

WANG COUNTEREXAMPLES LEAD TO NONCROSSED PRODUCTS

ERIC S. BRUSSEL

(Communicated by Ken Goodearl)

ABSTRACT. Two famous counterexamples in algebra and number theory are Wang's counterexample to Grunwald's Theorem and Amitsur's noncrossed product division algebra. In this paper we use Wang's counterexample to construct a noncrossed product division algebra.

In the 30's, Grunwald's Theorem was used in the proof of a major result of class field theory, that all division algebras over number fields are (cyclic) crossed products. It is ironic that now Grunwald-Wang's Theorem is the decisive factor in a noncrossed product construction.

0. INTRODUCTION

Two famous counterexamples in algebra and number theory are Wang's counterexample to Grunwald's Theorem (see [W]) and Amitsur's noncrossed product division algebra ([A]). In this paper we use Wang's counterexample to construct a noncrossed product division algebra.

In the 30's, Grunwald's Theorem was used in the proof of a major result of class field theory, that all division algebras over number fields are (cyclic) crossed products. It is ironic that now Grunwald-Wang's Theorem is the decisive factor in a noncrossed product construction.

Our construction exploits the same insight as did the one in [B], although the obstruction that produces the result is qualitatively different.

1. BACKGROUND AND NOTATION

Let " F -division algebra" mean a division ring whose center is a field F and whose F -dimension is finite. Call the square root of the F -dimension the *index*. Call A a *central simple F -algebra* if A is a simple F -algebra, that is, a simple ring whose center is F and whose F -dimension is finite. By Wedderburn's Theorem, A is a matrix ring over some F -division algebra; denote it by $\Delta(A)$. Define the index and degree of A to be the index of $\Delta(A)$ and the square root of $\dim_F(A)$, respectively.

Say a field extension L/F *splits* A if the scalar extension $A \otimes_F L$ is isomorphic to a matrix ring over L . Call an embedded F -field extension a *subfield* of A . Then all *maximal subfields* of $\Delta(A)$ (obvious meaning) split A .

Received by the editors April 12, 1995 and, in revised form, December 1, 1995.

1991 *Mathematics Subject Classification*. Primary 16S35; Secondary 11R37.

The author's research was supported in part by an Alfred P. Sloan Foundation Doctoral Dissertation Fellowship and by NSF Grant DMS-9100148.

Let the *classical Brauer group* $\text{Br}(F)$ be the set of equivalence classes of central simple F -algebras A defined by $A \sim A' \Leftrightarrow \Delta(A) \cong \Delta(A')$ (F -isomorphism). Define the group structure of $\text{Br}(F)$ by the F -algebra tensor product. If L/F is a finite Galois extension, the set of classes of $\text{Br}(F)$ split by L form a subgroup $\text{Br}(L/F)$; call it the *relative (classical) Brauer group*.

Let *cohomological Brauer group* mean the 2-dimensional Galois cohomology group $\text{H}^2(\mathfrak{G}_F, F_{\text{sep}}^\bullet) = \varinjlim \text{H}^2(G, L^\bullet)$, where L and $G = \text{Gal}(L/F)$ vary over all finite Galois extensions of F , and \mathfrak{G}_F is the absolute Galois group of F . Let the *relative (cohomological) Brauer group* be $\text{H}^2(G, L^\bullet)$.

The Crossed Product Construction. An isomorphism between the classical and cohomological Brauer groups is achieved via the *crossed product construction* ([R]). This construction yields presentations of central simple F -algebras directly from relative 2-cocycles (also called *factor sets*). The original crossed product construction (given by Dickson) was defined *ad hoc*, as a means for effectively constructing division algebras. Remarkably, this construction is also the bridge (discovered by Noether) between the classical and cohomological Brauer groups. Following is a brief sketch.

If L/F is a Galois extension, and A/F is a crossed product via some 2-cocycle $f \in \mathbb{Z}^2(G, L^\bullet)$, then it is immediate from the construction that L is a maximal subfield of A of degree equal to $\text{deg}(A)$. Conversely, if L is a Galois maximal subfield A , then it has degree $\text{deg}(A)$, and A is a crossed product via some factor set $f \in \mathbb{Z}^2(G, L^\bullet)$. This shows that if A is a central simple F -algebra, then

$$A \text{ is a crossed product} \iff A \text{ has a Galois maximal subfield.}$$

Every division algebra has a separable maximal subfield (this is classical), hence is split by a finite Galois extension. Thus for every division algebra D , it is possible to adjust n so that the matrix ring $M_n(D)$ is a crossed product via this Galois extension. This correspondence produces the isomorphism $\text{Br}(F) \cong \text{H}^2(\mathfrak{G}_F, F_{\text{sep}}^\bullet)$.

The Noncrossed Product Question. The above correspondence is between classes of central simple algebras and classes of factor sets. As every classical Brauer class has a distinguished representative (the division algebra), it is natural to ask whether every cohomological Brauer class also has one, corresponding to the division algebra. In other words, *do there exist noncrossed product division algebras?*

It is easy to find noncrossed product central simple algebras. For example, take any nontrivial matrix ring over an algebraically closed field. It is much harder to find noncrossed product division algebras; after their existence was postulated, it took almost 40 years to find one! In spite of this, the constructions in [B] could have been carried out in the 30's. The following construction, however, could not have appeared until after Wang's paper.

The Set-Up. Let k be a number field, and let $k(t)$ and $k((t))$ be the rational function field over k and the field of formal power series with coefficients in k , respectively. By [S], Ch. XII, there is a noncanonically split exact sequence

$$(1.0.1) \quad 1 \rightarrow \text{Br}(k) \rightarrow \text{Br}(k((t))) \rightarrow \mathbf{X}(k) \rightarrow 1$$

where $\mathbf{X}(k)$ is the character group $\text{Hom}(\text{Gal}(k_{\text{sep}}/k), \mathbb{Q}/\mathbb{Z})$. Thus there is associated to a character χ a $k((t))$ -division algebra $X := \Delta((\chi, t))$. By [P], §19.5, there is a

noncanonical split injection

$$(1.0.2) \quad \sigma : \text{Br}(k((t))) \hookrightarrow \text{Br}(k(t)).$$

By (1.0.1), any construction over $k((t))$ can be made over $k(t)$, since the defining components exist over k . The map σ can be defined so that the resulting $k(t)$ -Brauer element is the image under σ of the original $k((t))$ -construction. By [B], Lemma 4, the index computations are the same. Thus the constructions over $k((t))$ “remain intact” when mapped to $k(t)$ via σ .

From now on, let $F = k(t)$ or $k((t))$. The standard set-up consists of a k -division algebra A , a character $\chi \in \mathbf{X}(k)$ with associated F -division algebra X , and an F -division algebra $D \cong \Delta(A \otimes_F X)$, as per (1.0.1). Associated to χ is a cyclic extension of degree $|\chi|$, which will be denoted throughout by K/k .

The following result was proved by Nakayama in the 30’s. For proof, see [B], Lemma 4.

Index Formula 1.1. *In the above set-up,*

$$\text{ind}(D) = |\chi| \cdot \text{ind}(A \otimes K).$$

Grunwald-Wang’s Theorem. Grunwald-Wang’s Theorem is critical in the following constructions, and it is presented here in order to fix notation. See Chapter 10 of [AT] for a full treatment.

Let k be a number field, C its idèle class group, and \mathfrak{G} its absolute Galois group. By the Existence Theorem, the Artin map induces an isomorphism $\mathbf{X}(k) \xrightarrow{\sim} \mathbf{X}(C)$. Similarly, by local class field theory, $\mathbf{X}(k_{\mathfrak{p}}) \xrightarrow{\sim} \text{Hom}(k_{\mathfrak{p}}^{\bullet}, \mathbb{Q}/\mathbb{Z})$.

Let μ_m denote the group of m^{th} roots of unity. Let r and s be maximal such that $\mu_{2^r} \subset k^{\bullet}$ and $\mu_{2^s} \subset k(\mu_{2^{r+1}})^{\bullet}$. For all $a \in \mathbb{N}$, fix a primitive 2^a -th root of unity ζ_{2^a} , and set $\eta_a = \zeta_{2^a} + \zeta_{2^a}^{-1}$. Note that $|\eta_a| = |2 \cos \frac{2\pi}{2^a}|$, $\eta_{a+1}^2 = \eta_a + 2$, and $\eta_3 = 2 \cos \frac{\pi}{4} = \sqrt{2}$.

Grunwald-Wang’s Theorem 1.2. *Let k be a number field, let S be a finite set of primes of k , and for each $\mathfrak{p} \in S$ let $\psi_{\mathfrak{p}}$ be a character of $k_{\mathfrak{p}}^{\bullet}$ of order $m_{\mathfrak{p}}$. Let $S_0 = \{\mathfrak{p} \mid k_{\mathfrak{p}}(\zeta_{2^{s+1}})/k_{\mathfrak{p}} \text{ is noncyclic}\}$. Then there exists a global character ψ with restrictions the $\psi_{\mathfrak{p}}$. Furthermore, there is one of order $m := \text{lcm}\{m_{\mathfrak{p}}\}$ if and only if $S_0 \not\subseteq S$, or $2^{s+1} \nmid m$, or*

$$(1.2.1) \quad \sum_{\mathfrak{p} \in S_0} \psi_{\mathfrak{p}}(\eta_{s+1}^m) = 0 \quad \text{in } \mathbb{Q}/\mathbb{Z}.$$

There is always one of order $2m$.

Remarks 1.2.2. (i) If a global character of order m exists, say that the set $\{\psi_{\mathfrak{p}} \mid \mathfrak{p} \in S\}$ has a *Grunwald lift*. If not, say that $\{\psi_{\mathfrak{p}} \mid \mathfrak{p} \in S\}$ gives a *Wang counterexample*. Refer to the case where $2^{s+1} \mid m$ and $S_0 \subseteq S$ as the *Special Case*. When k has a Special Case with S_0 nonempty, say k has a *nonempty Special Case*.

(ii) If 2^{s+1} divides m , $\eta_{s+1}^m = (1 + \zeta_{2^s})^m$. The argument of $1 + \zeta_{2^s}$ is one half the argument of ζ_{2^s} , which in turn is $\frac{2\pi}{2^s}$. Thus η_{s+1}^m is always a real number, and $\eta_{s+1}^m = |\eta_{s+1}|^m = (2 \cos \frac{2\pi}{2^{s+1}})^m$.

(iii) By definition, $\eta_s + 2 \in k_{\mathfrak{p}}^{\bullet} \forall \mathfrak{p} \in S_0$. Consequently, in the sum (1.2.1), $\psi_{\mathfrak{p}}(\eta_{s+1}^m) = \psi_{\mathfrak{p}}((\eta_s + 2)^{\frac{m}{2}}) = (\frac{m}{2} \cdot \psi_{\mathfrak{p}})(\eta_s + 2)$. The character $\frac{m}{2} \cdot \psi_{\mathfrak{p}}$ has order

dividing 2, and is nontrivial if and only if $\frac{m}{m_p}$ is odd. Thus

$$\sum_{\mathfrak{p} \in S_0} \psi_{\mathfrak{p}}(\eta_{s+1}^m) = \sum_{\mathfrak{p} \in S_0, \frac{m}{m_p} \text{ odd}} \chi_{\mathfrak{p}}(\eta_s + 2),$$

where for each $\mathfrak{p} \in S_0$, $\chi_{\mathfrak{p}}$ is character of order 2 that extends to the character $\psi_{\mathfrak{p}}$ of order $m_{\mathfrak{p}}$.

2. THE CROSSED PRODUCT THEOREM

The main theorem in [B] will now be stated in a way that distinguishes between two constructions of noncrossed products over $k(t)$ and $k((t))$. First, some notation is needed, from Neukirch (p.47, [N]).

Let Γ be a fixed finite group. The homomorphisms of arbitrary profinite groups \mathfrak{G} into Γ are the objects of a category, with morphisms ψ the homomorphisms $\mathfrak{G} \rightarrow G$ that commute with the respective maps to Γ . Two morphisms $\psi, \psi' : \mathfrak{G} \rightarrow G$ are defined to be equivalent if their images are pointwise conjugate by a fixed element in $\ker(G \rightarrow \Gamma)$. The equivalence classes are denoted by $[\psi]$, and the set of all equivalence classes is denoted by $\text{Hom}_{\Gamma}(\mathfrak{G}, G)$. The set of all surjective morphisms is denoted by $\text{Hom}_{\Gamma}(\mathfrak{G}, G)_{\text{sur}}$.

When k is a number field, $\mathfrak{G} = \text{Gal}(k_{\text{sep}}/k)$, G is a finite group, and the defining homomorphisms $\mathfrak{G} \rightarrow \Gamma$ and $G \rightarrow \Gamma$ are *surjective*, an element $[\psi]$ of $\text{Hom}_{\Gamma}(\mathfrak{G}, G)$ corresponds to the solution of an embedding problem in the following sense: The map $\mathfrak{G} \rightarrow \Gamma$ corresponds to a (finite) Galois extension K/k with group Γ . Any representative of $[\psi]$ corresponds to a Galois extension $L/K/k$ with group $\text{Gal}(L/k) = \psi(\mathfrak{G}) \subseteq G$. If ψ is surjective, then $\text{Gal}(L/k) = G$. Thus $\text{Hom}_{\Gamma}(\mathfrak{G}, G)_{\text{sur}}$ is non-empty if and only if there exists a solution to the problem of embedding a Γ -Galois extension K/k into a G -Galois extension L/k , in a manner consistent with $G \rightarrow \Gamma$.

If k is a number field, and if $[\psi]$ is an element of $\text{Hom}_{\Gamma}(\mathfrak{G}, G)$, then corresponding to every prime \mathfrak{q} of k is an element $[\psi_{\mathfrak{q}}] \in \text{Hom}_{\Gamma}(\mathfrak{G}_{\mathfrak{q}}, G)$, where $\mathfrak{G}_{\mathfrak{q}}$ is the decomposition group of \mathfrak{G} at \mathfrak{q} . Thus there is obtained a canonical map $\text{Hom}_{\Gamma}(\mathfrak{G}, G) \rightarrow \prod \text{Hom}_{\Gamma}(\mathfrak{G}_{\mathfrak{q}}, G)$, corresponding to the fact that the solution of a global embedding problem produces solutions of local embedding problems involving the decomposition groups of \mathfrak{G}, G , and Γ .

Theorem 2.1. *Let k be a number field, let $F = k(t)$ or $k((t))$, let $D \cong \Delta(A \otimes X)$ be an F -division algebra, and let $\Gamma = \text{Gal}(K/k)$ (notation as in §1). Then D is a crossed product if and only if*

- I. *For some group G of order $\text{ind}(D)$ and surjection $G \rightarrow \Gamma$, there exists for each prime \mathfrak{q} of k an element $[\psi_{\mathfrak{q}}] \in \text{Hom}_{\Gamma}(\mathfrak{G}_{\mathfrak{q}}, G)$ that splits $A_{\mathfrak{q}}$.*
- II. *For the same group G , there exists an element $[\psi] \in \text{Hom}_{\Gamma}(\mathfrak{G}, G)$ whose local images are the $[\psi_{\mathfrak{q}}]$.*

Condition (I) asks for compatible local constructions. Condition (II) asks for a lift of these local constructions. A noncrossed product construction must obstruct one or the other. If condition (I) is obstructed, say the construction is of “type I”. Otherwise, say that it is of “type II”. All of the constructions in [B] are of type I.

3. WANG COUNTEREXAMPLES

A dissection of the Special Case is now performed, in order to control the appearance of Wang counterexamples.

Lemma 3.1. *Let k be a number field. Then there exists a Wang counterexample if and only if k has a nonempty Special Case. Equivalently, for some $\mathfrak{p} \in S_0$ there exists a character $\chi_{\mathfrak{p}}$ of $k_{\mathfrak{p}}^{\bullet}$ of order 2, such that $\chi_{\mathfrak{p}}(-1) = 0$ and $\chi_{\mathfrak{p}}(\eta_s + 2) \neq 0$. Such a $\chi_{\mathfrak{p}}$ extends to a character $\psi_{\mathfrak{p}}$ of any order $m_{\mathfrak{p}}$ divisible by 2. For every such extension, $\psi_{\mathfrak{p}}(\eta_{s+1}^{m_{\mathfrak{p}}}) \neq 0$.*

Proof. If there exists a Wang counterexample, then by Theorem 1.2 there must be a nonempty Special Case. Moreover, any character $\psi_{\mathfrak{p}}$ as in the lemma with $m_{\mathfrak{p}} = |\psi_{\mathfrak{p}}|$ divisible by 2^{s+1} easily gives a Wang counterexample: Set $m_{\mathfrak{p}} = m$, and consider the set consisting of $\psi_{\mathfrak{p}}$ and the trivial characters for each $\mathfrak{q} \in S_0 \setminus \{\mathfrak{p}\}$. Then the sum (1.2.1) equals the value $\psi_{\mathfrak{p}}(\eta_{s+1}^m)$, which is nonzero by hypothesis. This proves the first statement.

To prove the rest of the lemma it will be shown first that every $\chi_{\mathfrak{p}}$ extends to a $\psi_{\mathfrak{p}}$ as in the lemma, and that all $\psi_{\mathfrak{p}}$ have the stated property. It will then be enough to show that k has a Special Case only if the $\chi_{\mathfrak{p}}$ exist. \square

Lemma 3.2. *Let μ_n be the group of roots of unity in $k_{\mathfrak{p}}^{\bullet}$. Then a character χ of $k_{\mathfrak{p}}^{\bullet}$ of order m extends to one of order ℓm if and only if $\mu_z \subseteq \ker(\chi)$, where $z = \frac{n(\ell, n)}{(\ell m, n)}$.*

Proof. (\Rightarrow): Suppose that ψ is a character of order ℓm extending χ . Assume $\ell\psi = \chi$. If $\mu_j \subseteq \ker(\psi)$ for some j , then $\chi(\mu_{(j\ell, n)}) = \psi(\mu_{(j\ell, n)}^{\ell}) = 0$, since $\mu_{(j\ell, n)}^{\ell} \subseteq \mu_j$. Thus $\mu_{(j\ell, n)} \subseteq \ker(\chi)$. Since ψ is a homomorphism onto $\frac{1}{\ell m}\mathbb{Z}/\mathbb{Z}$, $\mu_{\frac{n}{(\ell m, n)}} \subseteq \ker(\psi)$. Setting $j = \frac{n}{(\ell m, n)}$ yields $(j\ell, n) = \frac{n}{(\ell m, n)}(\ell, (\ell m, n)) = z$; hence $\mu_z \subseteq \ker(\chi)$, as desired.

(\Leftarrow): Suppose $\mu_z \subseteq \ker(\chi)$. There is a decomposition $k_{\mathfrak{p}}^{\bullet} = \langle \pi \rangle \times \mu_n \times (\mathbb{Z}_p)^N$, where π is a uniformizer for $k_{\mathfrak{p}}$, $p = \text{char}(\bar{k}_{\mathfrak{p}})$, \mathbb{Z}_p is the ring of p -adic integers, and $N = [k_{\mathfrak{p}} : \mathbb{Q}_p]$ ([S], Ch. XIV, §4, Prop.10). Let g_1, \dots, g_{N+2} be (topological) generators of the respective direct summands. Define a map $\psi : k_{\mathfrak{p}}^{\bullet} \rightarrow \frac{1}{\ell m}\mathbb{Z}/\mathbb{Z}$ via $\psi(g_i) = \frac{1}{\ell}\chi(g_i)$ if $i \neq 2$, and $\psi(g_2) = \psi(\zeta_n) = \frac{1}{(\ell, n)}\chi(\zeta_n')$, where ζ_n' is a $\frac{\ell}{(\ell, n)}$ th root of ζ_n (note $\langle \zeta_n' \rangle = \langle \zeta_n \rangle$). *Claim:* This is a surjective homomorphism. The lemma follows at once, since clearly ψ is continuous, and $\ell\psi = \chi$. Surjectivity is immediate, since for some i , $\chi(\langle g_i \rangle) = \frac{1}{m}\mathbb{Z}/\mathbb{Z}$. It remains to prove ψ is a homomorphism on each summand. For all but the second summand, there is nothing to prove, since they are free. For the second summand, it suffices to check that the order of the group $\psi(\mu_n)$ divides the order n of the group μ_n . If $\mu_n \subseteq \ker(\chi)$, then by definition $\mu_n \subseteq \ker(\psi)$, and so $|\psi(\mu_n)| = 1$, which divides n . If $\mu_n \not\subseteq \ker(\chi)$, then by inspection $|\psi(\mu_n)| = (\ell, n) \cdot |\chi(\mu_n)|$. But by hypothesis, $\mu_{(\ell, n)} \subseteq \mu_z \subseteq \ker(\chi)$, and so $(\ell, n) \cdot |\chi(\mu_n)|$ divides $|\ker(\chi|_{\mu_n})| |\chi(\mu_n)| = n$. Therefore $|\psi(\mu_n)|$ divides n . This proves the claim, and hence the lemma. \square

Continue proof of Lemma 3.1. By Lemma 3.2, a character $\chi_{\mathfrak{p}}$ of order 2 extends to a character $\psi_{\mathfrak{p}}$ of any order $m_{\mathfrak{p}}$ divisible by 2 if and only if $\mu_z \subseteq \ker(\chi_{\mathfrak{p}})$, where $z = \frac{n(m_{\mathfrak{p}}/2, n)}{(m_{\mathfrak{p}}, n)}$. Let v_2 denote the additive 2-adic valuation on \mathbb{Z} . It is easy to check that $v_2(z) = v_2(n) - 1$ if $v_2(n) \geq v_2(m_{\mathfrak{p}})$, and $v_2(z) = v_2(n)$ if $v_2(n) < v_2(m_{\mathfrak{p}})$. Since $|\chi_{\mathfrak{p}}| = 2$, already $\mu_{z/2} \subseteq \ker(\chi_{\mathfrak{p}})$, and so $\mu_z \subseteq \ker(\chi_{\mathfrak{p}})$

if and only if $\chi_{\mathfrak{p}}(\zeta_{2v_2(z)}) = 0$. In the Special Case, $v_2(n) = 1$. If in addition $m_{\mathfrak{p}}$ is divisible by 2^{s+1} , then $2 < s + 1 \leq v_2(m_{\mathfrak{p}})$. Then $v_2(z) = v_2(n) = 1$, and so $\mu_z \subseteq \ker(\chi_{\mathfrak{p}}) \Leftrightarrow \chi_{\mathfrak{p}}(-1) = 0$.

Suppose that k has a Special Case. It has been shown that for every $\mathfrak{p} \in S_0$, the set of characters $\psi_{\mathfrak{p}}$ of order $m_{\mathfrak{p}}$ such that $\psi_{\mathfrak{p}}(\eta_{s+1}^{m_{\mathfrak{p}}}) \neq 0$ is the set of extensions of order $m_{\mathfrak{p}}$ of the set of characters $\chi_{\mathfrak{p}}$ of order 2 such that $\chi_{\mathfrak{p}}(\eta_s + 2) \neq 0$. Furthermore, it has been shown that there exist such $\psi_{\mathfrak{p}}$ extending $\chi_{\mathfrak{p}}$ if and only if $\chi_{\mathfrak{p}}(-1) = 0$. To finish the proof, it remains to produce for some $\mathfrak{p} \in S_0$ a character $\chi_{\mathfrak{p}}$ of order 2, such that $\chi_{\mathfrak{p}}(-1) = 0$ and $\chi_{\mathfrak{p}}(\eta_s + 2) \neq 0$.

For $i = 1, \dots, N+2$, let $G_i \subset k_{\mathfrak{p}}^{\bullet}$ be the open (and closed) subgroup $\langle g_i^2, g_j \mid j \neq i \rangle$ of index 2 (notation as in the proof of Lemma 3.2). Recall that g_2 generates the group of roots of unity in $k_{\mathfrak{p}}^{\bullet}$. Since this is the Special Case, $-1, \eta_s + 2$, and $-(\eta_s + 2)$ are all non-squares in $k_{\mathfrak{p}}^{\bullet}$. Hence none of these elements are contained in every G_i ; indeed then they would be contained in the intersection subgroup $\langle g_1^2, \dots, g_{N+2}^2 \rangle = k_{\mathfrak{p}}^{\bullet 2}$. If $i \neq 2$, then $-1 \in G_i$, since $-1 \in k_{\mathfrak{p}}^{\bullet}$, and $-1 \notin G_2$, since -1 is not a square. If $\eta_s + 2$ is not contained in some $G_i, i \neq 2$, then this G_i defines the character via the natural projection, done. If $\eta_s + 2 \in G_i$ for all $i \neq 2$, then $\eta_s + 2 \notin G_2$, since $\eta_s + 2$ is not a square. Since the index of each G_i in $k_{\mathfrak{p}}^{\bullet}$ is 2, this implies that $-(\eta_s + 2) \in G_i$ for all i . This is a contradiction, since $-(\eta_s + 2)$ is not a square. This completes the proof. \square

Remarks 3.2.1. (i) If there is a Wang counterexample for k , then Lemma 3.1 shows that there is one such that $\text{lcm}\{m_{\mathfrak{q}}\} = 2^{s+1}$.

(ii) If $k = \mathbb{Q}$, then $s = 2$, and $\eta_s + 2 = 2$. It is well known that for the character χ_2 corresponding to either the unramified quadratic extension $\mathbb{Q}_2(\sqrt{-3})$ or the totally ramified extension $\mathbb{Q}_2(\sqrt{6})$, $\chi_2(-1) = 0$ and $\chi_2(2) \neq 0$. Thus any cyclic extension of \mathbb{Q}_2 of degree divisible by $2^{s+1} = 8$ that contains either of these quadratic extensions gives a Wang counterexample.

Lemma 3.3. *Let k be a number field and let $p \neq \text{char}(k)$ be a prime of \mathbb{Q} . Let r and s be maximal such that $\mu_{p^r} \subset k^{\bullet}$ and $\mu_{p^s} \subset k(\zeta_{p^{r+1}})^{\bullet}$. Then*

$$k(\zeta_{p^{N+1}})/k(\zeta_{p^N}) \text{ is nontrivial} \iff N \in \{r\} \cup [s, \infty) \subseteq \mathbb{N}.$$

Proof. Exercise. \square

4. WANG COUNTEREXAMPLES LEAD TO NONCROSSED PRODUCTS

A type II noncrossed product satisfies condition (I) of Theorem 2.1, i.e., there exists a group G of order $\text{ind}(D)$ such that for each prime \mathfrak{q} of k there exists a Galois extension $M_{\mathfrak{q}}/K_{\mathfrak{q}}/k_{\mathfrak{q}}$ of degree divisible by $\text{ind}(A_{\mathfrak{q}})$ with Galois group $G_{\mathfrak{q}}$ a subgroup of G , and such that there is a normal subgroup $N \subseteq G$ of index $|\chi|$ such that $N \cap G_{\mathfrak{q}} = \text{Gal}(M_{\mathfrak{q}}/K_{\mathfrak{q}})$ for each \mathfrak{q} . Condition (II) is *not* satisfied, so for any such G there are no G -Galois extensions $M/K/k$ with $N = \text{Gal}(M/K)$ and with completions the $M_{\mathfrak{q}}$.

Wang’s counterexamples will provide this final obstruction. Consequently, these type II examples only exist over number fields with nonempty Special Case.

Theorem 4.1. *Let k be a number field that has a nonempty Special Case, and let $F = k(t)$ or $k((t))$. Let s be maximal such that $\mu_{2^s} \subset k(i)^{\bullet}$. Then there exist noncrossed product F -division algebras of type II, of all indexes divisible by 2^{s+2} .*

Proof. Fix a number $2^a m$ where m is odd and $a \geq s + 2$. As usual, let S_0 be the (nonempty) set of primes of k for which $k_{\mathfrak{p}}(\zeta_{2^{s+1}})/k_{\mathfrak{p}}$ is noncyclic.

Since k has a Special Case, by Lemma 3.1 there is a prime $\mathfrak{q}_0 \in S_0$ and a character $\chi_{\mathfrak{q}_0}$ of $k_{\mathfrak{q}_0}^\bullet$ of order 2 such that $\chi_{\mathfrak{q}_0}(\eta_s + 2) \neq 0$ and $\chi_{\mathfrak{q}_0}(-1) = 0$. For every $\mathfrak{p} \neq \mathfrak{q}_0$ of S_0 , let $\chi_{\mathfrak{p}}$ be the trivial character. By Cebotarev’s Density Theorem and Lemma 3.3, there exist primes $\mathfrak{q}_1, \mathfrak{q}_2$, and \mathfrak{q}_3 not in S_0 and not dividing $2m$ such that

- \mathfrak{q}_1 splits completely in $k(\zeta_{2^a m})$;
- \mathfrak{q}_2 does not split completely in $k(\zeta_{2^2})$;
- \mathfrak{q}_3 splits completely in $k(\zeta_{2^{a-1}})$ but not in $k(\zeta_{2^a})$.

Let A be the k -division algebra whose nontrivial invariants are

$$\text{inv}_{\mathfrak{q}_0}(A) = \text{inv}_{\mathfrak{q}_1}(A) = -\text{inv}_{\mathfrak{q}_2}(A) = -\text{inv}_{\mathfrak{q}_3}(A) = \frac{1}{2^a m}.$$

Let $\chi_{\mathfrak{q}_0}$ and $\{\chi_{\mathfrak{p}} \mid \mathfrak{p} \in S_0 \setminus \{\mathfrak{q}_0\}\}$ be as above, and let $\chi_{\mathfrak{q}_1}, \chi_{\mathfrak{q}_2}$, and $\chi_{\mathfrak{q}_3}$ be unramified, unramified, and totally ramified characters of each $k_{\mathfrak{q}_i}^\bullet$, of order 2. By Grunwald-Wang’s Theorem, there exists a global character χ of order 2 with all of the above characters as completions. Let X be the F -division algebra corresponding to χ in (1.0.1), and as usual, let K be the associated extension.

Let D be the division algebra $\Delta(A \otimes X)$. By direct computation, $\text{ind}(D) = |\chi| \text{ind}(A \otimes K) = 2^a m$.

First it will be shown that D satisfies condition (I). Here, that means finding a single group G of order $2^a m$ for Galois extensions $M_{\mathfrak{q}_i}/k_{\mathfrak{q}_i}$ ($i = 0, 1, 2, 3$) of degree $2^a m$ such that the $K_{\mathfrak{q}_i}$ are the fixed fields of a unique subgroup of G .

Since $\mu_{2^a m} \subset k_{\mathfrak{q}_1}^\bullet$, G must be abelian, by local class field theory (see [B2], Albert’s Theorem 1.3). Therefore, assume that $m = 1$: For $G \cong P \oplus Q$, where $|P| = 2^a$ and $|Q| = m$. The quotient $G/Q \cong P$ is the group for a Galois extension of degree 2^a that contains K , and has local degrees equal to 2^a at the primes \mathfrak{q}_i .

Since $\mu_2 \subset k_{\mathfrak{q}_2}^\bullet$ and $\mu_{2^2} \not\subset k_{\mathfrak{q}_2}^\bullet$, the largest totally ramified Galois 2-extension of $k_{\mathfrak{q}_2}$ has degree 2. Therefore, $G \cong c(2^a)$ or $c(2) \oplus c(2^{a-1})$. Similarly, since $\mu_{2^{a-1}} \subset k_{\mathfrak{q}_3}^\bullet$, but $\mu_{2^a} \not\subset k_{\mathfrak{q}_3}^\bullet$, the largest totally ramified Galois 2-extension of $k_{\mathfrak{q}_3}$ has degree 2^{a-1} . Since already $K_{\mathfrak{q}_3}$ is totally ramified, this means G cannot be cyclic, and so $G \cong c(2) \oplus c(2^{a-1})$.

Claim. At each \mathfrak{q}_i ($i = 0, 1, 2, 3$) there exists a G -Galois extension $M_{\mathfrak{q}_i}$ that contains $K_{\mathfrak{q}_i}$ and at \mathfrak{q}_2 , this extension necessarily contains $K_{\mathfrak{q}_2}$ in a cyclic subextension of degree 2^{a-1} . For at \mathfrak{q}_1 and \mathfrak{q}_2 , $K_{\mathfrak{q}_1}$ and $K_{\mathfrak{q}_2}$ are unramified and hence embed in the unique unramified extensions of degree 2^{a-1} . Moreover, since $\mu_{2^2} \not\subset k_{\mathfrak{q}_2}$, this is forced at \mathfrak{q}_2 . Since $\mu_{2^{a-1}} \subset k_{\mathfrak{q}_3}^\bullet$, $K_{\mathfrak{q}_3}$ embeds in a totally ramified cyclic extension of degree 2^{a-1} . Since $\chi_{\mathfrak{q}_0}(-1) = 0$, $K_{\mathfrak{q}_0}$ embeds in a cyclic extension of degree 2^{a-1} by Lemma 3.1. Thus each $K_{\mathfrak{q}_i}$ is embedded in a cyclic extension, as desired. By composing this cyclic extension with any quadratic extension disjoint from $K_{\mathfrak{q}_i}$, a Galois extension $M_{\mathfrak{q}_i}$ with group $G \cong c(2) \oplus c(2^{a-1})$ is constructed, proving the claim. Clearly, the normal subgroups of each $G_{\mathfrak{q}_i}$ fixing each $K_{\mathfrak{q}_i}$ may be identified in G . Thus G satisfies condition (I), and no other group does.

To finish, it is enough to show that this noncyclic G cannot satisfy condition (II), i.e., that there is no G -Galois extension $M/K/k$ of degree 2^a with full degree at the \mathfrak{q}_i . By the proof of the claim above, any such M must contain K in a cyclic subextension of degree 2^{a-1} .

Let $\{\psi_{\mathfrak{p}} \mid \mathfrak{p} \in S_0\}$ be any set of local characters of order $m_{\mathfrak{p}}$ that extend the characters $\{\chi_{\mathfrak{p}}\}$ above (including $\chi_{\mathfrak{q}_0}$) by a fixed amount, such that $m_{\mathfrak{q}_0}$ is divisible by 2^{s+1} . If $\mathfrak{p} \neq \mathfrak{q}_0$, then since $\chi_{\mathfrak{p}}$ is trivial, $|\chi_{\mathfrak{q}_0}| |\psi_{\mathfrak{p}}| = 2m_{\mathfrak{p}}$ divides $m_{\mathfrak{q}_0}$. Consequently, $m_{\mathfrak{p}} \mid m_{\mathfrak{q}_0}/2$, and $\frac{m_{\mathfrak{q}_0}}{2} \cdot \psi_{\mathfrak{p}}$ is trivial. By Lemma 3.1, $\psi_{\mathfrak{q}_0}(\eta_{s+1}^{m_{\mathfrak{q}_0}}) = \chi_{\mathfrak{q}_0}(\eta_s + 2) \neq 0$. By Remark 1.2.2(iii), $\psi_{\mathfrak{p}}(\eta_{s+1}^m) = \frac{m}{2} \cdot \psi_{\mathfrak{p}}(\eta_s + 2)$. Therefore if $m = \text{lcm}\{m_{\mathfrak{p}}\} \equiv m_{\mathfrak{q}_0}$,

$$\sum_{\mathfrak{p} \in S_0} \psi_{\mathfrak{p}}(\eta_{s+1}^m) = \sum_{\mathfrak{p} \in S_0} \left(\frac{m_{\mathfrak{q}_0}}{2} \cdot \psi_{\mathfrak{p}}\right)(\eta_s + 2) = \chi_{\mathfrak{q}_0}(\eta_s + 2) \neq 0.$$

Thus the set $\{\psi_{\mathfrak{p}}\}$ gives a Wang counterexample. This means that *any* cyclic extension Z/k that contains K and whose completion at \mathfrak{q}_0 has degree divisible by 2^{a-1} ($a \geq s + 2$) must have degree $[Z : k]$ divisible by 2^a .

Since M must have full degree at \mathfrak{q}_0 and must contain K in a cyclic subextension of degree 2^{a-1} , M must have a cyclic subextension of degree 2^a . This is a contradiction, since M is noncyclic of degree 2^a . Conclude that condition (II) cannot be satisfied, and therefore D is a noncrossed product of type II. \square

Remark 4.1.1. If $k = \mathbb{Q}$, then $s = 2$. Therefore the lowest index achieved for these type II noncrossed products is $2^4 = 16$.

REFERENCES

- [A] Amitsur, S.A.: On central division algebras. *Israel J. Math.* **12** (1972), 408-422. MR **47**:6763
- [AT] Artin, E., Tate, J.: *Class Field Theory*, Addison-Wesley, Reading, Mass., 1967. MR **91b**:11129
- [B] Brussel, E.: Noncrossed products and nonabelian crossed products over $\mathbb{Q}(t)$ and $\mathbb{Q}((t))$. *Amer. Jour. Math.* **117** (1995), 377-393. MR **96a**:16014
- [B2] Brussel, E.: Division algebras not embeddable in crossed products. *Jour. Alg.* **179** (1996), 631-655. CMP 96:06
- [N] Neukirch, J.: On solvable number fields. *Invent. Math.* **53** (1979), 135-164. MR **81e**:12009
- [P] Pierce, R. S.: *Associative Algebras*, Springer-Verlag, New York, 1982. MR **84c**:16001
- [R] Reiner, I.: *Maximal Orders*, Academic Press, London, 1975. MR **52**:13910
- [S] Serre, J.-P.: *Local Fields*, Springer-Verlag, New York, 1979. MR **82e**:12016
- [W] Wang, S.: On Grunwald's theorem. *Ann. of Math. (2)* **51** (1950), 471-484. MR **11**:489h

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MASSACHUSETTS 02143
E-mail address: `brussel@math.harvard.edu`