

[1] Heath T. A history of Greek mathematics. Vol. I. Dover Publications, Inc., New York, 1981. ISBN 0-486-24073-8. From Thales to Euclid, Corrected reprint of the 1921 original.

[2] Niven I. The roots of a quaternion. *Amer. Math. Monthly*, 1942. **49**:386–388. doi:10.2307/2303134. URL `https://doi.org/10.2307/2303134`.

[3] Vignéras MF. Arithmétique des algèbres de quaternions, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980. ISBN 3-540-09983-2.

[4] Voight J. Quaternion algebras, volume 288 of *Graduate Texts in Mathematics*. Springer, Cham, [2021] ©2021. ISBN 978-3-030-56692-0; 978-3-030-56694-4. doi:10.1007/978-3-030-56694-4. URL `https://doi.org/10.1007/978-3-030-56694-4`.

[5] Lam TY. Introduction to quadratic forms over fields, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005. ISBN 0-8218-1095-2.

[6] Gordon B, Motzkin TS. On the zeros of polynomials over division rings. *Trans. Amer. Math. Soc.*, 1965. **116**:218–226. doi:10.2307/1994114. URL `https://doi.org/10.2307/1994114`.

[7] Cohen H. Advanced topics in computational number theory, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. ISBN 0-387-98727-4. doi:10.1007/978-1-4419-8489-0. URL `https://doi.org/10.1007/978-1-4419-8489-0`.

[8] Fieker C, Jurk A, Pohst M. On solving relative norm equations in algebraic number fields. *Math. Comp.*, 1997. **66**(217):399–410. doi:10.1090/S0025-5718-97-00761-8. URL `https://doi.org/10.1090/S0025-5718-97-00761-8`.

[9] Fincke U, Pohst M. A procedure for determining algebraic integers of given norm. In: Computer algebra (London, 1983), volume 162 of *Lecture Notes in Comput. Sci.*, pp. 194–202. Springer, Berlin, 1983. doi:10.1007/3-540-12868-9_103. URL `https://doi.org/10.1007/3-540-12868-9_103`.

[10] Garbanati DA. An algorithm for finding an algebraic number whose norm is a given rational number. *J. Reine Angew. Math.*, 1980. **316**:1–13. doi:10.1515/crll.1980.316.1. URL `https://doi.org/10.1515/crll.1980.316.1`.

[11] Simon D. Solving norm equations in relative number fields using S-units. *Math. Comp.*, 2002. **71**(239):1287–1305. doi:10.1090/S0025-5718-02-01309-1. URL `https://doi.org/10.1090/S0025-5718-02-01309-1`.

[12] Czogała A. Witt rings of Hasse domains of global fields. *J. Algebra*, 2001. **244**(2):604–630. doi:10.1006/jabr.2001.8918. URL `https://doi.org/10.1006/jabr.2001.8918`.

[13] Cannon J, Bosma W, Fieker C, (eds) AS. Handbook of Magma Functions, 2.26-4 edition, 2021.

[14] Koprowski P. Computing singular elements modulo squares. *Fund. Inform.*, 2021. **179**(3):227–238. doi:10.3233/fi-2021-2022. URL `https://doi.org/10.3233/fi-2021-2022`.

[15] Koprowski P, Rothkegel B. The anisotropic part of a quadratic form over a number field. *J. Symbolic Comput.*, 2023. **115**:39–52. doi:10.1016/j.jsc.2022.07.003. URL `https://doi.org/10.1016/j.jsc.2022.07.003`.

[16] Koprowski P, Czogała A. Computing with quadratic forms over number fields. *J. Symbolic Comput.*, 2018. **89**:129–145. doi:10.1016/j.jsc.2017.11.009. URL `https://doi.org/10.1016/j.jsc.2017.11.009`.

[17] Leep D, Wadsworth A. The Hasse norm theorem mod squares. *J. Number Theory*, 1992. **42**(3):337–348. doi:10.1016/0022-314X(92)90098-A. URL `https://doi.org/10.1016/0022-314X(92)90098-A`.