



Galois subfields of inertially split division algebras

Timo Hanke

Lehrstuhl D für Mathematik, RWTH Aachen, Templergraben 64, D-52062 Aachen, Germany

ARTICLE INFO

Article history:

Received 23 October 2010

Available online 15 September 2011

Communicated by Michel Van den Bergh

MSC:

primary 16K20

secondary 16S35

Keywords:

Noncommutative valuation

Division algebra

Maximal subfield

Galois subfield

Residue field

Crossed product

Noncrossed product

Generic construction

ABSTRACT

Let D be a valued division algebra, finite-dimensional over its center F . Assume D has an unramified splitting field. The paper shows that if D contains a maximal subfield which is Galois over F (i.e. D is a crossed product) then the residue division algebra \bar{D} contains a maximal subfield which is Galois over the residue field \bar{F} . This theorem captures an essential argument of previously known noncrossed product proofs in the more general language of noncommutative valuations. The result is particularly useful in connection with explicit constructions.

© 2011 Elsevier Inc. All rights reserved.

1. Introduction

Let (F, v) be an arbitrary valued field. By a valuation v on F we mean a Krull valuation, i.e. there is no restriction on the rank or divisibility of the value group. Let D be a finite-dimensional central F -division algebra. Assume v extends to a valuation on D and denote this extension also by v . By a valuation on D we mean a valuation in the sense of Schilling [12], i.e. v corresponds to an invariant valuation ring of D . We call (D, v) *inertially split* if there exists an unramified field extension L/F such that L splits D .¹ Let \bar{F}, \bar{D} denote the residue field of (F, v) and the residue division algebra of (D, v) , respectively. A *maximal subfield* of D means a commutative subfield of D which is maximal with respect to inclusion.

¹ E-mail address: hanke@math.rwth-aachen.de.

¹ In other words, D is inertially split if and only if D is split by the maximal unramified extension F_{nr}^h of the Henselization F^h of (F, v) .

Theorem 1. *Let (D, v) be inertially split, $F = Z(D)$. If D contains a maximal subfield Galois over F then \bar{D} contains a maximal subfield Galois over \bar{F} . The converse holds if v is Henselian.*

A division algebra D is called a *crossed product* if it contains a maximal subfield Galois over its center, otherwise a *noncrossed product*. The existence as well as the construction of noncrossed products has spawned research interest from around 1930, when the question of existence first arose, to the present day. Since Amitsur's existence proof in 1972 more examples were found or constructed by various authors and by various methods. In this context, Theorem 1 is regarded as a noncrossed product criterion for valued division algebras which is formulated purely “on the residue level”. Note that the condition ‘ \bar{D} does not contain a maximal subfield Galois over \bar{F} ’ is weaker than ‘ \bar{D} is a noncrossed product’ because \bar{F} is in general a strict subfield of the center of \bar{D} .

Valuations on division rings have played a crucial role in works on noncrossed products (explicitly or implicitly, as [14, §5] points out). So it comes as no surprise that special cases of Theorem 1 can be identified as a key ingredient in previously known noncrossed product proofs (even where valuations on division rings are not explicitly mentioned), starting with Brussel [2]. In fact, it was the motivation of the present paper to provide an abstraction of this useful argument in the language of noncommutative valuations, which seems to capture its essence best. The precise relation of Theorem 1 to the relevant literature is discussed in several remarks. We also point out its usefulness in connection with explicit noncrossed product constructions.

For the most part the paper contains condensed material from the author's thesis [4], described in its historical context up to recent work in [7].

2. The main theorem

Let D be a division algebra, finite-dimensional over its center $Z(D)$. Jacob and Wadsworth show in [8, Thm. 5.15(b)] that if D is inertially split² and contains a maximal subfield L Galois over $Z(D)$ then \bar{D} contains the maximal subfield $\bar{L}Z(\bar{D})$, which is normal over $\bar{Z}(\bar{D})$. They conclude further that \bar{D} is a crossed product using a result of Saltman [10, Lem. 3]. This section points out that replacing [10, Lem. 3] by a slightly stronger statement (see Proposition 2 below) leads to Theorem 1. In the preface of [4] Theorem 1 appears as “Noncrossed Product Criterion”, and in the text as Theorem 5.20.

Proposition 2. *Let $F \subseteq Z(D)$ be a subfield such that $Z(D)/F$ is finite and separable. If D contains a maximal subfield that is normal over F then D also contains a maximal subfield that is Galois over F .*

The case $F = Z(D)$ is [10, Lem. 3]. An inspection of the proof reveals that it also handles the case when $Z(D)/F$ is finite and separable. Further details can be found in the appendix of [4]. Note that this is essentially a statement about p -algebras.

Theorem 3. *Let (D, v) be inertially split, $F \subseteq Z(D)$ a finite degree subfield. Suppose $Z(D)/F$ and $Z(\bar{D})/\bar{F}$ are Galois. If D contains a maximal subfield which is Galois over F then \bar{D} contains a maximal subfield which is Galois over \bar{F} . The converse holds if v is Henselian.*

If $F = Z(D)$ then the hypothesis ‘ $Z(\bar{D})/\bar{F}$ is Galois’ is automatically satisfied [8, Lem. 5.1]. Thus Theorem 1 is a special case of Theorem 3. The generality of Theorem 3 lends itself to an iterated application for composite valuations, which is possible but not pursued further in this paper.

Proof of Theorem 3. Let L be a maximal subfield of D which is Galois over F . Following the lines of proof of [8, Thm. 5.15], $\bar{L}Z(\bar{D})$ is a maximal subfield of \bar{D} . Since L/F is Galois, \bar{L}/\bar{F} is normal [3, p. 107]. Since $Z(\bar{D})/\bar{F}$ is Galois by hypothesis, $\bar{L}Z(\bar{D})/\bar{F}$ is normal. Proposition 2 shows that \bar{D} contains a maximal subfield Galois over \bar{F} .

² We may assume the valuation to be Henselian by passing to the Henselization of D in the sense of [9].

Conversely, let L be a maximal subfield of \bar{D} which is Galois over \bar{F} . Assume v is Henselian. By [8, Thm. 2.9], D contains an inertial lift \tilde{L} of L over F and \tilde{L}/F is Galois. Hence $M := Z(D)\tilde{L}$ is Galois over F and inertial over $Z(D)$. Since $\bar{M} = L$ we have $[M : Z(D)] = [L : Z(\bar{D})] = \text{ind } D$ by the index formula in [8, Thm. 5.15]. Thus, M is maximal in D . \square

3. Existence of inertially split division algebras

Assume (F, v) is Henselian. The inertially split division algebras over F then form a subgroup of the Brauer group; this subgroup is the relative Brauer group $\text{Br}(F_{nr}/F)$, where F_{nr} is the maximal unramified extension of F . Let $G = \text{Gal}(\bar{F}_{sep}/\bar{F})$, $\Gamma = v(F^*)$, Δ the divisible hull of Γ . Any continuous homomorphism $\chi \in \text{Hom}_c(G, \Delta/\Gamma)$ has a finite image when Δ/Γ is equipped with the discrete topology because G is profinite. Thus, denoting the fixed field of $\ker(\chi)$ by $\bar{F}(\chi)$, the extension $\bar{F}(\chi)/\bar{F}$ is finite abelian. Moreover, $\text{Gal}(\bar{F}(\chi)/\bar{F})$ has rank at most the rank of v . Let $\text{res}_{\bar{F} \rightarrow \bar{F}(\chi)} : \text{Br}(\bar{F}) \rightarrow \text{Br}(\bar{F}(\chi))$, $\alpha \mapsto \alpha^\chi$ denote the restriction map. There is a (noncanonical) exact sequence, due to Witt [15] and Scharlau [11]:

$$0 \rightarrow \text{Br}(\bar{F}) \rightarrow \text{Br}(F_{nr}/F) \xrightarrow{\gamma} \text{Hom}_c(G, \Delta/\Gamma) \rightarrow 0. \quad (1)$$

The interpretation of the cohomological data in this sequence has been extensively studied by Jacob and Wadsworth in [8, p. 154ff]: Let (D, v) be inertially split with center F . Then $Z(\bar{D}) = \bar{F}(\gamma[D])$ [8, Thm. 5.6(b)] and $\text{ind } D = \text{ind } \bar{D} \cdot [\bar{F}(\gamma[D]) : \bar{F}]$ [8, Thm. 5.15(a)]. There exists a splitting map δ for γ such that

$$\bar{D} \text{ is a field for each } [D] \in \text{im}(\delta) \quad (2)$$

[8, Rem. 5.9(ii)]. For any such δ , if $[D] = \alpha + \delta(\chi)$ with $\alpha \in \text{Br}(\bar{F})$ and $\chi \in \text{Hom}_c(G, \Delta/\Gamma)$ then $[\bar{D}] = \alpha^\chi$ (following the proof of [8, Thm. 5.15(a)]). Proposition 4 below is an immediate consequence of these facts. Suppose E is a finite-dimensional division algebra over \bar{F} (not necessarily central).

Proposition 4. *E is the residue of an F -central inertially split (D, v) if and only if $Z(E) = \bar{F}(\chi)$ for some $\chi \in \text{Hom}_c(G, \Delta/\Gamma)$ and $[E] \in \text{im}(\text{res}_{\bar{F} \rightarrow Z(E)})$.*

An F -central inertially split (D, v) with residue division algebra E will be called an F -central lift of E (v is not required to be Henselian for this definition). Proposition 4 appears in the preface of [4] as “Lift Theorem”, and in the text as Theorem 5.25. All F -central lifts of E are obtained by taking, for a fixed δ satisfying (2), the underlying division algebras of $\alpha + \delta(\chi)$ where χ runs over all $\chi \in \text{Hom}_c(G, \Delta/\Gamma)$ with $\bar{F}(\chi) = Z(E)$ and α runs over all $\alpha \in \text{Br}(\bar{F})$ with $\alpha^\chi = [E]$. There is, however, no canonical F -central lift because there is no canonical choice for α .³ Translating Theorem 1 in terms of α and χ yields

Corollary 5. *Suppose δ satisfies (2). Given a pair $(\alpha, \chi) \in \text{Br}(\bar{F}) \times \text{Hom}_c(G, \Delta/\Gamma)$, the division algebra D underlying $\alpha + \delta(\chi)$ is a crossed product if and only if there is a Galois extension M/\bar{F} of degree $\text{ind } D$ that contains $\bar{F}(\chi)$ and splits α .*

Proof. Let $M \supseteq \bar{F}(\chi)$. Since $\alpha^\chi = [\bar{D}]$, M splits α if and only if M splits \bar{D} . Since $\text{ind } D = \text{ind } \bar{D} \cdot [\bar{F}(\chi) : \bar{F}]$, M is a maximal subfield of \bar{D} if and only if $[M : \bar{F}] = \text{ind } D$. The assertion is thus equivalent to Theorem 1. \square

³ As a consequence, for instance, the exponent of an F -central lift of E is in general not determined by E . Note that δ can be chosen order preserving by [8, Ex. 4.3]. In that case, following the proof of [8, Thm. 5.15(a)], one derives $\exp D = \text{lcm}(\exp \alpha, \exp \chi)$. This expression is in general not determined by E ; see [4, Ex. 5.13] for an example.

The existence of noncrossed products over F can thus be shown by exhibiting pairs (α, χ) for which no M as in Corollary 5 exists. This approach is original to [2] and has been followed in [7] (see remark b) in Section 5 below).

4. Construction of inertially split division algebras

Let (F, v) be an arbitrary valued field. Let E be a finite-dimensional division algebra over \bar{F} . Assume $Z(E) = \bar{F}(\chi)$ for some $\chi \in \text{Hom}_c(G, \Delta/\Gamma)$ and $[E] \in \text{im}(\text{res}_{\bar{F} \rightarrow Z(E)})$. Proposition 4 states the existence of an F -central lift of E (over any Henselian valued field (F, v) with residue field \bar{F}) but does not give a direct construction of the lift. Here, a construction is *direct* if we are not required to pass from some representative of the class $\alpha + \delta(\chi)$ to its underlying division algebra. This section points out that if one is allowed to choose F then a lift can be obtained by Tignol's construction [13] of a *generic abelian extension* of E . The construction is as follows, similar to the generic abelian crossed products of Amitsur and Saltman in [1].

Since $[E]$ lies in the image of $\text{res}_{\bar{F} \rightarrow Z(E)}$, there is a central-simple \bar{F} -algebra A and an \bar{F} -algebra embedding of E into A such that E is the centralizer of $Z(E)$ in A . Suppose A as well as the embedding of E are explicitly given, and identify E with its image in A . Choose a minimal set of generators $(\sigma_1, \dots, \sigma_r)$ of the abelian group $\text{Gal}(Z(E)/\bar{F})$. By the Skolem–Noether theorem, choose for each $1 \leq i \leq r$ an element $z_i \in A$ so that $z_i a z_i^{-1} = \sigma_i(a)$ for all $a \in Z(E)$. Let $E[x_1, \dots, x_r; z]$ denote the twisted polynomial ring defined by the relations

$$x_i a = (z_i a z_i^{-1}) x_i, \quad x_i x_j = (z_i z_j z_i^{-1} z_j^{-1}) x_j x_i,$$

for all $a \in E$, $1 \leq i, j \leq r$. Note that $z_i a z_i^{-1}$ and $z_i z_j z_i^{-1} z_j^{-1}$ lie in E . Let $E(x_1, \dots, x_r; z)$ denote the ring of central quotients of $E[x_1, \dots, x_r; z]$. As in the proof of [13, Thm. 2.3] one may verify

Theorem 6. $E(x_1, \dots, x_r; z)$ is an F -central lift of E where F is isomorphic to the rational function field $\bar{F}(t_1, \dots, t_r)$.

Theorem 6 appears in [4] as Theorem 11.14. Theorems 1 and 6 allow to construct explicit examples of noncrossed products by exhibiting division algebras E as above that do not contain a maximal subfield Galois over \bar{F} . Here, an example is *explicit* if the structure constants of the noncrossed product are known. This approach is original to [4] and has been followed in [5,6].

5. Rank 1 valuations

Assume v has rank 1. We conclude with remarks and references about this important case.

- a) Every tame division algebra (in the sense of Jacob and Wadsworth [8, §6]) is inertially split. This can be seen as follows: By [8, Lem. 6.2], any tame D has a decomposition $D \sim S \otimes T$ where S is inertially split and T is tame and totally ramified. In the rank 1 case, T must be trivial because there are no non-trivial tame and totally ramified division algebras.
- b) If v is discrete (i.e. $\Gamma = \mathbb{Z}$) then (1) is split exact and the splitting homomorphism δ satisfies (2). Thus, one recovers Witt's theorem

$$\text{Br}(F_{nr}/F) \cong \text{Br}(\bar{F}) \oplus \text{Hom}_c(G, \mathbb{Q}/\mathbb{Z}). \quad (3)$$

Moreover, in Corollary 5, (α, χ) is the decomposition of D according to (3). In this form, Corollary 5 is not new; it is original to Brussel [2] where it appears as “Corollary” on p. 381 (for $\text{char } \bar{F} = 0$). It also appears in [7, §6] as “Brussel's Lemma”. Note that $\text{Br}(F_{nr}/F) = \text{Br}(F)$ if \bar{F} is perfect.

- c) Replacing in [7] the use of Corollary 5 by Theorem 1 leads to the following reformulation of the main result of [7]: Suppose \bar{F} is a global field and v is discrete. For any finite cyclic extension K/\bar{F} and any $m \in \mathbb{N}$ let $B_m(K)$ denote the set of all inertially split F -central division algebras with $Z(\bar{D}) = K$ and $\text{ind } \bar{D} = m$. The sets $B_m(K)$ form a partition of $\text{Br}(F_{nr}/F)$. There is a formal product⁴ $b(K) = \prod_{p \in \mathbb{P}} p^{b_p}$ with $b_p \in \mathbb{N} \cup \{\infty\}$ such that

$B_m(K)$ consists entirely of crossed products if and only if $m|b(K)$.

If $m \nmid b(K)$ then $B_m(K)$ contains infinitely many noncrossed products. The numbers $b(K)$ are computed in [7] by a precise formula in terms of the number of roots of unity in K and a measure for the embeddability of the cyclic extension K/\bar{F} into larger cyclic extensions. For example, if $\bar{F} = \mathbb{Q}$ then $b_2(\mathbb{Q}(\sqrt{-1})) = 2$, hence $B_2(\mathbb{Q}(\sqrt{-1}))$ and $B_4(\mathbb{Q}(\sqrt{-1}))$ consist entirely of crossed products while $B_8(\mathbb{Q}(\sqrt{-1}))$ contains infinitely many noncrossed products. All elements of $B_8(\mathbb{Q}(\sqrt{-1}))$ have index 16.

- d) The result formulated in c) holds not only for discrete v . In the non-discrete case, however, certain sets $B_m(K)$ can be empty. In order to get a partition of $\text{Br}(F_{nr}/F)$ we have to restrict ourselves to the cyclic extensions K/\bar{F} of the form $K = \bar{F}(\chi)$ for some $\chi \in \text{Hom}_c(G, \Delta/\Gamma)$.

References

- [1] S. Amitsur, D. Saltman, Generic abelian crossed products and p -algebras, *J. Algebra* 51 (1978) 76–87.
- [2] E. Brussel, Noncrossed products and nonabelian crossed products over $\mathbb{Q}(t)$ and $\mathbb{Q}((t))$, *Amer. J. Math.* 117 (1995) 377–393.
- [3] O. Endler, *Valuation Theory*, Springer-Verlag, New York, 1972.
- [4] T. Hanke, A direct approach to noncrossed product division algebras, Dissertation, Universität Potsdam, 2001, arXiv:1109.1580.
- [5] T. Hanke, An explicit example of a noncrossed product division algebra, *Math. Nachr.* 271 (2004) 51–68.
- [6] T. Hanke, A twisted Laurent series ring that is a noncrossed product, *Israel J. Math.* 150 (2005) 199–204.
- [7] T. Hanke, J. Sonn, The location of noncrossed products in the Brauer group of Laurent series fields over global fields, *Math. Ann.* 350 (2011) 313–337.
- [8] B. Jacob, A. Wadsworth, Division algebras over Henselian fields, *J. Algebra* 128 (1990) 126–179.
- [9] P. Morandi, The Henselization of a valued division algebra, *J. Algebra* 122 (1989) 232–243.
- [10] D. Saltman, Noncrossed products of small exponent, *Proc. Amer. Math. Soc.* 68 (1978) 165–168.
- [11] W. Scharlau, Über die Brauer-Gruppe eines Hensel-Körpers, *Abh. Math. Sem. Univ. Hamburg* 33 (1969) 243–249.
- [12] O. Schilling, *The Theory of Valuations*, Math. Surveys, vol. 4, Amer. Math. Soc., Providence, RI, 1950.
- [13] J.-P. Tignol, Generalized Crossed Products, *Semin. Math. (N. S.)*, vol. 106, Université Catholique de Louvain, Louvain-la-Neuve, Belgium, 1987.
- [14] A. Wadsworth, Valuation theory on finite dimensional division algebras, in: *Proceedings of the 1999 Saskatoon Conference on Valuation Theory*, 1999.
- [15] E. Witt, Schiefkörper über diskret bewerteten Körpern, *J. Reine Angew. Math.* 176 (1936) 153–156.

⁴ Called a *supernatural number* or *Steinitz number*.