An explicit example of a noncrossed product division algebra

Timo Hanke*

Universität Potsdam
Institut für Mathematik
Postfach 60 15 53
14415 Potsdam
Germany
e-mail : hanke@math.uni-potsdam.de

Key words noncrossed products, twisted polynomials, skew polynomials, twisted Laurent series, skew Laurent series, noncommutative valuations, computational algebraic number theory, relative norm equations, extension of automorphisms.
MSC (2000) Primary 16S35; Secondary 16K20, 16W60, 11Y40

The paper presents an explicit example of a noncrossed product division algebra of index and exponent 8 over the field $\mathbb{Q}(s)(t)$. It is an iterated twisted function field in two variables $D(x,\sigma)(y,\tau)$ over a quaternion division algebra D which is defined over the number field $\mathbb{Q}(\sqrt{3},\sqrt{-7})$. The automorphisms σ and τ are computed by solving relative norm equations in extensions of number fields. The example is explicit in the sense that its structure constants are known. Moreover, it is pointed out that the same arguments also yield another example, this time over the field $\mathbb{Q}(\!(s)\!)(\!(t)\!)$, given by an iterated twisted Laurent series ring $D(\!(x,\sigma)\!)(\!(y,\tau)\!)$ over the same quaternion division algebra D.

1 Introduction

Context. Let K be a field that is fixed throughout the following. We assume that all algebras considered have K as their center (unless stated otherwise) and are finite-dimensional over K. By the classical structure theorem of Wedderburn, the simple algebras are precisely the matrix rings over division algebras. In fact, Wedderburn's theorem states that any simple algebra A is isomorphic to $M_n(D)$ for a division algebra D that is unique up to isomorphism and a unique $n \in \mathbb{N}$. We call D the *underlying division algebra* of A. A simple algebra A is called a *crossed product* if it contains a maximal subfield (i.e. a commutative subfield L with $[L:K]^2 = \dim_K A$) that is Galois over K. Otherwise, A is called a *noncrossed product*.

It is a classical result from number theory that all simple algebras are crossed products if K is a global or local field. In fact, in these cases they even contain a cyclic maximal subfield. The question that naturally arises, and that was open for several decades, is whether this is true for any field K. The negative answer was given in 1972 by Amitsur's paper [1], which presented the first noncrossed product division algebra.

What mainly accounts for the importance of crossed products is their correspondence to *cocycles*. Any crossed product algebra A has a vector space basis over K such that the *structure constants* of A with respect to this basis are described in an easy fashion by a Galois 2-cocycle. The structure constants are the coefficients of the entries of the multiplication table with respect to a fixed basis. Conversely, we

* Supported in part by the DAAD (Kennziffer D/99/13304).

have the *crossed product construction* that assigns to each Galois 2-cocycle a simple algebra by defining the structure constants in the same easy fashion in terms of the cocycle.

The correspondence to cocycles is relevant in different ways. On the one hand, the construction from cocycles is very useful to obtain simple algebras *explicitly*. It goes back to the very first examples of algebras, starting with Hamiltons quaternions. On the other hand, it is the key to the important cohomological description of the *Brauer group*. The elements of the Brauer group (of K) are the classes of simple algebras with the same underlying division algebra, so that each class is represented by a unique division algebra (up to isomorphism). Simple algebras with the same underlying division algebra are called *similar*. The cohomological description of the Brauer group now arises from the classical theorem that every simple algebra is similar to a crossed product, hence every class is represented by a Galois 2-cocycle. For a reference on crossed products, Brauer groups and related topics see Pierce [13] or Jacobson [10].

We are mainly interested in the construction of (noncrossed product) *division algebras*. It is elegant for many purposes to describe a division algebra up to similarity, i.e. by giving its Brauer class, rather than up to isomorphism. We call this an *indirect approach*, in contrast to a *direct approach* that constructs division algebras up to isomorphism. An example for the latter are the *twisted Laurent series rings*[1,2].

Others that come to mind are quotient rings of certain noncommutative rings, e.g. *twisted function fields*[2] and *generic division rings*.

The approach has consequences on the explicitness of the construction. By an *explicit algebra construction* we mean a construction that gives us the structure constants with respect to some basis over the center. An explicit algebra construction will enable us to compute explicitly with elements from the algebra. An indirect approach is in general *not* explicit, because, given a simple algebra, it is (at this time) practically impossible to obtain the structure constants of the underlying division algebra. The Wedderburn structure theorem only gives us the existence and uniqueness of the underlying division ring, but the explicitness is generally lost in this passage. From the explicit viewpoint, an indirect approach is rather an existence proof than a construction. A direct approach on the other hand may be explicit or not. To my knowledge the generic division rings are not explicit either, because the centers are generally unknown[3] and so are the structure constants. The twisted Laurent series rings and twisted function fields are explicit provided that all involved parameters are known explicitly.

After Amitsur's first example many noncrossed product constructions have been suggested. A lot of them can be viewed as variations of Amitsur [1]. But the constructions in Jacob-Wadsworth [8] and Brussel [2] differ from Amitsur [1] in the approach, the ideas of proof, and in some of the properties of the obtained examples. We can classify different noncrossed product examples for instance by the centers and their "size", the algebra degrees, and the explicitness of the construction. These properties are discussed below for [1], [8] and [2]. A detailed survey on the various noncrossed product constructions can be found in Wadsworth [17, § 5].

It is known that the "smallest" centers that admit noncrossed products are $\mathrm{Q}(\mathrm{t})$ and $\mathrm{Q}(\!(\mathrm{t})\!)$. This was proved by Brussel [2] in 1995. In Jacob-Wadsworth [8] the transcendence degree of the center gets higher, while in Amitsur [1] the center remains unknown. The smallest degrees for which noncrossed products are known to exist at this time are 8 and p^2 for odd primes p. These degrees are obtained in all of [1], [8] and [2]. It is unknown if there are noncrossed products of prime degree $p \geq 5$, but there are none of degree 4. The constructions used are basically of two types. Either the noncrossed products are generic division rings, which is the case for [1] and its variations. Or they appear as the underlying division algebra of some other simple algebra that is constructed, which is the case for [8] and [2]. Thus, [1] represents a direct approach, while [8] and [2] represent indirect approaches. None of these constructions is explicit in the sense formulated above.

Motivation. From the explicit viewpoint, the striking dichotomy between crossed products and noncrossed products is that crossed products have a presentation with structure constants given by

[1] Twisted Laurent series can be traced back historically to a construction of Hilbert of (infinite-dimensional) ordered division rings in his "Foundation of Geometry" that he called "algebra of segments".

[2] The construction will be recalled in § 2 of this paper.

[3] There is a substantial theory on the centers of generic division rings. For a reference see Saltman [15, Chapter 14].

a Galois 2-cocyle, while noncrossed products lack such a presentation. If division algebras are given non-explicitly this dichotomy does not show up because we lack the structure constants in any case, whether they are crossed products or not. To make the dichotomy accessible an *explicit* noncrossed product example is required. The following quote nicely illustrates the problem.

> "To a division algebra specialist the lack of an alternative presentation [to the cocycle presentation] is unsatisfactory. Finding a noncrossed product over a field is like discovering an uncharted island by plane. The territory remains unexplored even after it is put on the map. Still it is an interesting find, indicating the theory of division algebras over the field is nontrivial. Moreover, the fact that existence is provable hints that the theory is accessible."
>
> — Eric Brussel, from the introduction of [3]

Our goal is to land on one of these islands. And finding the structure constants is like finding a natural airstrip (as bumpy as it may be). It enables us to land and explore by foot. We want to give an explicit example of a noncrossed product with center and degree as small as possible. It is clear that a direct approach of construction will be required. Furthermore, it is natural to expect that if the example is explicit then we can give a rather elementary and direct proof of the fact that it is a noncrossed product.

Accomplishment. In this paper an explicit example of a noncrossed product division algebra is given. It is the first explicit one. The degree is 8, which is the smallest one for which existence of noncrossed products is currently known. The only drawback is that the center is *not* the smallest one possible : it is $Q(s)(t)$.

The direct construction used here is the one of iterated twisted function fields in two variables over division algebras over number fields. These algebras are denoted by $D(x,\sigma)(y,\tau)$ where D is the division algebra and σ and τ are outer automorphisms of D that define conjugation of elements from D with the indeterminates x and y respectively (see § 2 for a precise definition and algorithmic construction). By carefully choosing the parameters involved (see the example in § 4), this construction yields a noncrossed product. The parameters are surprisingly small. For instance, D can be chosen to be the quaternion division algebra $(3+\sqrt{3},\frac{-7+\sqrt{-7}}{2})_K$ over the biquadratic number field $K=\mathbb{Q}(\sqrt{3},\sqrt{-7})$.

In general, it is very difficult to explicitly compute outer automorphisms of division algebras or central simple algebras. But in very special cases the problem can be reduced to the solution of norm equations in field extensions (see § 3). Since we work over number fields, methods from computational algebraic number theory can then be applied. This paper gives an example of a division algebra D that meets two requirements at the same time : it admits explicit computation of outer automorphisms *and* its iterated twisted function field is a noncrossed product. This is tricky because the two requirements work against each other. Roughly spoken, the former needs certain "nice subfields" in D while the latter prohibits the existence of subfields that are "too nice".

A self-contained and elementary proof is given of the fact that the example presented is a noncrossed product. Like in most of the previous examples noncommutative valuation theory is present[2]. The valuation is the x-adic valuation of twisted function fields $D(x,\sigma)$, which is in complete analogy to its commutative counterpart and can be regarded as common knowledge. In the main theorem (see Theorem 5.2) the x-adic valuation is used to relate the subfields of $D(x,\sigma)$ to the subfields of D. It is essentially this theorem that allows the direct approach with twisted function fields. A further number theoretic part (see Theorem 6.2) shows that the chosen quaternion division algebra does not contain maximal subfields Galois over $\mathbb{Q}$ (a proper subfield of its center). This completes the proof.

It is pointed out that the presented arguments also yield a noncrossed product division algebra that is an iterated twisted Lauent series ring. The center is $Q(\!(s)\!)(\!(t)\!)$ this time.

Methods and constructions of this paper are related to other noncrossed product examples. For instance, twisted Laurent series rings also play an important role in Amitsur [1]. Amitsur constructs twisted Laurent series over *fields* such that only certain groups can occur as Galois groups of maximal

[2] Wadsworth [17, § 5] nicely demonstrates the use of noncommutative valuations in most of the noncrossed product constructions so far.

subfields.[3] From this, he derives that generic division rings can be noncrossed products.[4] It is now interesting to see that by considering twisted Laurent series over *division algebras* instead of fields we can get noncrossed products directly. Furthermore, the number theoretic part of the proof given here is similar in technique to a corresponding argument[5] in Brussel [2].

Finally, in § 7, using the theory of inertially split division algebras, it is shown that the noncrossed product has exponent 8 (the order in the Brauer group).

Outlook. There are potentially "smaller" and "simpler" noncrossed product examples than the one presented here, namely twisted function fields in *one* variable $D(x,\sigma)$ with center $Q(t)$. This was shown in my thesis [7]. But the example given there is not fully explicit. More precisely, D is given explicitly but the automorphism σ is not. Instead, the existence of σ is proved by local-global principles. The reason that σ cannot be computed explicitly is basically that D is a cubic algebra and not a quaternion algebra as in this paper.

There is a result[6] that limits the hope of finding an explicit noncrossed product example of the form $D(x,\sigma)$: If D is a quaternion algebra over a local or global field then any $D(x,\sigma)$ is a crossed product. With this result in mind, it is clear that even though we do not achieve the smallest possible center here, we do achieve the smallest possible dimension of D over $\mathbb{Q}$.

Requirements. The reader should be familiar with the valuation theory of algebraic number fields (e.g. from Neukirch [12, Kapitel II]), and the basic facts on quaternion algebras (e.g. from Pierce [13, Chapter 1]) and central simple algebras and their subfields (e.g. from Pierce [13, Chapter 12 and 13]). Another reference on central simple algebras is Jacobson [10]. Up to this foundation the paper is self-contained. Only § 7 on the exponent requires substantially more background in form of the theory of inertially split division algebras. This can be found in Jacob-Wadsworth [9] or Wadsworth [17].

2 Construction of iterated twisted function fields and Laurent series

Twisted function fields and twisted Laurent series rings are introduced at various points in the literature, for instance in Cohn [4, § 5.2]. Twisted Laurent series are also discussed in Lam [11, (1.8)] and in greater detail in Pierce [13, § 19.7] and Jacobson [10, § 1.10]. We start with summarizing the matter that is relevant for our purposes.

Let K/F be a finite cyclic field extension with $\mathrm{Gal}(K/F) = \langle\,\sigma\,\rangle$ and $[K:F] = n$. Furthermore, let D be a finite-dimensional central K-division algebra, and suppose that σ extends to an F-algebra automorphism $\widetilde{\sigma}$ of D. Denote by $D[x;\widetilde{\sigma}]$ the set of all polynomials

$$D[x;\widetilde{\sigma}] := \{\sum_{i=0}^{k} d_i x^i \mid k \in \mathbb{N}_0, d_i \in D\},$$

and by $D(\!(x,\widetilde{\sigma})\!)$ the set of all formal series

$$D(\!(x;\widetilde{\sigma})\!) := \{\sum_{i\geq k} d_i x^i \mid k \in \mathbb{Z}, d_i \in D\}.$$

A ring structure is given on $D[x;\widetilde{\sigma}]$ and $D(\!(x;\widetilde{\sigma})\!)$ by componentwise addition and the multiplication rule

$$xd = \widetilde{\sigma}(d)x \quad \text{for all } d \in D.$$

We shall identify D with the subring Dx^0 of $D[x;\widetilde{\sigma}]$ and $D(\!(x;\widetilde{\sigma})\!)$. It is easily verified that $D[x;\widetilde{\sigma}]$ is a domain and that $D(\!(x;\widetilde{\sigma})\!)$ is a division ring, since the inverse of an element of $D(\!(x;\widetilde{\sigma})\!)$ can be recursively computed as in the case of commutative Laurent series. $D[x;\widetilde{\sigma}]$ is called the *twisted (or skew) polynomial*

[3] cf. Pierce [13, Theorem 19.9]
[4] cf. Pierce [13, Amitsur's Theorem 20.8]
[5] compare Theorem 6.2 of this paper to Brussel [2, Lemma 5]
[6] to be published in a subsequent paper

ring and $D(\!(x;\widetilde{\sigma})\!)$ is called the *twisted (or skew) Laurent series ring*. Denote by $D(x;\widetilde{\sigma})$ the ring of central quotients of $D[x;\widetilde{\sigma}]$, i.e.

$$D(x;\widetilde{\sigma}) := \{f/g \mid f \in D[x;\widetilde{\sigma}], g \in Z(D[x;\widetilde{\sigma}])\} \tag{2.1}$$

with $Z(\cdot)$ denoting the center. Since $D[x;\widetilde{\sigma}]$ is a domain, so is $D(x;\widetilde{\sigma})$, and $D(x;\widetilde{\sigma})$ can be regarded as a subring of $D(\!(x;\widetilde{\sigma})\!)$.

By the Skolem-Noether theorem, $\widetilde{\sigma}^n$ is an inner automorphism of D since it is the identity on the center K. Moreover, as a consequence of Hilbert's Theorem 90, we have

Lemma 2.1 *There exists an $\alpha \in D^\times$ with*

$$\widetilde{\sigma}^n = \mathrm{Inn}(\alpha) \quad \textit{and} \quad \widetilde{\sigma}(\alpha) = \alpha. \tag{2.2}$$

Here, $\mathrm{Inn}(\alpha)$ denotes the inner automorphism of D defined by $\mathrm{Inn}(\alpha)(x) := \alpha x \alpha^{-1}$ for all $x \in D$. Moreover, such an element α can be found by solving systems of linear equations only.

Note that (2.2) determines $\alpha \in D^\times$ up to multiplication by elements from $F^\times$.

P r o o f. The existence of an element $\alpha \in D^\times$ satisfying (2.2) is proved e.g. in Pierce [13, Lemma 19.7] or in Jacobson [10, Theorem 1.1.22]. We recall the easy proof here in order to point out that it is in fact constructive.

By the Skolem-Noether theorem there is an element $\alpha' \in D^\times$ with $\widetilde{\sigma}^n = \mathrm{Inn}(\alpha')$. Computationally, α' is just the solution to a system of linear equations. We have $x := \alpha'^{-1}\widetilde{\sigma}(\alpha') \in K$ since $\mathrm{Inn}(x)$ is clearly the identity on D. It is easily verified that $N_{K/F}(x) = 1$. Therefore, by Hilbert's Theorem 90, there is an element $a \in K$ with $x = \frac{a}{\sigma(a)}$. Again, a is the solution to a system of linear equations. Obviously, the element $\alpha := a\alpha'$ then satisfies (2.2). □

Let $\alpha \in D^\times$ be an element as in Lemma 2.1. Then $s := \alpha^{-1}x^n$ is a commuting indeterminate over D and the centers of $D[x;\widetilde{\sigma}]$, $D(\!(x;\widetilde{\sigma})\!)$ and $D(x;\widetilde{\sigma})$ are

$$\begin{aligned} Z(D[x;\widetilde{\sigma}]) &= F[s] = \{\sum_{i=0}^{k} a_i(\alpha^{-1}x^n)^i \mid a_i \in F, k \in \mathbb{N}_0\}, \\ Z(D(\!(x;\widetilde{\sigma})\!)) &= F(\!(s)\!) = \{\sum_{i\geq k} a_i(\alpha^{-1}x^n)^i \mid a_i \in F, k \in \mathbb{Z}\} \end{aligned}$$

and

$$Z(D(x;\widetilde{\sigma})) = Q(Z(D[x;\widetilde{\sigma}])) = F(s) \tag{2.3}$$

respectively, where $Q(R)$ denotes the quotient field of an integral domain R. Obviously the set $\{1, x, \ldots, x^{n-1}\}$ forms a basis of $D[x;\widetilde{\sigma}]$, $D(x;\widetilde{\sigma})$ and $D(\!(x;\widetilde{\sigma})\!)$ over $D[s]$, $D(s)$ and $D(\!(s)\!)$ respectively (as free modules). Hence

$$[D(x;\widetilde{\sigma}) : F(s)] = [D(\!(x;\widetilde{\sigma})\!) : F(\!(s)\!)] = n[D : F],$$

where $[V : F]$ denotes the dimension of a vector space V over a field F. Since $D(x;\widetilde{\sigma})$ is a domain that is finite-dimensional over the field $F(s)$, $D(x;\widetilde{\sigma})$ is a division ring. $D(x;\widetilde{\sigma})$ is called the *twisted (or skew) function field*. Summarizing the above, $D(x;\widetilde{\sigma})$ and $D(\!(x;\widetilde{\sigma})\!)$ are division algebras with

$$\mathrm{ind}\, D(x;\widetilde{\sigma}) = \mathrm{ind}\, D(\!(x;\widetilde{\sigma})\!) = n \,\mathrm{ind}\, D. \tag{2.4}$$

Iterated twisted function fields. Now we iterate the process of building twisted function fields and twisted Laurent series rings from D. For the sake of simplicity this will be formulated only for one kind of these twisted algebras, the twisted function fields. The arguments hold analogously in the case of twisted Laurent series rings.

Let K/F be a finite abelian Galois extension with $\mathrm{Gal}(K/F) = \langle\,\sigma\,\rangle \oplus \langle\,\tau\,\rangle$, $\mathrm{ord}\,\sigma = n_1$, $\mathrm{ord}\,\tau = n_2$, $[K : F] = n_1 n_2 = n$. Let D be a finite-dimensional central K-division algebra and suppose that σ and τ extend to F-algebra automorphisms $\widetilde{\sigma}$ and $\widetilde{\tau}$ of D respectively. Let $F_\sigma \subseteq K$ be the fixed field of σ. Since K/F_σ is cyclic with $\mathrm{Gal}(K/F_\sigma) = \langle\,\sigma\,\rangle$, we can build $D(x;\widetilde{\sigma})$ as in (2.1). By (2.3), $Z(D(x;\widetilde{\sigma})) = F_\sigma(s)$ for some indeterminate s over F_σ. If we set $\tau(s) := s$ then $F_\sigma(s)/F(s)$ is cyclic with $\mathrm{Gal}(F_\sigma(s)/F(s)) = \langle\,\tau\,\rangle$. To build an iterated twisted function field, which is a twisted function field of the form $D(x;\widetilde{\sigma})(y;\hat{\tau})$, we need to extend τ to an $F(s)$-automorphism $\hat{\tau}$ of $D(x;\widetilde{\sigma})$. The following theorem gives a criterion when this is possible. Note that $s = \alpha^{-1}x^{n_1}$ is not uniquely determined since α is only determined up to multiplication by elements from $F_\sigma^\times$.

Theorem 2.2 *If there are elements $\alpha, \beta, \gamma \in D^\times$ satisfying*

$$\begin{aligned}
&(i) \quad \widetilde{\sigma}^{n_1} = \mathrm{Inn}(\alpha), \quad \widetilde{\sigma}(\alpha) = \alpha, && (iv) \quad \widetilde{\tau}(\alpha)\alpha^{-1} = \gamma\widetilde{\sigma}(\gamma)\cdots\widetilde{\sigma}^{n_1-1}(\gamma),\\
&(ii) \quad \widetilde{\tau}^{n_2} = \mathrm{Inn}(\beta), \quad \widetilde{\tau}(\beta) = \beta, && (v) \quad \beta\widetilde{\sigma}(\beta)^{-1} = \widetilde{\tau}^{n_2-1}(\gamma)\cdots\widetilde{\tau}(\gamma)\gamma,\\
&(iii) \quad \widetilde{\tau}\widetilde{\sigma} = \mathrm{Inn}(\gamma)\widetilde{\sigma}\widetilde{\tau},
\end{aligned}$$

then τ extends to the automorphism $\hat{\tau}$ of $D(x;\widetilde{\sigma})$ defined by

$$\hat{\tau}(\sum d_i x^i) := \sum \widetilde{\tau}(d_i)(\gamma x)^i, \tag{2.5}$$

such that $\hat{\tau}(s) = s$ for $s := \alpha^{-1}x^{n_1}$. Moreover,

$$Z(D(x;\widetilde{\sigma})(y;\hat{\tau})) = F(s)(t)$$

for $t := \beta^{-1}y^{n_2}$, and

$$\mathrm{ind}\, D(x;\widetilde{\sigma})(y;\hat{\tau}) = n\,\mathrm{ind}\, D.$$

Proof. To see that (2.5) defines an automorphism we only have to check the relation $\hat{\tau}(xd) = \hat{\tau}(x)\hat{\tau}(d)$ for all $d \in D$. But since $\hat{\tau}(xd) = \hat{\tau}(\widetilde{\sigma}(d)x) = \widetilde{\tau}\widetilde{\sigma}(d)\gamma x$ and $\hat{\tau}(x)\hat{\tau}(d) = \gamma x\widetilde{\tau}(d) = \gamma\widetilde{\sigma}\widetilde{\tau}(d)x$, this is equivalent to $\widetilde{\tau}\widetilde{\sigma}(d) = \gamma\widetilde{\sigma}\widetilde{\tau}(d)\gamma^{-1}$, which follows from (iii).

For $s = \alpha^{-1}x^{n_1}$ we have

$$\hat{\tau}(s) = \hat{\tau}(\alpha^{-1}x^{n_1}) = \widetilde{\tau}(\alpha)^{-1}(\gamma x)^{n_1} = \widetilde{\tau}(\alpha)^{-1}\gamma\widetilde{\sigma}(\gamma)\cdots\widetilde{\sigma}^{n_1-1}(\gamma)x^{n_1}.$$

Therefore $\hat{\tau}(s) = s$ is equivalent to $\widetilde{\tau}(\alpha)^{-1}\gamma\widetilde{\sigma}(\gamma)\cdots\widetilde{\sigma}^{n_1-1}(\gamma) = \alpha^{-1}$, which follows from (iv).

We know from (2.3) and (i) that $Z(D(x;\widetilde{\sigma})) = F_\sigma(s)$ for $s = \alpha^{-1}x^{n_1}$, and we have $\mathrm{Gal}(F_\sigma(s)/F(s)) = \langle\,\hat{\tau}|_{F_\sigma(s)}\,\rangle$. To show $Z(D(x;\widetilde{\sigma})(y;\hat{\tau})) = F(s)(t)$ for $t = \beta^{-1}y^{n_2}$ using (2.3), we have to verify that $\hat{\tau}^{n_2}$ is the inner automorphism of $D(x;\widetilde{\sigma})$ induced by β and $\hat{\tau}(\beta) = \beta$. Since $\widetilde{\tau}^{n_2} = \mathrm{Inn}(\beta)$ and $\widetilde{\tau}(\beta) = \beta$ by (ii), it remains to show $\hat{\tau}^{n_2}(x) = \beta x\beta^{-1}$. But this follows from (v), because

$$\hat{\tau}^{n_2}(x) = \widetilde{\tau}^{n_2-1}(\gamma)\cdots\widetilde{\tau}(\gamma)\gamma x.$$

Finally, (2.4) implies

$$\mathrm{ind}\, D(x;\widetilde{\sigma})(y;\hat{\tau}) = n_2\,\mathrm{ind}\, D(x;\widetilde{\sigma}) = n_1 n_2\,\mathrm{ind}\, D = n\,\mathrm{ind}\, D.$$

□

Remark 2.3 The algebra $D(x;\widetilde{\sigma})(y;\hat{\tau})$ in Theorem 2.2 is completely described by the rules

$$xd = \widetilde{\sigma}(d)x, \quad yd = \widetilde{\tau}(d)y, \quad yx = \gamma xy$$

for all $d \in D$. Therefore we also denote it by $D(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)$ and the analogously built Laurent series ring by $D(\!(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)\!)$.

The conditions (iv) and (v) of Theorem 2.2 look somewhat like two simultaneous "norm" conditions on γ. However, there is only a single norm equation (in a field extension) involved in

Algorithm 2.4 If there exist elements $\alpha, \beta, \gamma \in D^\times$ satisfying (i)–(v) of Theorem 2.2 then such elements can be constructed by performing the following steps.

1. Choose any $\alpha', \beta', \gamma' \in D^\times$ satisfying (i), (ii) and (iii) respectively.
2. Set $x := \gamma' \widetilde{\sigma}(\gamma') \cdots \widetilde{\sigma}^{n_1-1}(\gamma') \alpha' \widetilde{\tau}(\alpha')^{-1} \in F_\sigma$ and $y := \widetilde{\tau}^{n_2-1}(\gamma') \cdots \widetilde{\tau}(\gamma') \gamma' \widetilde{\sigma}(\beta') \beta'^{-1} \in F_\tau$.
3. Solve the norm equation $N_{K/F}(c) = N_{F_\sigma/F}(x)^{-1}$ for $c \in K$ and set $\gamma := c\gamma'$.
4. Choose an element $a \in F_\sigma$ with $\frac{\tau(a)}{a} = N_{K/F_\sigma}(c)x$ and set $\alpha := a\alpha'$.
5. Choose an element $b \in F_\tau$ with $\frac{b}{\sigma(b)} = N_{K/F_\tau}(c)y$ and set $\beta := b\beta'$.

P r o o f. We first show that if there exist $\alpha, \beta, \gamma \in D^\times$ satisfying (i)–(v) then each step of the algorithm has a solution. By Lemma 2.1, Step 1 has a solution in any case and the elements α', β', γ' can be constructed.

Now suppose that $\alpha, \beta, \gamma \in D^\times$ are elements satisfying (i)–(v), and let $a, b, c \in D^\times$ be such that $\alpha = a\alpha', \beta = b\beta', \gamma = c\gamma'$. Then a, b, c lie in K by the Skolem-Noether theorem. Furthermore, (i) and (ii) imply that $a \in F_\sigma$ and $b \in F_\tau$. Step 2: By definition of x and y we have

$$\gamma \widetilde{\sigma}(\gamma) \cdots \widetilde{\sigma}^{n_1-1}(\gamma) \alpha \widetilde{\tau}(\alpha)^{-1} = N_{K/F_\sigma}(c) \frac{a}{\tau(a)} x \tag{2.6}$$

and

$$\widetilde{\tau}^{n_2-1}(\gamma) \cdots \widetilde{\tau}(\gamma) \gamma \widetilde{\sigma}(\beta) \beta^{-1} = N_{K/F_\tau}(c) \frac{\sigma(b)}{b} y. \tag{2.7}$$

Because of (iv) and (v) the left sides of these equations are both equal to 1. This proves $x \in F_\sigma$ and $y \in F_\tau$. Step 3: The fact that the right sides of (2.6) and (2.7) are equal to 1 implies

$$N_{K/F}(c) = N_{F_\sigma/F}(\frac{\tau(a)}{a} x^{-1}) = N_{F_\sigma/F}(x)^{-1} \tag{2.8}$$

and

$$N_{K/F}(c) = N_{F_\tau/F}(\frac{b}{\sigma(b)} y^{-1}) = N_{F_\tau/F}(y)^{-1}. \tag{2.9}$$

This shows that the norm equation of step 3, which is precisely (2.8), has a solution. Moreover, it shows that $N_{F_\sigma/F}(x) = N_{F_\tau/F}(y)$, i.e. any solution c to (2.8) is also a solution to (2.9). In the following, let c be an arbitrary solution of (2.8) and (2.9) instead of the particular c chosen before. Steps 4 and 5: From (2.8) and (2.9) we get $N_{F_\sigma/F}(N_{K/F_\sigma}(c)x) = N_{K/F}(c) N_{F_\sigma/F}(x) = 1$ and $N_{F_\tau/F}(N_{K/F_\tau}(c)y) = N_{K/F}(c) N_{F_\tau/F}(y) = 1$. Hence a and b exist by Hilbert's Theorem 90.

Now we proof that if each step has a solution then $\alpha, \beta, \gamma \in D^\times$ satisfy (i)–(v). The conditions (i)–(iii) are clear because $a \in F_\sigma, b \in F_\tau$ and $c \in K$. Again, by definition of x and y, (2.6) and (2.7) hold. The elements a and b are chosen such that the right sides of both (2.6) and (2.7) are equal to 1. This proves (iv) and (v). □

Remark 2.5 1. Steps 1, 4 and 5 in the algorithm are just solutions to systems of linear equations. Step 3 is a single norm equation in a field extension. Over number fields methods from computational algebraic number theory can be applied here. The computer algebra software KASH [5] has implemented an algorithm for solving relative norm equations. Provided that the degrees n_1, n_2 and the base field F are small enough, this software can be used to carry out the algorithm.

2. It is clear from the proof that any solution $\alpha, \beta, \gamma \in D^\times$ to the conditions (i)–(v) can be obtained by the algorithm. Moreover, the element γ is uniquely determined up to multiplication by elements $c \in K^\times$ with $\mathrm{N}_{K/F}(c) = 1$. If γ is fixed, then α and β are determined up to multiplication by elements from $F^\times$.

3. The existence of a solution $\alpha, \beta, \gamma \in D^\times$ to the conditions (i)–(v) does not depend on the choice of extensions $\widetilde{\sigma}, \widetilde{\tau}$ of σ, τ respectively. To see this, it can be verified that if $\widetilde{\sigma}, \widetilde{\tau}$ are replaced by $\mathrm{Inn}(\eta)\widetilde{\sigma}, \mathrm{Inn}(\xi)\widetilde{\tau}$ respectively, $\eta, \xi \in D^\times$, then we can replace α, β, γ by

$$\eta\widetilde{\sigma}(\eta)\cdots\widetilde{\sigma}^{n_1-1}(\eta)\alpha, \quad \xi\widetilde{\tau}(\xi)\cdots\widetilde{\tau}^{n_2-1}(\xi)\beta, \quad \xi\widetilde{\tau}(\eta)\gamma\widetilde{\sigma}(\xi)^{-1}\eta^{-1},$$

respectively.

4. For different choices of γ the resulting division rings $D(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)$ (or $D(\!(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)\!)$ respectively) are in general not isomorphic.

3 Automorphisms of quaternion algebras

In the construction of the twisted function field $D(x; \widetilde{\sigma})$ we started with the automorphism σ of K and assumed that it extends to an automorphism $\widetilde{\sigma}$ of D. The question arises when it is possible to extend σ and how an extension can be found. Proposition 3.2 below settles this question for a special case of quaternion algebras that will be sufficient for our purposes.

Let K be any field and let $a, b \in K^\times$. The quaternion algebra $(a, b)_K$ is the K-space with basis $1, i, j, ij$ and multiplication $i^2 = a, j^2 = b, ij = -ji$. It is a simple algebra with center K (see Pierce [13, § 1.6]).

Lemma 3.1 *Let σ be an automorphism of K. Then σ extends to an automorphism $\widetilde{\sigma}$ of $(a, b)_K$ if and only if $(a, b)_K \cong (\sigma(a), \sigma(b))_K$.*

Proof. We have $(a, b)_K \cong (\sigma(a), \sigma(b))_K$ if and only if there is a K-basis $1, u, v, uv$ of $(a, b)_K$ with $u^2 = \sigma(a), v^2 = \sigma(b)$ and $vu = -uv$. If σ extends to $\widetilde{\sigma}$ then such a basis is obviously given by $u := \widetilde{\sigma}(i)$ and $v := \widetilde{\sigma}(j)$. Conversely, an extension $\widetilde{\sigma}$ is obtained from u, v by setting $\widetilde{\sigma}(i) := u, \widetilde{\sigma}(j) := v$. □

In the case $\sigma(b) = b$ we get

Proposition 3.2 *Let σ be an automorphism of K with $\sigma(b) = b$. Then σ extends to an automorphism $\widetilde{\sigma}$ of $(a, b)_K$ if and only if there exists $\lambda \in K(j)$ with*

$$\mathrm{N}_{K(j)/K}(\lambda) = \frac{\sigma(a)}{a}.$$

For any such λ, an extension $\widetilde{\sigma}$ of σ is defined by

$$\widetilde{\sigma}(i) := \lambda i, \quad \widetilde{\sigma}(j) := j.$$

Proof. By Lemma 3.1, σ extends to $\widetilde{\sigma}$ if and only if $(a, b)_K \cong (\sigma(a), b)_K$. It is a standard argument about cyclic algebras (cf. Pierce [13, Lemma 15.1]) that this is equivalent to the existence of $\lambda \in K(j)$ with $\mathrm{N}_{K(j)/K}(\lambda) = \frac{\sigma(a)}{a}$. Moreover, for any such λ, setting $u := \lambda i, v := j$ yields a K-basis $1, u, v, uv$ of $(a, b)_K$ with $u^2 = \sigma(a), v^2 = b = \sigma(b), uv = -vu$. Hence, as in the proof of Lemma 3.1, an extension $\widetilde{\sigma}$ is defined by $\widetilde{\sigma}(i) := \lambda i, \widetilde{\sigma}(j) := j$. □

Remark 3.3 Proposition 3.2 can be proved analogously for symbol algebras $(a, b)_{K,\zeta}$ where $\zeta \in K$ is a primitive n-th root of unity and $a, b \in K^\times$.

4 The Example

In this section we construct an explicit example of an iterated twisted function field following step by step the general construction from § 2. We will point out certain properties during this process that we tag (N·). Precisely these properties enable us later in § 6 to show that the example is in fact a noncrossed product. With the same parameters we also get an iterated twisted Laurent series ring that is a noncrossed product.

The field K. Let p and q be the primes $p = 3$ and $q = 7$. Note that

$$p \equiv q \equiv 3 \mod 4. \tag{N1}$$

Let K be the biquadratic extension $K = \mathbb{Q}(\sqrt{3}, \sqrt{-7})$ of $\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle \oplus \langle \tau \rangle$, where

$$\begin{aligned} \sigma(\sqrt{3}) &= -\sqrt{3}, & \sigma(\sqrt{-7}) &= \sqrt{-7}, \\ \tau(\sqrt{3}) &= \sqrt{3}, & \tau(\sqrt{-7}) &= -\sqrt{-7}. \end{aligned}$$

Write

$$K_1 = \mathbb{Q}(\sqrt{3}), \qquad K_2 = \mathbb{Q}(\sqrt{-7}).$$

We now discuss the extensions of the p- and q-adic valuations v_p and v_q of $\mathbb{Q}$ to K. Obviously v_p is totally ramified in K_1, and v_q is totally ramified in K_2. The primes p and q are chosen such that $-q$ is not a square modulo p and p is not a square modulo q. This shows that v_p is inertial in K_2 that v_q is inertial in K_1. Altogether, it is now clear that

$$v_p \text{ and } v_q \text{ uniquely extend to valuations on } K, \tag{N2}$$

$$\text{the inertia fields of } v_p \text{ and } v_q \text{ in } K \text{ are different}, \tag{N3}$$

$$K \text{ is not real.} \tag{N4}$$

The unique extensions of v_p and v_q to K will be denoted by w_p and w_q, respectively.

The quaternion division algebra D. Let $a_0 \in K_1$ and $b_0 \in K_2$ be the elements

$$a_0 = 1 + \sqrt{3}, \qquad b_0 = \frac{1 + \sqrt{-7}}{2}.$$

Note that

$$\mathrm{N}_{K_1/\mathbb{Q}}(a_0) = a_0\sigma(a_0) = -2, \qquad \mathrm{N}_{K_2/\mathbb{Q}}(b_0) = b_0\tau(b_0) = 2. \tag{4.1}$$

Define the quaternion algebra $D = (a, b)_K$ by

$$a := a_0\sqrt{3} = 3 + \sqrt{3}, \qquad b := b_0\sqrt{-7} = \frac{-7 + \sqrt{-7}}{2}.$$

To see that D is a division algebra, we show the stronger result :

$$D \otimes_K K_w = (a, b)_{K_w} \quad \text{is a division algebra for } w = w_p \text{ and } w = w_q, \tag{N5}$$

where K_w denotes the completion of K with respect to w. In the following $\bar{\cdot}$ denotes the residue field with respect to the fixed valuation w.

We first consider $w = w_p$. The residue field of K with respect to w_p is $\overline{K} = \overline{K}_2$. The element b is a valuation unit with respect to w_p and has $N_{K_2/\mathbb{Q}}(b) = 2 \cdot 7 = 14$. Since $\overline{14}$ is not a square in $\overline{\mathbb{Q}}$, the field of 3 elements, $\bar{b}$ is not a square in $\overline{K}_2 = \overline{K}$. This shows that w_p is inertial in $K(j)/K$. Obviously, a_0 is a valuation unit with respect to w_p, so that $a = a_0\sqrt{3}$ is a uniformizer for w_p. Therefore, a cannot be a norm in the inertial extension $K_{w_p}(j)/K_{w_p}$. This implies that $(a, b)_{K_{w_p}}$ is a division algebra (cf. Pierce [13, Exercise 4 in § 1.6 or Corollary 15.1d]).

Analogously, the argument goes on for $w = w_q$, but with a and b replaced. Now $\overline{K} = \overline{K}_1$, and the element a is a valuation unit with $N_{K_1/\mathbb{Q}}(a) = (-2) \cdot (-3) = 6$. Since $\overline{6}$ is not a square in $\overline{\mathbb{Q}}$, the field of 7 elements, $\bar{a}$ is not a square in $\overline{K}_1 = \overline{K}$. This shows that w_q is inertial in $K(i)/K$. Obviously, b_0 is a valuation unit with respect to w_q, so that $b = b_0\sqrt{-7}$ is a uniformizer for w_q. Therefore, b cannot be a norm in the inertial extension $K_{w_q}(i)/K_{w_q}$. This implies that $(a, b)_{K_{w_q}}$ is a division algebra. Hence (N5) is proved.

Extensions of σ and τ. The elements $a, b \in K$ were specially chosen such that $a \in K_1$ and $b \in K_2$. Therefore, we can use Proposition 3.2 to find extensions of σ and τ to D. Let $\lambda_0 \in K_1(i)$ and $\mu_0 \in K_2(j)$ be the elements

$$\lambda_0 = \sigma(a_0)(-1+i), \qquad \mu_0 = b_0 + j.$$

Note that

$$\mathrm{N}_{K_1(i)/K_1}(\lambda_0) = -2, \qquad \mathrm{N}_{K_2(j)/K_2}(\mu_0) = 2. \tag{4.2}$$

Define the elements $\lambda \in K(i)$ and $\mu \in K(j)$ by

$$\lambda := \frac{\lambda_0}{b_0}, \qquad \mu := \frac{\mu_0}{a_0}.$$

Using (4.2) and (4.1) we get

$$\mathrm{N}_{K(j)/K}(\mu) = \frac{2}{{a_0}^2} = -\frac{a_0\sigma(a_0)}{{a_0}^2} = -\frac{\sigma(a_0)}{a_0} = \frac{\sigma(a)}{a}$$

and

$$\mathrm{N}_{K(i)/K}(\lambda) = \frac{-2}{{b_0}^2} = -\frac{b_0\tau(b_0)}{{b_0}^2} = -\frac{\tau(b_0)}{b_0} = \frac{\tau(b)}{b}.$$

Therefore, by Proposition 3.2, extensions $\widetilde{\sigma}$, $\widetilde{\tau}$ of σ,τ to D are defined by

$$\begin{aligned} \widetilde{\sigma}(i) &= \mu i, \qquad & \widetilde{\sigma}(j) &= j, \\ \widetilde{\tau}(i) &= i, \qquad & \widetilde{\tau}(j) &= \lambda j. \end{aligned}$$

The elements α, β and γ. To define an iterated twisted function field $D(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)$ and an iterated twisted Laurent series ring $D(\!(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)\!)$ over D, we now give elements $\alpha, \beta, \gamma \in D^\times$ satisfying (i)–(v) of Theorem 2.2. These are

$$\alpha := \frac{1}{b_0}\mu_0 j, \qquad \beta := \sqrt{3}\lambda_0 i, \qquad \gamma := \frac{1}{2\sigma(a_0)}(\lambda_0\overline{\mu}_0 - 2).$$

Note that $\alpha \in K(j)$ and $\beta \in K(i)$. By Theorem 2.2,

$$\begin{aligned} Z(D(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)) &= \mathbb{Q}(s)(t), \\ Z(D(\!(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)\!)) &= \mathbb{Q}(\!(s)\!)(\!(t)\!), \end{aligned}$$

where $s = \alpha^{-1}x^2$, $t = \beta^{-1}y^2$, and

$$\operatorname{ind} D(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma) = \operatorname{ind} D(\!(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)\!) = 8.$$

The given elements α, β, γ were found with Algorithm 2.4. The rest of this section gives solutions to each step of the algorithm together with ideas how to verify their correctness. We use the notation $\overline{\lambda}_0$ for the conjugate of λ_0 in $K_1(i)/K_1$ and $\overline{\mu}_0$ for the conjugate of μ_0 in $K_2(j)/K_2$, i.e. $\overline{\lambda}_0 = \sigma(a_0)(-1-i)$ and $\overline{\mu}_0 = b_0 - j$. The following relations, as well as (4.1), will be frequently used without further mentioning them :

$$\begin{array}{lllll} \lambda_0\overline{\lambda}_0 = -2, & \widetilde{\sigma}(\mu_0) = \mu_0, & \widetilde{\tau}(\lambda_0) = \lambda_0, & i\lambda_0 = \lambda_0 i, & j\lambda_0 = \overline{\lambda}_0 j, \\ \mu_0\overline{\mu}_0 = 2, & \widetilde{\sigma}(\overline{\mu}_0) = \overline{\mu}_0, & \widetilde{\tau}(\overline{\lambda}_0) = \overline{\lambda}_0, & i\mu_0 = \overline{\mu}_0 i, & j\mu_0 = \mu_0 j. \end{array}$$

Also note that $n_1 = n_2 = 2$.

Step 1. The chosen elements α', β', γ' that satisfy (i)–(iii) are

$$\alpha' := \mu_0 j, \qquad \beta' := \lambda_0 i, \qquad \gamma' := \lambda_0\overline{\mu}_0 - 2.$$

Note that $\alpha' \in K(j)$ and $\beta' \in K(i)$. It is immediate from the definition of $\widetilde{\sigma}$ and $\widetilde{\tau}$ that $\widetilde{\sigma}(\alpha') = \alpha'$ and $\widetilde{\tau}(\beta') = \beta'$. To verify the identities about the inner automorphisms we use

Lemma 4.1 *Let D be a quaternion division algebra over K, and let φ be an inner automorphism of D. If $x, y \in D\backslash K$ with $x \notin K(y)$ such that $\varphi(x) = x$ and $\varphi(y) = xyx^{-1}$, then $\varphi = \mathrm{Inn}(x)$.*

Proof. If $x \notin K(y)$ then $\{1, x\}$ is a $K(y)$-basis of D. Therefore φ is already determined by $\varphi(x)$ and $\varphi(y)$. □

First apply Lemma 4.1 to $\widetilde{\sigma}^2$ and $\widetilde{\tau}^2$. Obviously, $\widetilde{\sigma}^2(\alpha') = \alpha'$ and $\widetilde{\tau}^2(\beta') = \beta'$. Furthermore,

$$\widetilde{\sigma}^2(i)\alpha' = \widetilde{\sigma}(\frac{\mu_0}{a_0}i)\alpha' = \frac{\mu_0}{\sigma(a_0)}\frac{\mu_0}{a_0}i\mu_0 j = \mu_0\frac{\mu_0\overline{\mu_0}}{a_0\sigma(a_0)}ij = \mu_0 ji = \alpha' i$$

and

$$\widetilde{\tau}^2(j)\beta' = \widetilde{\tau}(\frac{\lambda_0}{b_0}j)\beta' = \frac{\lambda_0}{\tau(b_0)}\frac{\lambda_0}{b_0}j\lambda_0 i = \lambda_0\frac{\lambda_0\overline{\lambda}_0}{b_0\tau(b_0)}ji = \lambda_0 ij = \beta' j.$$

Since $\alpha' \notin K(i)$ and $\beta' \notin K(j)$, Lemma 4.1 shows $\widetilde{\sigma}^2 = \mathrm{Inn}(\alpha')$ and $\widetilde{\tau}^2 = \mathrm{Inn}(\beta')$. This completes the verification of (i) and (ii). Now, in order to prove (iii), apply Lemma 4.1 with $\varphi = \widetilde{\tau}\widetilde{\sigma}\widetilde{\tau}^{-1}\widetilde{\sigma}^{-1}$, $x = \gamma'$ and $y = \widetilde{\sigma}\widetilde{\tau}(i)$. The identity $\widetilde{\tau}\widetilde{\sigma}\widetilde{\tau}^{-1}\widetilde{\sigma}^{-1}(\gamma') = \gamma'$ is shown by giving an element δ such that $\widetilde{\sigma}\widetilde{\tau}(\delta) = \widetilde{\tau}\widetilde{\sigma}(\delta) = \gamma'$. This element is

$$\delta = -\frac{a_0}{b_0}\delta', \quad \text{where} \quad \delta' = \overline{\lambda}_0\mu_0 + 2.$$

For the calculation it is pointed out that :

$$\begin{aligned}
\widetilde{\sigma}(\delta') &= \widetilde{\sigma}(\overline{\lambda}_0)\mu_0 + 2 = a_0(-1 - \frac{\mu_0}{a_0}i)\mu_0 + 2 = a_0(-\mu_0 + \sigma(a_0)i) + 2 \\
&= a_0(\sigma(a_0)(-1+i) - \mu_0) = a_0(\lambda_0 - \mu_0), \\
\widetilde{\tau}(\delta') &= \overline{\lambda}_0\widetilde{\tau}(\mu_0) + 2 = \overline{\lambda}_0(\tau(b_0) + \frac{\lambda_0}{b_0}j) + 2 = \tau(b_0)(\overline{\lambda}_0 - j) + 2 \\
&= \tau(b_0)(\overline{\lambda}_0 + (b_0 - j)) = \tau(b_0)(\overline{\lambda}_0 + \overline{\mu}_0).
\end{aligned}$$

Then

$$\begin{aligned}
\widetilde{\tau}\widetilde{\sigma}(\delta) &= -\frac{\sigma(a_0)}{\tau(b_0)}a_0(\lambda_0 - \widetilde{\tau}(\mu_0)) = b_0(\lambda_0 - (\tau(b_0) + \frac{\lambda_0}{b_0}j)) \\
&= b_0\lambda_0 - 2 - \lambda_0 j = \lambda_0(b_0 - j) - 2 = \gamma', \\
\widetilde{\sigma}\widetilde{\tau}(\delta) &= -\frac{\sigma(a_0)}{\tau(b_0)}\tau(b_0)(\widetilde{\sigma}(\overline{\lambda}_0) + \overline{\mu}_0) = -\sigma(a_0)(a_0(-1 - \frac{\mu_0}{a_0}i) + \overline{\mu}_0) \\
&= -2 + \sigma(a_0)i\overline{\mu}_0 - \sigma(a_0)\overline{\mu}_0 = \sigma(a_0)(-1+i)\overline{\mu}_0 - 2 = \gamma'.
\end{aligned}$$

Next, check the hypothesis $\gamma' \notin K(y)$ of Lemma 4.1. Since $\delta = \widetilde{\tau}^{-1}\widetilde{\sigma}^{-1}(\gamma')$,

$$\gamma' \in K(y) \Leftrightarrow \delta \in K(i) \Leftrightarrow \delta' \in K(i).$$

But $\delta' = \overline{\lambda}_0\mu_0 + 2 \notin K(i)$ is obvious from $\overline{\lambda}_0 \in K(i)$ and $\mu_0 \notin K(i)$. It remains to check that $\widetilde{\tau}\widetilde{\sigma}(i)\gamma' = \gamma'\widetilde{\sigma}\widetilde{\tau}(i)$. First note that

$$\begin{aligned}
\widetilde{\tau}(\mu_0)(\lambda_0\mu_0 - 2) &= (\tau(b_0) + \frac{\lambda_0}{b_0}j)(\lambda_0\mu_0 - 2) = \tau(b_0)(\lambda_0\mu_0 - 2 - \mu_0 j - \lambda_0 j) \\
&= \tau(b_0)(\lambda_0(\mu_0 - j) - (\mu_0 j + 2)) = \tau(b_0)(b_0\lambda_0 - b_0\mu_0) \\
&= 2(\lambda_0 - \mu_0) = (\lambda_0\overline{\mu}_0 - 2)\mu_0.
\end{aligned}$$

Then

$$\widetilde{\tau}\widetilde{\sigma}(i)\gamma' = \frac{\widetilde{\tau}(\mu_0)}{a_0}i(\lambda_0\overline{\mu}_0 - 2) = \frac{\widetilde{\tau}(\mu_0)}{a_0}(\lambda_0\mu_0 - 2)i = (\lambda_0\overline{\mu}_0 - 2)\frac{\mu_0}{a_0}i = \gamma'\widetilde{\sigma}\widetilde{\tau}(i).$$

Now, Lemma 4.1 can be applied and states that $\widetilde{\tau}\widetilde{\sigma}\widetilde{\tau}^{-1}\widetilde{\sigma}^{-1} = \mathrm{Inn}(\gamma')$. This completes the verification of (iii).

Step 2. The elements $x := \gamma'\widetilde{\sigma}(\gamma')\alpha'\tau(\alpha')^{-1} \in K_2$ and $y := \widetilde{\tau}(\gamma')\gamma'\widetilde{\sigma}(\beta')\beta'^{-1} \in K_1$ are

$$x = -4b_0^2 = -8\frac{b_0}{\tau(b_0)}, \qquad y = -4\sigma(a_0)^2 = 8\frac{\sigma(a_0)}{a_0}.$$

For the computation of x it is helpful to verify first :

$$\begin{aligned}
\gamma'\alpha' &= (\lambda_0\bar{\mu}_0 - 2)\mu_0 j = 2(\lambda_0 - \mu_0)j,\\
\widetilde{\sigma}^{-1}(\gamma') &= \widetilde{\tau}(\delta) = -\frac{a_0}{\tau(b_0)}\widetilde{\tau}(\delta') = -a_0(\overline{\lambda}_0 + \overline{\mu}_0)\\
\widetilde{\sigma}^{-1}(\gamma')\gamma'\alpha' &= -2a_0(\overline{\mu}_0\lambda_0 - \overline{\lambda}_0\mu_0 - 4)j,\\
\widetilde{\tau}(\alpha') &= (\tau(b_0) + \frac{\lambda_0}{b_0}j)\frac{\lambda_0}{b_0}j = \frac{2}{b_0^2}(\lambda_0 - j)j.
\end{aligned}$$

Then

$$\begin{aligned}
\gamma'\widetilde{\sigma}(\gamma')\alpha' &= \widetilde{\sigma}(\widetilde{\sigma}^{-1}(\gamma')\gamma'\alpha') = -2\sigma(a_0)(\overline{\mu}_0\widetilde{\sigma}(\lambda_0) - \widetilde{\sigma}(\overline{\lambda}_0)\mu_0 - 4)j\\
&= -2\sigma(a_0)(\overline{\mu}_0 a_0(-1 + \frac{\mu_0}{a_0}i) + a_0(1 + \frac{\mu_0}{a_0}i)\mu_0 - 4)j\\
&= -2\sigma(a_0)(-a_0\overline{\mu}_0 + 2i + a_0\mu_0 + 2i - 4)j\\
&= -2\sigma(a_0)(a_0(\mu_0 - \overline{\mu}_0) + 4(-1 + i))j\\
&= 4(\mu_0 - \overline{\mu}_0 - 2\lambda_0)j = 8(j - \lambda_0)j,
\end{aligned}$$

and

$$x = \gamma'\widetilde{\sigma}(\gamma')\alpha'\tau(\alpha')^{-1} = 8(j - \lambda_0)j \cdot \frac{b_0^2}{2}j^{-1}(\lambda_0 - j)^{-1} = -4b_0^2.$$

For the computation of y it is helpful to verify first :

$$\begin{aligned}
\beta'^{-1} &= -\frac{1}{2}i^{-1}\overline{\lambda}_0,\\
\beta'^{-1}\gamma' &= -\frac{1}{2}i^{-1}\overline{\lambda}_0(\lambda_0\overline{\mu}_0 - 2) = i^{-1}(\overline{\mu}_0 + \overline{\lambda}_0) = (\mu_0 + \overline{\lambda}_0)i^{-1},\\
\widetilde{\tau}^{-1}(\gamma') &= \widetilde{\sigma}(\delta) = -\frac{\sigma(a_0)}{b_0}\widetilde{\sigma}(\delta') = \tau(b_0)(\lambda_0 - \mu_0),\\
\beta'^{-1}\gamma'\widetilde{\tau}^{-1}(\gamma') &= \tau(b_0)(\mu_0 + \overline{\lambda}_0)(\lambda_0 - \overline{\mu}_0)i^{-1} = \tau(b_0)(\mu_0\lambda_0 - \overline{\lambda}_0\overline{\mu}_0 - 4)i^{-1},\\
\sigma(\beta') &= a_0(-1 + \frac{\mu_0}{a_0}i)\frac{\mu_0}{a_0}i = (-\mu_0 + \frac{2}{a_0}i)i = -(\sigma(a_0)i + \mu_0)i.
\end{aligned}$$

Then

$$\begin{aligned}
\beta'^{-1}\widetilde{\tau}(\gamma')\gamma' &= \widetilde{\tau}(\beta'^{-1}\gamma'\widetilde{\tau}^{-1}(\gamma')) = b_0(\widetilde{\tau}(\mu_0)\lambda_0 - \overline{\lambda}_0\widetilde{\tau}(\overline{\mu}_0) - 4)i^{-1}\\
&= b_0((\tau(b_0) + \frac{\lambda_0}{b_0}j)\lambda_0 - \overline{\lambda}_0(\tau(b_0) - \frac{\lambda_0}{b_0}j) - 4)i^{-1}\\
&= b_0(\tau(b_0)\lambda_0 - \frac{2}{b_0}j - \tau(b_0)\overline{\lambda}_0 - \frac{2}{b_0}j - 4)i^{-1}\\
&= b_0\tau(b_0)(\lambda_0 - j - \overline{\lambda}_0 - j - 2b_0)i^{-1}\\
&= 2(\lambda_0 - \overline{\lambda}_0 - 2\mu_0)i^{-1} = 4(\sigma(a_0)i - \mu_0)i^{-1},
\end{aligned}$$

and

$$\begin{aligned}
y = \beta'^{-1}\widetilde{\tau}(\gamma')\gamma'\widetilde{\sigma}(\beta') &= 4(\sigma(a_0)i - \mu_0)i^{-1}(-1)(\sigma(a_0)i + \mu_0)i = -4(\sigma(a_0)i - \mu_0)(\sigma(a_0)i + \overline{\mu}_0)\\
&= -4(\sigma(a_0)^2 a - 2) = -4\sigma(a_0)(-2\sqrt{3} + a_0) = -4\sigma(a_0)^2.
\end{aligned}$$

Step 3. We have $N_{K_2/\mathbb{Q}}(x) = 16 \cdot 2^2 = 64$. It is easy to find an element $c \in K$ with $N_{K/\mathbb{Q}}(c) = \frac{1}{64}$ because we already know the elements $a_0, b_0 \in K$ have norm 4. We choose

$$c = \frac{1}{2\sigma(a_0)}, \qquad \text{and set} \qquad \gamma := c\gamma' = \frac{1}{2\sigma(a_0)}(\lambda_0\overline{\mu}_0 - 2).$$

Step 4. We have $N_{K/K_2}(c) = N_{K_1/\mathbb{Q}}(c) = -\frac{1}{8}$, hence $N_{K/K_2}(c)x = \frac{b_0^2}{2} = \frac{b_0}{\tau(b_0)}$. Therefore, we choose

$$\alpha_0 = \frac{1}{b_0}, \qquad \text{and set} \qquad \alpha := \alpha_0\alpha' = \frac{1}{b_0}\mu_0 j.$$

Step 5. We have $N_{K/K_1}(c) = c^2 = \frac{1}{4\sigma(a_0)^2}$, hence $N_{K/K_2}(c)y = -1$. Therefore, we choose

$$\beta_0 = \sqrt{3}, \qquad \text{and set} \qquad \beta := \beta_0\beta' = \sqrt{3}\lambda_0 i.$$

This shows how the elements α, β, γ were found, and also proves that they satisfy (i)–(v) of Theorem 2.2. Another solution for steps 3–5 would be $c = \frac{1}{2b_0}, \alpha_0 = \sqrt{-7}$ and $\beta_0 = \frac{1}{a_0}$.

5 The x-adic valuation and the main theorem

In this section we introduce a natural discrete valuation (the x-adic valuation) on the division rings $D(x, \widetilde{\sigma})$ and $D(\!(x, \widetilde{\sigma})\!)$ and use it to relate their subfields to the subfields of D. We first state some basic facts. References for valuations on division rings are Wadsworth's survey [17], Endler's book [6] and Schilling's book [16].

Let D be a finite-dimensional division ring. A map

$$v : D \longrightarrow \mathbb{R} \cup \{\infty\}$$

is called a *valuation* on D if the following hold for all $x, y \in D$:

$$v(x) = \infty \iff x = 0. \tag{V1}$$

$$v(xy) = v(x) + v(y). \tag{V2}$$

$$v(x + y) \geq \min\{v(x), v(y)\}. \tag{V3}$$

Here, ∞ is a symbol satisfying $\infty + c = c + \infty = \infty + \infty = \infty$ and $c < \infty$ for all $c \in \mathbb{R}$. If D is a field, this definition is precisely the one of an exponential valuation. Associated to a valuation v on D we have the *valuation ring* $B_v := \{x \in D \,|\, v(x) \geq 0\}$, which is a subring of D with the unique maximal ideal $M_v := \{x \in D \,|\, v(x) > 0\}$ and unit group $U_v := \{x \in D \,|\, v(x) = 0\}$. The factor ring $\overline{D} := \overline{B_v} := B_v/M_v$ is a division ring and is called the *residue division ring*. For any $x \in B_v$ we write $\overline{x} = x + M_v$ for the image of x in $\overline{D}$ under the canonical residue map. The value group $v(D^\times)$ is a subgroup of the additive group of $\mathbb{R}$.

If v is a valuation on D and $L \subseteq D$ is a subfield, then $v|_L$ clearly is a valuation on L in the usual commutative sense. Moreover, $\overline{L}$ is a subfield of $\overline{D}$ and $v(L^\times)$ is a subgroup of $v(D^\times)$. If $[D : L] < \infty$ then we get the fundamental inequality

$$|v(D^\times) : v(L^\times)| \cdot [\overline{D} : \overline{L}] \leq [D : L] \tag{5.1}$$

with the same proof as in the commutative case.

By (V2), B_v and M_v are invariant under inner automorphisms of D. Hence any $d \in D^\times$ induces an automorphism $\overline{\iota}_d$ of $\overline{D}$ with $\overline{\iota}_d(\overline{x}) = \overline{dxd^{-1}}$ for all $x \in B_v$. Obviously

$$\overline{\iota}_{dd'} = \overline{\iota}_d\overline{\iota}_{d'} \quad \text{for all } d, d' \in D^\times. \tag{5.2}$$

If $d \in U_v$, then $\overline{\iota}_d$ is the inner automorphism of $\overline{D}$ induced by $\overline{d}$. Hence

$$\overline{\iota}_d|_{Z(\overline{D})} = \mathrm{id}_{Z(\overline{D})} \quad \text{for all } d \in U_v. \tag{5.3}$$

Now return to the division rings $D(x;\widetilde{\sigma})$ and $D(\!(x;\widetilde{\sigma})\!)$. We use the same notation as in § 2 : $Z(D) = K$, K/F cyclic, $[K:F] = n$, $\mathrm{Gal}(K/F) = \langle\, \sigma \,\rangle$, $\widetilde{\sigma}|_K = \sigma$, $\widetilde{\sigma}^n = \mathrm{Inn}(\alpha)$, $\widetilde{\sigma}(\alpha) = \alpha$, $s = \alpha^{-1}x^n$. Recall that $Z(D(x;\sigma)) = F(s)$ and $Z(D(\!(x;\sigma)\!)) = F(\!(s)\!)$.

Example 5.1 A valuation $v : D(\!(x;\widetilde{\sigma})\!) \longrightarrow \mathbb{R} \cup \{\infty\}$ on $D(\!(x;\widetilde{\sigma})\!)$ is defined by

$$v(\sum_{i\geq k} a_i x^i) := \min\{i \in \mathbb{Z} \,|\, a_i \neq 0\},$$

and v is called the *x-adic valuation*. The valuation ring of v is

$$B_v = \{\sum_{i\geq 0} a_i x^i \,|\, a_i \in D\}$$

with maximal ideal

$$M_v = \{\sum_{i\geq 1} a_i x^i \,|\, a_i \in D\}$$

and unit group

$$U_v = \{\sum_{i\geq 0} a_i x^i \,|\, a_i \in D, a_0 \neq 0\}.$$

The residue division ring is

$$\overline{D(\!(x;\widetilde{\sigma})\!)} \cong D$$

and if we identify D with $\overline{D(\!(x;\widetilde{\sigma})\!)}$ then the residue map is

$$B_v \longrightarrow D, \quad \sum_{i\geq 0} a_i x^i \longmapsto a_0.$$

The value group of v is

$$v(D(\!(x;\widetilde{\sigma})\!)^\times) = \langle\, v(x) \,\rangle = \mathbb{Z}.$$

The x-adic valuation v restricts to a valuation on $D(x;\widetilde{\sigma})$ with the same residue field and value group. We shall denote this restriction also by v. Moreover, $v|_{F(s)}$ and $v|_{F(\!(s)\!)}$ are precisely the (commutative) s-adic valuations, thus $\overline{F(s)} = \overline{F(\!(s)\!)} = F$ and $v(F(s)^\times) = v(F(\!(s)\!)^\times) = n\mathbb{Z}$. Furthermore, $\bar{\iota}_x = \widetilde{\sigma}$, hence $\bar{\iota}_x|_K = \sigma$ and $\bar{\iota}_{x^i}|_K = \sigma^i$ for all $i \in \mathbb{Z}$.

Investigation of the maximal subfields. The following will again be carried out only for $D(x;\widetilde{\sigma})$ and is analogous for $D(\!(x;\widetilde{\sigma})\!)$. We routinely endow $D(x;\widetilde{\sigma})$ with the x-adic valuation v. For a subfield L of $D(x;\widetilde{\sigma})$ write $\overline{L}$ for the residue field of L with respect to $v|_L$, hence $\overline{L} \subseteq D$. The x-adic valuation v is used to investigate the maximal subfields of $D(x;\widetilde{\sigma})$. For the application of the following theorem in § 6 it will be necessary to consider a subfield $F_0 \subseteq F$ such that K/F_0 is Galois. We restrict ourselves to the case $\mathrm{char}\, F_0 = 0$.

Theorem 5.2 *Suppose $F_0 \subseteq F$ is a subfield such that K/F_0 is a finite Galois extension and* $\mathrm{char}\, F_0 = 0$. *If $D(x;\widetilde{\sigma})$ contains a maximal subfield L such that L is Galois over $F_0(s)$, then D contains a maximal subfield M such that M is Galois over F_0.*

We first prove

Lemma 5.3 *If L is a maximal subfield of $D(x;\widetilde{\sigma})$, then $\overline{L}K$ is a maximal subfield of D.*

P r o o f. Let L be a maximal subfield of $D(x,\widetilde{\sigma})$, i.e. by (2.4),

$$[D(x;\widetilde{\sigma}) : L] = \mathrm{ind}\, D(x;\widetilde{\sigma}) = n\,\mathrm{ind}\, D.$$

We have to show $[D : \overline{L}K] = \mathrm{ind}\, D$. Since $\overline{L}K$ is a field, $[D : \overline{L}K] \geq \mathrm{ind}\, D$, so it remains to show $[D : \overline{L}K] \leq \mathrm{ind}\, D$.

Let $v(L^\times) = l\mathbb{Z}$ for $l \in \mathbb{N}$. The fundamental inequality (5.1) states

$$|v(D(x;\widetilde{\sigma})^\times) : v(L^\times)| \cdot [D : \overline{L}] \leq [D(x;\widetilde{\sigma}) : L],$$

thus

$$[D : \overline{L}] \leq \frac{n}{l} \operatorname{ind} D. \tag{5.4}$$

Note that $|v(D(x;\widetilde{\sigma})^\times) : v(L^\times)|$ divides $|v(D(x;\widetilde{\sigma})^\times) : v(F(s))^\times|$, i.e. l divides n. Also note that $K/K \cap \overline{L}$ is Galois since K/F is Galois and $F \subseteq \overline{L}$ (because $F(s) \subseteq L$). We will show

$$[K : K \cap \overline{L}] \geq \frac{n}{l}. \tag{5.5}$$

For then $[\overline{L}K : \overline{L}] \geq \frac{n}{l}$, so (5.4) implies

$$[D : \overline{L}K] = \frac{[D : \overline{L}]}{[\overline{L}K : \overline{L}]} \leq \operatorname{ind} D.$$

This proves the lemma.

Let $\pi \in L$ be an element with $v(\pi) = l$. Then $\pi x^{-l} \in U_v$, so by (5.3), $\bar{\iota}_{\pi x^{-l}}|_K = \mathrm{id}_K$. Thus (5.2) shows $\bar{\iota}_\pi|_K = \bar{\iota}_{x^l}|_K$. Since $\pi \in L$ and L is a field, $\bar{\iota}_\pi|_{\overline{L}} = \mathrm{id}\,|_{\overline{L}}$. Therefore $\bar{\iota}_{x^l}|_{K\cap\overline{L}} = \bar{\iota}_\pi|_{K\cap\overline{L}} = \mathrm{id}_{K\cap\overline{L}}$. Since $\bar{\iota}_{x^l}|_K = \sigma^l$, this implies that $K \cap \overline{L}$ is contained in the fixed field of σ^l in K. This proves (5.5) and we are done. □

Remark 5.4 Using the theory of inertially split division algebras Lemma 5.3 can also be derived from Jacob-Wadsworth [9, Theorem 5.15 b)].

Proof of Theorem 5.2. Let L be a maximal subfield of $D(x,\widetilde{\sigma})$ such that L is Galois over $F_0(s)$. Then $M := \overline{L}K$ is a maximal subfield of D by Lemma 5.3. Since $L/F_0(s)$ Galois, $\overline{L}/F_0$ is normal (cf. Neukirch [12, Kapitel II, Satz 9.9]), hence also Galois because we have $\operatorname{char} F_0 = 0$. K/F_0 is Galois by hypothesis, therefore $M = \overline{L}K$ is Galois over F_0. □

Remark 5.5

1. Theorem 5.2 also holds in the case $\operatorname{char} F_0 > 0$, but requires some rather lengthy calculations with p-algebras. It can be found in my thesis [7, Corollary 11.5]. The proof there is based on a lemma which is essentially Saltman [14, Lemma 3].

2. It is clear that the converse of Theorem 5.2 also holds. For if M is a maximal subfield of D that is Galois over F_0, then $M(s)$ is a maximal subfield of $D(x,\sigma)$ that is Galois over $F_0(s)$. Moreover, the Galois groups are isomorphic.

6 The Proof

This section shows that the division algebras $D(x,y;\widetilde{\sigma},\widetilde{\tau},\gamma)$ and $D((x,y;\widetilde{\sigma},\widetilde{\tau},\gamma))$ constructed in § 4 are noncrossed products. We will only treat the twisted function field here, the argument for the twisted Laurent series ring is analogous.

Valuation theoretic part. Assume that $D(x,y;\widetilde{\sigma},\widetilde{\tau},\gamma)$ is a crossed product, i.e. $D(x,y;\widetilde{\sigma},\widetilde{\tau},\gamma)$ contains a maximal subfield L that is Galois over $\mathbb{Q}(s)(t)$. Recall that we write $D(x,y;\widetilde{\sigma},\widetilde{\tau},\gamma)$ for $D(x;\widetilde{\sigma})(y;\hat{\tau})$. By construction in § 4, $\hat{\tau}$ is an automorphism of $D(x;\widetilde{\sigma})$,

$$Z(D(x;\widetilde{\sigma})) = \mathbb{Q}(\sqrt{-7})(s),$$
$$Z(D(x,y;\widetilde{\sigma},\widetilde{\tau},\gamma)) = \mathbb{Q}(s)(t),$$

where $s = \alpha^{-1}x^2$, $t = \beta^{-1}y^2$ for some $\alpha,\beta \in D^\times$, and $\hat{\tau}$ restricts to the generating automorphism of $\mathbb{Q}(\sqrt{-7})(s)$ over $\mathbb{Q}(s)$. We can therefore apply Theorem 5.2 with $D(x;\widetilde{\sigma})$ for D, y for x, $\hat{\tau}$ for $\widetilde{\sigma}$, $\mathbb{Q}(\sqrt{-7})(s)$ for K and $\mathbb{Q}(s)$ for $F = F_0$. Since $D(x,y;\widetilde{\sigma},\widetilde{\tau},\gamma)$ contains a maximal subfield L that is Galois over $\mathbb{Q}(s)(t)$, Theorem 5.2 states that $D(x;\widetilde{\sigma})$ contains a maximal subfield L' that is Galois

over $\mathbb{Q}(s)$. In turn, $\widetilde{\sigma}$ of D restricts to the generating automorphism of K over $\mathbb{Q}(\sqrt{-7})$, hence we can apply Theorem 5.2 to $D(x;\widetilde{\sigma})$ with $F=\mathbb{Q}(\sqrt{-7})$ and $F_0=\mathbb{Q}$. This shows that D contains a maximal subfield M that is Galois over $\mathbb{Q}$. It remains to prove that such M cannot exist.

Some facts. Before finishing the proof we recall some facts on Galois extensions of number fields. These can be found e.g. in Neukirch [12, Kapitel II]. Let K/F be a finite Galois extension of a number field, $[K:F]=n$ and $\mathrm{Gal}(K/F)=G$. Let v be a valuation on F that uniquely extends to a valuation w on K. We denote by F_v, K_w the completions and by $\overline{F}_v$,$\overline{K}_w$ the residue fields. Let $\mathrm{char}\,\overline{F}_v=p$ and $|\overline{F}_v|=q$. Then $\overline{F}_v^{\times}$ consists of the $(q-1)$-th roots of unity, hence $\overline{F}_v$ contains a primitive e-th root of unity iff $q\equiv 1 \bmod e$. The extension K_w/F_v is Galois and $\mathrm{Gal}(K_w/F_v)\cong G$ since w is the unique extension of v.

If $p\nmid n$ and v is totally ramified in K/F, i.e. $|w(K^{\times}):v(F^{\times})|=n$, then $K_w=F_v(\sqrt[n]{\xi})$ for some $\xi\in F_v$ (cf. Neukirch [12, Kapitel II, Satz 7.7]). It follows that G is cyclic and that F_v and $\overline{F}_v$ contain a primitive n-th root of unity, hence $q\equiv 1 \bmod n$.

The inertia group of v in K/F is the subgroup

$$I:=I_v(K/F)=\{\sigma\in G|\sigma(x)\equiv x \bmod \mathfrak{P}_w \text{ for all } x\in\mathcal{O}_w\}$$

of G and the inertia field of v in K/F is the fixed field of I in K

$$T:=T_v(K/F)=\mathrm{Fix}(I_v(K/F)).$$

Then I is a normal subgroup of G and $G/I\cong\mathrm{Gal}(\overline{K}_w/\overline{F}_v)$ (cf. Neukirch [12, Satz 9.9]), which is a cyclic group since $\overline{K}_w$ is a finite field. Thus T/F is a cyclic extension. Moreover T/F is the maximal unramified subextension of K/F and K/T is totally ramified with respect to v (cf. Neukirch [12, Satz 9.11]). Hence if $p\nmid n$, then I and G/I are both cyclic.

Number theoretic part. For the proof of the main theorem of this section we need the following lemma. By a real field we mean a subfield of $\mathbb{R}$.

Lemma 6.1 *Let F be a real field and let L/F be a finite Galois extension. Then L is real or there exists a real intermediate field $F\subseteq K\subset L$ such that $[L:K]=2$.*

Proof. Since L/F is Galois and F is real, L is closed under complex conjugation. Let K be the fixed field of the complex conjugation in L. Then K is real and, clearly, $K=L$ or $[L:K]=2$. □

Theorem 6.2 *Let F be a real number field, and let K/F be a biquadratic extension such that K is not real. Suppose there are valuations v_1 and v_2 of F such that*

(i) $|\overline{F}_{v_i}|\equiv 3 \bmod 4$ *for* $i=1,2$,

(ii) v_1 *and* v_2 *extend uniquely to valuations of* K,

(iii) $T_{v_1}(K/F)\neq T_{v_2}(K/F)$.

If L/K is a field extension, $[L:K]=2$, such that v_1 and v_2 extend uniquely to valuations of L, then L/F is not Galois.

Proof. Assume there exists such an L with L/F Galois and $\mathrm{Gal}(L/K)=G$. Then $|G|=8$. We now check all possible cases of G, i.e. all groups of order 8 up to isomorphism. Note that by (i), $\mathrm{char}\,\overline{F}_{v_i}\neq 2$ for $i=1,2$, hence we can use the facts on Galois extension of number fields that were recalled above.
Case 1 : G is the dihedral group. Then G has only one normal subgroup I such that I and G/I are cyclic. Therefore $T_{v_1}(L/F)=T_{v_2}(L/F)$, hence $T_{v_1}(K/F)=T_{v_1}(L/F)\cap K=T_{v_2}(L/F)\cap K=T_{v_2}(K/F)$, which contradicts (iii).
Case 2 : G is the quaternion group. Since K is not real, L is not real. Hence by Lemma 6.1 there is a real subfield $L_0\subset L$ with $[L:L_0]=2$. Then $L_0\neq K$ and $[L_0:F]=4$. But G contains only one subgroup of order 2, a contradiction.
Case 3 : G is abelian. Let L_0 be as in case 2. Since G is abelian, L_0/F is Galois. We show that w.l.o.g. v_1

is totally ramified in L_0/F. Then $\overline{F}_{v_1}$ must contain a primitive 4-th root of unity, i.e. $|\overline{F}_{v_1}| \equiv 1 \bmod 4$, which contradicts (i).

Since $\mathrm{Gal}(K/F)$ is not cyclic, $[T_{v_i}(K/F) : F] = 2$ for $i = 1, 2$, and from $L_0 \neq K$ we get $[L_0 \cap K : F] \leq 2$. Therefore, because of (iii), we can assume w.l.o.g. that $L_0 \cap T_{v_1}(K/F) = F$. Since $T_{v_1}(L/F)$ is cyclic over F and of prime power degree, its subfields are linearly ordered, so $T_{v_1}(K/F)$ is the unique subfield of $T_{v_1}(L/F)$ of degree 2 over F. Therefore, $L_0 \cap T_{v_1}(K/F) = F$ implies $L_0 \cap T_{v_1}(L/F) = F$, i.e. v_1 is totally ramified in L_0/F. □

Remark 6.3 It should be mentioned here that the question whether a biquadratic extension K/F embeds into a Galois extension with group isomorphic to the quaternion group is completely treated in Witt [18, § VI].

To complete the proof we have to show that D as defined in § 4 does not contain a maximal subfield M such that M is Galois over $\mathbb{Q}$. Because of (N1)–(N4) we can apply Theorem 6.2 with K/F as in § 4 and $v_1 = v_p, v_2 = v_q$. By (N5), $D \otimes_K K_w$ is a division algebra for $w = w_p, w_q$, thus $M \otimes_K K_w$ is a field for $w = w_p, w_q$. This shows that w_p and w_q uniquely extend to valuations on M. Therefore, $M/\mathbb{Q}$ is not Galois by Theorem 6.2. We have now completed the proof that $D(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)$ and $D(\!(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)\!)$ are noncrossed product division algebras.

7 The Exponent

The following outlines the calculation of the exponents of the noncrossed product division algebras $D(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)$ and $D(\!(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)\!)$. For the rest of this paper it is assumed that the reader is familiar with some noncommutative valuation theory, including inertially split division algebras, as contained e.g. in Wadsworth's survey [17, § 1–3].

We endow the division algebra $D(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)$ with the *composite valuation* of the y-adic and the x-adic valuation (see e.g. Wadsworth's survey [17, p. 397] for a definition). This is a *rank 2* valuation and not a valuation in the sense of § 5. The completion of the valued division algebra $D(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)$ is $D(\!(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)\!)$. If we show that the latter has exponent equal to its index, the same also holds for the former. Note that the residue field in both cases is D.

The algebra $D(\!(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)\!)$ is obviously inertially split, since for any maximal subfield L of D the field $L(\!(s)\!)(\!(t)\!)$ is an inertial maximal subfield of $D(\!(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)\!)$. We will apply

Lemma 7.1 *Let D be a valued division algebra with $F = \overline{Z(D)}$ a global field. Suppose that D is inertially split and suppose that each prime divisor of $[Z(\overline{D}) : F]$ divides $\operatorname{ind}\overline{D}$. If there is a valuation v on F that uniquely extends to a valuation w on $Z(\overline{D})$ and the completion $\overline{D}_w$ is a division algebra, then $\exp D = \operatorname{ind} D$.*

P r o o f. Let $K = Z(\overline{D})$ and let $n = [K : F]$. From the theory of inertially split division algebras (see Jacob-Wadsworth [9, Theorem 5.15]) we know that $\operatorname{ind} D = n \operatorname{ind}\overline{D}$ and $\exp D = \operatorname{lcm}(\exp \mathrm{Gal}(K/F), \exp A)$ for a certain central simple F-algebra A with $A \otimes_F K \sim \overline{D}$. In particular, $A_v \otimes_{F_v} K_w \sim \overline{D}_w$. The theory of division algebras over local fields (e.g. Pierce [13, Proposition 17.10]) states that $\operatorname{inv}\overline{D}_w = [K_w : F_v] \operatorname{inv} A_v = n \operatorname{inv} A_v$. It follows that

$$\operatorname{ind}\overline{D} = \exp\overline{D}_w = \frac{\exp A_v}{(\exp A_v, n)}. \tag{7.1}$$

The hypothesis that each prime divisor of n divides $\operatorname{ind}\overline{D}$ then implies $n | \exp A_v$. In turn, (7.1) yields $\operatorname{ind} D = n \operatorname{ind}\overline{D} = \exp A_v$. Finally, since $\exp \mathrm{Gal}(K/F) | n | \exp A_v | \exp A$,

$$\operatorname{ind} D = \exp A_v | \exp A = \operatorname{lcm}(\exp \mathrm{Gal}(K/F), \exp A) = \exp D | \operatorname{ind} D.$$

This proves the lemma. □

In the application of Lemma 7.1 with $D(\!(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)\!)$ for D and $\mathbb{Q}$ for F we choose v to be any one of the valuations v_p, v_q on $\mathbb{Q}$. Obviously 2, the only prime divisor of $[K : \mathbb{Q}]$, divides $\operatorname{ind} D$ because D is a quaternion division algebra. By (N2), v uniquely extends to a valuation w on K, and by (N5), $D_w = D \otimes_K K_w$ is a division algebra. Therefore, Lemma 7.1 yields

$$\exp D(\!(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)\!) = \operatorname{ind} D(\!(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)\!) = 8.$$

The result is

$$\exp D(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma) = \exp D(\!(x, y; \widetilde{\sigma}, \widetilde{\tau}, \gamma)\!) = 8.$$

Acknowledgements I am greatly indebted to Joachim Gräter for his guidance and support during the work on my Ph.D. thesis including this paper at Potsdam, Germany. Furthermore, I would like to thank Darrel Haile for his invitation to IU Bloomington, USA, in 1999 and for his support during my stay there in which parts of the results of this paper were obtained. The financial support for this visit from the DAAD is also acknowledged. Particular appreciation goes to the referees for their kind and detailed suggestions on improvements of the paper.

References

[1] S. A. Amitsur, *On central division algebras*, Israel J. Math. **12** (1972), 408–420.
[2] E. S. Brussel, *Noncrossed products and nonabelian crossed products over $\mathbb{Q}(t)$ and $\mathbb{Q}((t))$*, American Journal of Mathematics **117** (1995), 377–393.
[3] ———, *Noncrossed products over $k_{\mathfrak{p}}(t)$*, Trans. Amer. Math. Soc. **353** (2001), 2115–2129.
[4] P. M. Cohn, *Introduction to Ring Theory*, Springer-Verlag, London, 2000.
[5] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, and K. Wildanger, *KANT V4*, J. Symbolic Comp. **24** (1997), 267–283.
[6] O. Endler, *Valuation Theory*, Springer-Verlag, New York, 1972.
[7] T. Hanke, *A direct approach to noncrossed product division algebras*, Dissertation, Universität Potsdam, 2001.
[8] B. Jacob and A. R. Wadsworth, *A new construction of noncrossed product algebras*, Trans. Amer. Math. Soc. **293** (1986), 693–721.
[9] ———, *Division algebras over Henselian fields*, J. Algebra **128** (1990), 126–179.
[10] N. Jacobson, *Finite dimensional division algebras over fields*, Springer-Verlag, Berlin, 1996.
[11] T. Y. Lam, *A first course in noncommutative rings*, Springer-Verlag, New York, 1991.
[12] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, Berlin, 1992.
[13] R. S. Pierce, *Associative Algebras*, Springer-Verlag, New York, 1982.
[14] D. J. Saltman, *Noncrossed products of small exponent*, Proc. Amer. Math. Soc. **68** (1978), 165–168.
[15] ———, *Lectures on division algebras*, CBMS Regional Conference Series in Mathematics, vol. 94, Amer. Math. Soc., Providence, 1999.
[16] O. F. G. Schilling, *The theory of valuations.*, Math. Surveys No. 4, Amer. Math. Soc., Providence, R.I., 1950.
[17] A. R. Wadsworth, *Valuation theory on finite dimensional division algebras*, Proceedings of the 1999 Saskatoon Conference on Valuation Theory, 1999.
[18] E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f*, J. Reine Angew. Math. **174** (1936), 237–245.