Common subfields of p-algebras of prime degree

Adam Chapman

Abstract

We prove that if two division p-algebras of prime degree share an inseparable field extension of the center then they also share a cyclic separable one. We show that the converse is in general not true. We also point out that sharing all the inseparable field extensions of the center does not imply sharing all the cyclic separable ones.

1 Introduction

A p-algebra is a central simple algebra of degree p^m over a field F of characteristic p for some prime p and positive integer m. If a p-algebra is cyclic of prime degree p then it has a symbol presentation $[\alpha, \beta)_{p,F}$ for some $\alpha \in F$ and $\beta \in F^\times$ which stands for the algebra generated over F by x and y subject to the relations $x^p - x = \alpha$, $y^p = \beta$ and $yxy^{-1} = x + 1$.

The symbol presentation of an algebra is not unique. For example $[\alpha, \beta)_{p,F}$ and $[\alpha + \beta, \beta)_{p,F}$ present the same algebra. We say that two algebras are right linked if they have symbol presentations sharing the right slot, e.g. $[\alpha, \beta)_{p,F}$ and $[\gamma, \beta)_{p,F}$ are right linked. We say that two algebras are left linked if they have symbol presentations sharing the left slot, e.g. $[\alpha, \beta)_{p,F}$ and $[\alpha, \delta)_{p,F}$ are left linked.

In [Dra75] Draxl proved that if two p-algebras of degree 2 (i.e. quaternion algebras) are right linked then they are also left linked. In [Lam03] Lam gave a

Received by the editors in March 2015 - In revised form in June 2015.
Communicated by S. Caenepeel.
2010 *Mathematics Subject Classification* : 16K20.
Key words and phrases : Central Simple Algebras, Cyclic Algebras, p-Algebras, Linkage, Division Algebras.

simpler proof and showed that the converse is not true. In [EV05] this was generalized to Hurwitz algebras, and in [Fai06] this was translated and generalized to arbitrary n-fold Pfister forms.

In this note we prove for cyclic division p-algebras of prime degree that being right linked implies being left linked and that the converse is in general not true. We also point out that sharing all the inseparable field extensions of the center does not imply sharing all the cyclic separable ones.

2 Artin-Schreier and p-central elements

Given a cyclic division p-algebra A of prime degree p over F, a noncentral element $x \in A$ satisfying $x^p - x \in F$ is called Artin-Schreier, and a noncentral element $y \in A$ satisfying $y^p \in F$ is called p-central. Each Artin-Schreier element in A generates a cyclic separable field extension of the center, and every cyclic separable field extension of the center has an Artin-Screier generator. The p-central elements are exactly the elements generating pure inseparable field extensions over the center.

If two nonzero elements x and y in A satisfy $yxy^{-1} = x + 1$ then x is Artin-Schreier, y is p-central and $A = [x^p - x, y^p)_{p,F}$.

For any Artin-Schreier element $x \in A$ there exists an element $y \in A$ such that $yxy^{-1} = x + 1$ (see [Alb68, Chapter 5, Theorem 9]). Furthermore, the set $Cy \setminus \{0\}$ is the set of all $y' \in A^\times$ satisfying $y'xy'^{-1} = x + 1$ where $C = F[x]$ is the centralizer of x in A. So the set Cy does not depend on the choice of y. The same holds for the set Cy^i for any integer i. Therefore, the algebra A decomposes uniquely as $A = \otimes_{i \in \mathbb{Z}/p\mathbb{Z}} A_i$ where for each $i \in \mathbb{Z}/p\mathbb{Z}$, $A_i = \{z \in A : zx - xz = iz\} = Cy^i$. Consequently, every $t \in A$ decomposes uniquely as $t = t_0 + \cdots + t_{p-1}$ where $t_i x - x t_i = i t_i$ for each $i \in \mathbb{Z}/p\mathbb{Z}$.

Similarly, for any p-central element $y \in A$ there exists an element $x \in A$ such that $yxy^{-1} = x + 1$ (see [Alb68, Chapter 7, Lemma 10]).

Therefore, two p-algebras of prime degree p over F contain a common purely inseparable degree p field extension of the center if and only if they are right linked. They contain a common cyclic separable degree p extension of the center if and only if they are left linked.

3 Right linkage implies left linkage

We shall now show that being right linked implies being left linked.

Lemma 3.1. *In a cyclic division p-algebra A of prime degree p over F, if two nonzero elements x and y satisfy $yx - xy = ky$ for some k in $(\mathbb{Z}/p\mathbb{Z})^\times$, then $(x+y)^p - (x+y) = x^p - x + y^p$.*

Proof. The element $x + y$ is Artin-Schreier, because it satisfies $y^m(x+y)y^{-m} = x + y + 1$ where m is an integer satisfying $mk \equiv 1 \pmod{p}$. Therefore $(x+y)^p - (x+y) \in F$. There is a unique decomposition of $(x+y)^p - (x+y)$ as $t_0 + \cdots + t_{p-1}$ where $t_i x - x t_i = i t_i$ for each $i \in \mathbb{Z}/p\mathbb{Z}$. Let $x^a * y^b$ denote the sum of all products of a copies of x and b copies of y in any possible order. Then $(x+y)^p = \sum_{i=0}^{p} x^{p-i} * y^i$. Each monomial summand s of $x^{p-i} * y^i$ satisfies $sx - xs = iks$. Hence, $t_{ik} = x^{p-i} * y^i$ for each i with $2 \leq i \leq p-1$, $t_k = x^{p-1} * y - y$ and $t_0 = x^p + y^p - x$. Since $(x+y)^p - (x+y) \in F$, we have $(x+y)^p - (x+y) = t_0$. ■

Theorem 3.2. *If two cyclic division p-algebras of prime degree p are right linked then they are left linked.*

Proof. Let $A = F[x, y : x^p - x = \alpha, y^p = \beta, yxy^{-1} = x+1]$ and $A' = F[x', y' : x'^p - x' = \gamma, y'^p = \beta, y'x'y'^{-1} = x'+1]$ be two right linked algebras. Let λ be the unique solution to the linear equation $\alpha + \beta(\alpha - \lambda) = \gamma$ over F. Since $z = x + \lambda y + xy$ satisfies $(\lambda y + xy)z - z(\lambda y + xy) = \lambda y + xy$, by Lemma 3.1, z is an Artin-Schreier element in A satisfying

$$z^p - z = (x^p - x) + (\lambda y + xy)^p = \alpha + N_{F[x]/F}(\lambda + x)y^p = \alpha + (\alpha + \lambda^p - \lambda)\beta.$$

Therefore A has the symbol presentation $A = [\alpha + (\alpha + \lambda^p - \lambda)\beta, (\alpha + \lambda^p - \lambda)\beta)_{p,F} = [\gamma + \lambda^p\beta, (\alpha + \lambda^p - \lambda)\beta)_{p,F}$.

Another way of seeing that $A = [\alpha + (\alpha + \lambda^p - \lambda)\beta, (\alpha + \lambda^p - \lambda)\beta)_{p,F}$ is by noticing that $[\alpha + (\alpha + \lambda^p - \lambda)\beta, (\alpha + \lambda^p - \lambda)\beta)_{p,F}$ is Brauer equivalent to

$$[\alpha, (\alpha + \lambda^p - \lambda)\beta)_{p,F} \otimes [(\alpha + \lambda^p - \lambda)\beta, (\alpha + \lambda^p - \lambda)\beta)_{p,F}.$$

The second algebra in this product is split and the first one is isomorphic to $[\alpha, \beta)_{p,F}$.

Similarly, $z' = x' + \lambda y'$ is Artin-Schreier in B satisfying $y'z' - z'y' = y'$ and $z'^p - z' = \gamma + \lambda^p\beta$, and therefore $A' = [\gamma + \lambda^p\beta, \beta)_{p,F}$. Consequently A and A' are also left linked. ■

4 Counterexample for the converse

We want to construct a counterexample for the converse. Over fields of imperfect exponent 1 we cannot hope to find such counterexamples as the following proposition suggests:

Proposition 4.1. *If $[F : F^p] = p$ then all the p-algebras of prime degree over F are right linked.*

Proof. Let $F' = F[\lambda : \lambda^p = t]$ be the unique inseparable field extension of degree p of F. Every division p-algebra contains an inseparable field extension of degree p of F, which must be isomorphic to F', so every such algebra has a symbol presentation $[\alpha, t)_{p,F}$ for some $\alpha \in F$, and they are all right linked. ■

Such fields include all imperfect fields of transcendence degree 1 over a perfect field (see [FJ08, Chapter 2, Lemma 2.7.2]), e.g. global fields. It is important to note that there can be p-algebras over such fields of prime degree that do not share all the cyclic separable field extensions of the center. For example, take K to be the perfect closure of the function field $E(\alpha, \beta)$ in two algebraically independent variables over some field E of characteristic p, and take $F = K(t)$ to be the function field in one variable over K. Then $[\alpha, t)_{p,F}$ contains $F[\wp^{-1}(\alpha)]$ but $[\beta, t)_{p,F}$ does not. This is because the t-adic valuation on F extends to a valuation on the division algebra $[\beta, t)_{p,F}$ with residue field $K[\wp^{-1}(\beta)]$ which does not contain $\wp^{-1}(\alpha)$, whereas every division F-algebra containing $F[\wp^{-1}(\alpha)]$ must have $\wp^{-1}(\alpha)$ in its residue field. This means that sharing all the inseparable field extensions of the center does not imply sharing all the cyclic separable ones.

In order to construct examples of division p-algebras that are left linked but not right linked we must therefore turn to fields of greater imperfect exponent, and the place to start is function fields in two independent variables over perfect fields.

Example 4.2. *The algebras $[1, \alpha)_{p,F}$ and $[1, \beta)_{p,F}$ are not right linked when $F = \mathbb{F}_p(\alpha, \beta)$ with α and β algebraically independent over $\mathbb{F}_p$ or $F = \mathbb{F}_p((\alpha))((\beta))$.*

Proof. Let $F_0 = \mathbb{F}_p(\alpha, \beta)$, $F = \mathbb{F}_p((\alpha))(\beta))$, $A = [1, \alpha)_{p,F}$ and $B = [1, \beta)_{p,F}$. The case of F_0 follows from the case of F because $A = [1, \alpha)_{F_0} \otimes F$ and $B = [1, \beta)_{F_0} \otimes F$ with A and B division algebras.

The fact that A and B are division algebras can be seen in the following way: Consider the (α, β)-adic valuation v on F. Since $\mathbb{F}_p[\wp^{-1}(1)] = \mathbb{F}_{p^p}$, we have $F[\wp^{-1}] = \mathbb{F}_{p^p}((\alpha))((\beta))$ which is an unramified extension of F of degree p. Hence every norm from $F[\wp^{-1}(1)]$ to F has value in $p(\mathbb{Z} \times \mathbb{Z})$. Since α has value $(1, 0)$, it is not such a norm, so the cyclic algebra A is not split. A similar argument holds for B.

Since v is Henselian, it extends uniquely to any finite-dimensional division algebra over F (see [Sch50, pp. 53–54]). In particular it extends to A and to B.

There is the fundamental inequality $[A : F] \geq [\overline{A} : \overline{F}] \cdot [\Gamma_A : \Gamma_F]$ where $\overline{A}$ is the residue division algebra of A and Γ_A is the value group of A (see [TW15, Chapter 1, Proposition 1.3]). Now $[A : F] = p^2$, $[\overline{A} : \overline{F}] \geq p$ because $\overline{A}$ contains $\wp^{-1}(1)$, and $[\Gamma_A : \Gamma_F] \geq p$ because Γ_A contains $\frac{1}{p}v(\alpha)$. Therefore $p = [\overline{A} : \overline{F}] = [\Gamma_A : \Gamma_F]$. Hence the extended valuation from F to A is defectless, i.e.

$$[A : F] = [\overline{A} : \overline{F}] \cdot [\Gamma_A : \Gamma_F]$$

with $\overline{A} = \mathbb{F}_{p^p}$ and $\Gamma_A = \frac{1}{p}\mathbb{Z} \times \mathbb{Z}$. The defectless property is inherited by F-subalgebras of A, and so for any maximal subfield L of A either $[\overline{L} : \overline{F}] = p$ or $[\Gamma_L : \Gamma_F] = p$. The same thing holds for B, just with value group $\Gamma_B = \mathbb{Z} \times \frac{1}{p}\mathbb{Z}$.

If L is a maximal subfield of A, then since the rank of L is p, one of the following holds: either L/F is unramified, or it is totally ramified. If it is unramified, then its residue field is the residue field of the division algebra, hence L is separable. So if L is purely inseparable then it is totally ramified with value group $\frac{1}{p}\mathbb{Z} \times \mathbb{Z}$. Similarly, any purely inseparable maximal subfield of $[1, \beta)_{p,F}$ is a totally ramified extension of the center, with value group $\mathbb{Z} \times \frac{1}{p}\mathbb{Z}$. Therefore, $[1, \alpha)_{p,F}$ and $[1, \beta)_{p,F}$ do not share any maximal subfield that is a purely inseparable
extension of the center. ∎

In case $p = 2$, the algebras $[1,\alpha)_{2,F}$ and $[1,\beta)_{2,F}$ over the function field $F = \mathbb{F}_2(\alpha,\beta)$ in two variables over $\mathbb{F}_2$ were exactly the algebras given in [Lam03] as an example of a pair of left linked quaternion algebras which are not right linked. The proof here, however, is essentially different, making use of valuations instead of quadratic forms, in order to make it work for arbitrary prime numbers.

Acknowledgments

I thank Jean-Pierre Tignol for his help and support, and especially for suggesting the proof of Example 4.2. I thank also Uzi Vishne, Adrian Wadsworth and the anonymous referee for their comments on the manuscript.

References

[Alb68] A. Albert, *Structure of algebras*, Colloquium Publications, vol. 24, American Math. Soc., 1968.

[Dra75] Peter Draxl, *Über gemeinsame separabel-quadratische Zerfällungskörper von Quaternionenalgebren*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II (1975), no. 16, 251–259. MR 0480436 (58 #599)

[EV05] A. Elduque and O. Villa, *A note on the linkage of Hurwitz algebras*, Manuscripta Math. **117** (2005), no. 1, 105–110. MR 2142905 (2005m:11068)

[Fai06] F. Faivre, *Liaison des formes de Pfister et corps de fonctions de quadriques en caractéristique* 2, Ph.D. thesis, Université de Franche-Comté (2006).

[FJ08] Michael D. Fried and Moshe Jarden, *Field arithmetic*, third ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2008, Revised by Jarden. MR 2445111 (2009j:12007)

[Lam03] T.Y. Lam, *On the linkage of quaternion algebras*, Bull. Belg. Math. Soc. **9** (2003), 415–418.

[Sch50] O. F. G. Schilling, *The Theory of Valuations*, Mathematical Surveys, No. 4, American Mathematical Society, New York, N. Y., 1950. MR 0043776 (13,315b)

[TW15] J.-P. Tignol and A. R. Wadsworth, *Value functions on simple algebras, and associated graded rings*, Springer Monographs in Mathematics, Springer, 2015.

Department of Mathematics, Michigan State University,
East Lansing, MI 48824
email:adam1chapman@yahoo.com