THE ISOMORPHISM PROBLEM FOR CYCLIC ALGEBRAS AND APPLICATION

TIMO HANKE[1]

Abstract. The isomorphism problem means to decide if two given finite-dimensional simple algebras over the same centre are isomorphic and, if so, to construct an isomorphism between them. A solution to this problem has applications in computational aspects of representation theory, algebraic geometry and Brauer group theory.

The paper presents an algorithm for cyclic algebras that reduces the isomorphism problem to field theory and thus provides a solution if certain field theoretic problems including norm equations can be solved (this is satisfied over number fields). A detailed example is provided which serves to construct an explicit example of a noncrossed product division algebra.

1. Introduction

Let K be a field and let A_1 and A_2 be two finite-dimensional central-simple K-algebras (A_i has no proper two-sided ideal and the centre is K). The *isomorphism problem* for A_1 and A_2 means the problem to decide whether A_1 and A_2 are K-isomorphic and, if so, to construct a K-isomorphism between them. We assume that A_1 and A_2 have equal dimension, for otherwise they are trivially non-isomorphic.

The special case when A_2 is a full matrix ring $M_n(K)$ is called the *splitting problem* for A_1. We shall call a K-isomorphism $A_1 \longrightarrow M_n(K)$ a *splitting* of A_1.

The splitting and isomorphism problem several applications. For instance, to compute the irreducible representations over K of a finite group G with $|G|$ not divisible by $\operatorname{char} k$, one can decompose the semisimple group ring KG into its simple components[2] and then solve the splitting problem for each component. As another example, finding K-rational points on a Brauer-Severi variety V is equivalent[3] to the splitting problem for the central-simple K-algebra associated with V. The splitting problem also appears if one wants to compute sets of orthogonal idempotent generators in central-simple algebras. In this paper we provide an application that is related to explicit algebra constructions. Because various constructions make use of automorphisms of simple algebras that are non-trivial on the centre, we study (in section 5) the problem of extending an automorphism of the field K to an automorphism of the central-simple K-algebra A, and show that this *extension problem*

Date: February 2, 2007.

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

Key words and phrases. isomorphism, automorphism, finite-dimensional central-simple algebras, algorithm, computation, extension, construction, bicyclic crossed product, abelian crossed product, cyclic norm equation, relative norm equation, noncrossed product.

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

[2]see Eberly [5] for an algorithm over finite fields and number fields

[3]see de Graaf-Harrison-Schicho-Pílniková [4]

reduces to the isomorphism problem. A detailed example is given, which leads to the construction of an explicit noncrossed product division algebra.

This paper solves the isomorphism problem for cyclic algebras. A *cyclic algebra* is a central-simple algebra that contains a maximal subfield which is a cyclic field extension of the centre. We always assume here that a cyclic algebra is also presented as such an algebra. For instance, if the algebra is given to us by structure constants, it is not enough to have the theoretical information that the algebra is cyclic. Instead, we need to know explicitly an element that generates a cyclic maximal subfield. Over number fields, for example, every central-simple algebra is known to be cyclic. However, it is another problem not discussed in this paper to find a cyclic maximal subfield.

The algorithms presented here work by reducing the isomorphism problem to norm equations. Norm equations are in general hard to solve, but algorithms are known over number fields (e.g. Simon [13]) and of course over finite fields. Using computer algebra systems like KASH [3] and MAGMA [2] for those norm equations, our algorithms actually become applicable over number fields (and finite fields).

Acknowledgements. I would like to thank the department of mathematics at the Universidad Nacional Autónoma de México and in particular my host José Antonio de la Peña for their kind invitation and support. I am also indebted to Adrian Wadsworth and the department of mathematics at the University of California at San Diego. It was at San Diego where the first results of this work were obtained. The financial support for this visit from the German Academic Exchange Service (DAAD) under grant D/02/00701 is greatly acknowledged. Many thanks go to the MAGMA group for making available the system to me and for the support in its use.

2. Preliminaries

Let K be a field. Unless stated otherwise, all algebras are finite-dimensional K-algebras. The tensor product $\otimes$ and the isomorphism $\cong$ without subscripts mean tensor product and isomorphism over K, respectively. A K-algebra A is called *central-simple* if A has no proper two-sided ideals and its centre $Z(A)$ is K. The reader is assumed to be familiar with the basic theory of central-simple algebras as in the textbook sources Pierce [10] or Reiner [11]. A few relevant terms are briefly recalled in the sequel.

Let A be a central-simple K-algebra. The *degree* of A, denoted $\deg A$, is the square root of the dimension $\dim_K A$ (the dimension is always a square). The algebra A is called *split* if $A \cong M_n(K)$ where $n = \deg A$. The *opposite algebra* A° of A is the K-space A with multiplication redefined by $a \circ b := ba$. If B is another central-simple K-algebras of degree n then

$$A \cong B \iff A \otimes B^\circ \cong M_{n^2}(K). \tag{1}$$

A *maximal subfield* of A shall mean a commutative subfield of A with $[L : K] = \deg A$. The algebra A is called a *crossed product* if A contains a maximal subfield that is Galois over K. Moreover, A is called *cyclic* (resp. *bicyclic*) if A contains a maximal subfield that is cyclic (resp. bicyclic) over K.

2.1. **Cyclic algebras.** Suppose A is cyclic, let L be a maximal subfield cyclic over K with $\mathrm{Gal}(L/K) = \langle \sigma \rangle$. By the Skolem-Noether theorem there is an element

$v \in A^*$ such that $vxv^{-1} = \sigma(x)$ for all $x \in L$. For any such v we have $v^n \in K$ and

$$A = \oplus_{i=0}^{n-1} Lv^i$$

as a K-space. Setting $a = v^n$ we denote this algebra by

$$A = (L/K, \sigma, a, v)$$

(in the literature v is usually omitted from the notation). For any integer k relatively prime to n,

$$(L/K, \sigma, a, v) = (L/K, \sigma^k, a^k, v^k). \tag{2}$$

We have

$$(L/K, \sigma, a, v) \cong M_n(K) \iff a \in N_{L/K}(L) \tag{3}$$

and

$$(L/K, \sigma, a, v) \cong (L/K, \sigma, b, w) \iff a/b \in N_{L/K}(L). \tag{4}$$

2.2. **Generalized cyclic algebras.** Suppose A contains a subfield L that is cyclic over K but not necessarily a maximal subfield. Then A is called a *generalized cyclic algebra* (cf. generalized crossed products in Kursov-Yanchevskiĭ [9] or Tignol [14]). Let σ generate $\mathrm{Gal}(L/K)$ and let B denote the centralizer $C_A(L)$. By the Skolem-Noether theorem there is an element $v \in A^*$ such that $vxv^{-1} = \sigma(x)$ for all $x \in L$. For any such v we have $v^n \in B$ and

$$A = \oplus_{i=0}^{n-1} Bv^i$$

as a K-space. The inner automorphism $\mathrm{Inn}(v)$ of A restricts to an automorphism of B which we denote $\widetilde{\sigma}$ because it extends σ. Setting $a = v^n$ we write

$$A = (B/K, \widetilde{\sigma}, a, v). \tag{5}$$

Also by Skolem-Noether, for any extension $\widetilde{\sigma}$ of σ to B there is $v \in A^*$ and $a \in B$ such that (5) holds. If we fix an extension $\widetilde{\sigma}$ then

$$(B/K, \widetilde{\sigma}, a, v) \cong (B/K, \widetilde{\sigma}, b, w) \iff a/b \in N_{L/K}(L) \tag{6}$$

(a/b lies in K if a and b arise in this way). An introduction of generalized cyclic algebras with proofs can be found in Hanke [6, § 10.4].

2.3. **Bicyclic algebras.** We will use for bicyclic algebras the notation that was introduced in Amitsur-Saltman [1, § 1] for the more general abelian crossed products (see also Jacobson [8, §4.6, pp. 174]). Suppose A is bicyclic with maximal subfield F, and F bicyclic over K. Let $G := \mathrm{Gal}(F/K) = G_1 \times G_2$ with $G_i = \langle\, \sigma \,\rangle$. Set $n_i := |G_i|$ and $n := |G| = n_1 n_2$. We denote by F_i and L_i the fixed fields of σ_i and σ_{3-i} respectively. Moreover, N_i denotes the norm map of the extension F/F_i. Clearly, $F_i/K, F/L_i$ are both cyclic with group G_{3-i} and $L_i/K, F/F_i$ both have group G_i. There are elements $z_1, z_2 \in A^*$ such that $z_i x z_i^{-1} = \sigma_i(x)$ for all $x \in F, i = 1, 2$. For any such z_1, z_2 we have

$$A = \bigoplus_{i=0}^{n_1-1} \bigoplus_{j=0}^{n_2-1} F z_1^i z_2^j$$

as a K-space. Since A is determined up to isomorphism by the elements

$$b_1 := z_1^{n_1}, \quad b_2 := z_2^{n_2} \quad \text{and} \quad u := z_2 z_1 z_2^{-1} z_1^{-1},$$

this algebra is denoted by

$$A = (F/K, z, u, b).$$

The elements $b_1, b_2, u \in F^*$ satisfy the relations

$$N_1(u) = \frac{\sigma_2(b_1)}{b_1}, \quad N_2(u) = \frac{b_2}{\sigma_1(b_2)}, \quad b_i \in F_i \tag{7}$$

(cf. [1, Lem. 1.2]), and the relations (7) are also sufficient for given elements $b_1, b_2, u \in F^*$ to define a bicyclic algebra (cf. [1, Thm. 1.3]). If $u = 1$ then (7) imply $b_1, b_2 \in K$ and we have the canonical decomposition

$$(F/K, z, 1, b) \cong (L_1/K, \sigma_1, b_1, z_1) \otimes (L_2/K, \sigma_2, b_2, z_2). \tag{8}$$

This implies that $(F/K, z, 1, 1)$ is split.

Theorem 1. *$A = (F/K, z, u, b)$ is split if and only if there are $x_1, x_2 \in F^*$ such that*

$$N_1(x_1) = b_1, \quad N_2(x_2) = b_2 \quad \textit{and} \quad \frac{\sigma_2(x_1)}{x_1}\frac{x_2}{\sigma_1(x_2)} = u. \tag{9}$$

Proof. Since $(F/K, z, 1, 1) \cong M_n(K)$ the statement is a special case of [1, Thm. 1.4]. □

3. The splitting problem

Let A be a central-simple K-algebra of degree n.

Splitting Problem. Decide whether A is split and, if so, compute an explicit splitting of A, i.e. a K-isomorphism $A \longrightarrow M_n(K)$.

For cyclic algebras the splitting problem quite obviously reduces to the solution of a norm equation. The point of this section is to show the same for bicyclic algebras. However, we start with the details of the cyclic case.

Algorithm 2 (Splitting of cyclic algebra)**.** Let $A = (L/K, \sigma, a, v)$ be a cyclic algebra of degree n. The splitting problem for A 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 matrix $X \in M_n(K)$ such that $\mathrm{Inn}(X)|_L = \sigma$ and define $b := X^n$. We have $b \in K$.
3. Solve the norm equation $N_{L/K}(x) = a/b$ for $x \in L$. If there is no solution then A is not split, otherwise ψ extends to an isomorphism $A \longrightarrow M_n(K)$ by mapping v to $\psi(x)X$.

Proof. Step 1 amounts to computing the minimal polynomial over K of a primitive element of L. The matrix X in step 2 exists by the Skolem-Noether theorem and is computed using only linear algebra. For this X we have $b := X^n \in K$ and $M_n(K) = (L/K, \sigma, b, X)$. Step 3. By (3), A is split if and only if $a/b \in N_{L/K}(L)$. If $x \in L$ is a solution to the equation $N_{L/K}(x) = a/b$ then $(\psi(x)X)^n = \psi(N_{L/K}(x)b) = a$. This shows that mapping v to $\psi(x)X$ indeed defines an extension of ψ. □

Now turn to bicyclic algebras. Let $A = (F/K, z, u, b)$. First note that because of the canonical isomorphism (8) we can use Algorithm 2 twice to compute a splitting of $(F/K, w, 1, 1)$. By Theorem 1, A splits if and only if the system of equations (9) has a solution. Suppose this is the case and a solution to (9) is known. Then the

proof of [1, Thm. 1.4] gives a construction of an isomorphism $A \longrightarrow (F/K, w, 1, 1)$, and together with a splitting of $(F/K, w, 1, 1)$ we have a splitting of A. Thus, it remains to solve the system (9). This covers the rest of this section.

Lemma 3 (Bicyclic Hilbert 90)**.** *Let $x_1, x_2 \in F^*$ such that*

$$N_1(x_1) = 1, \quad N_2(x_2) = 1 \quad \text{and} \quad \frac{\sigma_2(x_1)}{x_1}\frac{x_2}{\sigma_1(x_2)} = 1.$$

There is $y \in F^*$ with $x_i = \frac{\sigma_i(y)}{y}, i = 1, 2$.

Proof. The lemma should be compared to the more general statement [8, Prop. 4.6.30, p. 179]. Let $x_1 = \frac{\sigma_1(y_1)}{y_1}$, by Hilbert's Theorem 90. Then

$$\frac{\sigma_1(x_2)}{x_2} = \frac{\sigma_2(x_1)}{x_1} = \frac{\sigma_2\sigma_1(y_1)\cdot y_1}{\sigma_2(y_1)\cdot\sigma_1(y_1)} = \frac{\sigma_1(\frac{\sigma_2(y_1)}{y_1})}{\frac{\sigma_2(y_1)}{y_1}},$$

hence $x_2 = c \cdot \frac{\sigma_2(y_1)}{y_1}$ for some $c \in F_1^*$. It follows $N_2(c) = 1$. Let $c = \frac{\sigma_2(y_2)}{y_2}$ with $y_2 \in F_1^*$, by Hilbert's Theorem 90. Defining $y := y_1y_2$ we get $x_i = \frac{\sigma_i(y)}{y}$ for $i = 1, 2$. □

Proposition 4. *Let $(F/K, z, u, b)$ be split and let (x_1, x_2) be a solution to (9). The set*

$$S := \{(x_1\frac{\sigma_1(y)}{y}, x_2\frac{\sigma_2(y)}{y}) \mid y \in F^*\}$$

is the set of all solutions to (9). In particular, for any $x_1' \in F^*$ with $N_1(x_1') = b_1$ there is $x_2' \in F^*$ such that $(x_1', x_2') \in S$.

Proof. An easy calculation shows that any $(x_1', x_2') \in S$ solves (9). For the converse apply Lemma 3. The second statement is another application of Hilbert's Theorem 90. □

Algorithm 5. If $(F/K, z, u, b)$ is split then a solution (x_1, x_2) to (9) is computed as follows. Conversely, if all steps have a solution then $(F/K, z, u, b)$ is split.

1. Solve $N_1(x_1) = b_1$ for $x_1 \in F^*$.
2. Solve
$$\frac{\sigma_1(x_2')}{x_2'} = u\frac{x_1}{\sigma_2(x_1)} \quad \text{for } x_2' \in F^*.$$
3. Solve $N_2(x_2'') = b_2N_2(x_2')$ for $x_2'' \in F_1^*$.
4. Define $x_2 := {x_2'}^{-1}x_2''$.

Proof. A straight-forward calculation using (7) verifies that any (x_1, x_2) computed by these steps is a solution to (9). Conversely, suppose that $(F/K, z, u, b)$ is split and show each step has a solution. Step 1 is obvious. Step 2 has a solution by Hilbert's Theorem 90 because, using (7),

$$N_1(u\frac{x_1}{\sigma_2(x_1)}) = N_1(u)\frac{b_1}{\sigma_2(b_1)} = 1.$$

Step 3: Since $(F/K, z, u, b)$ is split by assumption, Proposition 4 shows the existence of an element $x_2 \in F^*$ with $(x_1, x_2) \in S$. Setting $x_2'' := x_2x_2'$, (9) implies $\sigma_1(x_2'')/x_2'' = 1$ and $N_2(x_2'') = b_2N_2(x_2')$. This shows that step 3 has a solution. □

Algorithm 5 reduces the splitting of a bicyclic algebra to two consecutive (*not* simultaneous) norm equations. The rest of the algorithm (step 2) is linear algebra. Note that the first norm equation (step 1) lives in the larger fields F/F_1 whereas the second one (step 3) in F_1/F.

Remark. The splitting problem has two parts : first to decide whether the algebra is split, and second to compute a splitting. One could be lead to thinking that the first part only requires to show the solvability of norm equation instead of actually finding solutions, and that it therefore be easier. This is true for cyclic algebras where only norm equation need to be solved. Then the Hasse norm principle can be used (cf. [**?**]) to prove the solvability.

For bicyclic algebras, however, this doesn't apply simply because the second norm equation in the algorithm is built from a solution to the first. So at least the first norm equation has to be solved explicitly.

Solving norm equations is very hard. For algorithms over number fields we refer to Simon [13] and the references cited therein. These algorithms involve factoring algebraic integers. On the hand, the splitting problem for quaternion algebras was shown to be at least as hard as factoring integers (Rónyai [12], under the generalized Riemann hypothesis). Since we are reducing the splitting problem to something that is as hard as factoring integers, we will not discuss complexity issues any further.

4. The isomorphism problem

Let A_1 and A_2 be central-simple K-algebras of degree n.

Isomorphism Problem. Decide whether A_1 and A_2 are K-isomorphic and, if so, compute a K-isomorphism between them.

We will show in this section how the isomorphism problem reduces to the splitting problem. To demonstrate the idea, we will first discuss general A_1 and A_2. When specializing thereafter to cyclic algebras, we will see that the isomorphism problem eventually reduces to norm equations. The following algorithm uses the equivalence (1) to find a K-isomorphism between A_1 and A_2.

Remark 6. An isomorphism $\varphi : A_1 \otimes A_2^\circ \longrightarrow M_{n^2}(K)$ is equivalent to a pair (φ_1, φ_2) where $\varphi_1 : A_1 \longrightarrow M_{n^2}(K)$ is a K-embedding and $\varphi_2 : A_2 \longrightarrow M_{n^2}(K)$ is a K-anti-embedding such that $\varphi_1(A_1)$ is the centralizer $C_{M_{n^2}(K)}(\varphi_2(A_2))$. Of course, φ_1, φ_2 are obtained from φ by composition with the canonical embedding $\varepsilon_1 : A_1 \longrightarrow A_1 \otimes A_2^\circ$ and anti-embedding $\varepsilon_1 : A_2 \longrightarrow A_1 \otimes A_2^\circ$, respectively.

Algorithm 7. Given a pair (φ_1, φ_2) as in Remark 6. Then K-isomorphisms $\chi : A_1 \longrightarrow A_2$ and $\chi' : A_2 \longrightarrow A_1$ are computed as follows.

1. Fix a K-basis of A_1 and identify $M_{n^2}(K)$ with $\mathrm{End}_K(A_1)$.
2. Choose a matrix $X \in M_{n^2}(K)$ such that $\mathrm{Inn}(X) \circ \varphi_1 = \lambda$, the left-regular representation of A_1.
3. Set $\varphi_2' := \mathrm{Inn}(X) \circ \varphi_2$. Then $\varphi_2'(A_2) = \rho(A_1)$, where ρ is the right-regular representation of A_1.
4. Define $\chi := {\varphi_2'}^{-1} \circ \rho : A_1 \longrightarrow A_2$ and $\chi' := \rho^{-1} \circ \varphi_2' : A_2 \longrightarrow A_1$.

Proof. The left-regular representation

$$\lambda : A_1 \longrightarrow \mathrm{End}_K(A_1), \quad a \longmapsto \lambda_a, \quad \lambda_a(x) := ax$$

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

$$\rho : A_1 \longrightarrow \mathrm{End}_K(A_1), \quad a \longmapsto \rho_a, \quad \rho_a(x) := xa$$

is a K-algebra anti-isomorphism. The matrix X in step 2 exists by the Skolem-Noether theorem and its computation is equivalent to finding the solution to a linear equation system. It follows

$$\varphi_2'(A_2) = C_{M_{n^2}(K)}(X\varphi_1(A_1)X^{-1}) = C_{M_{n^2}(K)}(\lambda(A_1)) = \rho(A_1).$$

Since ρ and φ_2' are both anti, χ and χ' as defined in step 4 are isomorphisms. □

Algorithm 7 shows that the isomorphism problem for A_1 and A_2 is constructively equivalent to the splitting problem for $A_1 \otimes A_2^\circ$. Our approach to the isomorphism problem is based on this reduction.

Remark. It is certainly quite inefficient to reduce a problem about algebras of dimension n to one in dimension n^2. On the other hand, it is doubtful if one can improve on this complexity because the two problems are actually equivalent.

Over number fields another approach to the first part of the isomorphism problem would be by computing and comparing the local invariants (Hasse invariants). However, it is not clear how to compute all invariants.

Now turn to the isomorphism problem for two cyclic algebras

$$A_1 = (L_1/K, \sigma_1, a_1, v_1) \quad \text{and} \quad A_2 = (L_2/K, \sigma_2, a_2, v_2)$$

of degree n. Consider L_1, L_2 as subfields of some common overfield. We distinguish two special cases and the general case.

Special case 1 : $L_1 \cong_K L_2$. Let $\chi : L_1 \longrightarrow L_2$ be a K-isomorphism. Obviously, $\chi\sigma_1\chi^{-1} = \sigma_2^i$ for some i relatively prime to n. Replacing v_2 with v_2^i we can assume by (2) that $\chi\sigma_1\chi^{-1} = \sigma_2$. Then, by (4),

$$A_1 \cong A_2 \iff a_1/a_2 \in N_{L_2/K}(L_2).$$

This equivalence is constructive : if $x \in L_2$ is an element with $N_{L_2/K}(x) = a_1/a_2$ then mapping $v_1 \longmapsto xv_2$ extends χ to a K-isomorphism $A_1 \longrightarrow A_2$. The isomorphism problem for A_1 and A_2 is thus reduced to finding a solution to a norm equation in the field extension L_2/K.

Special case 2 : $L_1 \cap L_2 = K$. We reduce this case with Algorithm 7 to the splitting of $A_1 \otimes A_2^\circ$. Since $L_1 \cap L_2 = K$, the Galois extensions $L_1/K, L_2/K$ are linearly disjoint, i.e. $L_1 \otimes_K L_2$ is a field. Moreover, $L_1 \otimes L_2$ is a maximal subfield of $A_1 \otimes A_2^\circ$ and has bicyclic Galois group over K. Hence, $A_1 \otimes A_2^\circ$ is a bicyclic algebra. The splitting problem for $A_1 \otimes A_2^\circ$ reduces to norm equations by Algorithm 5.

Remark 8. The opposite algebra A_2° is identified with $(L_2/K, \sigma_2, a_2^{-1}, w)$ and an anti-isomorphism $A_2 \longrightarrow A_2^\circ$ is defined by $\lambda v_2^i \longmapsto w^{-i}\lambda$ for all $\lambda \in L_2$.

Remark. If the degree n is a prime then we are in one of the special cases.

General case. Let $L_0 = L_1 \cap L_2$ and consider the centralizers $B_1 = C_{A_1}(L_0)$ and $B_2 = C_{A_2}(L_0)$. If $A_1 \cong A_2$ then $B_1 \cong_{L_0} B_2$ so we can first solve the isomorphism problem for B_1 and B_2 over L_0 with special case 2. Assuming that an L_0-isomorphism $\chi : B_1 \longrightarrow B_2$ is computed we identify B_1 and B_2 under χ and simply write B for both of them. Fix an extension $\widetilde{\sigma}$ of σ to B. There are $w_1 \in A_1^*, w_2 \in A_2^*$ and $b_1, b_2 \in B^*$ such that

$$A = (B/K, \widetilde{\sigma}_1, b_1, w_1) \quad \text{and} \quad A_2 = (B/K, \widetilde{\sigma}_2, b_2, w_2).$$

The elements w_1, w_2 are predicted by the Skolem-Noether theorem and are computable with linear algebra. We proceed as in special case 1 but for generalized cyclic algebras. By (6),

$$A_1 \cong A_2 \iff b_1/b_2 \in N_{L_0/K}(L_0).$$

The equivalence is constructive : if $x \in L_0$ is an element with $N_{L_0/K}(x) = b_1/b_2$ then mapping $w_1 \longmapsto xw_2$ defines a K-isomorphism $A_1 \longrightarrow A_2$. The isomorphism problem for A_1 and A_2 is thus completely reduced to finding solutions to norm equations.

5. Application : extending field automorphisms to simple algebras

Let A be a central-simple K-algebra and let $\sigma \in \mathrm{Aut}(K)$ be an automorphism of finite order.

Extension Problem. Decide whether σ extends to an automorphism of A and, if so, compute an extension.

It is convenient to reformulate this problem using the algebra ${}_{\sigma^{-1}}A$ which is obtained from A by redefining the K-action as $\lambda \circ a := \sigma^{-1}(\lambda)a$ for all $\lambda \in K$. Then σ extends to A if and only if A and ${}_{\sigma^{-1}}A$ are isomorphic as K-algebras. In fact, any K-algebra isomorphism ${}_{\sigma^{-1}}A \longrightarrow A$ becomes an extension of σ after identifying ${}_{\sigma^{-1}}A$ as a ring (*not* a K-algebra) with A. The extension problem is therefore just a special case of the isomorphism problem. If A is cyclic then ${}_{\sigma^{-1}}A$ is also cyclic, hence, by the results of the preceding sections, the extension problem for cyclic algebras reduces to norm equations.

Remark. To clarify the identification of ${}_{\sigma^{-1}}A$ and A as rings let $A = (L/K, \tau, a, v)$. Fix an extension of σ to some Galois closure containing L and call it also σ. Then

$${}_{\sigma^{-1}}A = (\sigma L/K, \sigma\tau\sigma^{-1}, \sigma a, w).$$

The ring identity map $A \longrightarrow {}_{\sigma^{-1}}A$ is defined by $\sigma : L \longrightarrow \sigma L$ and $v \longmapsto w$.

We finish with a detailed example for the solution of the extension problem. Let K be the cubic number field

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

of discriminant 49 (the maximal real subfield of the 7-th cyclotomic field). It is $\mathrm{Gal}(K/\mathbb{Q}) = \langle\, \sigma \,\rangle$ with

$$\sigma(\alpha) = -\alpha^2 - \alpha + 1.$$

Let L be the cubic extension

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

which is cyclic and has $\mathrm{Gal}(L/K) = \langle\, \tau \,\rangle$ with

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

In the following we will solve the extension problem for σ and the cyclic algebra

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

With the extension $\widetilde{\sigma}$ we can then form the *twisted Laurent series ring* $D((\mathbf{x}; \widetilde{\sigma}))$, i.e. the ring of all formal series $\sum_{i \geq k} d_i \mathbf{x}^i, k \in \mathbb{Z}$, with multiplication of monomials $d\mathbf{x}^i \cdot d'\mathbf{x}^j = d\widetilde{\sigma}^i(d')\mathbf{x}^{i+j}$. Then $D((\mathbf{x}; \widetilde{\sigma}))$ is a division algebra of degree 9 over the power series field $\mathbb{Q}((\mathbf{t}))$. The D in this example is the division algebra from

Hanke [7] with the property that 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"). It is also shown in [7] that this particular property implies that $D((\mathbf{x};\widetilde{\sigma}))$ is a noncrossed product. When $\widetilde{\sigma}$ is computed we have thus constructed a fully explicit noncrossed product example over $\mathbb{Q}((\mathbf{t}))$. Once $\widetilde{\sigma}$ is known, the existence of noncrossed products (a proof of which formerly required the use of deep local-global principles) can now be verified by direct computation in this explicit example.

In order to solve the extension problem for D and σ we solve the isomorphism problem for D and ${}_{\sigma^{-1}}D$. We have ${}_{\sigma^{-1}}D = (\sigma L/K, \sigma\tau\sigma^{-1}, \sigma a, w)$ where

$$\begin{aligned}
&\sigma L = K(\eta), \quad \mathrm{Irr}(\eta, K) = x^3 + (-\alpha^2 - \alpha - 1)x^2 + (\alpha^2 + \alpha - 2)x + 1,\\
&\sigma\tau\sigma^{-1}(\eta) = -\eta^2 + (\alpha^2 + \alpha)\eta + 2,\\
&\sigma(a) = 2(\alpha^2 + 2\alpha - 1)
\end{aligned}$$

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

Since $L \cap \sigma L = K$ we are in the special case 2 of the isomorphism problem. This means we have to write $D \otimes_{\sigma^{-1}} D^\circ$ as a bicyclic algebra with respect to the maximal subfield $L \otimes_K \sigma L$, and then solve the splitting problem for it with Algorithm 5. By (8) and Remark 8, $D \otimes {}_{\sigma^{-1}}D^\circ$ is canonically isomorphic to the bicyclic algebra

$$C := (F/K, z, 1, b)$$

where

$$\begin{aligned}
&L_1 = F_2 = L, && \sigma_1 := \tau, && b_1 := a = 2(\alpha^2 - \alpha - 2),\\
&L_2 = F_1 = \sigma L, && \sigma_2 := \sigma\tau\sigma^{-1}, && b_2 := \sigma a^{-1} = \frac{1}{14}(\alpha^2 + 3\alpha - 3)
\end{aligned}$$

and $F = L_1L_2$. The canonical embedding and anti-embedding of Remark 6 are given by

$$\varepsilon_1 : D \longrightarrow C,\ \lambda v^i \longmapsto \lambda z_1^i, \quad \varepsilon_2 : {}_{\sigma^{-1}}D \longrightarrow C,\ \mu w^i \longmapsto \mu z_2^i$$

for all $\lambda \in L, \mu \in \sigma L$. Now we apply Algorithm 5 to split C.
Step 1. A solution that was found with the computer algebra system 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 was a few minutes (less than 10) on a 800 MHz processor.
Step 2. As a solution to a linear equation system one finds

$$\begin{aligned}
x_2' =& \frac{1}{28}\big((81\alpha^2 - 261\alpha - 173) + (194\alpha^2 + 428\alpha + 132)\eta + (-70\alpha^2 - 98\alpha - 21)\eta^2\\
&+ (-19\alpha^2 - 120\alpha + 8)\theta + (287\alpha^2 - 266\alpha - 196)\eta\theta + (-92\alpha^2 + 130\alpha + 45)\eta^2\theta\\
&+(7\alpha^2 + 70\alpha + 14)\theta^2 + (-202\alpha^2 - 179\alpha - 24)\eta\theta^2 + (63\alpha^2 + 28\alpha + 7)\eta^2\theta^2\big)\,.
\end{aligned}$$

Step 3. Exceptionally in this example, the element

$$b_2N_2(x_2') = \frac{1}{56}(-1601\alpha^2 + 693\alpha + 609)$$

lies in K. We compute as a cubic root :

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

Step 4. Finally, we get

$$\begin{aligned} x_2 = &\frac{1}{14}\left((-8\alpha^2 - 3\alpha + 10) + (-2\alpha^2 - 13\alpha - 1)\eta + (2\alpha^2 + 6\alpha - 6)\eta^2\right. \\ &+ (-3\alpha^2 + 5\alpha + 2)\theta + (6\alpha^2 - 10\alpha + 10)\eta\theta + (-2\alpha^2 + \alpha - 1)\eta^2\theta \\ &\left.+(2\alpha^2 - \alpha - 6)\theta^2 + (\alpha^2 + 10\alpha - 3)\eta\theta^2 + (-\alpha^2 - 3\alpha + 3)\eta^2\theta^2\right). \end{aligned}$$

This completes Algorithm 5. At this point we have shown that C splits, hence σ extends to D. We continue to use (x_1, x_2) to compute an extension of σ. First, since (x_1, x_2) is a solution to (9), we obtain an isomorphism $\varphi : C \longrightarrow M_9(K)$ according to Theorem 1. This φ can be computed as described after Algorithm 5. Two images are printed here only to give an expression on how complicated the matrices get :

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

$$\varphi(z_1) = \frac{1}{2} \cdot \begin{pmatrix} -3\alpha^2+9\alpha+3 & -12\alpha^2-2\alpha+1 & 5\alpha^2-\alpha-2 & -17\alpha^2+13\alpha+11 & \\ -5\alpha^2+\alpha+2 & -\alpha^2+6\alpha & \alpha^2-2\alpha-2 & -8\alpha^2+5\alpha+5 & \\ -\alpha^2+2\alpha+2 & -3\alpha^2+2\alpha & -\alpha-4 & -6\alpha^2+\alpha+4 & \\ 5\alpha^2-10\alpha-8 & 3\alpha^2+12\alpha+6 & -2\alpha^2-3\alpha & -4\alpha^2-3\alpha+6 & \\ 2\alpha^2+3\alpha & 5\alpha^2-8\alpha-5 & -3\alpha^2+\alpha+3 & 4\alpha^2-5\alpha-1 & \\ 3\alpha^2-\alpha-3 & -\alpha^2+3\alpha+5 & -\alpha^2-5\alpha-1 & -3\alpha^2-3\alpha & \\ 19\alpha^2+\alpha-11 & -23\alpha^2-3\alpha+3 & 5\alpha^2-\alpha+1 & -31\alpha^2+15\alpha+28 & \\ -5\alpha^2+\alpha-1 & 18\alpha^2-5\alpha-8 & -7\alpha^2+3 & 2\alpha^2-8\alpha+2 & \\ 7\alpha^2-3 & -8\alpha^2+5\alpha+5 & -9\alpha-5 & -14\alpha^2+8 & \end{pmatrix}$$

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

Using Algorithm 7 with $\varphi_1 = \varphi \circ \varepsilon_1$ and $\varphi_2 = \varphi \circ \varepsilon_2$ we continue to compute a K-isomorphism $\chi' : {}_{\sigma^{-1}}D \longrightarrow D$ to be 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

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

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

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

References

1. S. A. Amitsur and D. J. Saltman, *Generic abelian crossed products and p-algebras*, J. Algebra **51** (1978), 76–87.
2. 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/).
3. M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, and K. Wildanger, *KANT V4*, J. Symbolic Comp. **24** (1997), 267–283.
4. W. de Graaf, M. Harrison, J. Pílniková, and J. Schicho, *A Lie algebra method for rational parametrization of Severi-Brauer surfaces.*, J. Algebra **303** (2006), no. 2, 514–529.
5. W. Eberly, *Decomposition of algebras over finite fields and number fields.*, Comput. Complexity **1** (1991), no. 2, 183–210.
6. T. Hanke, *A direct approach to noncrossed product division algebras*, Dissertation, Universität Potsdam, 2001.
7. ———, *A twisted Laurent series ring that is a noncrossed product*, Israel J. Math. **150** (2005), 199–204.
8. N. Jacobson, *Finite dimensional division algebras over fields*, Springer-Verlag, Berlin, 1996.
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. R. Pierce, *Associative Algebras*, Springer-Verlag, New York, 1982.
11. I. Reiner, *Maximal Orders*, Academic Press, London, 1975.
12. L. Rónyai, *Zero divisors in quaternion algebras.*, J. Algorithms **9** (1988), no. 4, 494–506.
13. D. Simon, *Solving norm equations in relative number fields using S-units*, Math. Comp. **71** (2002), no. 239, 1287–1305 (electronic).
14. J.-P. Tignol, *Generalized crossed products*, Séminaire Mathématique (nouvelle série), No. 106, Université Catholique de Louvain, Louvain-la-Neuve, Belgium, 1987.

Department of Mathematics, Technion – Israel Institute of Technology, Haifa, 32000, Israel. e-mail : hanke@math.uni-potsdam.de