

AN ARITHMETIC OBSTRUCTION TO DIVISION ALGEBRA DECOMPOSABILITY

ERIC S. BRUSSEL

(Communicated by Ken Goodearl)

ABSTRACT. This paper presents an indecomposable finite-dimensional division algebra of p -power index that decomposes over a prime-to- p degree field extension, obtained by adjoining p -th roots of unity to the base. This shows that the theory of decomposability has an arithmetic aspect.

Suppose F is a field and D is an indecomposable F -division algebra, that is, a division algebra that cannot be expressed as the tensor product of two nontrivial F -division algebras. It is easy to see that the (Schur) index of D must be a power of some prime p . In “Problem 6” of [Sa], Saltman asks if in general D remains indecomposable upon arbitrary prime-to- p extension. At issue is the nature of indecomposability, in particular whether or not it is “geometric”. For example in [K], Karpenko showed a certain generic class of division algebras are indecomposable by computing the degrees of cycles on their Brauer-Severi varieties. As noted in [K], it is immediate from the geometric nature of the proof that these algebras remain indecomposable over all prime-to- p extensions.

This paper presents an indecomposable division algebra that decomposes over a prime-to- p extension, namely the cyclotomic extension defined by p -th roots of unity. Thus it is proved that (in)decomposability can have an arithmetic aspect.

Let p be an odd prime of \mathbb{Q} , let k be a number field that does not contain a p^{th} root of unity, and let $k[s, t]$ be the polynomial ring in two variables over k . Define

$$v : k[s, t] \rightarrow \mathbb{Z} \oplus \mathbb{Z}, \\ f \mapsto (a, b)$$

where b is smallest such that $f \in (t^b)$ and a is smallest such that $f \in (s^a, t^{b+1})$. The map v is a valuation, with value group $\mathbb{Z} \oplus \mathbb{Z}$ ordered reverse lexicographically, so $(a, b) < (a', b')$ if $b < b'$, or if $b = b'$ and $a < a'$. The field of iterated power series

$$F = k((s))((t))$$

is Henselian with respect to v , with valuation ring

$$R = k[[s]] + t k((s))[[t]] \subset k((s))[[t]].$$

R is a non-Noetherian 2-dimensional Henselian local ring, with maximal ideal $(s) = (s, t)$ and residue field k . The ideal (s) properly contains the (infinitely generated) prime ideal $t k((s))[[t]] = (t, \frac{t}{s}, \frac{t}{s^2}, \dots)$.

Received by the editors June 10, 1998 and, in revised form, October 6, 1998.
1991 *Mathematics Subject Classification.* Primary 16K20; Secondary 11R37.

For any field l , let $X(l)$ denote the *character group* of l , consisting of all continuous homomorphisms from the Galois group G_l to the group of roots of unity $\mu(\mathbb{C})$. If $\xi \in X(l)$, let $l(\xi)/l$ denote the cyclic extension (of degree $|\xi|$) determined by ξ . Let $\langle \psi, \theta \rangle \subset X(l)$ denote the subgroup determined by ψ and θ . If $G \subset X(l)$ is any subgroup, let $l(G)$ denote the composite of the extensions determined by the elements of G .

Let μ_n denote the n -th roots of unity in \mathbb{C} . By Kummer theory if $\mu_n \subset l^*$, there is an isomorphism

$$l/l^{*n} \xrightarrow{\sim} X(l)_n$$

where $X(l)_n$ denotes the n -torsion of $X(l)$. If $\xi \in X(l)_n$ is represented by $u \bmod l^{*n}$, then $k(\xi) \cong l(u^{1/n})$.

In the Brauer group $\text{Br}(l)$ let (ξ, t) denote the *cyclic element* determined by character ξ and element $t \in l^*$. If $\mu_n \subset l$ and $\xi \in X(l)_n$ is represented by $u \bmod l^{*n}$, then $(\xi, t) = (u, t)_n$, the *symbol* defined by u and t .

There is an exact sequence

$$(1) \quad 0 \rightarrow \text{Br}(k) \rightarrow \text{Br}(F) \xrightarrow{T} \prod X(k((s))) \prod X(k((t))) \xrightarrow{\text{ord}} \mu(k) \rightarrow 0.$$

The maps: $\text{Br}(k) \rightarrow \text{Br}(F)$ is the usual restriction. T is the sum of the two residue maps corresponding to the discrete valuations t (on $F = k((s))((t))$) and s (on $k((t))((s))$). The natural isomorphism $\text{Br}(k((s))((t))) \cong \text{Br}(k((t))((s)))$ shows both are defined on $\text{Br}(F)$. Finally, ord is the ramification with respect to the valuation v .

Exactness of (1) is proved in [B] by iteratively applying Witt’s theorem ([Se]), which describes the Brauer group of discretely Henselian fields with perfect residue field. Briefly, the kernel of T consists of the v -unramified elements α of $\text{Br}(F)$, and since R is Henselian this is $\text{Br}(k)$. The residue maps are separately surjective, and thus the image of T and the kernel of ord both consist of elements of the form $(\psi + s^{m/n}, \theta + t^{-m/n})$ where $\psi, \theta \in X(k)$, $n = |\mu(k)|$, $m \in \{0, 1, \dots, n - 1\}$, and $s^{m/n}$ and $t^{-m/n}$ stand for the characters they determine under the Kummer map.

By Witt’s theorem, (1) “splits”, so that any $\delta \in \text{Br}(F)$ has the form

$$(2) \quad \delta = \alpha + (\psi, s) + (\theta, t) + m(s, t)_n$$

with $\alpha \in \text{Br}(k)$, $\psi, \theta \in X(k)$, $n = |\mu(k)|$, and $m \in \{0, 1, \dots, n - 1\}$.

In the following write $D(\delta)$ for the division algebra underlying a Brauer element δ . Write $\text{ind}(D)$ and $\text{per}(D)$ for the *index* and *period* of D , respectively. Assume always that p is an odd prime and $\mu_p \not\subset F$. Then $\mu(k)(p)$ is trivial and so the symbol term in (2) is trivial. More generally, for all $\delta \in \text{Br}(F)$ of the form $\delta = \alpha + (\psi, s) + (\theta, t)$, the index formula is

$$(3) \quad \text{ind}(\delta) = |G| \text{ind}(\alpha^{k(G)})$$

where $G = \langle \psi, \theta \rangle$ and $\alpha^{k(G)}$ is the restriction of α to $\text{Br}(k(G))$. This and a more general index formula are proved by iteratively applying Nakayama’s index formula for discretely Henselian fields ([B]).

Theorem. *Let p be an odd prime, k a number field not containing μ_p , and let F be the twice iterated power series field above. Then there exists an indecomposable F -division algebra D of period p^4 and index p^5 that becomes decomposable over the prime-to- p extension $k(\mu_p)$.*

Proof. Select three primes $\mathfrak{q}, \mathfrak{q}'$, and \mathfrak{p} of k , such that:

$$\begin{aligned} \mu_{p^2} &\subset k_{\mathfrak{q}}, k_{\mathfrak{q}'} \\ \mu_p &\not\subset k_{\mathfrak{p}}. \end{aligned}$$

Let $\psi_{\mathfrak{q}}$ and $\psi_{\mathfrak{q}'}$ be totally ramified (local) characters of order p^2 , let $\theta_{\mathfrak{q}}$ and $\theta_{\mathfrak{q}'}$ be unramified of order p^2 , let $\psi_{\mathfrak{p}}$ be trivial, and let $\theta_{\mathfrak{p}}$ be unramified of order p . By Grunwald-Wang’s Theorem ([AT]), there exist (global) characters ψ and θ with

$$|\psi| = |\theta| = p^2$$

and with the above restrictions at $\mathfrak{p}, \mathfrak{q}$, and \mathfrak{q}' . Set $G = \langle \psi, \theta \rangle$. The groups $\langle \psi_{\mathfrak{q}} \rangle$ and $\langle \theta_{\mathfrak{q}} \rangle$ are disjoint in $X(k_{\mathfrak{q}})$, so $|G_{\mathfrak{q}}| = p^4$, and similarly $|G_{\mathfrak{q}'}| = p^4$. Therefore $\langle \psi \rangle$ and $\langle \theta \rangle$ are disjoint in $X(k)$, and $|G| = p^4$. Let α be the unramified element of $\text{Br}(F)$ with invariants

$$\begin{aligned} \text{inv}(\alpha_{\mathfrak{q}}) &= 1/p^4, \\ \text{inv}(\alpha_{\mathfrak{p}}) &= 1/p^2, \\ \text{inv}(\alpha_{\mathfrak{q}'}) &= 1 - \text{inv}(\alpha_{\mathfrak{q}}) - \text{inv}(\alpha_{\mathfrak{p}}). \end{aligned}$$

Let

$$D = D(\alpha + (\psi, s) + (\theta, t)),$$

as per (2). By direct computation,

$$\begin{aligned} \text{ind}(D) &= |G| \cdot \text{ind}(\alpha^{K(G)}) = p^4 \cdot p = p^5, \\ \text{per}(D) &= \text{lcm} \{ \text{ind}(\alpha), |\psi|, |\theta| \} = p^4. \end{aligned}$$

The index follows since $|G| = p^4$ and $k(G)$ splits α at every prime except \mathfrak{p} , while $\text{ind}(\alpha_{\mathfrak{p}}^{k(G_{\mathfrak{p}})}) = p$. The period uses (1) and the fact that period equals index in $\text{Br}(k)$.

Claim 1. D is indecomposable. Suppose not; let

$$D \cong D_1 \otimes D_2$$

be a nontrivial decomposition. By dimension count $\text{ind}(D) = \text{ind}(D_1)\text{ind}(D_2)$. In the following, let the subscripts “1” and “2” signify association with D_1 and D_2 . By (3),

$$|G| \text{ind}(\alpha^{k(G)}) = |G_1| \text{ind}(\alpha_1^{k(G_1)}) \cdot |G_2| \text{ind}(\alpha_2^{k(G_2)}).$$

Since $\psi = \psi_1 + \psi_2$ and $\theta = \theta_1 + \theta_2$, $G \subseteq G_1G_2$.

Assume without loss of generality that $\text{ind}(D_1) \leq \text{ind}(D_2)$. Then $\text{ind}(D_1) = p^2$ or p , and $\text{ind}(D_2) = p^3$ or p^4 . By (3), $|G_1|$ divides p^2 , and since $|G| = p^4$ and $G \subseteq G_1G_2$, p^2 divides $|G_2|$. Since $\alpha = \alpha_1 + \alpha_2$, $\text{per}(\alpha) = p^4$, and $\text{per}(\alpha_1)$ divides p^2 , by abelian group theory $\text{per}(\alpha_2) = p^4$. Therefore $\text{per}(D_2) = p^4$; hence $\text{ind}(D_2) = p^4$, and this forces $\text{ind}(D_1) = p$. It follows that

$$\begin{aligned} |G_1| &\text{ divides } p, \\ |G_2| &= p^2, p^3, \text{ or } p^4. \end{aligned}$$

If $|G_2| = p^2$, then since $G_1G_2 \supseteq G$ and $|G| = p^4$, necessarily $|G_1| = p^2$, which is not the case. If $|G_2| = p^3$, then again p^2 divides $|G_1|$, because G_1G_2 must contain the disjoint cyclic groups $\langle \theta \rangle$ and $\langle \psi \rangle$ each of which has order p^2 . Therefore it must be that $|G_2| = p^4$, and since $\text{ind}(D_2) = p^4$, $\text{ind}(\alpha_2^{k(G_2)}) = 1$. If G_1 is

trivial, then $G_2 = G$, and G does not split the invariants of α_2 at \mathfrak{q} , contradicting $\text{ind}(\alpha_2^{k(G_2)}) = 1$. Therefore $|G_1| = p$ and $\text{ind}(\alpha_1^{k(G_1)}) = 1$.

Since G_2 is abelian, $(G_2)_{\mathfrak{p}}$ is abelian, and since $\mu_p \not\subset k_{\mathfrak{p}}$, $(G_2)_{\mathfrak{p}}$ is cyclic. By abelian group theory $\text{ind}((\alpha_2)_{\mathfrak{p}}) = \text{ind}(\alpha_{\mathfrak{p}}) = p^2$, since $\text{ind}((\alpha_1)_{\mathfrak{p}}) \mid p$. Since G_2 splits α_2 , p^2 divides $|(G_2)_{\mathfrak{p}}|$; hence p^2 divides the group exponent of $(G_2)_{\mathfrak{p}}$. But $(G_2)_{\mathfrak{p}} \subseteq G_{\mathfrak{p}}(G_1)_{\mathfrak{p}}$, and the right side has group exponent p . This is a contradiction, proving claim 1.

Claim 2. $D(D \otimes F(\mu_p))$ is decomposable. This will be proved by a construction over $F(\mu_p)$. Since $F(\mu_p)/F$ has prime-to- p degree, the orders, degrees, and ramification behavior of the objects associated to D do not change from D to $D \otimes F(\mu_p)$. In the following, identify $\mathfrak{p}, \mathfrak{q}$, and \mathfrak{q}' with chosen extensions to $k(\mu_p)$.

Let $\varphi_{\mathfrak{p}} \in X(k(\mu_p)_{\mathfrak{p}})$ be totally ramified of order p (existence requires the root of unity), and let $\varphi_{\mathfrak{q}}$ and $\varphi_{\mathfrak{q}'}$ both be trivial. Let $\varphi \in X(k(\mu_p))$ be a character of order p with these restrictions. Note that $\theta_{\mathfrak{p}}$ and $\varphi_{\mathfrak{p}}$ are disjoint over $k(\mu_p)_{\mathfrak{p}}$, whereas there is only the unramified character over $k_{\mathfrak{p}}$, since $\mu_p \not\subset k_{\mathfrak{p}}$. Set

$$\begin{aligned}\psi_1 &= \theta_1 = \varphi, \\ \psi_2 &= \psi^{F(\mu_p)} - \varphi, \\ \theta_2 &= \theta^{F(\mu_p)} - \varphi, \\ \alpha_2 &= \alpha^{F(\mu_p)}.\end{aligned}$$

Then set $D_1 = D((\psi_1, s) + (\theta_1, t))$ and $D_2 = D(\alpha_2 + (\psi_2, s) + (\theta_2, t))$.

A simple check that $\psi^{F(\mu_p)} = \psi_1 + \psi_2$ and $\theta^{F(\mu_p)} = \theta_1 + \theta_2$ shows that $D \otimes F(\mu_p) \sim D_1 \otimes D_2$. To prove $D(D \otimes F(\mu_p)) \cong D_1 \otimes D_2$ it remains to show that the indexes are multiplicative. The index of D_1 is

$$\text{ind}(D_1) = |G_1| = |\langle \psi_1, \theta_1 \rangle| = |\langle \varphi \rangle| = p.$$

The order of $G_2 = \langle \psi_2, \theta_2 \rangle$ is p^4 : For

$$\langle G_2, \varphi \rangle = \langle G^{F(\mu_p)}, \varphi \rangle = \langle \psi^{F(\mu_p)}, \theta^{F(\mu_p)}, \varphi \rangle,$$

and since $\varphi_{\mathfrak{p}} \notin \langle \theta_{\mathfrak{p}}, \psi_{\mathfrak{p}} \rangle = \langle \theta_{\mathfrak{p}} \rangle$, $\varphi \notin G^{F(\mu_p)}$; hence $\varphi \notin G_2$ (else G_2 is a 3 generator group). Therefore $p \cdot |G_2| = p \cdot |G|$; hence $|G_2| = |G| = p^4$. Now compute $\text{ind}(\alpha_2^{k(G_2)})$: At \mathfrak{q} and \mathfrak{q}' , G_1 is trivial, so $|(G_2)_{\mathfrak{q}}| = |G_{\mathfrak{q}}| = p^4$ and $|(G_2)_{\mathfrak{q}'}| = |G_{\mathfrak{q}'}| = p^4$. At \mathfrak{p} , G_2 is the noncyclic group $\langle \theta^{F(\mu_p)} \rangle_{\mathfrak{p}}, \varphi_{\mathfrak{p}}$, so $|(G_2)_{\mathfrak{p}}| = p^2$. Therefore, by construction, G_2 splits α_2 at each prime in the locus of α_2 , so $\text{ind}(\alpha_2^{k(G_2)}) = 1$. Since $|G_2| = p^4$, and $\text{ind}(\alpha_2^{k(G_2)}) = 1$,

$$\text{ind}(D_2) = p^4.$$

Therefore $\text{ind}(D \otimes F(\mu_p)) = \text{ind}(D_1) \text{ind}(D_2) = p^5$, and so $D(D \otimes F(\mu_p))$ is decomposable. This proves claim 2, hence the theorem. \square

Remark. A general criterion for decomposability over F is given in [B].

REFERENCES

- [AT] Artin, E., Tate, J.: *Class Field Theory*, Addison-Wesley, Reading, Mass., 1967. MR **36**:6383
- [B] Brussel, E.: Division algebras over Henselian fields of rank two, (in preparation).
- [K] Karpenko, N.: Torsion in CH^2 of Severi-Brauer varieties and indecomposability of generic algebras, *Manuscripta Math.* **88** (1995), 109-117. MR **96g**:14007

- [Sa] Saltman, D.: Finite dimensional division algebras. *Azumaya Algebras, Actions, and Modules*, (D. Haile and J. Osterburg, eds.), Contemporary Math. Vol. 124, Amer. Math. Soc., Providence, R.I., 1992, 203-214. MR **93a**:16014
- [Se] Serre, J.-P: *Local Fields*, Springer Verlag, New York, 1979. MR **82e**:12016

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, EMORY UNIVERSITY, ATLANTA, GEORGIA 30322

E-mail address: `brussel@mathcs.emory.edu`