Indecomposable Division Algebras with a Baer Ordering

Patrick J. Morandi*
Department of Mathematical Sciences
New Mexico State University
Las Cruces, NM 88003
email: pmorandi@nmsu.edu

B. A. Sethuraman†
Department of Mathematics
California State University
Northridge, Northridge, CA 91330
email: asethuraman@vax.csun.edu

Abstract

In this paper we construct Baer ordered indecomposable division algebras of index p^n and exponent p^m for all primes p and for all n, m, with $n > m \geq 1$ ($n \geq 3$ if $p = 2$).

1 Introduction

This paper is a sequel to [MS]. In that paper we constructed Baer ordered noncrossed product division algebras of index p^n and exponent p^m for all primes p, and for all n, m with $n \geq m \geq 3$. In this paper we construct Baer ordered indecomposable division algebras of index p^n and exponent p^m for all primes p, and for all n, m satisfying $n > m \geq 1$ ($n \geq 3$ if $p = 2$). In particular, we obtain Baer ordered indecomposable division algebras of prime exponent,

and indecomposable division algebras that are Baer ordered with respect to an involution of the first kind.

The method we use to produce indecomposable division algebras is that developed in [JW]; that is, our examples will be the underlying division algebra of a tensor product of suitably chosen symbol algebras over a field $F = L_1 \cap \cdots \cap L_k$, where the L_i are p-Henselian fields. The key ingredients of our examples are indecomposable division algebras of exponent p (and of exponent 4) with suitable centers. For odd p, we use the algebras constructed in [J_2], for $p = 2$ and exponent 2 we use a generic elementary abelian crossed product of exponent 2, while for exponent 4, we use the algebras constructed in [Se]. We then combine these algebras with a tensor product of suitably chosen symbol algebras to produce our Baer ordered examples.

This paper is organized as follows. The remainder of this section gives some basic information on Baer orderings. In section two we obtain indecomposable division algebras with involution of prime exponent (and exponent 4), that satisfy certain properties. The main examples of this paper are constructed in section three. Finally, in an appendix, we describe the construction of a generic crossed product of prime index which is used in section two. We wish to thank David Saltman for a number of useful conversations about generic crossed products.

If D is either a field or a division ring equipped with an involution $*$ (an anti-automorphism of order 2), recall that a Baer ordering on D is a subset P of the set of symmetric elements of D under $*$ such that (1) $P + P \subseteq P$, (2) P contains 1 but not 0, (3) $dPd^* \subseteq P$ for every $d \in D - \{0\}$, and (4) if $d \neq 0$ is a symmetric element of D then either $d \in P$ or $-d \in P$. These orderings were first defined by Baer [Ba], and later studied by Holland and others (cf. [H], [C])

The method we will use to obtain Baer orderings on a division algebra D with involution is to construct a totally ramified valuation on D, and then lift a standard ordering on the symmetric subfield of $\overline{D}$. We recall the "lifting criterion" from [H], which allows us to do this. If D is a division ring with an

involution $*$, then a valuation v on D is said to be a $*$–*valuation* if $v(d^*) = v(d)$ for all $d \in D^\times = D - \{0\}$. That is, v is a $*$–valuation if $v \circ * = v$. If $\overline{D}$ is the residue division ring of D relative to a $*$–valuation, then $\overline{D}$ has an involution induced from $*$, which we will also denote by $*$, defined by $\overline{u}^* = \overline{u^*}$.

Let d be either a symmetric or a skew-symmetric element of $D^\times$. Then $d^* d^{-1} \in Z(D)$, the center of D, and it is easy to check that the map $x \mapsto d x^* d^{-1}$ is also an involution of D, and induces an involution on $\overline{D}$. Let c_d be the automorphism on $\overline{D}$ induced by conjugation by d. The element d is said to be *smooth* if the residue involution $c_d \circ *$ is equal to $\varphi \circ * \circ \varphi^{-1}$ for some automorphism φ of $\overline{D}$.

Now suppose that v is a $*$–valuation on D with $v(2) = 0$, that is, $\mathrm{char}(\overline{D}) \neq 2$. It can be seen that for every $\gamma \in \Gamma_D$, the value group of D, $v^{-1}(\gamma)$ either contains a symmetric or skew-symmetric element (see [H, §3]). A $*$–valuation v on D is said to be *smooth* if (1) $v(2) = 0$, and (2) for every $\gamma \in \Gamma_D$, if $v^{-1}(\gamma)$ contains a smooth element then it contains a smooth symmetric element, else $v^{-1}(\gamma)$ contains a smooth skew-symmetric element.

The following was proved by Holland.

Proposition 1 (H, Cor. 3.3). *If D is a division ring with involution $*$, and if v is a smooth $*$–valuation on D, then every Baer ordering on $\overline{D}$ defined with respect to the residue involution $*$ on $\overline{D}$ lifts to a Baer ordering on D with respect to $*$.*

In particular, suppose D is totally ramified with respect to a $*$–valuation v over $F = Z(D)$, such that the residue involution $*$ is nontrivial on $\overline{F}$. Then $\overline{D} = \overline{F}$, so $c_d = \mathrm{id}$ for every $d \in D^\times$. Therefore the valuation v is smooth. Let $\mathcal{K}$ be the symmetric subfield of $\overline{F}$ with respect to $*$, so $\overline{F} = \mathcal{K}(\sqrt{a})$ for some $a \in \mathcal{K}$. Suppose P is a (standard) ordering on $\mathcal{K}$, and suppose $a < 0$ with respect to P. If $x = \alpha + \beta\sqrt{a} \in F$, then $xx^* = \alpha^2 - \beta^2 a > 0$, hence property (3) of the definition of a Baer ordering is satisfied for P. The other properties of a Baer ordering are trivial to check, so P is a Baer ordering of $\overline{D}$. Thus, by Holland's theorem, P lifts to a Baer ordering on D. Similarly, if the residue

involution $*$ is trivial on $\overline{F}$, then since any standard ordering P on $\overline{F}$ is also a Baer ordering on $\overline{F}$, Holland's theorem shows that P lifts to a Baer ordering on D.

2 Indecomposable division algebras with involution

In this chapter we will use indecomposable division algebras constructed in [J$_2$] and [Se] along with generic G–crossed product division algebras to obtain indecomposable division algebras with involution, both of the first kind and of the second kind, with appropriate maximal subfields. The following theorem is the main result of this section.

Theorem 2. *Let p be a prime and $n \geq 2$ an integer. Then there exists an indecomposable division algebra D_0 of index p^n and exponent p (or exponent 4 if $p = 2$) with involution $*$ of the second kind, with the additional properties: 1) If K_0 is the symmetric subfield of the center F_0, then $F_0 = K_0(\omega)$ where ω is a primitive p-th root of unity (for p odd) and $F_0 = K_0(\sqrt{-1})$ for $(p = 2)$, 2) D_0 has an abelian Galois maximal subfield M/F_0 of the form $M = F_0\left(\sqrt[p^{r_1}]{a_1}, \ldots, \sqrt[p^{r_t}]{a_t}\right)$ with each $a_i \in K_0$ and such that $K_0\left(\sqrt[p^{r_1}]{a_1}, \ldots, \sqrt[p^{r_t}]{a_t}\right)$ is formally real. Also, there exists an indecomposable division algebra of index 2^n $(n \geq 3)$ and exponent 2 which has a formally real elementary abelian Galois maximal subfield.*

We will give a proof of this theorem in three separate propositions. The reason for breaking the proof up is that we need to consider three different constructions depending on whether the prime p is odd or even, and for $p = 2$, whether the exponent is 2 or 4. We use the algebras of [Se] for the case of exponent 4, and a generic elementary abelian crossed product for exponent 2.

We first handle the case of exponent 4.

Proposition 3. *If $n \geq 2$ then there exists an indecomposable division algebra D_0 of index 2^n and exponent 4 satisfying the statement of Theorem 2.*

Proof. In [Se], indecomposable division algebras of index p^n and exponent p^m are constructed for all primes p, and for all n, m, with $n \geq m \geq 2$. We recall enough details of the construction for $m = p = 2$ for our purposes. Let $k = \mathbb{Q}(\{\omega_r \mid r \geq 1\})$, where ω_r is a primitive 2^r–th root of unity, chosen so that $\omega_{r+1}^2 = \omega_r$. Then $k/\mathbb{Q}$ is Galois, hence complex conjugation restricted to k is an automorphism σ of order 2 on k. Let $k_0 = k^\sigma$, the fixed field of σ. Then $k_0 = k \cap \mathbb{R}$ is a formally real quadratic subfield of k, and $k = k_0(\sqrt{-1})$. Let $F_0 = k(x_0, x_1, \ldots, x_{n-2}, y)$ and $K_0 = k_0(x_0, x_1, \ldots, x_{n-2}, y)$, so $F_0 = K_0(\sqrt{-1})$. There is a unique extension of σ to F_0 such that $\sigma|_{K_0} = \mathrm{id}$. Let E be the tensor product of symbol algebras

$$E = (x_0, x_0^{2^{n-2}} - y; 2, F_0, -1) \otimes_{F_0} (x_1, x_1^{2^{n-1}} - y; 2, F_0, -1) \otimes_{F_0}$$

$$\cdots \otimes_{F_0} (x_{n-3}, x_{n-3}^2 - y; 2, F_0, -1) \otimes_{F_0} (x_{n-2}, x_{n-2} - y; 2, F_0, -1).$$

Then by [Se, Prop. 2], E is a division algebra of index 2^{n-1} and exponent 2, and is isomorphic to the symbol algebra $(y, a; 2^{n-1}, F_0, \omega_{n-1})$ for a suitable $a \in F_0$. Moreover, the description of a given in [Se] shows that $a \in K_0$. Let $D_0 = (y, a; 2^n, F_0, \omega_n)$. Then D_0 is an indecomposable division algebra of index 2^n and exponent 4, by [Se, Thm]. Since $a \in K_0$ and σ sends $\sqrt{-1}$ to its inverse, the proof of [MS, Lemma 6] shows that there is an involution on D_0 extending σ on F_0. The algebra D_0 has $F_0\left(\sqrt[2^n]{y}\right)$ as a splitting field. $F_0\left(\sqrt[2^n]{y}\right)$ contains the quadratic subfield $K_0\left(\sqrt[2^n]{y}\right)$, which is purely transcendental over k_0, and is hence formally real. Thus D_0 has all the desired properties. ∎

We next consider the case of index p^n and exponent p for p odd and $n \geq 2$.

Proposition 4. *If p is an odd prime and $n \geq 2$, then there is an indecomposable division algebra D_0 satisfying the statement of Theorem 2.*

Proof. In [J$_2$], Jacob constructs for each n an indecomposable division algebra of index p^n and exponent p. We will modify his base fields to obtain the extra properties we need.

Let $\mathcal{F}_0 = \mathbb{Z}_p(t)$ and $\mathcal{F} = \mathcal{F}_0(\tau_1, \ldots, \tau_{n-1})$, where $t, \tau_1, \ldots, \tau_{n-1}$ are variables. Let $a_1, \ldots, a_{n-1} \in \mathcal{F}_0$ be chosen so that $1 + t, a_1, \ldots, a_{n-1}$ are linearly independent in $\mathcal{F}_0^* / \mathcal{F}_0^{*p}$. Let $N = \mathbb{Q}(\{\omega_s \mid s \geq 1\})(t, \tau_1, \ldots, \tau_{n-1})$, where ω_s is a primitive p^s-th root of unity, and where we have abused notation and used the symbols $t, \tau_0, \ldots, \tau_{n-1}$ again. (We will write ω for ω_1 for convenience.) Let σ be the automorphism of N that sends each τ_i to itself, sends t to t, and acts as complex conjugation on $\mathbb{Q}(\{\omega_s \mid s \geq 1\})$. Then the fixed field N^σ is formally real, and $N = N^\sigma(\omega)$. If v is the p-adic valuation on $\mathbb{Q}$, then v extends uniquely to a totally ramified valuation on $\mathbb{Q}(\{\omega_s \mid s \geq 1\})$ so that the value group is $\frac{1}{p-1}\mathbb{Z}[1/p]$, a p-divisible group. If we extend v to N by setting $v(t) = v(\tau_1) = \cdots = v(\tau_{n-1}) = 0$ and requiring that the residues of $t, \tau_0, \ldots, \tau_{n-1}$ be the corresponding quantities in $\mathcal{F}$ (see [Bo, §10, Prop. 2]), we obtain a valuation on N whose residue field is $\mathcal{F}$. Furthermore, v restricts to a valuation on N^σ, whose residue field is also $\mathcal{F}$.

Let $N(p)$ be the p-closure of N (see [JW, §1]), and fix an extension of v to $N(p)$. Note that $N(p)$ is Galois over N^σ. Let E be the decomposition field of $N(p)/N^\sigma$. Then $N' := NE$ is the decomposition field of $N(p)/N$, hence N' is the p-Henselization of (N, v) (see [JW, §1] and [E, 15.6]). The extension N'/E is of degree 2, and from this, as well as the fact that N'/N is a compositum of finite extensions of degree a power of p, it is not hard to see that E/N^σ is also a compositum of finite extensions of degree a power of p. Since p is odd, E is formally real. Let R be a real closure of E in the algebraic closure C of N, and let σ' be the non-identity automorphism of C/R. Then $\sigma'|_N = \sigma$. For simplicity, we will write σ for σ'. Note that σ sends N' to itself, and that $N' = E(\omega)$. Also note that with respect to v we have $\overline{N'} = \overline{E} = \mathcal{F}$.

Let I be the underlying division algebra of $\bigotimes_{i=1}^{n-1}(a_i, \tau_i; p, N', \omega)$, where (abusing notation again) the a_i are lifts in E (note) of the corresponding elements of $\mathcal{F}$. The following lemma shows that the argument of [J$_2$, Thm. 2.2] carries over to our p-Henselian field N', and we find that I is split by $N'\left(\sqrt[p]{t_0}, \sqrt[p]{t_1}, \ldots, \sqrt[p]{t_{n-1}}\right)$, where $t_i = 1 + \tau_i$ for $i \geq 1$ and $t_0 = 1 + t$.

Lemma 5. *Let p be an odd prime, and let (F, v) be a p-Henselian field, containing a primitive p-th root of unity ω. Assume that $\operatorname{char}(\overline{F}) = p$. Then $1 - p^2 h \in F^{*p}$ for all $h \in F$ with $v(h) \geq 0$.*

Proof. Let $f(x) = x^p - (1 + p^2 h)$. Let $\pi = 1 - \omega$, so $v(\pi^{p-1}) = v(p)$. (This is well known, see [T, Lemma 1.3], for instance.) Let $g(x) = 1/\pi^p \cdot f(\pi x + 1)$. Then g is a monic polynomial in $V[x]$, where V is the valuation ring of F, with residue $\overline{g}(x) = x^p + \overline{u}x$ for $u = p/\pi^{p-1}$. It is clear that f splits over F (resp. has a root in F) iff g splits over F (resp. has a root in F). Now, since the splitting field of f over F is $F(\alpha)$ with $\alpha^p = 1 + p^2 h$, we see that the splitting field either has degree 1 or p over F, depending on whether $\alpha \in F$ or not. Therefore f either splits over F or is irreducible over F. Thus the same is true for g. Suppose g is irreducible over F. Since v extends uniquely to the p-closure $F(p)$, [E, 16.3] shows that $\overline{g}$ is a power of an irreducible polynomial. However, $\overline{g}(x) = x(x^{p-1} + \overline{u})$, which is not a power of an irreducible since $\overline{u} \neq 0$. Thus g is not irreducible, hence g splits over F. Thus f also splits over F, so $1 + p^2 h$ has a p–th root in F. ∎

The key result about I we need is Corollary 2.4 of $[J_2, \S 2]$. For the proof of this result to hold in our situation, we require that there be a well defined group homomorphism $Br_p(N') \to k_2(\mathcal{F})$, induced by $l(x) \otimes l(y) \to l(\overline{x}) \otimes l(\overline{y})$ for units $x, y \in N'$ (see $[J_1, \text{Lemma } 2.1]$ and $[J_2, \text{Lemma } 2.1]$ for more details). The existence and well definition of this map requires the p–divisibility of the value group $\Gamma_{N'}$, but not the Henselian assumption. Therefore the appropriate calculations in $[J_1]$ and everything in $[J_2, \S 2]$ (in particular, Corollary 2.4) carry over to the field extension $N'\left(\sqrt[p]{t_0}, \sqrt[p]{t_1}, \ldots, \sqrt[p]{t_r}\right)/N'$.

Let K_0 be a Henselian valued field with residue field E, such that if Γ_{K_0} is the value group of K_0, then $\Gamma_{K_0}/p\Gamma_{K_0} = (\mathbb{Z}/p\mathbb{Z})^n$. Note that since K_0 is Henselian and E is formally real, K_0 is also formally real [L, Thm. 3.16]. Let F_0 be the inertial extension of K_0 whose residue field is N', so $F_0 = K_0(\omega)$. Let $\pi_0, \ldots, \pi_{n-1}$ be elements of K_0 whose values are linearly independent in $\Gamma_{K_0}/p\Gamma_{K_0}$, and (abusing notation yet another time) let t_i $(i = 1, \ldots, n)$ be

lifts in K_0 of the corresponding elements in E. Finally, let D_0 be the underlying division algebra of $\bigotimes_{i=0}^{n-1}(t_i, \pi_i; p, F_0; \omega) \otimes_{F_0} I$. The proof of [J$_2$, Thm. 3.3] carries over to show that D_0 is an indecomposable division algebra of index p^n and exponent p. Moreover, D_0 is similar to a tensor product of symbol algebras, each of whose slots come from the quadratic subfield K_0 of F_0. If σ is a lift to F_0 of the N'/E automorphism σ, then σ sends ω to its inverse, so the proof of [MS, Lemma 6] shows that D_0 has an involution $*$ which extends σ. Furthermore, D_0 is an elementary abelian crossed product with maximal subfield $F_0\left(\sqrt[p]{t_0}, \sqrt[p]{t_1}, \ldots, \sqrt[p]{t_{n-1}}\right)$, which contains the quadratic subfield $K_0\left(\sqrt[p]{t_0}, \sqrt[p]{t_1}, \ldots, \sqrt[p]{t_{n-1}}\right)$. Since K_0 is formally real and p is odd, $K_0\left(\sqrt[p]{t_0}, \sqrt[p]{t_1}, \ldots, \sqrt[p]{t_{n-1}}\right)$ is also formally real. Therefore, D_0 has the properties we require. $\blacksquare$

Finally, we consider the case of exponent 2. While Jacob constructs in [J$_2$] an indecomposable division algebra of index 2^n and exponent 2, it is not clear that his example can be modified to satisfy the properties that we need. We instead use a generic construction, and invoke Jacob's example to show that this generic algebra is indecomposable.

Proposition 6. *If $n \geq 3$, then there exists an indecomposable division algebra of index 2^n and exponent 2 satisfying the statement of Theorem 2.*

Proof. Let I be the indecomposable division algebra of index 2^n and exponent 2 constructed in [J$_2$], with the ground field chosen to contain $\mathbb{Q}(\omega_r \mid r \geq 1)$, where ω_r is a primitive 2^r–th root of unity. Then I is shown to be an elementary abelian crossed product with respect to the group $G = (\mathbb{Z}/2\mathbb{Z})^n$ (see the comments preceding [J$_2$, Thm. 3.3]). Let $D_G^{(p)}$ be the generic G–crossed product described in the appendix. By an argument similar to that of [Sa$_1$, Thm. 1.13], the indecomposability of I shows that $D_G^{(p)}$ is indecomposable. To see that this algebra has a formally real maximal subfield, we first note that $D_G^{(p)}$ is the crossed product $(k(Q)/k(Q)^G, G, c)$, where Q is a G–lattice (see the

8

appendix). Since $k(Q)/k$ is rational, if we take $k = \mathbb{Q}$, the field $k(Q)$ will be formally real, and since G is elementary abelian, $k(Q)$ will be a formally real elementary abelian Galois maximal subfield of $D_G^{(p)}$. ∎

The division algebras we construct in the next section will have an inertial valuation whose residue division algebra is of the form $D_0 \otimes_{F_0} L$ with L/F_0 purely transcendental. The following lemma will be of use.

Lemma 7. *Let (F, v) be a valued field and I an F–central division algebra with valuation extending v, such that I/F is inertial. Then I is indecomposable if $\overline{I}$ is indecomposable. In particular, if D is an indecomposable division algebra with center k, then $D \otimes_k k(x_1, \ldots, x_n)$ is also indecomposable.*

Proof. Suppose $I = I_1 \otimes_F I_2$. The valuation on I then restricts to the I_i, and we have $\overline{I_1} \otimes_{\overline{F}} \overline{I_2} \subseteq \overline{I}$ since each $\overline{I_i} \subseteq \overline{I}$, and $\overline{I_1}$ and $\overline{I_2}$ commute elementwise with each other. Since I/F is inertial we have $\Gamma_{I_1} = \Gamma_{I_2} = \Gamma_F$. By [M, Thm. 1], $\overline{I_1 \otimes_F I_2} = \overline{I_1} \otimes_{\overline{F}} \overline{I_2}$, so $\overline{I} = \overline{I_1} \otimes_{\overline{F}} \overline{I_2}$. Since $\overline{I}$ is indecomposable, this forces one of the $\overline{I_i}$ to be trivial, say $\overline{I_2} = \overline{F}$. Then $\overline{I_1} = \overline{I}$, so by the fundamental inequality ([Sc, p. 21]), $I_1 = I$. Therefore I is indecomposable. The final statement of the lemma follows from the fact that $D \otimes_k k(x_1, \ldots, x_n)$ is inertial over $k(x_1, \ldots, x_n)$ with respect to the $(x_1, \ldots, x_n)$–adic valuation. ∎

3   Indecomposable Baer ordered division algebras

In this section we construct indecomposable Baer ordered division algebras of index p^n and exponent p^m for all primes p, and integers n, m with $n > m \geq 1$ ($n \geq 3$ if $p = 2$). The idea of our construction is as follows. First, if D_0/F_0 is one of the indecomposable division algebras with involution of index p^n and exponent p (or 4) constructed in the previous section, we consider a suitable

purely transcendental extension F_1 of F. We consider three suitable valuations on F_1 (two if $p = 2$ and the exponent is 2), and let F be the intersection of the p–Henselizations of F_1 with respect to these valuations (alternatively, we could use the Henselizations instead of p–Henselizations). We define D as the underlying division algebra of $D \otimes_{F_0} T$, where T/F is a totally ramified algebra of index p^n and exponent p^m and with involution. The machinery of [JW] applies, and we find that D inherits properties from both D_0 and T. In particular, D is indecomposable, and is totally ramified with respect to a suitable valuation. The residue of D turns out to be a formally real field, and the ordering on the residue then lifts to a Baer ordering on D.

In addition to the noncrossed product examples of [JW] and the noncrossed product Baer ordered examples of [MS], this method of using the intersection of Henselian valued fields was used to produce c-ordered division algebras which do not decompose into tensor products of quaternion algebras [CW, §4].

Because our argument for exponent 2 is slightly different from that for other exponents, we break our argument into two parts. We first consider the case of exponent different from 2. (Thus, $m \geq 2$ if $p = 2$.) Let D_0 be the indecomposable division algebra of index p^n and exponent p (exponent 4 if $p = 2$) that we constructed in the proof of Theorem 2, and let F_0, K_0, and $M = K_0 \left(\sqrt[p^{r_1}]{a_1}, \ldots, \sqrt[p^{r_t}]{a_t} \right)$ be as in that theorem. Let σ be the nonidentity automorphism of F_0/K_0.

Let $F_1 = F_0(x_1, y_1, \ldots, x_r, y_r, z)$ $(r = n - m + 1)$. Extend σ to F_1 by setting $\sigma(x_r) = y_r$, $\sigma(y_r) = x_r$, and letting σ fix all other variables. Let $K_1 = F_1^\sigma$. Note that $K_1 = K_0(x_1, y_1, \ldots, x_{r-1}, y_{r-1}, x_r + y_r, \omega(x_r - y_r), z)$, and $F_1 = K_1(\omega)$, where ω is a primitive p–th root of unity. (For $p = 2$, $K_1 = K_0(x_1, y_1, \ldots, x_{r-1}, y_{r-1}, x_r + y_r, \sqrt{-1}(x_r - y_r), z)$, and $F_1 = K_1(\sqrt{-1})$.) Let v_1 be the z–adic valuation on F_1, and v_2 the $(x_1, \ldots, y_r)$–adic valuation on F_1. We will fix an extension of v_1 and v_2 to the algebraic closure C of F_1, and continue to use v_1 and v_2 for these extensions. Note that $x_r y_r \in K_1$, and with respect to v_1, $E' = \overline{K_1} \left(\sqrt[p^{r_1}]{a_1}, \ldots, \sqrt[p^{r_t}]{a_t}, \sqrt[p^m]{x_1}, \sqrt[p]{x_2}, \ldots, \sqrt[p]{x_r y_r} \right)$ is formally real, as E' is a purely transcendental extension of $M = K_0 \left(\sqrt[p^{r_1}]{a_1}, \ldots, \sqrt[p^{r_t}]{a_t} \right)$.

Let E be an inertial lift of E' over the Henselization K_{1h} of K_1. (So E contains $\sqrt[p^{r_1}]{a_1}, \ldots, \sqrt[p^{r_t}]{a_t}$ as well as $\sqrt[p^m]{x_1}, \sqrt[p]{x_2}, \ldots, \sqrt[p]{x_r y_r}$.) As E is Henselian and E' is ordered, there is an ordering P on E compatible with v_1 by [L, Thm. 3.16]. Let R be a real closure of (E, P). Since R is Henselian with respect to v_1, if σ' is the nonidentity automorphism of C/R, then $v_1 \circ \sigma' = v_1$. Note that $\sigma'|_F = \sigma$. We will write σ in place of σ' for simplicity.

Let L_1 be a p–Henselization of (F_1, v_1) in C. Then $\sigma(L_1) = L_1$ by [E, 15.6]. Let L_2 be a p–Henselization of (F_1, v_2). Then $\sigma(L_2)$ is a p–Henselization of $(F_1, v_2 \circ \sigma)$. Let

$$L_1' = L_1 \left(\sqrt[p^m]{x_1}, \sqrt[p]{x_2}, \ldots, \sqrt[p]{x_r y_r} \right),$$

$$L_2' = L_2 \left(\sqrt[p^{r_1}]{a_1}, \ldots, \sqrt[p^{r_t}]{a_t} \right),$$

$$L_3' = \sigma(L_2').$$

Note that $\sigma(L_1') = L_1'$ and $\sigma(L_2') = \sigma(L_2) \left(\sqrt[p^m]{x_1}, \ldots, \sqrt[p]{x_r y_r} \right)$ as σ fixes $\sqrt[p^{r_1}]{a_1}, \ldots, \sqrt[p^{r_t}]{a_t}$ as well as $\sqrt[p^m]{x_1}, \sqrt[p]{x_2}, \ldots, \sqrt[p]{x_r y_r}$. Finally, set $F = L_1' \cap L_2' \cap L_3'$. This will be the center of our examples. We see that $\sigma(F) = F$. Let $K = F^\sigma$. The valuations v_1, v_2 and $v_2 \circ \sigma$ are pairwise independent on F_1 (see [MS, Lemma 3]), hence also on F since F/F_1 is algebraic. Thus the local–global principles of [JW] (see in particular Theorem 4.3, Remark 4.4(ii), Theorem 4.11, as well as the remark at the end of §4) hold for F and the L_i'.

Let $T = (x_1, y_1; p^m, F, \omega_m) \otimes_F (x_2, y_2; p, F, \omega) \otimes_F \cdots \otimes_F (x_r + y_r, x_r y_r; p, F, \omega)$. Let D be the underlying division algebra of $D_0 \otimes_{F_0} T$. We will show that D is our desired example.

Theorem 8. *Let D be as above. Then D is an indecomposable division algebra of index p^n and exponent p^m. Moreover, D has an involution $*$, and D contains a Baer ordering with respect to $*$.*

Proof. Since $x_1, \ldots, y_{r-1}$ as well as $x_r + y_r$ and $x_r y_r$ are fixed by σ, and since σ sends ω to ω^{-1} (σ sends $\sqrt{-1}$ to $1/\sqrt{-1}$ for $p = 2$), the proof of [MS, Lemma 6] shows that T has an involution $*_T$ that extends $\sigma|_F$. If $*_{D_0}$ is the involution on D_0 that extends $\sigma|_{F_0}$, then $*_{D_0} \otimes *_T$ is an involution on the central simple

11

algebra $D_0 \otimes_{F_0} T$. By Riehm's theorem ([D, p. 118]), there is an involution $*$ on D extending σ.

We use the local–global principles of [JW] to calculate the index and exponent of D. By construction of L_2' and L_3' we see $D \otimes_F L_2' \sim T \otimes_F L_2'$, and $D \otimes_F L_3' \sim T \otimes_F L_3'$ since both L_2' and L_3' split D_0. By [JW, Cor. 2.6], both $T \otimes_F L_2'$ and $T \otimes_F L_3'$ are division algebras of index p^n and exponent p^m, possessing a totally ramified valuation extending v_2 (resp. $v_2 \circ \sigma$). Moreover, since T is a crossed product of index p^n, the p–index of $T \otimes_F L_2'$ (resp. $T \otimes_F L_3'$) is p^n. Looking at L_1', we see that $D \otimes_F L_1' \sim D_0 \otimes_F L_1'$ since L_1' splits T. With respect to v_1, $D_0 \otimes_{F_0} L_1'$ is an inertial division ring with residue division ring $D_0 \otimes_{F_0} \overline{L_1'} = D_0 \otimes_{F_0} F_0 \left(\sqrt[p^m]{x_1}, \sqrt[p]{x_2}, \ldots, \sqrt[p]{x_r y_r}, y_1, \ldots, y_r \right)$. Thus the index of $D \otimes_F L_1'$ is p^n and its exponent is p (or 4 if $p = 2$). Furthermore, the p–index of $D \otimes_F L_1'$ is p^n since D_0 is a crossed product. Therefore by [JW, Thm. 4.11], D has index p^n. Since the index of D is at most p^m, and since $D \otimes_F L_2'$ has exponent p^m, we find that D also has exponent p^m. Now $\mathrm{ind}(D) = \mathrm{ind}(D_0 \otimes_F L_1')$, so $D \otimes_{F_0} L_1' = D_0 \otimes_{F_0} L_1'$. Since the algebra $D_0 \otimes_{F_0} L_1'$ is indecomposable by repeated applications of Lemma 7, D must also be indecomposable.

Finally, we construct a Baer ordering on D. As $\mathrm{ind}(D) = \mathrm{ind}(T \otimes_F L_2')$, we see that $D \otimes_F L_2' = T \otimes_F L_2'$. Hence $D \otimes_F L_2'$ is totally ramified with respect to v_2, with residue field $\overline{L_2'} = F_0(z) \left(\sqrt[p^{r_1}]{a_1}, \ldots, \sqrt[p^{r_t}]{a_t} \right)$. It follows easily that D is totally ramified with respect to $v_2|_D$, and that $\overline{D} = \overline{F} = F_0(z) \left(\sqrt[p^{r_1}]{a_1}, \ldots, \sqrt[p^{r_t}]{a_t} \right)$. This residue field contains the formally real quadratic subfield $H = K_0(z) \left(\sqrt[p^{r_1}]{a_1}, \ldots, \sqrt[p^{r_t}]{a_t} \right)$. Moreover, $\overline{D} = H(\sqrt{-3})$ ($\overline{D} = H(\sqrt{-1})$ if $p = 2$), and the induced involution $*$ on $\overline{D}$ is precisely the non–identity automorphism of $\overline{D}/H$. By the remarks at the end of §1, D has a Baer ordering with respect to $*$. ∎

We now consider the case of exponent 2. Let D_0 an indecomposable division algebra of index 2^n and exponent 2, with center F_0 a formally real field, such that $M = F_0 \left(\sqrt{a_1}, \ldots, \sqrt{a_n} \right)$ is a formally real maximal subfield of D_0. Let

$F_1 = F_0(x_1, y_1, \ldots, x_n, y_n, z)$. Let v_1 be the z–adic valuation on F_1 and v_2 the $(x_1, \ldots, y_n)$–adic valuation on F_1. Let L_i be a 2–Henselization of (F_1, v_i) in an algebraic closure of F_1 ($i = 1, 2$). Set $L_1' = L_1\left(\sqrt{x_1}, \ldots, \sqrt{x_n}\right)$ and $L_2' = L_2\left(\sqrt{a_1}, \ldots, \sqrt{a_n}\right)$. Finally, let $F = L_1' \cap L_2'$. If $T = \bigotimes_{i=1}^n (x_i, y_i; F, 2)$, let D be the underlying division algebra of $D_0 \otimes_{F_0} T$.

Theorem 9. *If D is the division algebra defined above, then D is an indecomposable division algebra of index 2^n and exponent 2, and if $*$ is any involution of the first kind on D, then there is a Baer ordering on D with respect to $*$.*

Proof. The proof of this theorem is very similar to the proof of Theorem 8, so we only provide a sketch. We see that $D \otimes_F L_1' \sim D_0 \otimes_{F_0} L_1'$ and $D \otimes_F L_2' \sim T \otimes_F L_2'$. Both of $D_0 \otimes_{F_0} L_1'$ and $T \otimes_{F_0} L_2'$ have index and 2–index 2^n, so D has index 2^n. Clearly the exponent of D is 2. Since $\mathrm{ind}(D) = \mathrm{ind}(T \otimes_F L_2')$, we see $D \otimes_F L_2' = T \otimes_F L_2'$, so with respect to the totally ramified valuation on $T \otimes_F L_2'$, there is a totally ramified valuation on D with residue field $\overline{L_2'} = M(z)$. Thus any ordering on the formally real field $M(z)$ lifts to a Baer ordering on D, with respect to any involution of the first kind on D. That D is indecomposable follows since $D \otimes_F L_1' = D_0 \otimes_{F_0} L_1'$, and this latter algebra is inertial with respect to v_1 with residue division ring $D_0 \otimes_{F_0} \overline{L_1'} = D_0 \otimes_{F_0} F_0\left(\sqrt{x_1}, \ldots, \sqrt{x_n}, y_1, \ldots, y_n\right)$, which is indecomposable by Lemma 7. Therefore, by applying Lemma 7 again, $D \otimes_F L_1'$ is indecomposable, and so D is also indecomposable. ∎

4 Appendix

In this appendix we describe the construction of a generic G-crossed product of prime exponent. Generic G-crossed products were introduced by Snider and Amitsur in [Sn] and [A$_1$] respectively. The description of generic G–crossed products we give below was suggested to us by Saltman.

Let G be a finite group, $\mathbb{Z}[G]$ the integral group ring of G, and I_G the augmentation ideal of $\mathbb{Z}[G]$. Let P be the free $\mathbb{Z}[G]$–module with basis d_σ for

$\sigma \in G - \{1\}$, and map P to I_G by sending d_σ to $\sigma - 1$. let M be the kernel. Thus we have the exact sequence of G–lattices

$$0 \to M \to P \to I_G \to 0.$$

Let $c(\sigma, \tau) = d_\sigma + \sigma d_\tau - d_{\sigma\tau}$. Then c represents a cocycle class in $H^2(G, M)$. If k is a field, let D_G be the crossed product algebra $D_G = \big(k(M)/k(M)^G, G, c\big)$. As stated in [Sa$_2$, p. 232] (see also [Sa$_2$, Lemma 2.3], as well as the remark after [Sa$_2$, Prop. 2.5]), the G–lattice M is generated by the $c(\sigma, \tau)$, the cocycle c has exponent $|G|$, and there is an embedding $H^2(G, M) \to H^2(G, k(M)^*)$. (In fact, the $c(\sigma, \tau)$ form a $\mathbb{Z}$ basis for M.) D_G is thus a division algebra of index and exponent $|G|$.

Let p be a prime dividing $n = |G|$, and let Q be the sub G–lattice of P generated by M and the $e_\sigma = pd_\sigma$, for $\sigma \in G - \{1\}$. Then $e_\sigma + \sigma(e_\tau) - e_{\sigma\tau} = pc(\sigma, \tau)$. It can be seen that Q is freely generated as an abelian group by the $c(\sigma, \tau)$ and the e_σ, and so it follows from [R$_2$, §4] that $k(Q)^G$ is the Brauer field $F_n(S)$, where S is the algebra $\big(k(M)/k(M)^G, G, c^p\big)$. Furthermore, the field $k(Q)^G$ is also the function field of the Brauer–Severi variety of S ([Ja, Thm. 4]), and is a purely transcendental extension the function field of the Brauer–Severi variety of the underlying division algebra of S. Hence by [SV, Thm. 1.6], as $S \sim D_G^{\otimes p}$, we have $\mathrm{ind}\big(D_G \otimes_{Z(D_G)} k(Q)^G\big) = \mathrm{ind}(D_G) = n$. For ease of notation we define $D_G^{(p)} = \big(D_G \otimes_{Z(D_G)} k(Q)^G\big)$. Then $D_G^{(p)}$ is the crossed product $\big(k(Q)/k(Q)^G, G, c\big)$. Since pc is a coboundary in $H^2(G, Q)$, $\exp(D_G^{(p)}) = p$. Say $D_G^{(p)} = \sum_\sigma k(Q)x_\sigma$, where the x_σ satisfy the usual multiplicative properties. Let $A = \sum_\sigma k[Q]x_\sigma$. We prove that $D_G^{(p)}$ is generic with respect to G–crossed product k–algebras of exponent p. The proof we give is similar to the proof of [Sn, §1, Thm. 1].

Theorem 10. *Let $E = (K/F, G, f)$ be a G–crossed product with $k \subseteq F$. Given a nonzero element $a \in A$, there exists a k–algebra homomorphism $\varphi : A \to E$ with $\varphi(a) \neq 0$.*

Corollary 11. *Let $E = (K/F, G, f)$ be a G–crossed product with $k \subseteq F$. If $d_0, d_1, \ldots, d_r \in D_G^{(p)}$, then there exists a subring B of $D_G^{(p)}$ containing each d_i,*

and a k–algebra homomorphism $\varphi : B \to E$ with $\varphi(d_0) \neq 0$ and $\varphi(B)F = E$. Therefore $D_G^{(p)}$ is generic for the class of G–crossed product k–algebras of exponent p.

Proof of the corollary. (This proof is very similar to the proofs of the corresponding results for other generic algebras. See [A$_2$], for instance, where this result is proved for the algebra of generic matrices.) Since $D_G^{(p)}$ is a central localization of A, there is an $\alpha \in Z(A)$ with $d_i\alpha \in A$ for each i. Let $b_1, \ldots, b_m \in A$ be a $Z(D_G^{(p)})$–basis of $D_G^{(p)}$. If C_m is the Capelli polynomial in $2m - 1$ variables, then by [Ro, p. 31], $C_m(b_1, \ldots, b_m, c_1, \ldots, c_{m-1}) \neq 0$ for elements $c_1, \ldots, c_{m-1}$ which can be chosen to be in A since A is an order in $D_G^{(p)}$. Let $a = d_0\alpha C_m(b_1, \ldots, b_m, c_1, \ldots, c_{m-1})$. Then by the theorem there is a k–algebra homomorphism $\varphi : A \to E$ with $\varphi(a) \neq 0$. The image of $C_m(b_1, \ldots, b_m, c_1, \ldots, c_{m-1})$ is $C_m(\varphi(b_1), \ldots, \varphi(b_m), \varphi(c_1), \ldots, \varphi(c_{m-1}))$, which is nonzero, so the $\varphi(b_i)$ form an F–basis for E by [Ro, p. 31]. Since $\alpha \in Z(A)$, $\varphi(\alpha) \in Z(\varphi(A)F) = F$. As $\varphi(\alpha) \neq 0$ and F is a field, $\varphi(\alpha)$ is invertible in E, so the map φ extends uniquely to $B = A[1/\alpha]$ by setting $\varphi(a/\alpha) = \varphi(a)/\varphi(\alpha)$. Since each $d_i \in B$, we are done. ∎

Proof of the theorem. Let $E = \sum Ky_\sigma$. Since $\exp(E) = p$, there are $u_\sigma \in K^*$ with $u_\sigma \sigma(u_\tau)u_{\sigma\tau}^{-1} = f^p(\sigma, \tau)$.

We define a map φ from $\sum k[Q]x_\sigma$ to E by $\varphi(x_\sigma) = b_\sigma y_\sigma = z_\sigma$, $\varphi(e_\sigma) = b_\sigma^p u_\sigma$, and $\varphi(c(\sigma, \tau)) = b_\sigma \sigma(b_\tau)b_{\sigma\tau}^{-1}f(\sigma, \tau)$, where the $b_\sigma \in K^*$ are to be determined. This uniquely determines a k–algebra homomorphism $A \to E$. The problem is to choose the b_σ so that $\varphi(a) \neq 0$.

Say $a = \sum r_\sigma x_\sigma$ with $r_\sigma \in k[Q]$. We have $\varphi(a) = \sum \varphi(r_\sigma)z_\sigma$, so by K–independence of the z_σ, it suffices to be able to choose the r_σ so that $\varphi(r_\sigma) \neq 0$ for some σ. As $k[Q]$ is isomorphic to a localization of the polynomial ring in variables $c(\sigma, \tau)$, e_σ, our theorem will be proven by the following lemma.

Lemma 12. *Let K/F be a G–Galois extension. Let $\sigma_1 = \mathrm{id}$, $\sigma_2, \ldots, \sigma_n$ be a denumeration of the elements of G. Let f_{σ_i, σ_j}, u_{σ_i}, $i, j = 2, \ldots, n$ be families of*

elements in K^*. Let k be a field contained in F, and let $C = k[x_{\sigma_i,\sigma_j}, y_{\sigma_i}]$ be the polynomial ring in the variables x_{σ_i,σ_j}, y_{σ_i}, $i, j = 2, \ldots, n$. If $c \in C$ is a nonzero polynomial, then there exist $b_{\sigma_i} \in K^*$ such that the k–algebra homomorphism $\varphi : C \to K$ given by $\varphi(x_{\sigma_i,\sigma_j}) = b_{\sigma_i}\sigma_i(b_{\sigma_j})b_{\sigma_i\sigma_j}^{-1}f_{\sigma_i,\sigma_j}$ and $\varphi(y_{\sigma_i}) = b_{\sigma_i}^p u_{\sigma_i}$ satisfies $\varphi(c) \neq 0$.

Proof. Consider $n(n-1)$ auxiliary variables suggestively denoted $\sigma_i(B_{\sigma_j})$ $(i = 1, \ldots, n,\ j = 2, \ldots, n)$, and consider the map ψ from C to the rational function field $K(\sigma_i(B_{\sigma_j}))$ given by $\psi(x_{\sigma_i,\sigma_j}) = B_{\sigma_i}\sigma_i(B_{\sigma_j})B_{\sigma_i\sigma_j}^{-1}f_{\sigma_i,\sigma_j}$ and $\psi(y_{\sigma_i}) = B_{\sigma_i}^p u_{\sigma_i}$. The images of x_{σ_i,σ_j} and y_{σ_i} are algebraically independent over K, so since $c \neq 0$, $\psi(c) \neq 0$. Now write $\psi(c) = h(\sigma_i(B_{\sigma_j}))/(B_{\sigma_2} \cdots B_{\sigma_n})^m$ (for suitable m). It follows that $h \neq 0$. We will show that we can find b_{σ_j} in K^* such that the map from $K[\sigma_i(B_{\sigma_j})]$ to K that sends $\sigma_i(B_{\sigma_j})$ to $\sigma_i(b_{\sigma_j})$ $(i = 1, \ldots, n,\ j = 2, \ldots, n)$ sends h to a non-zero element of K. This will clearly prove the lemma.

We do this by induction on the number of variables B_{σ_j} such that at least one of the associated variables $\sigma_i(B_{\sigma_j})$, $i = 1, \ldots, n$, appears in the polynomial h. If this number is one, we need to show that given a non-zero polynomial h in $K[x_1, x_2, \ldots, x_n]$, we can find a b in K^* such that $h(\sigma_1(b), \sigma_2(b), \ldots, \sigma_n(b)) \neq 0$. This is done below. For the general case, suppose that l is biggest such that at least one of the associated variables $\sigma_i(B_{\sigma_l})$, $i = 1, \ldots, n$, appears in h. Write h as a polynomial in $\sigma_i(B_{\sigma_l})$, with coefficients in $K[\sigma_i(B_{\sigma_j})]$ $(i = 1, \ldots, n,\ j = 2 \ldots, l-1)$. We can inductively find b_{σ_j} $(j = 2, \ldots, l-1)$ in K^* such that not all these coefficients become zero. We are then left with a non-zero polynomial in the variables $\sigma_i(B_{\sigma_l})$, which, by the first step of our induction, can be specialized to a non-zero element of K.

We finish the proof by proving the first step of our induction. By the normal basis theorem, there is an $\alpha \in K$ such that $\{\sigma_i(\alpha)\}$ is an F–basis for K, i.e., every $b \in K$ is of the form $\sum_i \sigma_i(\alpha)z_i$ for suitable $z_i \in F$. Write $g(z_1, \ldots, z_n)$ for $h(\sum_i \sigma_1\sigma_i(\alpha)z_i, \ldots, \sum_i \sigma_n\sigma_i(\alpha)z_i)$. Since the closure in the Zariski topology of F^n minus the origin in K^n is all of K^n, the zero set of g

cannot contain F^n minus the origin, so there exist $c_1, \ldots, c_n$ in F, not all zero, such that $g(c_1, \ldots, c_n) \neq 0$. This finishes the proof of the lemma. ∎

References

[A$_1$] S.A. Amitsur, *Division algebras, a survey*, Cont. Math. **13** (1982), 3–26.

[A$_2$] S.A. Amitsur, *Generic structures and division algebras*, unpublished.

[Ba] R. Baer, *Linear Algebra and Projective Geometry*, Academic Press, New York, 1952.

[Bo] N. Bourbaki, *Algèbre Commutative*, Chap. VI, Hermann, Paris, 1961.

[CW] M. Chacron and A. Wadsworth, *On decomposing c–valued division rings*, J. Algebra **134** (1990), 182–208.

[C] T. Craven, *Orderings and valuations on ∗–fields*, Proc. of the Corvallis Conf. on Quadratic Forms and Real Algebraic Geometry, Rocky Mountain J. Math **19** (1989), 629–646.

[D] P. Draxl, *Skew Fields*, London Math. Soc. Lecture Note Series, Vol. 81, Cambridge Univ. Press, Cambridge, 1983.

[E] O. Endler, *Valuation Theory*, Springer–Verlag, New York, 1972.

[H] S. Holland, *∗–valuations and ordered ∗–fields*, Trans. Amer. Math. Soc. **262** (1980), 219–243.

[J$_1$] B. Jacob, *The index and the symbol index of division algebras*, p. 293–309 in "Israel Math. Conf. Proc. vol. 1: Ring Theory 1989, in honor of S.A. Amitsur" (L. Rowen, ed.), Weizmann Science Press, Jersualem, 1989.

[J$_2$] B. Jacob, *Indecomposable division algebras of prime exponent*, J. Reine Angew. Math. **413** (1991), 181–197.

[Ja] N. Jacobson, *Splitting fields*, p. 362–380 in "Israel Math. Conf. Proc. vol. 1: Ring Theory 1989, in honor of S.A. Amitsur" (L. Rowen, ed.), Weizmann Science Press, Jersualem, 1989.

[JW] B. Jacob and A. Wadsworth, *A new construction of noncrossed product algebras*, Trans. Amer. Math. Soc. **293** (1986), 693–721.

[L] T.–Y. Lam, *Orderings, Valuations and Quadratic Forms*, CBMS Notes, No. 52, Amer. Math. Soc., 1983.

[M] P. Morandi, *The Henselization of a valued division algebra*, J. Algebra **122** (1989), 232–243.

[MS] P. Morandi and B.A. Sethuraman, *Noncrossed product division algebras with a Baer ordering*, preprint.

[R$_1$] P. Roquette, *On the Galois cohomology of the projective linear group and its applications to the construction of generic splitting fields of algebras*, Math. Ann. **150** (1963), 411–439.

[R$_2$] P. Roquette, *Isomorphisms of generic splitting fields of simple algebras*, J. Reine Angew. Math. **214** (1964), 207–226.

[Ro] L. Rowen, *Polynomial Identities in Ring Theory*, Academic Press, New York, 1980.

[Sa$_1$] D. Saltman, *Indecomposable division algebras*, Comm. Alg. **7** (1979), 791–817.

[Sa$_2$] D. Saltman, *Multiplicative field invariants*, J. Algebra **106** (1987), 221–238.

[Sc] O.F.G. Schilling, *The theory of valuations*, Math. Surveys, no. 4, Amer. Math. Soc., Providence, R.I., 1950.

[SV] A. Schofield and M. van den Bergh, *The index of a Brauer class on a Brauer–Severi variety*, Trans. Amer. Math. Soc. **333** (1992), 729–739.

[Se] B.A. Sethuraman, *Indecomposable division algebras*, Proc. Amer. Math. Soc. **114** (1992), 661–665.

[Sn] R. Snider, *Is the Brauer group generated by cyclic algebras?*, p. 279–301 in Lecture Notes in Math. Vol. 734, Springer–Verlag, New York, 1979.

[T] J.–P. Tignol, *Classification of wild cyclic field extensions and division algebras of prime degree over a Henselian field*, Cont. Math. **131** 1992, 491–508.