COMPUTATION OF OUTER AUTOMORPHISMS OF CENTRAL-SIMPLE ALGEBRAS

TIMO HANKE[1]

Abstract. The paper presents algorithms for extending a field automorphism to a given finite-dimensional central-simple algebra over that field and, more generally, for computing an isomorphism between two given central-simple algebras. It is assumed that a) the central-simple algebras are given as crossed products with solvable groups, and b) certain computational problems in field extensions of the centre can be solved. The requirements b) include the algorithmic solvability of norm equations in cyclic relative extensions. They can be regarded as met if the centre is a number field.

The algorithm can be used for the explicit construction of certain algebras, for instance skew polynomials and crossed products of simple algebras. In this way explicit non-crossed product division algebras have been obtained. Another application is the computation of sets of orthogonal idempotents in central-simple algebras.

1. Introduction

Various algebra constructions – notably skew polynomials and crossed products over simple algebras – involve automorphisms of finite-dimensional simple algebras that are generally non-trivial on the centre (not inner). In the process of construction it is common to have a non-trivial automorphism of the centre that one wishes to extend to the simple algebra. We formulate this as the

Extension Problem (EP). *Given a field K with automorphism σ and a finite-dimensional central-simple K-algebra A. Decide whether σ extends to an automorphism of A and, if so, compute an extension.*

For instance, the EP arises in the construction of explicit non-crossed product division algebras in both [5] and [6] where non-crossed products are obtained as (iterated) twisted Laurent series rings or twisted function fields over division algebras.

The paper discusses the EP for crossed product algebras A – a situation that is reasonable to assume if one works over local or global fields – and presents a reduction of the EP to purely field theoretic computational problems. The field theoretic problems are not in the scope of this paper but are known to have algorithmic solutions at least over number fields. The reduction itself, however, applies over arbitrary fields so that this paper does not require any number theory. Among the field theoretic problems that occur are the computation of minimal polynomials,

Date: February 2, 2007.

1991 *Mathematics Subject Classification.* Primary 16Z05; Secondary 16K20, 16S35, 16W20.

Key words and phrases. outer automorphism, isomorphism, extension, finite-dimensional central-simple algebra, explicit construction, algorithm, computation, orthogonal idempotent, explicit splitting, solvable crossed product, skew polynomial, cyclic norm equation, relative norm equation, finite group cohomology, 2-cocycle, non-crossed product.

[1]Supported by the German Academic Exchange Service (DAAD, Kennziffer D/02/00701) and by the Universidad Nacional Autónoma de México.

primitive elements, field composita and intersections, extensions of field automorphisms, embeddings of subfields and solutions of relative norm equations in cyclic extensions.

Our approach is based on interpreting the EP as a special case of the

Isomorphism Problem (IP). *Given two central-simple K-algebras A and B. Decide whether A and B are isomorphic as K-algebras and, if so, compute a K-algebra isomorphism between them.*

In the important special case when B is the full matrix ring the IP amounts to finding a set of orthogonal idempotent generators in A. Since this is a hard problem it is advisable to make simplifying assumptions. This paper assumes A and B to be crossed products, then the IP translates (modulo field theory) to the following computational problem from finite group cohomology.

Splitting Problem (SP). *Let G be a finite Galois group acting on a field L. Given a 2-cocycle $f \in Z^2(G, L^*)$. Decide whether f is split (a 2 coboundary) and, if so, compute a 1-cochain $l \in C^1(G, L^*)$ that maps to f under the coboundary map.*

For solvable group G the SP is shown to reduce to the case of cyclic G, which is well-known to be equivalent to a relative norm equation in L. The module L^* in this process can be replaced by any H^1-trivial G-module M. Combining all reductions we get an algorithm for the EP that is applicable to crossed products with solvable group over number fields.

Essential parts of the presented algorithm have been implemented in the computer algebra system MAGMA [1]. The algebras are stored as objects of MAGMA's category for associative algebras and are presented by structure constants (which in the case of crossed products are derived canonically from the defining 2-cocycles). Using MAGMA's built-in algebraic number theory capabilities, the implementation proved successful in solving the extension problem in an important example of a cubic division algebra D over a cubic number field. Namely, it is this example that leads to the explicit noncrossed product division algebra from [6]. The non-crossed product is the twisted Laurent series ring $D((\mathbf{x}, \widetilde{\sigma}))$ where $\widetilde{\sigma}$ is the automorphism of D that is obtained by extending a non-trivial automorphism σ of the centre.

It is assumed that the reader is familiar with the basic theory of simple algebras and Brauer groups as it is presented for instance in Pierce [11, Chapters 12–14]. The paper is structured as follows. Section 2 recalls preliminaries on crossed products of simple algebras. Not only is their construction an application of the algorithm, the use of crossed products of simple algebras is also required in one of the algorithm's steps (see Algorithm 4.7). The reduction of the extension problem to a cohomology computation is then presented in reverse order : section 3 treats the SP and its reduction to norm equations, section 4 treats the IP and its reduction to the SP, and section 5 treats the EP and its reduction to the IP. Finally, section 6 contains a step-by-step solution of the extension problem in the above mentioned example of a cubic division algebra over a cubic number field.

It shall be pointed out that results from this paper may also be used for the computation of sets of orthogonal idempotents in central-simple algebras, as this is just a special case of the IP.

2. Preliminaries

All algebras are assumed to be finite-dimensional over their centre and all field extensions are assumed to be finite as well. We write $\mathcal{A}(K)$ for the set of all finite-dimensional simple algebras with centre K. For any $A \in \mathcal{A}(K)$ the class of A in the Brauer group $\mathrm{Br}(K)$ is denoted by $[A]$. We write $A \sim A'$ if $[A] = [A']$.

2.1. **Outer automorphisms and extensions.** Let $A \in \mathcal{A}(K)$ and let $\mathrm{Aut}(A)$ be its automorphism group. Write $\mathrm{Inn}(A) \trianglelefteq \mathrm{Aut}(A)$ for the normal subgroup of all inner automorphisms $\mathrm{Inn}(x) : a \longmapsto xax^{-1}, x \in A^*$. The *outer automorphism group* is defined as $\mathrm{Out}(A) := \mathrm{Aut}(A)/\mathrm{Inn}(A)$. Clearly, $\mathrm{Inn}(A) \cong A^*/K^*$ and we have the exact sequence

$$1 \longrightarrow \mathrm{Inn}(A) \longrightarrow \mathrm{Aut}(A) \xrightarrow{\pi_A} \mathrm{Out}(A) \longrightarrow 1.$$

Let $\alpha : \mathrm{Aut}(A) \longrightarrow \mathrm{Aut}(K)$ denote the homomorphism defined by restricting automorphisms to K. Since $\mathrm{Inn}(A)$ fixes the centre K pointwise, α induces a homomorphism $\overline{\alpha} : \mathrm{Out}(A) \longrightarrow \mathrm{Aut}(K)$ with $\overline{\alpha} \circ \pi = \alpha$.

The theorem of Skolem-Noether states that $\overline{\alpha}$ is injective, and we shall from now on identify $\mathrm{Out}(A)$ with its image under $\overline{\alpha}$. Then $\mathrm{Out}(A) = \alpha(\mathrm{Aut}(A))$ consists precisely of the $\sigma \in \mathrm{Aut}(K)$ that extend to an automorphism of A. The EP in this context means to determine the subgroup $\mathrm{Out}(A) \leqslant \mathrm{Aut}(K)$ and to compute explicitly a section ω of the surjection π_A. We call a map $\omega : H \longrightarrow \mathrm{Aut}(A)$ defined on a subgroup $H \leqslant \mathrm{Out}(A)$ an *extension map* for H if $\pi_A \circ \omega = \mathrm{id}_H$ and $\omega(\mathrm{id}_K) = \mathrm{id}_A$.

2.2. **Crossed products of simple algebras.** References on crossed products of simple algebras are, for instance, Jehne [8], Kursov-Yanchevskiĭ[9] and Tignol [14]. We recall here briefly the basic definitions and propositions that will be required. Our notation may differ slightly from the cited references.

2.2.1. *Factor sets.* Throughout this subsection let $B \in \mathcal{A}(K)$ and let $H \leqslant \mathrm{Out}(B)$ be finite. Fix an extension map

$$\omega : H \longrightarrow \mathrm{Aut}(B), \quad \sigma \longmapsto \omega_\sigma.$$

The choice of ω defines the map

$$\phi : H \times H \longrightarrow \mathrm{Inn}(B), \quad (\sigma, \tau) \longmapsto \phi(\sigma, \tau) := \omega_\sigma \omega_\tau \omega_{\sigma\tau}^{-1}$$

with $\phi(\mathrm{id}_K, \mathrm{id}_K) = \mathrm{id}_B$.

Definition 2.1. A *factor set* of H in B^* (with respect to ω) is a map

$$f : H \times H \longrightarrow B^*, \quad (\sigma, \tau) \longmapsto f(\sigma, \tau)$$

such that $\phi = \mathrm{Inn} \circ f$ and for all $\rho, \sigma, \tau \in G$:

$$\omega_\rho(f(\sigma, \tau)) f(\rho, \sigma\tau) = f(\rho, \sigma) f(\rho\sigma, \tau). \tag{2.1}$$

Denote by $\mathcal{F}(H, B^*)$ (or $\mathcal{F}_\omega(H, B^*)$) the set of all factor sets of H in B^*. We will assume for the sake of simplicity that all factor sets satisfy $f(\mathrm{id}_K, \mathrm{id}_K) = 1$.

Note that in general $\mathcal{F}(H, B^*)$ can be empty. The situation when $\mathcal{F}(H, B^*)$ is non-empty is characterized in Corollary 2.12 below.

Example 2.2 (B field)**.** If B is a field then $K = B$, the extension map ω is just the inclusion $H \hookrightarrow \mathrm{Aut}(K)$, and $\mathcal{F}(H, B^*) = Z^2(H, K^*)$.

Example 2.3 (H cyclic)**.** Let $\sigma \in \mathrm{Out}(B)$ be of finite order n. Suppose that the extension map ω for $H = \langle\sigma\rangle$ is given by $\sigma^i \longmapsto \widetilde{\sigma}^i$, where $\widetilde{\sigma} \in \mathrm{Aut}(B)$ is some fixed extension of σ. As a consequence of Hilbert's Theorem 90 (cf. Pierce [11, Lemma 19.7]), there is an element $\alpha \in B^*$ such that

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

It is easily verified that for any such α a factor set $f_\alpha \in \mathcal{F}(H, B^*)$ is defined by

$$f_\alpha(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } i + j < n, \\ \alpha & \text{if } i + j \geq n, \end{cases} \tag{2.2}$$

$0 \leq i, j < n$. In particular, $\mathcal{F}(H, B^*)$ is non-empty.

Proposition 2.4. *If $\mathcal{F}(H,B^*)$ is non-empty and f is any element then*

$$Z^2(H,K^*) \longrightarrow \mathcal{F}(H,B^*), \quad c \longmapsto fc \tag{2.3}$$

is a bijection, where fc is the pointwise product.

Let $f,g \in \mathcal{F}(H,B^*)$. By Proposition 2.4 there is a unique $c \in Z^2(H,K^*)$ such that $f = gc$. Since c has image in the centre K^*, it is equal to both of the pointwise quotients fg^{-1} and $g^{-1}f$. We therefore simply write $c = f/g$.

Definition 2.5. Two factor sets $f,g \in \mathcal{F}(H,B^*)$ are said to be *cohomologous*, written $f \sim g$, if $f/g \in B^2(H,K^*)$. The quotient set modulo this equivalence relation is denoted $\mathcal{H}(H,B^*) := \mathcal{F}(H,B^*)/\sim$.

By definition of the relation $\sim$, if $\mathcal{F}(H,B^*)$ is non-empty and f is any element then (2.3) induces a well-defined bijection

$$H^2(H,K^*) \longrightarrow \mathcal{H}(H,B^*), \quad [c] \longmapsto [fc],$$

where $[\cdot]$ denotes equivalence classes.

2.2.2. *Crossed products.* Throughout this subsection let $H \leqslant \mathrm{Aut}(K)$ be finite, let $k = \mathrm{Fix}(H)$ be its fixed field, and let $B \in \mathcal{A}(K)$.

Definition 2.6. Let $H \leqslant \mathrm{Out}(B)$ and let $f \in \mathcal{F}(H,B^*)$. The *crossed product* (B,H,f) of the simple algebra B with H is the central-simple k-algebra A defined as the k-space $\bigoplus_{\sigma\in H} Bu_\sigma$ with multiplication rules

$$u_\sigma x = \omega_\sigma(x)u_\sigma \quad \text{and} \quad u_\sigma u_\tau = f(\sigma,\tau)u_{\sigma\tau} \quad \text{for all } \sigma,\tau \in H, x \in B.$$

It is $1_A = u_{\mathrm{id}}$ and we identify B with the subalgebra Bu_{id}. To point out the naming of the basis elements u_σ we also write $A = (B,H,f,u)$.

Example 2.7 (B field)**.** If B is a field then $K = B$ and the crossed product (B,H,f) is the usual crossed product $(K/k,H,f)$ of a field.

Remark 2.8. For a crossed product $A = (B,H,f)$ we have $C_A(K) = B$.

Example 2.9. Let $A = (L/k,G,f,u)$ be a crossed product of a field. Let K be an intermediate field $k \subseteq K \subseteq L$ and let $B = C_A(K)$. Then

$$B = (L/K, U, \mathrm{res}\, f, u) \subseteq A,$$

where $U = \mathrm{Gal}(L/K)$ and $\mathrm{res}\, f$ is the restriction of f to $U \times U$. Here, the subfield $L \subseteq B$ is identified with $L \subseteq A$ and the elements $u_\sigma \in B$ are identified with $u_\sigma \in A$ for all $\sigma \in U$.

Lemma 2.10. *Suppose $A \in \mathcal{A}(k)$ contains K as a subfield. Let $B = C_A(K)$. Then $H \leqslant \mathrm{Out}(B)$ and for any extension map $\omega : H \longrightarrow \mathrm{Aut}(B)$,*

$$A = (B,H,f) \quad \textit{for some } f \in \mathcal{F}_\omega(H,B^*).$$

Moreover, f can be computed with linear algebra.

Proof. Let $\sigma \in H$. By the Skolem-Noether theorem there is $z_\sigma \in A^*$ such that $\mathrm{Inn}(z_\sigma)|_K = \sigma$. Since $B = C_A(K)$ we have $\mathrm{Inn}(z_\sigma)(B) = B$, thus $\sigma \in \mathrm{Out}(B)$.

Now let $\omega : H \longrightarrow \mathrm{Aut}(B)$ be an extension map. Choose a family $\{z_\sigma\}_{\sigma\in H}$ in A^* such that $\mathrm{Inn}(z_\sigma)|_B = \omega_\sigma$ and assume $z_{\mathrm{id}} = 1$. Then

$$A = (B,H,f_z,z),$$

where $f_z \in \mathcal{F}_\omega(H,B^*)$ is defined by $f_z(\sigma,\tau) := z_\sigma z_\tau z_{\sigma\tau}^{-1}$. Note that the elements z_σ are obtained as solutions to linear equation systems. □

Proposition 2.11. *For $A \in \mathcal{A}(k)$ the following are equivalent :*

(1) $B \sim A \otimes_k K$,

(2) *B embeds (as k-algebra) into some $A' \in \mathcal{A}(k)$ with $A' \sim A$ such that $B = C_{A'}(K)$,*
(3) *$H \leqslant \mathrm{Out}(B)$ and there exists $f \in \mathcal{F}(H, B^*)$ such that $(B, H, f) \sim A$.*

Proof. (1) $\Rightarrow$ (2) follows from standard arguments on algebraic splitting fields (cf. Pierce [11, § 13.3]). (2) $\Rightarrow$ (3) is Lemma 2.10. (3) $\Rightarrow$ (1) : If $(B, H, f) \sim A$ then by Remark 2.8 and standard arguments on centralizers (cf. again Pierce [11, § 13.3]), $B \sim C_{(B,H,f)}(K) \sim (B, H, f) \otimes_k K \sim A \otimes_k K$. □

Writing res : $\mathrm{Br}(k) \longrightarrow \mathrm{Br}(K)$ for the restriction map $[A] \longmapsto [A \otimes_k K]$ we formulate two corollaries of Proposition 2.11.

Corollary 2.12. *The following are equivalent :*

(1) *$H \leqslant \mathrm{Out}(B)$ and $\mathcal{F}(H, B^*)$ is non-empty,*
(2) *$[B]$ lies in the image of* res*,*
(3) *B embeds into some $A \in \mathcal{A}(k)$ such that $C_A(K) = B$.*

In particular, these conditions depend only on the class of B.

Corollary 2.13. *(i) Let $f, g \in \mathcal{F}(H, B^*)$. Then $(B, H, f) \cong_k (B, H, g)$ if and only if $f \sim g$, i.e. the map*

$$\gamma : \mathcal{H}(H, B^*) \longrightarrow \mathrm{Br}(k), \quad [f] \longmapsto [(B, H, f)]$$

is well-defined and injective.

(ii) Identifying $\mathcal{H}(H, B^*)$ with its image under γ we have $\mathcal{H}(H, B^*) = \mathrm{res}^{-1}([B])$.

Proof. (i) is proved just like in the case of crossed products of fields (cf. Pierce [11, Lemma 14.2]). (ii) is the equivalence of (1) and (3) in Proposition 2.11. □

3. The splitting problem for 2-cocycles

Let G be a finite group and let M be a left G-module, written additively. Recall that the 2-cocycles $f \in Z^2(G, M)$ are the maps $f : G \times G \longrightarrow M$ satisfying

$$\rho f(\sigma, \tau) + f(\rho, \sigma\tau) = f(\rho\sigma, \tau) + f(\rho, \sigma), \tag{3.1}$$

the 1-cochains $l \in C^1(G, M)$ are the maps $l : G \to M, \sigma \longmapsto l_\sigma$ and the coboundary map $\partial : C^1(G, M) \longrightarrow Z^2(G, M)$ is defined by $\partial l(\sigma, \tau) := l_\sigma + \sigma l_\tau - l_{\sigma\tau}$. We suppose for the sake of simplicity that all 2-cocycles satisfy $f(1, 1) = 0$, which obviously implies $f(G, 1) = f(1, G) = 0$, and that all 1-cochains satisfy $l_1 = 0$.

Splitting Problem (SP). *Given $f \in Z^2(G, M)$. Decide whether f is split (a coboundary) and, if so, compute an $l \in C^1(G, M)$ with $f = \partial l$. Such an l is called an* explicit splitting *of f.*

Note that for finitely generated G-modules M there are known algorithms and also MAGMA implementations by D. Holt for first and second cohomology computations. However, since in our applications M is the multiplicative group of a field, we cannot assume M to be finitely generated. Our approach is to reduce the SP to norm equations.

3.1. **Cyclic 2-cocycles.** First, we recall that in the case of a cyclic group G the splitting problem is equivalent to a cyclic norm equation. Let $G = \langle\sigma\rangle$ be of order n. For each $0 \leq i < n$ set $N_i := 1 + \sigma + \ldots + \sigma^{i-1} \in \mathbb{Z}G$, and set $N := N_n$.

Cyclic norm equation. *Given $a \in M^G$. Decide whether $a \in NM$ and, if so, compute an element $x \in M$ such that $Nx = a$.*

It is well-known that $H^2(G,M) \cong \hat{H}^0(G,M) = M^G/NM$ (cf. Neukirch [10, Proposition 1.6.12, p. 68] for the cup product argument or Brown [2, Ch. III, §1, Example 2, p. 58] for the explicit computation with a periodic projective resolution). Hence, the SP for cyclic groups is equivalent to a cyclic norm equation. We formulate a constructive proof of this equivalence as

Algorithm 3.1 (Cyclic splitting problem)**.** Let G be cyclic and let $f \in Z^2(G,M)$. The splitting problem for f is solved as follows.

1. Choose a generator σ of G and set $a := \sum_{k=0}^{n-1} f(\sigma^k,\sigma) \in M^G$.
2. Solve the cyclic norm equation $Nx = a$ in M. If it has no solution then f is not split, otherwise let $x \in M$ be a solution and continue.
3. Define $l \in C^1(G,M)$ by

$$l_{\sigma^i} := N_i x - \sum_{k=0}^{i-1} f(\sigma^k,\sigma), \quad 0 \le i < n, \tag{3.2}$$

then $\partial l = f$.

Proof. 1. From (3.1) we get

$$\sigma^i f(\sigma^k,\sigma) = f(\sigma^{i+k},\sigma) + f(\sigma^i,\sigma^k) - f(\sigma^i,\sigma^{k+1}), \tag{3.3}$$

hence

$$\sigma a = \sum_{k=0}^{n-1} (f(\sigma^{k+1},\sigma) + f(\sigma,\sigma^k) - f(\sigma,\sigma^{k+1})) = a.$$

2. Suppose f is split, say $f = \partial l$, $l \in C^1(G,M)$. Then

$$a = \sum_{k=0}^{n-1} f(\sigma^k,\sigma) = \sum_{k=0}^{n-1} (l_{\sigma^k} + \sigma^k l_\sigma - l_{\sigma^{k+1}}) = \sum_{k=0}^{n-1} \sigma^k l_\sigma = N l_\sigma,$$

i.e. $Nx = a$ has a solution in M.
3. For all $0 \le i,j < n$ we have by (3.2)

$$\partial l(\sigma^i,\sigma^j) = l_{\sigma^i} + \sigma^i l_{\sigma^j} - l_{\sigma^{i+j}} =$$
$$(N_i x + \sigma^i N_j x - N_{\overline{i+j}} x) - (\sum_{k=0}^{i-1} f(\sigma^k,\sigma) + \sum_{k=0}^{j-1} \sigma^i f(\sigma^k,\sigma) - \sum_{k=0}^{\overline{i+j}-1} f(\sigma^k,\sigma)),$$

where $\overline{i+j}$ denotes $i+j$ reduced modulo n. Hence, using (3.3) we get for $i+j < n$:

$$\begin{aligned}\partial l(\sigma^i,\sigma^j) &= 0 - (\sum_{k=0}^{i-1} f(\sigma^k,\sigma) + \sum_{k=0}^{j-1} (f(\sigma^{i+k},\sigma) + f(\sigma^i,\sigma^k) - f(\sigma^i,\sigma^{k+1})) - \sum_{k=0}^{i+j-1} f(\sigma^k,\sigma)) \\ &= f(\sigma^i,\sigma^j) - f(\sigma^i,\sigma^0) = f(\sigma^i,\sigma^j),\end{aligned}$$

and for $i+j \ge n$:

$$\begin{aligned}\partial l(\sigma^i,\sigma^j) &= Nx - (\sum_{k=0}^{i-1} f(\sigma^k,\sigma) + \sum_{k=0}^{j-1} (f(\sigma^{i+k},\sigma) + f(\sigma^i,\sigma^k) - f(\sigma^i,\sigma^{k+1})) - \sum_{k=0}^{i+j-n-1} f(\sigma^k,\sigma)) \\ &= Nx - \sum_{k=0}^{n-1} f(\sigma^k,\sigma) + f(\sigma^i,\sigma^j) - f(\sigma^i,\sigma^0) = f(\sigma^i,\sigma^j).\end{aligned}$$

□

3.2. **Inverse Inflation.** A process called *inverse inflation* will enable us to reduce from the solvable to the cyclic case.

We call a G-module M *H^1-trivial* if $H^1(H, M) = 0$ for all $H \leqslant G$. Moreover, M is called *constructively H^1-trivial* if for any $H \leqslant G$ and any $l \in Z^1(H, M)$ we can effectively construct an element $m \in M$ such that $l_\sigma = \sigma m - m$ for all $\sigma \in H$. An example is the multiplicative group L^* of a field L on which G acts as Galois group, because the proof of Hilbert's theorem 90 is constructive.

Lemma 3.2. *Let M be a G-module and let $N \trianglelefteq G$. If M is (constructively) H^1-trivial then M^N is (constructively) H^1-trivial as a G/N-module.*

Proof. The inflation $H^1(G/N, M^N) \longrightarrow H^1(G, M)$ is injective : if $l \in Z^1(G/N, M^N)$ and $m \in M$ is an element with $l_{\sigma N} = \sigma m - m$ for all $\sigma \in G$ then $m \in M^N$ follows. Hence $H^1(G/N, M^N) = 0$ (in a constructive manner) if M is (constructively) H^1-trivial.

Now let $U \leqslant G/N$. Then $U = H/N$ for $H := \{g \in G \mid gN \in U\}$ and the same argument applied to H/N shows $H^1(U, M^N) = 0$. □

Let M be a constructively H^1-trivial G-module and let $N \trianglelefteq G$. Since $H^1(N, M) = 0$ we have the well known exact sequence

$$0 \longrightarrow H^2(G/N, M^N) \xrightarrow{\inf} H^2(G, M) \xrightarrow{\text{res}} H^2(N, M)$$

(cf. Neukirch [10, Prop. 1.6.6, p. 64] or Serre [13, Ch. VII, Prop. 5, p. 117]). We regard exactness at the term $H^2(G, M)$ as a computational problem as follows. Let inf and res denote also the respective maps on cocycles $Z^2(G/N, M^N) \longrightarrow Z^2(G, M)$ and $Z^2(G, M) \longrightarrow Z^2(N, M)$.

Inverse inflation problem. *Let $f \in Z^2(G, M)$ such that $\operatorname{res} f$ is split. Given $l \in C^1(N, M)$ with $\operatorname{res} f = \partial l$, compute elements $\bar{f} \in Z^2(G/N, M^N)$ and $m \in C^1(G, M)$ such that*

$$\inf \bar{f} = f + \partial m.$$

The solution given below in Algorithm 3.5 makes use of $G - N$ 2-cocycles as introduced in Saltman [12, Section One]. We provide the definition and a lemma.

Definition 3.3. Let M be a G-module and let $N \trianglelefteq G$. Define

$$Z^2_N(G, M) := \{f \in Z^2(G, M) \mid f(G, N) = 0\}.$$

The elements of this subgroup of $Z^2(G, M)$ are called $G - N$ 2-cocycles. Moreover, call $f \in Z^2_N(G, M)$ *normalized* if $f(N, G) = 0$.

Since we consider only normal subgroups N our definition coincides with Saltman's more general definition from [12, Section One].

Lemma 3.4. *Let M be a G-module, $N \trianglelefteq G$ and $f \in Z^2(G, M)$.*

a) The following are equivalent :

(1) $f \in Z^2_N(G, M)$,
(2) $f(g, g'h) = f(g, g')$ *for all* $g, g' \in G, h \in N$,
(3) $f(g, hg') = f(g, g')$ *for all* $g, g' \in G, h \in N$,

b) If $f \in Z^2_N(G, M)$ then for any $g \in G$ the map

$$f(-, g)|_N : N \longrightarrow M$$

is a 1-cocycle in $Z^1(N, M)$.

c) If $f \in Z^2_N(G, M)$ is normalized then

$$\bar{f}(gN, g'N) := f(g, g') \quad \text{for all } g, g' \in G$$

defines an element $\bar{f} \in Z^2(G/N, M^N)$ with $\inf \bar{f} = f$.

Proof. a) (1) $\Rightarrow$ (2) : By (3.1), $f(g,g'h) = f(gg',h)+f(g,g')-gf(g',h) = f(g,g')$. (2) $\Rightarrow$ (3) : N is a normal subgroup of G. (3) $\Rightarrow$ (1) : choose $g' = 1$ (we assume $f(G,1) = 0$ for all 2-cocycles).

b) Suppose $f \in Z^2_N(G,M)$ and fix $g \in G$. By (3.1) and (3) we have

$$f(hh',g) = f(h,h'g) + hf(h',g) - f(h,h') = f(h,g) + hf(h',g)$$

for all $h, h' \in N$.

c) Suppose $f \in Z^2_N(G,M)$ is normalized. By (3.1), (3) and the hypothesis we have

$$f(gh,g') = gf(h,g') + f(g,hg') - f(g,h) = f(g,g') \tag{3.4}$$

for all $g, g' \in G, h \in N$. Hence, by (3.4) and (2), the map

$$\bar{f} : G/N \times G/N \longrightarrow M, \quad (gN, g'N) \longmapsto f(g,g')$$

is well-defined. Using (3.1), the normality of N, (3.4) and the hypothesis we check

$$hf(g,g') = f(hg,g') + f(h,g) - f(h,gg') = f(g,g')$$

for all $g, g' \in G, h \in N$, so f has image in M^N. Since the 2-cocycle condition for $\bar{f}$ is inherited from f, we have $\bar{f} \in Z^2(G/N, M^N)$, and clearly $\inf \bar{f} = f$ by definition. □

Algorithm 3.5 (Inverse Inflation)**.** Let M be a constructively H^1-trivial G-module, $N \trianglelefteq G$ and $f \in Z^2(G,M)$ such that $\operatorname{res} f$ is split. The inverse inflation problem for f is solved as follows. Let $l \in C^1(N,M)$ be given with $\operatorname{res} f = \partial l$.

1. Fix a system of coset representatives $\{1 = g_1, g_2, \ldots, g_r\} \subset G$ of G/N.
2. Extend l to $l' \in C^1(G,M)$ by defining
$$l'_{g_i h} := g_i l_h - f(g_i, h) \quad \forall 1 \le i \le r, h \in N.$$
In particular all $l'_{g_i} = 0$ and $l'|_N = l$.
3. Define $f' := f - \partial l' \in Z^2(G,M)$, then $f' \in Z^2_N(G,M)$.
4. For each $i \in \{1, \ldots, r\}$ consider $f'(-,g_i)|_N \in Z^1(N,M)$ and choose $e_i \in M$ such that
$$he_i - e_i = f'(h,g_i) \quad \forall h \in N.$$
Choose $e_1 = 0$.
5. Define $e \in C^1(G,M)$ constant on cosets by
$$e_{g_i h} := e_i \quad \forall 1 \le i \le r, h \in N.$$
6. Define $f'' := f' - \partial e \in Z^2(G,M)$, then $f'' \in Z^2_N(G,M)$ is normalized.
7. Define $\bar{f} \in Z^2(G/N, M^N)$ by
$$\bar{f}(gN, g'N) := f''(g,g')$$
and $m \in C^1(G,M)$ by
$$m := -(l' + e),$$
then $\inf \bar{f} = f'' = f + \partial m$.

Proof. 3. Check for all $g = g_i h' \in G$ and $h \in N$:

$$\begin{aligned} f'(g,h) &= f(g_i h', h) - (l'_{g_i h'} + g_i h'(l'_h) - l'_{g_i h' h}) \\ &= f(g_i h', h) - g_i l_{h'} + f(g_i, h') - g_i h' l_h + g_i l_{h'h} - f(g_i, h'h) \\ &= f(g_i h', h) + f(g_i, h') - f(g_i, h'h) - g_i(l_{h'} + h' l_h - l_{h'h}) \\ &= f(g_i h', h) + f(g_i, h') - f(g_i, h'h) - g_i f(h', h) = 0. \end{aligned}$$

4. By Lemma 3.4 b), $f'(-, g_i) : N \longrightarrow M \in Z^1(N, M)$ for each $i \in \{1, \ldots, r\}$. The e_i can be chosen because M is constructively H^1-trivial.
6. Obviously, $(h-1)e_g = f'(h, g)$ and $e_h = 0$ for all $g \in G$ and $h \in N$. It follows, for all $g = g_i h' \in G$ and $h \in N$:

$$\partial e(g, h) = e_g + g e_h - e_{gh} = e_i + 0 - e_i = 0,$$
$$\partial e(h, g) = e_h + h e_g - e_{hg} = (h-1)e_g = f'(h, g).$$

This shows that f'' is a normalized $G - N$ 2-cocycle.
7. is clear from Lemma 3.4 c). □

3.3. **Solvable 2-cocycles.** Now we are ready to reduce the splitting problem for a solvable group G to splitting problems for cyclic groups, hence to norm equations. For non-solvable groups no algorithm is known.

Algorithm 3.6 (Solvable splitting problem)**.** Let G be a finite solvable group and let M be a constructively H^1-trivial G-module. The splitting problem for $f \in Z^2(G, M)$ is solved as follows.

1. Choose a cyclic normal subgroup $N \trianglelefteq G$. Let res and inf denote the restriction and inflation, respectively, corresponding to N.
2. Solve the splitting problem for $\operatorname{res} f$ (using Algorithm 3.1 for the cyclic group N). If $\operatorname{res} f$ is not split then f is not split, otherwise let $l \in C^1(N, M)$ with $\partial l = \operatorname{res} f$ and continue.
3. Solve the inverse inflation problem for f given l (using Algorithm 3.5). Let $\bar{f} \in Z^2(G/N, M^N)$ and $m \in C^1(G, M)$ such that
$$\inf \bar{f} = f + \partial m.$$
4. Solve the splitting problem for $\bar{f} \in Z^2(G/N, M^N)$ (using Algorithm 3.6 recursively). If $\bar{f}$ is not split then f is not split, otherwise let $\bar{l} \in C^1(G/N, M^N)$ with $\partial \bar{l} = \bar{f}$ and continue.
5. Define $l := \inf \bar{l} - m \in C^1(G, M)$, then $f = \partial l$.

Proof. 2. Trivially, if f is split then $\operatorname{res} f$ is split.
4. Clearly, f is split if and only if $\inf \bar{f}$ is split because they differ by a coboundary. Since inflation on H^2 is injective, $\inf \bar{f}$ is split if and only if $\bar{f}$ is split. Algorithm 3.6 can be invoked for $\bar{f}$ because M^N is constructively H^1-trivial as a G/N-module by Lemma 3.2.
5. Check $\partial l = \partial \inf \bar{l} - \partial m = \inf \partial \bar{l} - \partial m = \inf \bar{f} - \partial m = f$. □

4. The isomorphism problem for central-simple algebras

Isomorphism Problem (IP). *Given $A, A' \in \mathcal{A}(k)$. Decide whether $A \cong A'$ as k-algebras and, if so, compute a k-algebra isomorphism between them.*

Of course, we assume that A and A' have equal degree, say n. In the important special case when A' is the full matrix ring we call a k-isomorphism $A \longrightarrow M_n(k)$ a *splitting* of A. The fact that a splitting of A is equivalent to a set of orthogonal idempotent generators in A indicates that the IP in general is difficult and that some simplifying assumption should be made. In §4.2 below we assume that A and A' are crossed products.

4.1. **Reduction to splittings.** Denote by A° the opposite algebra of a A. The following algorithm uses the equivalence

$$A \cong_k A' \iff A \otimes_k A'^\circ \cong_k M_{n^2}(k)$$

to find a k-isomorphism between A and A'.

Remark 4.1. Recall that an isomorphism $\psi : A \otimes_k A'^{\circ} \longrightarrow M_{n^2}(k)$ is equivalent to a pair (φ, φ') where $\varphi : A \longrightarrow M_{n^2}(k)$ is a k-embedding and $\varphi' : A' \longrightarrow M_{n^2}(k)$ is a k-anti-embedding such that $\varphi(A)$ is the centralizer $C_{M_{n^2}(k)}(\varphi'(A'))$. Of course, φ, φ' are obtained from ψ by composing it with the canonical embedding $\varepsilon : A \longrightarrow A \otimes A'^{\circ}$ and anti-embedding $\varepsilon' : A' \longrightarrow A \otimes A'^{\circ}$, respectively.

Algorithm 4.2. Given a pair (φ, φ') as in Remark 4.1. Then k-isomorphisms $\chi : A \longrightarrow A'$ and $\chi' : A' \longrightarrow A$ are computed as follows.

1. Fix a k-basis of A and identify $M_{n^2}(k)$ with $\mathrm{End}_k(A)$.
2. Choose a matrix $X \in M_{n^2}(k)$ such that $\mathrm{Inn}(X) \circ \varphi = \lambda$, the left-regular representation of A.
3. Set $\varphi'' := \mathrm{Inn}(X) \circ \varphi'$. Then $\varphi''(A') = \rho(A)$, where ρ is the right-regular representation of A.
4. Define $\chi := \varphi''^{-1} \circ \rho : A \longrightarrow A'$ and $\chi' := \rho^{-1} \circ \varphi'' : A' \longrightarrow A$.

Proof. The left-regular representation

$$\lambda : A \longrightarrow \mathrm{End}_k(A), \quad a \longmapsto \lambda_a, \quad \lambda_a(x) := ax$$

is a k-algebra isomorphism and the right-regular representation

$$\rho : A \longrightarrow \mathrm{End}_k(A), \quad a \longmapsto \rho_a, \quad \rho_a(x) := xa$$

is a k-algebra anti-isomorphism. The matrix X in step 2 exists by the Skolem-Noether theorem and is obtained as a solution to a linear equation system. It follows

$$\varphi''(A') = C_{M_{n^2}(k)}(X\varphi(A)X^{-1}) = C_{M_{n^2}(k)}(\lambda(A)) = \rho(A).$$

Since ρ and φ'' are both anti, χ and χ' as defined in step 4 are isomorphisms. □

Remark 4.3. Algorithm 4.2 shows that the isomorphism problem for A and A' is constructively equivalent to a splitting of $A \otimes A'^{\circ}$.

4.2. **The IP for crossed products.** For the remaining discussion of the isomorphism problem we assume that A and A' are crossed products. Algorithms 4.4–4.7 together reduce this case of the IP to the SP for 2-cocycles with values in the multiplicative group of a field. While the reduction works for arbitrary crossed products it is pointed out that if A and A' are solvable crossed products then the SP is required only for solvable groups.

4.2.1. *Case of crossed products over the same B.* We start with the case when A and A' are crossed products of the same simple algebra B. So let $B \in \mathcal{A}(K), H \leqslant \mathrm{Out}(B)$ finite, $k = \mathrm{Fix}(H)$, and $\omega : H \longrightarrow \mathrm{Aut}(B)$ an extension map.

Algorithm 4.4 (IP with the same B)**.** Let $A = (B, H, f, u)$ and $A' = (B, H, f', u')$ be two crossed products, $f, f' \in \mathcal{F}_\omega(H, B^*)$. The isomorphism problem for A and A' is solved as follows.

1. Define $f_0 := f/f' \in Z^2(H, K^*)$.
2. Solve the splitting problem for f_0 (if H is solvable then Algorithm 3.6 can be used). If f_0 is not split then $A \ncong_k A'$, otherwise let $l \in C^1(H, K^*)$ with $\partial l = f_0$ and continue.
3. Define $\psi : A \longrightarrow A'$ by $B \xrightarrow{\mathrm{id}} B$ and $u_\sigma \longmapsto l_\sigma u'_\sigma, \sigma \in H$.

Proof. 1. f_0 lies in $Z^2(H, K^*)$ by Proposition 2.4. 2. Corollary 2.13 states that $A \cong_k A'$ if and only if f_0 is split. 3. Consider the family $\{z_\sigma\}_{\sigma \in G}, z_\sigma := l_\sigma u'_\sigma$, in A'. Since $f_z = \partial l f' = f = f_u$, ψ is a homomorphism. □

An important special case is when B is a field and A' is the full matrix ring $M_n(k)$. Since $M_n(k)$ is split it can be written as a crossed product of any field L with $[L : k] = n$, and then Algorithm 4.4 can be applied.

Algorithm 4.5 (Splitting of crossed product)**.** Let $A = (L/k, H, f, u)$ be a crossed product, L a field, $[L : k] = n$. The isomorphism problem for A and $M_n(k)$ is solved as follows.

1. Fix a k-embedding $\psi : L \longrightarrow M_n(k)$ and identify L with its image in $M_n(k)$.
2. Compute a family $\{x_\sigma\}_{\sigma\in H}$ in $M_n(k)$ such that
$$\mathrm{Inn}(x_\sigma)|_L = \sigma \quad \text{for all } \sigma \in H,$$
and define $f_x \in Z^2(H, L^*)$ by $f_x(\sigma, \tau) := x_\sigma x_\tau x_{\sigma\tau}^{-1}$.
3. Write $M_n(k) = (L/k, H, f_x, x)$ and solve the isomorphism problem using Algorithm 4.4.

Proof. 1. amounts to computing the minimal polynomial over k of a primitive element of L. The family $\{x_\sigma\}$ in 2. exists by the Skolem-Noether theorem and is computed using only linear algebra. 3. $M_n(k) = (L/F, H, f_x, x)$ by Lemma 2.10. □

4.2.2. *Case of crossed products over linearly disjoint fields.* Next is the case when A and A' are crossed products of linearly disjoint fields. So let L/k and L'/k be two linearly disjoint field extensions of equal degree n.

Algorithm 4.6 (IP with linearly disjoint fields)**.** Let $A = (L/k, H, f, u)$ and $A' = (L'/k, H', f', u')$. The isomorphism problem for A and A' is solved as follows.

1. Compute the field compositum LL' and identify L and L' with subfields of LL'.
2. Compute $\mathrm{Gal}(LL'/k)$ and identify it with $H \times H'$.
3. Define $C := (LL'/k, H \times H', \inf f(\inf f')^{-1})$ where inf means the respective inflation to $H \times H'$.
4. Define the canonical k-embedding
$$\phi : A \longrightarrow C, \quad L \longrightarrow LL', u_\sigma \longmapsto w_{(\sigma,1)}$$
and the canonical k-anti-embedding
$$\phi' : A' \longrightarrow C, \quad L' \longrightarrow LL', v_{\sigma'} \longmapsto w_{(1,\sigma')},$$
then $\mathrm{im}\,\phi = C_C(\mathrm{im}\,\phi')$.
5. Solve the isomorphism problem for C and $M_{n^2(k)}$ (using Algorithm 4.5). If $C \ncong_k M_{n^2}(k)$ then $A \ncong_k A'$, otherwise let $\psi : C \longrightarrow M_{n^2}(k)$ be a k-isomorphism and continue.
6. Define $\varphi := \psi \circ \phi$ and $\varphi' := \psi \circ \phi'$.
7. Use Algorithm 4.2 to compute a k-algebra isomorphism $A \longrightarrow A'$.

Proof. 5. Since $A \otimes_k A'^\circ \cong_k C$, $A \cong_k A'$ if and only if $C \cong_k M_{n^2}(k)$. □

4.2.3. *Case of crossed products over arbitrary fields.* Now, we turn to the general case when A and A' are crossed products of arbitrary fields.

Algorithm 4.7 (IP with arbitrary fields)**.** Let $A = (L/k, G, f, u)$ and $A' = (L'/k, G', f', u')$ be two crossed products of fields of equal degree n over k. The isomorphism problem for A and A' is solved as follows.

1. Compute the field compositum LL' and identify L and L' with subfields of LL'.
2. Compute the intersection $K := L \cap L'$.
3. Compute the Galois groups $N := \mathrm{Gal}(L/K), N' := \mathrm{Gal}(L'/K), H := \mathrm{Gal}(K/k)$.
4. Define $B := (L/K, N, \mathrm{res}\, f, u) \subseteq A$ and $B' := (L'/K, N', \mathrm{res}\, f', u') \subseteq A'$ (as in Example 2.9).

5. Solve the IP for B and B' over K (using Algorithm 4.6). If $B \ncong_K B'$ then $A \ncong_k A'$, otherwise let $\psi : B \longrightarrow B'$ be an K-isomorphism and continue.
6. Identify B' with B and $\mathrm{Aut}(B')$ with $\mathrm{Aut}(B)$ via ψ.
7. Choose any extension map $\omega : H \longrightarrow \mathrm{Aut}(B)$ and write $A = (B, H, f)$ and $A' = (B, H, f')$ for some $f, f' \in \mathcal{F}_w(H, B^*)$ (using Lemma 2.10).
8. Solve the isomorphism problem for A and A' (using Algorithm 4.4).

Proof. 4. It is $B = C_A(K)$ and $B' = C_{A'}(K)$ by Example 2.9. 5. L and L' are linearly disjoint over K, so we can apply Algorithm 4.6. □

Remark 4.8. If G and G' in Algorithm 4.7 are solvable then $N \times N'$ and H are solvable, hence the SP is required only for solvable groups.

5. Extension problem

Extension Problem (EP). *Given $A \in \mathcal{A}(K)$ and $\sigma \in \mathrm{Aut}(K)$. Decide whether $\sigma \in \mathrm{Out}(A)$ and, if so, compute an extension to A.*

5.1. **The EP and conjugation of algebras.** Let $\sigma \in \mathrm{Aut}(K)$ and let A be any K-algebra.

Definition 5.1. Define the *conjugate algebra* σ_*A of A to be the K-algebra obtained from the ring A with scalar multiplication defined by $x \circ a := \sigma^{-1}(x)a$. Denote by σ_A the identity map $A \longrightarrow \sigma_*A$ as rings.

Proposition 5.2. *The identity map $\sigma_A : A \longrightarrow \sigma_*A$ is a ring isomorphism that extends σ. For any K-algebra B,*

$$\sigma_*A \cong_K B \iff \sigma \text{ extends to a ring isomorphism } A \longrightarrow B.$$

Proof. The first statement is clear from a consideration of the different canonical embeddings of K into A and σ_*A, respectively, as illustrated in :

$$\begin{array}{ccc} A & \xrightarrow{\sigma_A} & \sigma_*A \\ \uparrow{\scriptstyle \cdot 1_A} & & \uparrow{\scriptstyle \circ 1_A} \\ K & \xrightarrow{\sigma} & K \end{array}$$

The diagram commutes because $\sigma_A(\lambda \cdot 1_A) = \lambda \cdot 1_A = \sigma(\lambda) \circ 1_A$ for all $\lambda \in K$.

For the second statement, let $\varphi : \sigma_*A \longrightarrow B$ and $\psi : A \longrightarrow B$ be maps such that $\psi = \varphi \circ \sigma_A$. Clearly, ψ is a ring isomorphism extending σ if and only if φ is a K-algebra isomorphism. □

Example 5.3 (Conjugation of separable fields)**.** Suppose A/K is a separable field extension and $\sigma \in \mathrm{Aut}(K)$ has finite order. Let $k = \mathrm{Fix}(\sigma)$. Then A/k is separable and σ extends to a k-embedding $\widehat{\sigma}$ of A into some Galois closure of A/k. We have

$$\sigma_*A = \widehat{\sigma}A.$$

Proof. Clearly, $\widehat{\sigma} : A \longrightarrow \sigma A$ is a ring isomorphism extending σ. The assertion follows from Proposition 5.2. □

Example 5.4 (Conjugation of crossed products)**.** Suppose that A is a crossed product $(L/K, H, f)$ of a field and let $\sigma \in \mathrm{Aut}(K)$. Then

$$\sigma_*(L/K, H, f) \cong_K (\sigma L/K, {}^{\sigma}H, f^{\sigma}), \tag{5.1}$$

where ${}^{\sigma}H = \sigma H \sigma^{-1}$ and f^{σ} is the well-known conjugation of 2-cocycles (cf. Neukirch [10, §5, p. 44]) :

$$f^{\sigma}(\tau_1, \tau_2) = \sigma f(\sigma^{-1}\tau_1\sigma, \sigma^{-1}\tau_2\sigma). \tag{5.2}$$

If H is cyclic and $a \in K^*$ then for $f_a \in Z^2(H, L^*)$ defined as in Example 2.3 we have

$$(f_a)^\sigma = f_{\sigma a}.$$

Proof. The map

$$\widehat{\sigma} : (L/K, H, f, u) \longrightarrow ({}^\sigma L/K, {}^\sigma H, f^\sigma, v), \quad L \xrightarrow{\sigma} {}^\sigma L, \quad u_\tau \longmapsto v_{\sigma\tau\sigma^{-1}}$$

is a ring isomorphism extending σ. The isomorphism (5.1) follows from Proposition 5.2. The calculation of $(f_a)^\sigma$ in the cyclic case is immediate from (5.2). □

Definition 5.5. The *conjugation* induced by σ on $\mathrm{Br}(K)$ is the automorphism

$$\sigma_* : \mathrm{Br}(K) \longrightarrow \mathrm{Br}(K), \quad [A] \longmapsto [\sigma_* A].$$

Theorem 5.6. *The following are equivalent :*

(1) $\sigma \in \mathrm{Out}(A)$,
(2) $A \cong \sigma_* A$ *as* K*-algebras,*
(3) $[A] \in \mathrm{Br}(K)^{\sigma_*}$, *the fixed subgroup of* $\mathrm{Br}(K)$.

In particular, the condition $\sigma \in \mathrm{Out}(A)$ *depends only on the class of* A.

Now suppose that σ *has finite order and let* $k = \mathrm{Fix}(\sigma)$. *Denote by* res *the restriction* $\mathrm{Br}(k) \longrightarrow \mathrm{Br}(K)$. *Then* (1)–(3) *are equivalent to :*

(4) $[A] \in \mathrm{res}(\mathrm{Br}(k))$.

Proof. (1) $\iff$ (2) is Proposition 5.2. (3) is a reformulation of (2). (1) $\Rightarrow$ (4) : If $\sigma \in \mathrm{Out}(A)$ has finite order then $\mathcal{F}(\langle\sigma\rangle, A^*)$ is non-empty by Example 2.3. Hence, $[A] \in \mathrm{res}(\mathrm{Br}(k))$ by Corollary 2.12. (4) $\Rightarrow$ (1) : Let $A \sim B \otimes_k K$ with $B \in \mathcal{A}(k)$. Clearly, σ extends to $\mathrm{id}_B \otimes \sigma \in \mathrm{Aut}(B \otimes_k K)$, i.e. $\sigma \in \mathrm{Out}(B \otimes_k K)$. This proves (1) because (1) depends only on the class of A. □

Note that the equivalence of (1) and (2) is even constructive by the proof of Proposition 5.2. Therefore, the extension problem can be regarded as a special case of the isomorphism problem for central-simple algebras.

Remark 5.7. The equivalence of (1) and (4) in Theorem 5.6 is originally due to Eilenberg-McLane [4, Corollary 7.3]. Their cohomology argument showing

$$\mathrm{Br}(K)^{\sigma_*} = \mathrm{res}(\mathrm{Br}(k))$$

can be summarized as follows. In our proof above, the part of the cohomology argument is taken over by the construction of a cyclic factor set in Example 2.3.

Proof. Let L/k be a Galois extension containing K and denote $\mathrm{Gal}(L/k) = G$ and $\mathrm{Gal}(L/K) = H$. The sequence

$$H^2(G, L^*) \xrightarrow{\mathrm{res}} H^2(H, L^*)^{G/H} \xrightarrow{\mathrm{tg}} H^3(G/H, K^*) \tag{5.3}$$

is exact because $H^1(H, L^*) = 1$ (cf. Neukirch [10, Prop. 1.6.6, p. 64] or Serre [13, Ch. VII, Prop. 5, p. 117]). Note that the action of $G/H = \langle\sigma\rangle$ on $H^2(H, L^*)$ in this sequence is precisely the one defined in (5.2). Therefore, (5.3) is translated by Example 5.4 into the exact sequence

$$\mathrm{Br}(L/k) \xrightarrow{\mathrm{res}} \mathrm{Br}(L/K)^{\sigma_*} \longrightarrow H^3(G/H, K^*).$$

Passing to direct limits we get

$$\mathrm{Br}(k) \xrightarrow{\mathrm{res}} \mathrm{Br}(K)^{\sigma_*} \longrightarrow H^3(G/H, K^*).$$

Since $G/H = \langle\sigma\rangle$ is cyclic we have $H^3(G/H, K^*) \cong H^1(G/H, K^*) = 1$, hence $\mathrm{Br}(K)^{\sigma_*} = \mathrm{res}(\mathrm{Br}(k))$. □

For algebraic number fields K the conditions (1)–(4) of Theorem 5.6 are characterizable in terms of Hasse invariants. Recall that for each (finite or infinite) prime $\mathfrak{p}$ of K, the Hasse invariant $\mathrm{inv}_{\mathfrak{p}} A$ is the element of $\mathbb{Q}/\mathbb{Z}$ that corresponds to the class of the completion $A \otimes_K K_{\mathfrak{p}}$ in the Brauer group $\mathrm{Br}(K_{\mathfrak{p}})$.

Proposition 5.8 (Deuring's Criterion)**.** *Let K be an algebraic number field. The conditions (1)–(4) of Theorem 5.6 are equivalent to*

(5) *the local invariants of A are stable under conjugation by σ, i.e.*

$$\mathrm{inv}_{\mathfrak{p}} A = \mathrm{inv}_{\sigma\mathfrak{p}} A \quad \text{for all primes } \mathfrak{p} \text{ of } K.$$

Proof. Deuring shows in [3, Satz 4] that (5) is equivalent to the condition

(6) A embeds into some $B \in \mathcal{A}(k)$ such that $A = C_B(K)$,

which is known to be equivalent to (4) by Corollary 2.12. □

Remark 5.9. A direct proof of Deuring's criterion is given by Janusz in [7]. His proof of the equivalence of (1) and (5) does not refer to Deuring [3] and consequently does not use condition (6).

The equivalence of (4) and (5) also follows from the description of the global Brauer group in terms of Hasse invariants (see Pierce [11, Theorem 18.5]).

5.2. **The EP for crossed products.** Suppose that $A = (L/K, H, f)$ is a crossed product of a field and let $\sigma \in \mathrm{Aut}(K)$. By Theorem 5.6 and Example 5.4 the extension problem for A and σ is equivalent to the isomorphism problem for $(L/K, H, f, u)$ and $({}^{\sigma}L/K, {}^{\sigma}H, f^{\sigma}, u')$. The details are contained in the following algorithm.

Algorithm 5.10 (Extension Problem)**.** Let $A = (L/K, H, f)$ and let $\sigma \in \mathrm{Aut}(K)$. The extension problem for A and σ is solved as follows.

1. Compute the fixed field k of σ.
2. Compute ${}^{\sigma}L$ and $\mathrm{Gal}({}^{\sigma}L/K)$ and identify $\mathrm{Gal}({}^{\sigma}L/K)$ with ${}^{\sigma}H$.
3. Define $A' := ({}^{\sigma}L, {}^{\sigma}H, f^{\sigma}, u')$.
4. Solve the isomorphism problem for A and A' over K (using Algorithm 4.7). If $A \ncong_K A'$ then $\sigma \notin \mathrm{Out}(A)$, otherwise let $\psi : A' \longrightarrow A$ be a K-isomorphism and continue.
5. Define $\widetilde{\sigma} := \psi \circ \hat{\sigma} : A \longrightarrow A$ where

$$\hat{\sigma} : A \longrightarrow A', \quad L \xrightarrow{\sigma} {}^{\sigma}L, \quad u_\tau \longmapsto u'_{\sigma\tau\sigma^{-1}}.$$

Proof. Since $A' \cong_K \sigma_* A$ by Example 5.4, the algorithm is clear from the equivalence of (1) and (2) in Theorem 5.6. Note that $\hat{\sigma}$ is the ring isomorphism from the proof of Example 5.4 and restricts to σ. Since, ψ is a K-isomorphism, $\psi \circ \hat{\sigma} \in \mathrm{Aut}(A)$ also restricts to σ. □

Remark 5.11. If H is solvable then so is ${}^{\sigma}H$, hence the SP is required only for solvable groups (cf. Remark 4.8).

6. Example

Let K be the cubic number field $K = \mathbb{Q}(\alpha)$ of discriminant 49,

$$\mathrm{Irr}(\alpha, \mathbb{Q}) = x^3 + x^2 - 2x - 1,$$

which is the maximal real subfield of the 7-th cyclotomic field. A non-identity automorphism of $K/\mathbb{Q}$ is

$$\sigma : \alpha \longmapsto -\alpha^2 - \alpha + 1.$$

Let L be the cubic extension $L = K(\theta)$ defined by

$$\mathrm{Irr}(\theta, K) = x^3 + (\alpha - 2)x^2 + (-\alpha - 1)x + 1.$$

The extension L/K is cyclic because

$$\tau : \theta \longmapsto -\theta^2 + (-\alpha + 1)\theta + 2.$$

is checked to be a non-identity automorphism of L/K. Finally, let D be the cyclic algebra

$$D = (L/K, \tau, a, v), \quad a = 2(\alpha^2 - \alpha - 2).$$

This section demonstrates a solution of the extension problem for D and σ following the algorithms of this paper. The resulting example is precisely the one that leads to the noncrossed product divison algebra of the form $D((\mathbf{x}; \widetilde{\sigma}))$ from [6].

According to Algorithm 5.10 we need to solve the IP for D and

$$D' = (L'/K, \tau', a', v'),$$

where

$$L' = \sigma L = K(\eta) \text{ with } \operatorname{Irr}(\eta, K) = x^3 + (-\alpha^2 - \alpha - 1)x^2 + (\alpha^2 + \alpha - 2)x + 1,$$
$$\tau' = \sigma\tau\sigma^{-1} : \eta \longmapsto -\eta^2 + (\alpha^2 + \alpha)\eta + 2,$$
$$a' = \sigma a = 2(\alpha^2 + 2\alpha - 1)$$

Of course, $\operatorname{Irr}(\eta, K)$ is obtained from $\operatorname{Irr}(\theta, K)$ by applying σ to each coefficient.

Since $L \cap L' = K$ we are in the case of §4.2.2 (Algorithm 4.6), which means we have to split the crossed product

$$C = (LL'/K, G, f, z),$$

where $G = \langle\tau\rangle \times \langle\tau'\rangle$ and $f \in Z^2(G, (LL')^*)$ is defined by

$$f(\tau^i\tau'^{i'}, \tau^j\tau'^{j'}) = f_a(\tau^i, \tau^j) f_{\sigma a^{-1}}(\tau'^{i'}, \tau'^{j'}), \tag{6.1}$$

f_a and $f_{\sigma a^{-1}}$ as in (2.2). Note that $\sigma a^{-1} = \frac{1}{14}(\alpha^2 + 3\alpha - 3)$. The canonical k-(anti-)embeddings of D and D' into C are given by

$$\phi : D \longrightarrow C,\ \lambda v^i \longmapsto \lambda z_\tau^i, \quad \phi' : D' \longrightarrow C,\ \lambda' v'^i \longmapsto \lambda' z_{\tau'}^i$$

for all $\lambda \in L, \lambda' \in L'$.

When splitting the crossed product C with Algorithm 4.5 we use the K-embedding $\psi : LL' \longrightarrow M_9(K)$ that is defined by the two images

$$\psi(\theta) = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & \alpha+1 & 0 & 0 & -\alpha+2 & 0 & 0 \\ 0 & -1 & 0 & 0 & \alpha+1 & 0 & 0 & -\alpha+2 & 0 \\ 0 & 0 & -1 & 0 & 0 & \alpha+1 & 0 & 0 & -\alpha+2 \end{pmatrix},$$

$$\psi(\eta) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & -\alpha^2-\alpha+2 & \alpha^2+\alpha+1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & -\alpha^2-\alpha+2 & \alpha^2+\alpha+1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & -\alpha^2-\alpha+2 & \alpha^2+\alpha+1 \end{pmatrix}.$$

Furthermore, we use the family $\{x_\sigma\}_{\sigma \in G}$ defined by

$$x_\tau = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -\alpha & 0 & 0 & \alpha-2 & 0 & 0 & 1 & 0 & 0 \\ 0 & -\alpha & 0 & 0 & \alpha-2 & 0 & 0 & 1 & 0 \\ 0 & 0 & -\alpha & 0 & 0 & \alpha-2 & 0 & 0 & 1 \\ \alpha^2-\alpha+2 & 0 & 0 & -\alpha^2+3\alpha-3 & 0 & 0 & -\alpha+1 & 0 & 0 \\ 0 & \alpha^2-\alpha+2 & 0 & 0 & -\alpha^2+3\alpha-3 & 0 & 0 & -\alpha+1 & 0 \\ 0 & 0 & \alpha^2-\alpha+2 & 0 & 0 & -\alpha^2+3\alpha-3 & 0 & 0 & -\alpha+1 \end{pmatrix},$$

$$x_{\tau'} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \alpha^2+\alpha-1 & -\alpha^2-\alpha-1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \alpha^2+2\alpha+3 & -3\alpha^2-4\alpha-2 & \alpha^2+\alpha & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^2+\alpha-1 & -\alpha^2-\alpha-1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha^2+2\alpha+3 & -3\alpha^2-4\alpha-2 & \alpha^2+\alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2+\alpha-1 & -\alpha^2-\alpha-1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2+2\alpha+3 & -3\alpha^2-4\alpha-2 & \alpha^2+\alpha \end{pmatrix}$$

and

$$x_{\tau^i\tau'^j} = x_\tau^i x_{\tau'}^j.$$

This choice of $\{x_\sigma\}$ happens to give us as f_x the trivial 2-cocycle in step 2 of Algorithm 4.5. Therefore, when solving the IP for $C = (LL'/K, G, f, z)$ and $M_9(K) = (LL'/K, G, 1, x)$ with Algorithm 4.4, we are left with the splitting problem for $f_0 = f \in Z^2(G, (LL')^*)$.

We solve the SP for f by choosing $N = \langle\tau\rangle$ in Algorithm 3.6. Instead of giving the results of all intermediate steps of Algorithm 3.6, it is probably of most interest here to present the two norm equations that arise on the two levels of recursion and their solutions. The first norm equation obviously reads

$$N_{LL'/L'}(x_1) = a.$$

A solution that was found with MAGMA is

$$\begin{aligned} x_1 =& \frac{1}{2}\big((-7\alpha^2+9\alpha+4) + 2(-2\alpha^2+6\alpha-1)\eta + (\alpha^2-6\alpha+4)\eta^2 \\ &+ (14\alpha^2-12\alpha-9)\theta + (20\alpha^2-7\alpha-14)\eta\theta + (-12\alpha^2+3\alpha+12)\eta^2\theta \\ &+(-3\alpha^2+3\alpha+2)\theta^2 + (-7\alpha^2-\alpha+5)\eta\theta^2 + (4\alpha^2-5)\eta^2\theta^2\big). \end{aligned}$$

Computation time for x_1 was a few minutes (less than 10) on an 800 Mhz processor. Using this x_1 for the inverse inflation, the second norm equation that arises in the recursion is

$$N_{L'/K}(x_2) = \frac{1}{56}(-1601\alpha^2+693\alpha+609). \tag{6.2}$$

Exceptionally for this example, the right handside of (6.2) lies in K. A cubic root of the right handside, hence a solution to (6.2), is

$$x_2 = \frac{1}{14}(-19\alpha^2-\alpha-6).$$

Using the solutions x_1 and x_2, a splitting $\psi : C \longrightarrow M_9(K)$ of C is defined in step 3 of Algorithm 4.4. It is our K-embedding $\psi : LL' \longrightarrow M_9(K)$ from above extended to C by defining the two images

$$\psi(z_\tau) = \frac{1}{2}\cdot \begin{pmatrix} -3\alpha^2+9\alpha+3 & -12\alpha^2-2\alpha+1 & 5\alpha^2-\alpha-2 & -17\alpha^2+13\alpha+11 \\ -5\alpha^2+\alpha+2 & -\alpha^2+6\alpha & \alpha^2-2\alpha-2 & -8\alpha^2+5\alpha+5 \\ -\alpha^2+2\alpha+2 & -3\alpha^2+2\alpha & -\alpha-4 & -6\alpha^2+\alpha+4 \\ 5\alpha^2-10\alpha-8 & 3\alpha^2+12\alpha+6 & -2\alpha^2-3\alpha & -4\alpha^2-3\alpha+6 \\ 2\alpha^2+3\alpha & 5\alpha^2-8\alpha-5 & -3\alpha^2+\alpha+3 & 4\alpha^2-5\alpha-1 \\ 3\alpha^2-\alpha-3 & -\alpha^2+3\alpha+5 & -\alpha^2-5\alpha-1 & -3\alpha^2-3\alpha \\ 19\alpha^2+\alpha-11 & -23\alpha^2-3\alpha+3 & 5\alpha^2-\alpha+1 & -31\alpha^2+15\alpha+28 \\ -5\alpha^2+\alpha-1 & 18\alpha^2-5\alpha-8 & -7\alpha^2+3 & 2\alpha^2-8\alpha+2 \\ 7\alpha^2-3 & -8\alpha^2+5\alpha+5 & -9\alpha-5 & -14\alpha^2+8 \end{pmatrix}$$

$$\begin{pmatrix} -13\alpha^2+11\alpha+6 & 8\alpha^2-5\alpha-5 & 5\alpha^2-5\alpha-4 & 7\alpha^2+\alpha-2 & -4\alpha^2+3 \\ -12\alpha^2+10\alpha+6 & 6\alpha^2-\alpha-4 & 4\alpha^2-3 & 2\alpha^2-4\alpha+2 & -2\alpha^2+1 \\ -4\alpha^2+3\alpha-2 & 2\alpha^2+9\alpha+1 & 2\alpha^2-1 & 3\alpha^2+\alpha-1 & -3\alpha^2-5\alpha+3 \\ 14\alpha^2-9\alpha-6 & -4\alpha^2+5\alpha+1 & 2\alpha^2+4\alpha-1 & -5\alpha^2-\alpha-1 & \alpha^2-\alpha+1 \\ -5\alpha^2+3 & 3\alpha^2+3\alpha & -\alpha^2+\alpha-1 & \alpha^2+2\alpha+2 & -\alpha^2-2\alpha-1 \\ 4\alpha^2-8\alpha-4 & 4\alpha^2+12\alpha+6 & \alpha^2+2\alpha+1 & 3\alpha-1 & -3\alpha^2-6\alpha-1 \\ 22\alpha^2-20\alpha-14 & -2\alpha^2+8\alpha-2 & 7\alpha^2-6\alpha-9 & -2\alpha^2+11\alpha+5 & -\alpha^2-4\alpha+1 \\ -29\alpha^2+19\alpha+16 & 14\alpha^2-8 & \alpha^2+4\alpha-1 & 6\alpha^2-6\alpha-3 & -4\alpha^2-\alpha+2 \\ 10\alpha^2-14\alpha-14 & 5\alpha^2+25\alpha+8 & 4\alpha^2+\alpha-2 & -\alpha^2+6\alpha+4 & -4\alpha^2-11\alpha-2 \end{pmatrix},$$

$$\psi(z_{\tau'}) = \frac{1}{28}\cdot\begin{pmatrix} -6\alpha^2+10\alpha-24 & 10\alpha^2+16\alpha+12 & -8\alpha^2-10\alpha+10 & 10\alpha^2+16\alpha-44 \\ -40\alpha^2-36\alpha+22 & 60\alpha^2+26\alpha+16 & -14\alpha^2-14 & -10\alpha^2-58\alpha+58 \\ -78\alpha^2-80\alpha-74 & 172\alpha^2+152\alpha+44 & -54\alpha^2-36\alpha+8 & 60\alpha^2-58\alpha-124 \\ 8\alpha^2+10\alpha-24 & -2\alpha^2+22\alpha+6 & -4\alpha^2-12\alpha+12 & -16\alpha^2+8\alpha-8 \\ -14\alpha^2-28\alpha+28 & 2\alpha^2+20\alpha+8 & 4\alpha^2-2\alpha-12 & -12\alpha^2-8\alpha+8 \\ 12\alpha^2-34\alpha-64 & 12\alpha^2+92\alpha+20 & -10\alpha^2-30\alpha+16 & -44\alpha^2-6\alpha-22 \\ 4\alpha^2+12\alpha-12 & -4\alpha^2+2\alpha+12 & -2\alpha^2-6\alpha+6 & -4\alpha^2+2\alpha-16 \\ -4\alpha^2+2\alpha+12 & -2\alpha^2-20\alpha+6 & 2\alpha^2+6\alpha-6 & -16\alpha^2-34\alpha+20 \\ 10\alpha^2+30\alpha-16 & -4\alpha^2-40\alpha-2 & -2\alpha^2+8\alpha+6 & -18\alpha^2-68\alpha-58 \end{pmatrix}$$

$$\begin{pmatrix} -24\alpha^2+40\alpha+2 & 2\alpha^2-22\alpha+22 & -8\alpha^2-10\alpha+24 & 2\alpha^2-22\alpha-6 & 4\alpha^2+12\alpha-12 \\ -12\alpha^2+48\alpha+8 & 12\alpha^2-6\alpha-22 & 14\alpha^2+28\alpha-28 & -2\alpha^2-20\alpha-8 & -4\alpha^2+2\alpha+12 \\ -52\alpha^2+180\alpha+30 & 2\alpha^2-64\alpha+36 & -12\alpha^2+34\alpha+64 & -12\alpha^2-92\alpha-20 & 10\alpha^2+30\alpha-16 \\ -12\alpha^2-8\alpha+8 & 4\alpha^2-2\alpha+2 & -4\alpha^2-12\alpha+12 & 4\alpha^2-2\alpha-12 & 2\alpha^2+6\alpha-6 \\ 40\alpha^2-6\alpha+6 & -12\alpha^2+6\alpha-6 & 4\alpha^2-2\alpha-12 & 2\alpha^2+20\alpha-6 & -2\alpha^2-6\alpha+6 \\ 80\alpha^2+16\alpha+12 & -24\alpha^2-2\alpha+2 & -10\alpha^2-30\alpha+16 & 4\alpha^2+40\alpha+2 & 2\alpha^2-8\alpha-6 \\ -4\alpha^2+16\alpha-2 & 2\alpha^2-8\alpha+8 & -16\alpha^2-20\alpha+20 & 2\alpha^2-8\alpha-20 & 4\alpha^2+12\alpha-12 \\ 22\alpha^2+38\alpha+4 & -2\alpha^2-6\alpha-8 & 2\alpha^2-8\alpha-20 & 26\alpha^2+36\alpha-8 & -12\alpha^2-8\alpha+8 \\ 52\alpha^2+142\alpha+26 & -18\alpha^2-40\alpha+12 & -44\alpha^2-62\alpha+20 & 52\alpha^2+86\alpha+12 & -10\alpha^2-16\alpha-12 \end{pmatrix}.$$

Finally, we use Algorithm 4.2 with $\varphi = \psi\circ\phi$ and $\varphi' = \psi\circ\phi'$ to compute a K-isomorphism $\chi' : D' \longrightarrow D$. The K-basis of D that we fix in step 1 is

$$(1, \theta, \theta^2, v, \theta v, \theta^2 v, v^2, \theta v^2, \theta^2 v^2).$$

A suitable matrix $X \in M_9(K)$ in step 2 is determined to be

$$X = \frac{1}{2}\cdot\begin{pmatrix} 0 & 0 & 0 & 0 \\ -10\alpha^2-4\alpha-6 & -10\alpha^2-10\alpha-2 & 4\alpha^2+2\alpha+2 & 36\alpha+20 \\ -20\alpha^2+22\alpha & -10\alpha^2+10\alpha+6 & 6\alpha^2-8\alpha & -34\alpha^2+32\alpha+26 \\ -10\alpha^2+4\alpha+5 & -19\alpha^2-8\alpha+5 & 9\alpha^2+\alpha-5 & -19\alpha^2+12\alpha+11 \\ 17\alpha^2-9\alpha-9 & 6\alpha^2-9\alpha-2 & -5\alpha^2+5\alpha+2 & 13\alpha^2-32\alpha-10 \\ 45\alpha^2-9\alpha-23 & 16\alpha^2+\alpha-1 & -13\alpha^2+3\alpha+6 & 17\alpha^2-78\alpha-21 \\ -18\alpha^2+48\alpha+24 & 54\alpha+30 & 6\alpha^2-22\alpha-14 & -64\alpha^2-10\alpha+8 \\ -80\alpha^2+54\alpha+48 & -36\alpha^2+24\alpha+20 & 28\alpha^2-18\alpha-18 & -100\alpha^2+102\alpha+64 \\ -262\alpha^2+240\alpha+166 & -118\alpha^2+130\alpha+84 & 92\alpha^2-84\alpha-60 & -420\alpha^2+260\alpha+206 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 2 \\ -12\alpha^2+18\alpha+10 & 6\alpha^2-10\alpha-6 & 12\alpha^2+20\alpha+10 & 10\alpha^2+8\alpha & -4\alpha^2-2\alpha \\ -52\alpha^2+32\alpha+24 & 26\alpha^2-18\alpha-14 & 8\alpha^2-6\alpha+4 & 12\alpha^2-18\alpha-10 & -6\alpha^2+10\alpha+6 \\ -\alpha^2+50\alpha+17 & 5\alpha^2-18\alpha-7 & 6\alpha^2-3\alpha-3 & 21\alpha^2+28\alpha+1 & -12\alpha^2-8\alpha+5 \\ 39\alpha^2-7\alpha-13 & -17\alpha^2+9\alpha+7 & -8\alpha^2-3\alpha-2 & -2\alpha^2+20\alpha+6 & \alpha^2-11\alpha \\ 70\alpha^2-47\alpha-37 & -30\alpha^2+30\alpha+14 & -23\alpha^2-24\alpha-7 & -20\alpha^2+15\alpha+8 & 8\alpha^2-10\alpha-2 \\ -82\alpha^2-12\alpha+2 & 38\alpha^2-4\alpha-6 & -10\alpha^2-52\alpha-16 & -6\alpha^2-74\alpha-40 & 30\alpha+12 \\ -152\alpha^2+108\alpha+76 & 76\alpha^2-60\alpha-40 & 32\alpha^2-6\alpha-16 & 42\alpha^2-42\alpha-24 & -26\alpha^2+18\alpha+18 \\ -546\alpha^2+406\alpha+286 & 282\alpha^2-210\alpha-152 & 70\alpha^2-118\alpha-72 & 152\alpha^2-162\alpha-106 & -82\alpha^2+82\alpha+54 \end{pmatrix}.$$

Note that this matrix X is not the one that was obtained in the first place. Instead, the original solution was modified in order to produce more zero coefficients in the final result. Our choice of X leads to the isomorphism $\chi' : D' \longrightarrow D$ defined by

$$\chi'(\eta) = (1,\theta,\theta^2)\cdot\frac{1}{673}\cdot\begin{pmatrix} 303\alpha^2-154\alpha-276 & 314\alpha^2+218\alpha-326 & -48\alpha^2+151\alpha+157 \\ 390\alpha^2+708\alpha-855 & 40\alpha^2-238\alpha+430 & -397\alpha^2-27\alpha+275 \\ -106\alpha^2+25\alpha+543 & -128\alpha^2-46\alpha-30 & 135\alpha^2+38\alpha-63 \end{pmatrix}\cdot\begin{pmatrix} 1 \\ v \\ v^2 \end{pmatrix}.$$

and

$$\chi'(v') = (1,\theta,\theta^2)\cdot\begin{pmatrix} 0 & \alpha^2+\alpha & 0 \\ 0 & -\alpha+1 & 0 \\ 0 & -1 & 0 \end{pmatrix}\cdot\begin{pmatrix} 1 \\ v \\ v^2 \end{pmatrix} = \left((\alpha^2+\alpha)+(-\alpha+1)\theta-\theta^2\right)v.$$

The resulting extension $\widetilde{\sigma}$ of σ is

$$\widetilde{\sigma} : D \longrightarrow D, \quad \theta \longmapsto \chi'(\eta), \quad v \longmapsto \chi'(v').$$

Using $\widetilde{\sigma}$ we can now define the *twisted Laurent series ring* $D((\mathbf{x};\widetilde{\sigma}))$, the ring of all formal series $\sum_{i\geq k} d_i\mathbf{x}^i, k\in\mathbb{Z}$, with multiplication of monomials $d\mathbf{x}^i\cdot d'\mathbf{x}^j = d\widetilde{\sigma}^i(d')\mathbf{x}^{i+j}$. $D((\mathbf{x};\widetilde{\sigma}))$ is a division algebra of degree 9 over the power series field $\mathbb{Q}((\mathbf{t}))$. In Hanke [6] it is shown that **a)** D does not contain a maximal subfield that is Galois over $\mathbb{Q}$ (we also say D does not contain an absolute Galois splitting field), and **b)** the property a) implies that $D((\mathbf{x};\widetilde{\sigma}))$ is a non-crossed product. We have thus proved the existence of a non-crossed product over $\mathbb{Q}((\mathbf{t}))$ by explicit computation plus some valuation theoretic arguments from [6]. In particular, we have not used the local-global principle of algebraic number theory.

Acknowledgements. I would like to thank the Department of Mathematics at UC San Diego and in particular my host Adrian Wadsworth for their kind hospitality

and invaluable support during my visit in 2002–2004 where this work originated. The fellowship from the German Academic Exchange Service (DAAD, Kennziffer D/02/00701) is greatly acknowledged.

I am furthermore indebted to the Instituto de Matematicas at Universidad Nacional Autónoma de México, Mexico City, and in particular to my host José Antonio de la Peña for their kind invitation and hospitality during my visit in 2005 which made the completion of this work possible. The financial support from the UNAM is greatly acknowledged.

Thanks also go to the MAGMA group for providing their computer algebra system to me.

References

1. W. Bosma, J. Cannon, and C. Playoust, *The magma algebra system I : The user language*, J. Symb. Comp. **24** (1997), no. 3/4, 235–265, (Also see the Magma home page at http://www.maths.usyd.edu.au:8000/u/magma/).
2. K. S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York, 1994, Corrected reprint of the 1982 original.
3. M. Deuring, *Einbettung von Algebren in Algebren mit kleinerem Zentrum*, J. Reine Angew. Math. **175** (1936), 124–128.
4. S. Eilenberg and S. MacLane, *Cohomology and Galois theory. I. Normality of algebras and Teichmueller's cocycle.*, Trans. Am. Math. Soc. **64** (1948), 1–20.
5. T. Hanke, *An explicit example of a noncrossed product division algebra*, Math. Nachr. **271** (2004), 51–68.
6. ———, *A twisted Laurent series ring that is a noncrossed product*, Israel J. Math. **150** (2005), 199–204.
7. G. J. Janusz, *Automorphism groups of simple algebras and group algebras*, Representation theory of algebras (Proc. Conf., Temple Univ., Philadelphia, Pa., 1976), 1978, pp. 381–388. Lecture Notes in Pure Appl. Math., Vol. 37.
8. W. Jehne, *Separable adel algebras and a presentation of weil groups*, J. Reine und Angew. Math. **375/376** (1987), 211–237.
9. V. V. Kursov and V. I. Yanchevskiĭ, *Crossed products of simple algebras and their automorphism groups*, Amer. Math. Soc. Transl. **154** (1992), no. 2.
10. J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2000.
11. R. S. Pierce, *Associative Algebras*, Springer-Verlag, New York, 1982.
12. D. J. Saltman, *Triality, cocycles, crossed products, involutions, clifford algebras and invariants*, preprint.
13. J.-P. Serre, *Local fields*, Springer-Verlag, New York, 1979.
14. J.-P. Tignol, *Generalized crossed products*, Séminaire Mathématique (nouvelle série), No. 106, Université Catholique de Louvain, Louvain-la-Neuve, Belgium, 1987.

Universidad Nacional Autónoma de México, Instituto de Matematicas, Área de la investigación científica, Circuito Exterior, Ciudad Universitaria Coyoacán 04510, 04510 México, D.F., Mexico, e-mail : hanke@matem.unam.mx