1

Quaternion algebras

As a prelude to the book, we present here our main objects of study in the simplest case, that of quaternion algebras. Many concepts that will be ubiquitous in what follows, such as division algebras, splitting fields or norms appear here in a concrete and elementary context. Another important notion we shall introduce is that of the conic associated with a quaternion algebra; these are the simplest examples of Severi–Brauer varieties, objects to which a whole chapter will be devoted later. In the second part of the chapter two classic theorems from the 1930s are proven: a theorem of Witt asserting that the associated conic determines a quaternion algebra up to isomorphism, and a theorem of Albert that gives a criterion for the tensor product of two quaternion algebras to be a division algebra. The discussion following Albert's theorem will lead us to the statement of one of the main theorems proven later in the book, that of Merkurjev concerning division algebras of period 2.

The basic theory of quaternion algebras goes back to the nineteenth century. The original references for the main theorems of the last two sections are Witt [1] and Albert [1], [5], respectively.

1.1 Basic properties

In this book we shall study finite-dimensional algebras over a field. Here by an algebra over a field k we mean a k-vector space equipped with a not necessarily commutative but associative k-linear multiplication. All k-algebras will be tacitly assumed to have a unit element.

Historically the first example of a finite-dimensional noncommutative algebra over a field was discovered by W. R. Hamilton during a walk with his wife (presumably doomed to silence) on 16 October 1843. It is the *algebra of quaternions*, a 4-dimensional algebra with basis $1, i, j, k$ over the field $\mathbf{R}$ of real numbers, the multiplication being determined by the rules

$$i^2 = -1, \;\; j^2 = -1, \;\; ij = -ji = k.$$

This is in fact a *division algebra* over $\mathbf{R}$, which means that each nonzero element x has a two-sided multiplicative inverse, i.e. an element y with $xy = yx = 1$. Hamilton proved this as follows.

For a quaternion $q = x + yi + zj + wk$, introduce its *conjugate*

$$\overline{q} = x - yi - zj - wk$$

and its *norm* $N(q) = q\overline{q}$. A computation gives $N(q) = x^2 + y^2 + z^2 + w^2$, so if $q \neq 0$, the quaternion $\overline{q}/N(q)$ is an inverse for q.

We now come to an easy generalization of the above construction. *Henceforth in this chapter, unless otherwise stated, k will denote a field of characteristic not* 2.

Definition 1.1.1 For any two elements $a, b \in k^\times$ define the *(generalized) quaternion algebra* (a, b) as the 4-dimensional k-algebra with basis $1, i, j, ij$, multiplication being determined by

$$i^2 = a, \;\; j^2 = b, \;\; ij = -ji.$$

One calls the set $\{1, i, j, ij\}$ a *quaternion basis* of (a, b).

Remark 1.1.2 The isomorphism class of the algebra (a, b) depends only on the classes of a and b in $k^\times/k^{\times 2}$, because the substitution $i \mapsto ui, j \mapsto vj$ induces an isomorphism

$$(a, b) \xrightarrow{\sim} (u^2 a, v^2 b)$$

for all $u, v \in k^\times$. This implies in particular that the algebra (a, b) is isomorphic to (b, a); indeed, mapping $i \mapsto abj, j \mapsto abi$ we get

$$(a, b) \cong (a^2 b^3, a^3 b^2) \cong (b, a).$$

Given an element $q = x + yi + zj + wij$ of the quaternion algebra (a, b), we define its *conjugate* by

$$\overline{q} = x - yi - zj - wij.$$

The map $(a, b) \to (a, b)$ given by $q \mapsto \overline{q}$ is an anti-automorphism of the k-algebra (a, b), i.e. it is a k-vector space automorphism of (a, b) satisfying $\overline{(q_1 q_2)} = \overline{q}_2 \overline{q}_1$. Moreover, we have $\overline{\overline{q}} = q$; an anti-automorphism with this property is called an *involution* in ring theory.

We define the *norm* of $q = x + yi + zj + wij$ by $N(q) = q\overline{q}$. A calculation yields

$$N(q) = x^2 - ay^2 - bz^2 + abw^2 \in k, \tag{1.1}$$

so $N : (a, b) \to k$ is a *nondegenerate quadratic form*. The computation

$$N(q_1q_2) = q_1q_2\overline{q}_2\overline{q}_1 = q_1N(q_2)\overline{q}_1 = N(q_1)N(q_2)$$

shows that the norm is a multiplicative function, and the same argument as for Hamilton's quaternions yields:

Lemma 1.1.3 *An element q of the quaternion algebra (a, b) is invertible if and only if it has nonzero norm. Hence (a, b) is a division algebra if and only if the norm $N : (a, b) \to k$ does not vanish outside 0.*

Remark 1.1.4 In fact, one can give an intrinsic definition of the conjugation involution (and hence of the norm) on a quaternion algebra (a, b) which does not depend on the choice of the basis $(1, i, j, ij)$. Indeed, call an element q of (a, b) a *pure quaternion* if $q^2 \in k$ but $q \notin k$. A straightforward computation shows that a nonzero $q = x + yi + zj + wij$ is a pure quaternion if and only if $x = 0$. Hence a general q can be written uniquely as $q = q_1 + q_2$ with $q_1 \in k$ and q_2 pure, and conjugation is given by $\overline{q} = q_1 - q_2$. Moreover, a pure quaternion q satisfies $N(q) = -q^2$.

Example 1.1.5 (The matrix algebra $M_2(k)$) Besides the classical Hamilton quaternions, the other basic example of a quaternion algebra is the k-algebra $M_2(k)$ of 2×2 matrices. Indeed, the assignment

$$i \mapsto I := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad j \mapsto J := \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix}$$

defines an isomorphism $(1, b) \cong M_2(k)$, because the matrices

$$\mathrm{Id} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \ I = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \ J = \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix} \text{ and } IJ = \begin{bmatrix} 0 & b \\ -1 & 0 \end{bmatrix} \tag{1.2}$$

generate $M_2(k)$ as a k-vector space, and they satisfy the relations

$$I^2 = \mathrm{Id}, \quad J^2 = b\,\mathrm{Id}, \quad IJ = -JI.$$

Definition 1.1.6 A quaternion algebra over k is called *split* if it is isomorphic to $M_2(k)$ as a k-algebra.

Proposition 1.1.7 *For a quaternion algebra (a, b) the following statements are equivalent.*

1. *The algebra (a, b) is split.*
2. *The algebra (a, b) is not a division algebra.*
3. *The norm map $N : (a, b) \to k$ has a nontrivial zero.*
4. *The element b is a norm from the field extension $k(\sqrt{a})|k$.*

Of course, instead of (4) another equivalent condition is that a is a norm from the field extension $k(\sqrt{b})|k$.

Proof The implication $(1) \Rightarrow (2)$ is obvious and $(2) \Rightarrow (3)$ was proven in Lemma 1.1.3. For $(3) \Rightarrow (4)$ we may assume a is not a square in k, for otherwise the claim is obvious. Take a nonzero quaternion $q = x+yi+zj+wij$ with norm 0. Then equation (1.1) implies $(z^2 - aw^2)b = x^2 - ay^2$, and so in particular $z^2 - aw^2 = (z + \sqrt{a}w)(z - \sqrt{a}w) \neq 0$, for otherwise a would be a square in k. Denoting by $N_{K|k}$ the field norm from $K = k(\sqrt{a})$ we get

$$b = N_{K|k}(x + \sqrt{a}y)N_{K|k}(z + \sqrt{a}w)^{-1},$$

whence (4) by multiplicativity of $N_{K|k}$. Finally, we shall show assuming (4) that $(a, b) \cong (1, 4a^2)$, whence (1) by the isomorphism in Example 1.1.5. To see this, we may again assume that a is not a square in k. If b is a norm from K, then so is b^{-1}, so by (4) and our assumption on a we find $r, s \in k$ satisfying $b^{-1} = r^2 - as^2$. Putting $u = rj + sij$ thus yields $u^2 = br^2 - abs^2 = 1$. Moreover, one verifies that $ui = -iu$, which implies that the element $v = (1 + a)i + (1 - a)ui$ satisfies $uv = (1 + a)ui + (1 - a)i = -vu$ and $v^2 = (1 + a)^2a - (1 - a)^2a = 4a^2$. Passing to the basis $(1, u, v, uv)$ thus gives the required isomorphism $(a, b) \cong (1, 4a^2)$. □

Remark 1.1.8 Over a field of characteristic 2 one defines the generalized quaternion algebra $[a, b)$ by the presentation

$$[a, b) = \langle i, j \mid i^2 + i = a,\ j^2 = b,\ ij = ji + j \rangle$$

where $a \in k$ and $b \in k^\times$. This algebra has properties analogous to those in the above proposition (see Exercise 4).

1.2 Splitting over a quadratic extension

We now prove a structure theorem for division algebras of dimension 4. Recall first that the centre $Z(A)$ of a k-algebra A is the k-subalgebra consisting of

elements $x \in A$ satisfying $xy = yx$ for all $y \in A$. By assumption we have $k \subset Z(A)$; if this inclusion is an equality, one says that A is *central* over k. If A is a division algebra, then $Z(A)$ is a field. We then have:

Proposition 1.2.1 *A 4-dimensional central division algebra D over k is isomorphic to a quaternion algebra.*

We first prove:

Lemma 1.2.2 *If D contains a commutative k-subalgebra isomorphic to a nontrivial quadratic field extension $k(\sqrt{a})$ of k, then D is isomorphic to a quaternion algebra (a, b) for suitable $b \in k^\times$.*

Proof A k-subalgebra as in the lemma contains an element q with $q^2 = a \in k$. By assumption, q is not in the centre k of D and hence the inner automorphism of D given by $x \mapsto q^{-1}xq$ has exact order 2. As a k-linear automorphism of D, it thus has -1 as an eigenvalue, which means that there exists $r \in D$ such that $qr + rq = 0$. This relation shows that $r \notin k(q)$ (for otherwise r and q would commute), and therefore 1 and r form a basis of D as a 2-dimensional $k(q)$-vector space. It follows that the elements $1, q, r, qr$ form a k-basis of D and moreover they are fixed by the k-linear automorphism $x \mapsto r^{-2}xr^2$. Thus r^2 belongs to the centre of D, which is k by assumption. The lemma follows by setting $r^2 = b \in k^\times$. □

Proof of Proposition 1.2.1 Let d be an element of $D \setminus k$. As D is finite dimensional over k, the powers $\{1, d, d^2, \dots\}$ are linearly dependent, so there is a polynomial $f \in k[x]$ with $f(d) = 0$. As D is a division algebra, it has no zero divisors and we may assume f irreducible. This means there is a k-algebra homomorphism $k[x]/(f) \to D$ which realizes the field $k(d)$ as a k-subalgebra of D. Now the degree $[k(d) : k]$ cannot be 1 as $d \notin k$, and it cannot be 4 as D is not commutative. Hence $[k(d) : k] = 2$, and the lemma applies. □

The crucial ingredient in the above proof was the existence of a quadratic extension $k(\sqrt{a})$ contained in D. Observe that the algebra $D \otimes_k k(\sqrt{a})$ then splits over $k(\sqrt{a})$. In fact, it follows from basic structural results to be proven in the next chapter (Lemma 2.2.2 and Wedderburn's theorem) that any 4-dimensional central k-algebra for which there exists a quadratic extension of k with this splitting property is a division algebra or a matrix algebra.

It is therefore interesting to characterize those quadratic extensions of k over which a quaternion algebra splits.

Proposition 1.2.3 *Consider a quaternion algebra A over k, and fix an element $a \in k^\times \setminus k^{\times 2}$. The following statements are equivalent:*

1. *A is isomorphic to the quaternion algebra (a, b) for some $b \in k^\times$.*
2. *The $k(\sqrt{a})$-algebra $A \otimes_k k(\sqrt{a})$ is split.*
3. *A contains a commutative k-subalgebra isomorphic to $k(\sqrt{a})$.*

Proof To show (1) $\Rightarrow$ (2), note that $(a, b) \otimes_k k(\sqrt{a})$ is none but the quaternion algebra (a, b) defined over the field $k(\sqrt{a})$. But a is a square in $k(\sqrt{a})$, so $(a, b) \cong (1, b)$, and the latter algebra is isomorphic to $M_2(k(\sqrt{a}))$ by Example 1.1.5. Next, if A is split, the same argument shows that (1) always holds, so to prove (3) $\Rightarrow$ (1) one may assume A is nonsplit, in which case Lemma 1.2.2 applies.

The implication (2) $\Rightarrow$ (3) is easy in the case when $A \cong M_2(k)$: one chooses an isomorphism $M_2(k) \cong (1, a)$ as in Example 1.1.5 and takes the subfield $k(J)$, where J is the basis element with $J^2 = a$. We now assume A is nonsplit, and extend the quaternion norm N on A to $A \otimes_k k(\sqrt{a})$ by base change. Applying part (3) of Proposition 1.1.7 to $A \otimes_k k(\sqrt{a})$ one gets that there exist elements $q_0, q_1 \in A$, not both 0, with $N(q_0 + \sqrt{a}q_1) = 0$. Denote by $B : A \otimes_k k(\sqrt{a}) \times A \otimes_k k(\sqrt{a}) \to k(\sqrt{a})$ the symmetric bilinear form associated with N (recall that $B(x, y) = (N(x + y) - N(x) - N(y))/2$ by definition, hence $B(x, x) = N(x)$). We get

$$0 = B(q_0 + \sqrt{a}q_1, q_0 + \sqrt{a}q_1) = N(q_0) + aN(q_1) + 2\sqrt{a}B(q_0, q_1).$$

Now note that since $q_0, q_1 \in A$, the elements $B(q_0, q_1)$ and $N(q_0) + aN(q_1)$ both lie in k. So it follows from the above equality that

$$N(q_0) = -aN(q_1) \quad \text{and} \quad 2B(q_0, q_1) = q_0\overline{q}_1 + q_1\overline{q}_0 = 0.$$

Here $N(q_0), N(q_1) \neq 0$ as A is nonsplit. The element $q_2 := q_0\overline{q}_1 \in A$ satisfies

$$q_2^2 = q_0\overline{q}_1 q_0\overline{q}_1 = -q_0\overline{q}_0 q_1\overline{q}_1 = -N(q_0)N(q_1) = aN(q_1)^2.$$

The square of the element $q := q_2 N(q_1)^{-1}$ is then precisely a, so mapping $\sqrt{a}$ to q embeds $k(\sqrt{a})$ into A. □

We conclude this section by another characterization of the quaternion norm.

Proposition 1.2.4 *Let (a, b) be a quaternion algebra over a field k, and let $K = k(\sqrt{a})$ be a quadratic splitting field for (a, b). Then for all $q \in (a, b)$ and all K-isomorphisms $\phi : (a, b) \otimes_k K \xrightarrow{\sim} M_2(K)$ we have $N(q) = \det(\phi(q))$.*

Proof First note that $\det(\phi(q))$ does not depend on the choice of ϕ. Indeed, if $\psi : (a,b) \otimes_k K \xrightarrow{\sim} M_2(K)$ is a second isomorphism, then $\phi \circ \psi^{-1}$ is an automorphism of $M_2(K)$. But it is well known that all K-automorphisms of $M_2(K)$ are of the form $M \to CMC^{-1}$ for some invertible matrix C (check this by hand or see Lemma 2.4.1 for a proof in any dimension), and that the determinant map is invariant under such automorphisms.

Now observe that by definition the quaternion norm on $(a,b) \otimes_k K$ restricts to that on (a,b). Therefore to prove the proposition it is enough to embed (a,b) into $M_2(K)$ via ϕ and check that on $M_2(K)$ the quaternion norm (which is intrinsic by Remark 1.1.4) is given by the determinant. For this, consider a basis of $M_2(K)$ as in (1.2) with $b = 1$ and write

$$\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} = \left(\frac{a_1+a_4}{2}\right)\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \left(\frac{a_1-a_4}{2}\right)\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} + \\ + \left(\frac{a_2+a_3}{2}\right)\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \left(\frac{a_2-a_3}{2}\right)\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Then equation (1.1) yields

$$N\left(\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}\right) = \left(\frac{a_1+a_4}{2}\right)^2 - \left(\frac{a_1-a_4}{2}\right)^2 - \left(\frac{a_2+a_3}{2}\right)^2 + \left(\frac{a_2-a_3}{2}\right)^2 \\ = a_1a_4 - a_2a_3 = \det\left(\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}\right).$$

□

1.3 The associated conic

We now introduce another important invariant of a quaternion algebra (a,b), the *associated conic* $C(a,b)$. By definition, this is the projective plane curve defined by the homogeneous equation

$$ax^2 + by^2 = z^2 \tag{1.3}$$

where x, y, z are the homogeneous coordinates in the projective plane $\mathbf{P}^2$. In the case of $(1,1) \xrightarrow{\sim} M_2(k)$ we get the usual circle

$$x^2 + y^2 = z^2.$$

Remark 1.3.1 In fact, the conic $C(a,b)$ is canonically attached to the algebra (a,b) and does not depend on the choice of a basis. To see why, note first that the conic $C(a,b)$ is isomorphic to the conic $ax^2+by^2=abz^2$ via the substitution $x\mapsto by, y\mapsto ax, z\mapsto abz$ (after substituting, divide the equation by ab). But $ax^2+by^2-abz^2$ is exactly the square of the pure quaternion $xi+yj+zij$ and hence is intrinsically defined by Remark 1.1.4.

This observation also shows that if two quaternion algebras (a,b) and (c,d) are isomorphic as k-algebras, then the conics $C(a,b)$ and $C(c,d)$ are also isomorphic over k. Indeed, constructing an isomorphism $(a,b)\cong(c,d)$ is equivalent to finding a k-basis in (a,b) that satisfies the multiplicative rule in (c,d).

Recall from algebraic geometry that the conic $C(a,b)$ is said to have a *k-rational point* if there exist $x_0,y_0,z_0\in k$, not all zero, that satisfy equation (1.3) above.

We can now give a complement to Proposition 1.1.7.

Proposition 1.3.2 *The quaternion algebra (a,b) is split if and only if the conic $C(a,b)$ has a k-rational point.*

Proof If (x_0,y_0,z_0) is a k-rational point on $C(a,b)$ with $y_0\neq 0$, then $b=(z_0/y_0)^2-a(x_0/y_0)^2$ and part (4) of Proposition 1.1.7 is satisfied. If y_0 happens to be 0, then x_0 must be nonzero and we get similarly that a is a norm from the extension $k(\sqrt{b})|k$. Conversely, if $b=r^2-as^2$ for some $r,s\in k$, then $(s,1,r)$ is a k-rational point on $C(a,b)$. □

Remark 1.3.3 Again, the proposition has a counterpart in characteristic 2; see Exercise 4.

Example 1.3.4 For $a\neq 1$, the projective conic $ax^2+(1-a)y^2=z^2$ has the k-rational point $(1,1,1)$, hence the quaternion algebra $(a,1-a)$ splits by the proposition. This innocent-looking fact is a special case of the so-called *Steinberg relation* for symbols that we shall encounter later.

Remark 1.3.5 It is a well-known fact from algebraic geometry that a smooth projective conic defined over a field k is isomorphic to the projective line $\mathbf{P}^1$ over k if and only if it has a k-rational point. The isomorphism is given by taking the line joining a point P of the conic to some fixed k-rational point O and then taking the intersection of this line with $\mathbf{P}^1$ embedded as, say, some coordinate axis in $\mathbf{P}^2$. In such a way we get another equivalent condition for

the splitting of a quaternion algebra, which will be substantially generalized later.

In the remainder of this section we give examples of how Proposition 1.3.2 can be used to give easy proofs of splitting properties of quaternion algebras over special fields.

Example 1.3.6 Let k be the finite field with q elements (q odd). Then any quaternion algebra (a, b) over k is split.

To see this, it suffices by Proposition 1.3.2 to show that the conic $C(a, b)$ has a k-rational point. We shall find a point (x_0, y_0, z_0) with $z_0 = 1$. As the multiplicative group of k is cyclic of order $q-1$, there are exactly $1+(q-1)/2$ squares in k, including 0. Thus the sets $\{ax^2 : x \in k\}$ and $\{1 - by^2 \mid y \in k\}$ both have cardinality $1 + (q - 1)/2$, hence must have an element in common.

The next two examples concern the field $k(t)$ of rational functions over a field k, which is by definition the fraction field of the polynomial ring $k[t]$. Note that sending t to 0 induces a k-homomorphism $k[t] \to k$; we call it the *specialization* map attached to t.

Example 1.3.7 Let (a, b) be a quaternion algebra over k. Then (a, b) is split over k if and only if $(a, b) \otimes_k k(t)$ is split over $k(t)$.

Here necessity is obvious. For sufficiency, we assume given a point (x_t, y_t, z_t) of $C(a, b)$ defined over $k(t)$. As the equation (1.3) defining $C(a, b)$ is homogeneous, we may assume after multiplication by a suitable element of $k(t)$ that x_t, y_t, z_t all lie in $k[t]$ and one of them has a nonzero constant term. Then specialization gives a k-point $(x_t(0), y_t(0), z_t(0))$ of $C(a, b)$.

Finally we give an example of a splitting criterion for a quaternion algebra over $k(t)$ that does not come from k.

Example 1.3.8 For $a \in k^\times$ the $k(t)$-algebra (a, t) is split if and only if a is a square in k.

Here sufficiency is contained in Example 1.1.5. For necessity, assume given a $k(t)$-point (x_t, y_t, z_t) of $C(a, b)$ as above. Again we may assume x_t, y_t, z_t are all in $k[t]$. If x_t and z_t were both divisible by t, then equation (1.3) would imply the same for y_t, so after an eventual division we may assume they are not. Then setting $t = 0$ gives $ax_t^2(0) = z_t(0)^2$ and so $a = x_t^2(0)^{-1}z_t(0)^2$ is a square.

1.4 A theorem of Witt

In this section we prove an elegant theorem which characterizes isomorphisms of quaternion algebras by means of the function fields of the associated conics. Recall that the function field of an algebraic curve C is the field $k(C)$ of rational functions defined over some Zariski open subset of C. In the concrete case of a conic $C(a,b)$ as in the previous section, the simplest way to define it is to take the fraction field of the integral domain $k[x,y]/(ax^2+by^2-1)$ (this is also the function field of the affine curve of equation $ax^2+by^2=1$).

A crucial observation for the sequel is the following.

Remark 1.4.1 The quaternion algebra $(a,b)\otimes_k k(C(a,b))$ is always split over $k(C(a,b))$. Indeed, the conic $C(a,b)$ always has a point over this field, namely $(x,y,1)$ (where we also denote by x,y their images in $k(C(a,b))$). This point is called the *generic point* of the conic.

Now we can state the theorem.

Theorem 1.4.2 (Witt) *Let $Q_1=(a_1,b_1)$, $Q_2=(a_2,b_2)$ be quaternion algebras, and let $C_i=C(a_i,b_i)$ be the associated conics. The algebras Q_1 and Q_2 are isomorphic over k if and only if the function fields $k(C_1)$ and $k(C_2)$ are isomorphic over k.*

Remark 1.4.3 It is known from algebraic geometry that two smooth projective curves are isomorphic if and only if their function fields are. Thus the theorem states that *two quaternion algebras are isomorphic if and only if the associated conics are isomorphic as algebraic curves.*

In Chapter 5 we shall prove a broad generalization of the theorem, due to Amitsur. We now begin the proof by the following easy lemma.

Lemma 1.4.4 *If (a,b) is a quaternion algebra and $c\in k^\times$ is a norm from the field extension $k(\sqrt{a})|k$), then $(a,b)\cong(a,bc)$.*

Proof By hypothesis, we may write $c=x^2-ay^2$ with $x,y\in k$. Hence we may consider c as the norm of the quaternion $q=x+yi+0j+0ij$ and set $J=qj=xj+yij$. Then J is a pure quaternion satisfying

$$iJ+Ji=0,\quad J^2=-N(J)=-N(q)N(j)=bc,$$

and $1,i,J,iJ$ is a basis of (a,b) over k (by a similar argument as in the proof of Lemma 1.2.1). The lemma follows. □