DIVISION ALGEBRAS WITH AN ANTI-AUTOMORPHISM BUT WITH NO INVOLUTION

P.J. MORANDI, B.A. SETHURAMAN, AND J.-P. TIGNOL

1. Introduction

In this note we give examples of division rings which posses an anti-automorphism but no involution. The motivation for such examples comes from geometry. If D is a division ring and V a finite-dimensional right D-vector space of dimension ≥ 3, then the projective geometry $\mathbb{P}(V)$ has a duality (resp. polarity) if and only if D has an anti-automorphism (resp. involution) [2, p. 97, p. 111]. Thus, the existence of a division ring with an anti-automorphism but no involution gives examples of projective geometries with dualities but no polarities.

All the division rings considered in this paper are finite-dimensional algebras over their center. The anti-automorphisms we construct are *not* linear over the center (i.e. they do not restrict to the identity on the center) since a theorem of Albert [1, Theorem 10.19] shows that every finite-dimensional central division algebra with a linear anti-automorphism has an involution. Several proofs of this result can be found in the literature, see for instance [5] or [10, Chapter 8, §8].

The paper is organized as follows. Section 2 collects some background information on central division algebras. Section 3 establishes the existence of division algebras over algebraic number fields which have anti-automorphisms but no involution, and gives two explicit constructions of such algebras. The proofs rely on deep classical results on the Brauer group of number fields. Section 4 gives examples whose center has a more complicated structure (they are Laurent series fields over local fields), but the proof that these algebras have no involution is more elementary. Sections 3 and 4 are independent of each other.

2. Central division algebras

As pointed out in the introduction, all the division algebras considered in this paper are finite-dimensional over their center. Their dimension is the square of an integer called the *degree* of the algebra. The degree of a central division algebra D is denoted $\deg D$. Division algebras of degree 2 are quaternion algebras. They have a canonical (conjugation) involution. The division algebras we construct in this paper therefore have degree at least 3.

The first and second authors wish to thank the Mathematisches Forschungsinstitut Oberwolfach, for hospitality while work on this paper was carried out as part of a Research in Pairs visit.

The second author was supported in part by an NSF grant.

The third author gratefully acknowledges the hospitality of An Coláiste Ollscoile, Baile Átha Cliath (Ollscoil na hÉireann) while this paper was written. He is supported in part by the National Fund for Scientific Research (Belgium) and by the European Community's Human Potential Programme under contract HPRN-CT-2002-00287, KTAGS.

For any central division algebra D over a field F, we let D^{op} denote the opposite division algebra,

$$D^{\mathrm{op}} = \{x^{\mathrm{op}} \mid x \in D\}$$

with the operations

$$x^{\mathrm{op}} + y^{\mathrm{op}} = (x+y)^{\mathrm{op}}, \qquad x^{\mathrm{op}} y^{\mathrm{op}} = (yx)^{\mathrm{op}}, \qquad \lambda \cdot x^{\mathrm{op}} = (\lambda x)^{\mathrm{op}}$$

for x, $y \in D$, $\lambda \in F$. Thus, a map $f\colon D \to D$ is a linear anti-automorphism if and only if the map $f'\colon D \to D^{\mathrm{op}}$ given by $f'(x) = f(x)^{\mathrm{op}}$ is an isomorphism of F-algebras.

If τ is an automorphism of F, we let ${}^{\tau}D$ denote the conjugate F-algebra

$${}^{\tau}D = \{{}^{\tau}x \mid x \in D\}$$

with the operations

$${}^{\tau}x + {}^{\tau}y = {}^{\tau}(x+y), \qquad {}^{\tau}x\,{}^{\tau}y = {}^{\tau}(xy), \qquad \lambda \cdot {}^{\tau}x = {}^{\tau}(\tau^{-1}(\lambda)x)$$

for x, $y \in D$ and $\lambda \in F$. Thus, ${}^{\tau}D$ is obtained from D by letting τ act on the structure constants. A map $f\colon D \to D$ is a ring anti-automorphism which restricts to τ on F if and only if the map $f'\colon {}^{\tau}D \to D^{\mathrm{op}}$ defined by $f'({}^{\tau}x) = f(x)^{\mathrm{op}}$ is an isomorphism of F-algebras.

For background on the Brauer group of fields, we refer to the standard texts [1], [3], [7] or [9]. We summarize below the results we use in this paper. For any central division algebra D over a field F, there is an integer $e \geq 1$ such that $D^{\otimes e} = \underbrace{D \otimes \cdots \otimes D}_{e}$ is isomorphic to a matrix algebra over F. The smallest such integer e is called the *exponent* of D and denoted $\exp D$. It is the order of the Brauer equivalence class of D in the Brauer group $\operatorname{Br} F$. Since the inverse of the Brauer class of D is the Brauer class of D^{op}, the condition $D \simeq D^{\mathrm{op}}$ is equivalent to $\exp D = 1$ or 2. If F is a number field, $\exp D = \deg D$ for every central division F-algebra D. Therefore, a central division F-algebra D has an F-linear involution if and only if $D = F$ or D is a quaternion algebra.

3. Examples over number fields

We start with a few general observations.

Lemma 3.1. *Let f be an anti-automorphism of a noncommutative division ring D. Suppose k is an integer such that $f^k = \mathrm{Id}$. Then k is even, and k is a multiple of 4 if D has no involution.*

Proof. Odd powers of f are anti-automorphisms, so k is even if $f^k = \mathrm{Id}$. Moreover, if $k = 2m$ with m odd, then f^m is an involution. □

The key observation on which the construction of the examples in this section relies is the following:

Proposition 3.2. *Let F/F_0 be a Galois field extension and D be a central division F-algebra such that $D \not\simeq D^{\mathrm{op}}$. If every element of order 2 in $\mathrm{Gal}(F/F_0)$ extends to an automorphism of D, then D has no involution which restricts to the identity on F_0. In particular, if F_0 has no nontrivial automorphism (e.g. $F_0 = \mathbb{Q}$), then D has no involution at all.*

Proof. Suppose φ is an involution on D which is the identity on F_0. The restriction $\varphi|_F \in \mathrm{Gal}(F/F_0)$ is not the identity since $D \not\simeq D^{\mathrm{op}}$, hence it has order 2. By hypothesis, there is an automorphism θ of D such that $\theta|_F = \varphi|_F$. Then $\theta \circ \varphi$ is an anti-automorphism of D such that $(\theta \circ \varphi)|_F = \mathrm{Id}$. This is impossible since $D \not\simeq D^{\mathrm{op}}$. □

Note that the argument actually proves a stronger result: A has no anti-automorphism φ such that $\varphi|_{F_0} = \mathrm{Id}$ and $\varphi|_F^2 = \mathrm{Id}$.

Corollary 3.3. *Let $m \geq 1$ be an integer, and let F/F_0 be a cyclic field extension of degree $4m$. Let also D be a central division F-algebra such that $D \not\simeq D^{\mathrm{op}}$. If D has an anti-automorphism f such that the restriction $f|_F$ generates $\mathrm{Gal}(F/F_0)$, then D has no involution which restricts to the identity on F_0. In particular, if F_0 has no nontrivial automorphism (e.g. $F_0 = \mathbb{Q}$), then D has no involution at all.*

Proof. The Galois group $\mathrm{Gal}(F/F_0)$ contains a unique element of order 2, namely $(f|_F)^{2m}$, which extends to the automorphism f^{2m} of D. □

Using the corollary above and the description of the Brauer group of algebraic number fields afforded by class field theory (see [7, Chapter 18] or [9] for an exposition of the main results), it is easy to establish the existence of finite-dimensional division algebras over $\mathbb{Q}$ which have an anti-automorphism but no involution, as we now show.

Let $n > 2$ and $m \geq 1$ be integers, and let v be a non-archimedean valuation on $\mathbb{Q}$. By the Grunwald–Wang theorem (see [7, p. 359]), there is a cyclic field extension F of $\mathbb{Q}$ of degree $4m$ such that v splits completely in F. Denote by τ a generator of $\mathrm{Gal}(F/\mathbb{Q})$, and by v_1 one of the extensions of v to F. Then the extensions of v to F are

$$v_1, \quad v_2 = v_1 \circ \tau, \quad v_3 = v_1 \circ \tau^2, \ \ldots, \ v_{4m} = v_1 \circ \tau^{4m-1}.$$

Let D be the central division algebra over F with local invariants

$$\mathrm{inv}_w D = \begin{cases} 1/n \in \mathbb{Q}/\mathbb{Z} & \text{if } w = v_i \text{ with } i \text{ odd}, \\ -1/n \in \mathbb{Q}/\mathbb{Z} & \text{if } w = v_i \text{ with } i \text{ even}, \\ 0 & \text{if } w \neq v_1, \ldots, v_{4m}. \end{cases}$$

(The existence of D follows from [7, Theorem, p. 357].) The invariant of ${}^{\tau}D$ at any valuation w of F is the invariant of D at $w \circ \tau$, so

$$\mathrm{inv}_w {}^{\tau}D = -\mathrm{inv}_w D \qquad \text{for all valuations } w \text{ of } F.$$

It follows that ${}^{\tau}D \simeq D^{\mathrm{op}}$, so D has an anti-automorphism which restricts to τ on F. On the other hand, since $n > 2$, we have $1/n \neq -1/n$ in $\mathbb{Q}/\mathbb{Z}$, hence $\mathrm{inv}_{v_1} D \neq \mathrm{inv}_{v_1} D^{\mathrm{op}}$, and therefore $D \not\simeq D^{\mathrm{op}}$. Applying Corollary 3.3, we see that D has no involution.

Since it relies on the Grunwald–Wang theorem and the description of the Brauer group of algebraic number fields by local invariants, the proof above is not constructive. Our goal in the rest of this section is to give explicit examples of division algebras over number fields based on the cyclic or symbol algebra construction.

3.1. **Cyclic algebras.** Recall from [7, Chapter 15] the cyclic algebra construction: let K/F be a cyclic field extension of degree n, let σ be a generator of $\mathrm{Gal}(K/F)$ and $u \in F^\times$. Denote

$$(K/F, \sigma, u) = \bigoplus_{i=0}^{n-1} Kz^i$$

where z is a symbol, and define a multiplication on this vector space by

$$zx = \sigma(x)z \quad \text{for } x \in K, \qquad z^n = u.$$

The F-algebra $(K/F, \sigma, u)$ is central simple of degree n (see [7, p. 277]).

Proposition 3.4. *Let $n > 2$, $m \geq 1$ be integers and let G be the metacyclic group generated by two elements σ, τ subject to the relations*

$$\sigma^n = \tau^{4m} = 1, \qquad \tau\sigma = \sigma^{-1}\tau.$$

Let $K/\mathbb{Q}$ be a Galois field extension with Galois group G, let $F \subset K$ be the fixed field of σ and let $u \in \mathbb{Q}^\times$. Then the cyclic algebra $D = (K/F, \sigma, u)$ has an anti-automorphism f such that $f|_K = \tau$ and $f(z) = z$. If D is a division algebra, then it has no involution.

Proof. Straightforward computations show that the map $f\colon D \to D$ defined by

$$f\Big(\sum_{i=0}^{n-1} a_i z^i\Big) = \sum_{i=0}^{n-1} \sigma^i\tau(a_i)z^i$$

is an anti-automorphism. If D is a division algebra, then $D \ncong D^{\mathrm{op}}$ since its degree is $n > 2$ and the exponent of any central division algebra over a number field is equal to its degree. Therefore, Corollary 3.3 shows that D has no involution. □

To give an explicit example, choose $n = 3$ and $m = 1$. Let F be the splitting field of $x^4 + 5x + 5$ over $\mathbb{Q}$. Then $F/\mathbb{Q}$ is cyclic Galois of degree 4 and $\mathbb{Q}(\sqrt{5})$ is the unique intermediate field of $F/\mathbb{Q}$, by [6, Ex. 13.7]. Also, let $p(x) = x^3 - 18x + 18$, which is irreducible over $\mathbb{Q}$ by the Eisenstein criterion. We have $\mathrm{disc}(p) = 5 \cdot (54)^2$, so $\mathrm{disc}(p) \notin \mathbb{Q}^{\times 2}$. If M is the splitting field over $\mathbb{Q}$ of p, then $M/\mathbb{Q}$ is Galois with Galois group the symmetric group S_3, and $\mathbb{Q}(\sqrt{5})$ is a subfield of M. Set $K = MF$. Since M and F are linearly disjoint over $\mathbb{Q}(\sqrt{5})$, we see that $K/\mathbb{Q}$ is Galois of degree 12 with Galois group $\langle \sigma, \tau \rangle$ of the form we wish.

Finally, let $u = 11$. To see that the cyclic algebra $D = (K/F, \sigma, 11)$ is a division algebra, we work over the field $\mathbb{Q}_{11}$ of 11-adic numbers. Since $x^4 + 5x + 5$ has a simple root in $\mathbb{F}_{11}$, Hensel's lemma shows that F embeds in $\mathbb{Q}_{11}$. Moreover, since $x^3 - 18x + 18$ has no root in $\mathbb{F}_{11}$, the extension $M\mathbb{Q}_{11}$ is an unramified extension of $\mathbb{Q}_{11}$ of degree 3. Therefore $K\mathbb{Q}_{11} = M\mathbb{Q}_{11}$, and $D \otimes_F \mathbb{Q}_{11} = (K\mathbb{Q}_{11}/\mathbb{Q}_{11}, \sigma, 11)$ is a division algebra by [7, §17.10] or [9, Theorem 13.1]. Therefore, D is a division algebra.

3.2. **Symbol algebras.** Let $n \geq 2$ be an integer and let F be a field containing a primitive n-th root of unity ω. For $a, b \in F^\times$, the F-algebra $(a, b)_{\omega,F}$ generated by two elements i, j subject to

$$i^n = a, \qquad j^n = b, \qquad ji = \omega ij$$

is central simple of degree n (see [3, p. 78]). It is called a *symbol algebra.*[1] In the sequel, we consider the particular case where $b = \omega$.

Proposition 3.5. *Every automorphism ρ of F such that $\rho(a) = a$ (resp. $\rho(a) = a^{-1}$) extends to an automorphism (resp. an anti-automorphism) of $(a, \omega)_{\omega,F}$.*

Proof. Since $\rho(\omega)$ is a primitive n-th root of unity, we have $\rho(\omega) = \omega^t$ for some integer t prime to n. Let i, j be the standard generators of $A = (a, \omega)_{\omega,F}$. If $\rho(a) = a$, then i and j^t satisfy

$$i^n = a = \rho(a), \qquad (j^t)^n = \omega^t = \rho(\omega), \qquad j^t i = \omega^t i j^t = \rho(\omega) i j^t,$$

hence ρ extends to an automorphism of A which fixes i and maps j to j^t.

If $\rho(a) = a^{-1}$, then

$$(i^{-1})^n = \rho(a), \qquad (j^t)^n = \omega^t = \rho(\omega), \qquad i^{-1} j^t = \omega^t j^t i^{-1} = \rho(\omega) j^t i^{-1},$$

hence ρ extends to an anti-automorphism of A which maps i to i^{-1} and j to j^t. □

Corollary 3.6. *Suppose $n > 2$, $F/\mathbb{Q}$ is a Galois extension and $a \in F^\times$ is such that*

1. *$\rho(a) = a$ for all $\rho \in \mathrm{Gal}(F/\mathbb{Q})$ of order 2,*
2. *$\tau(a) = a^{-1}$ for some $\tau \in \mathrm{Gal}(F/\mathbb{Q})$,*
3. *the symbol algebra $D = (a, \omega)_{\omega,F}$ is a division algebra.*

Then D has an anti-automorphism but no involution.

Proof. The degree of D is $n > 2$, hence $D \not\simeq D^{\mathrm{op}}$ since the exponent of central division algebras over number fields is equal to the degree. The corollary then follows from Propositions 3.2 and 3.5. □

To construct explicit examples, let $n \geq 3$ and set $l = \mathrm{lcm}(5, n)$. Let ν be a primitive l-th root of unity and $F = \mathbb{Q}(\nu)$. The field F contains a primitive 5-th root of unity μ, hence also $2\mu + 2\mu^{-1} + 1 = \pm\sqrt{5}$. Every element $\rho \in \mathrm{Gal}(F/\mathbb{Q})$ of order 2 satisfies $\rho(\mu) = \mu$ or μ^{-1}, hence $\rho(\sqrt{5}) = \sqrt{5}$. On the other hand, there is an element $\tau \in \mathrm{Gal}(F/\mathbb{Q})$ such that $\tau(\mu) = \mu^2$, hence $\tau(\sqrt{5}) = -\sqrt{5}$. By Dirichlet's theorem, we may find a prime p with $p \equiv 1 + l \bmod l^2$. Then l divides $p - 1$, so $\mathbb{F}_p$ contains a primitive l-th root of unity, and, by Hensel's lemma, we may embed $F \hookrightarrow \mathbb{Q}_p$. We have $\frac{p-1}{l} \equiv 1 \bmod l$ and $p \equiv 1 \bmod l$, so for every integer k,

$$\frac{p^k - 1}{l} \equiv \frac{p-1}{l}(p^{k-1} + \cdots + 1) \equiv k \bmod l.$$

Therefore, l^2 divides $p^k - 1$ if and only if l divides k, which means that $\mathbb{Q}_p(\sqrt[l]{\nu})$ is an inertial extension of degree l of $\mathbb{Q}_p$. If $\omega \in F$ is a primitive n-th root of unity, then $\mathbb{Q}_p(\sqrt[n]{\omega})$ is then an inertial extension of $\mathbb{Q}_p$ of degree n.

Let v be the restriction of the p-adic valuation to F, under the chosen embedding $F \hookrightarrow \mathbb{Q}_p$. Since τ restricts to the nontrivial automorphism of $\mathbb{Q}(\sqrt{5})$, we have $v \circ \tau|_{\mathbb{Q}(\sqrt{5})} \neq v$. Therefore, by the weak approximation theorem [4, Cor. 11.17], there exists $x \in \mathbb{Q}(\sqrt{5})$ with $v(x) = 1$ and $v(\tau(x)) = 0$. Let $a = x/\tau(x)$. Then $\tau(a) = a^{-1}$ and $\rho(a) = a$ for each $\rho \in \mathrm{Gal}(F/\mathbb{Q})$ of order 2, and $v(a) = 1$. Since $\mathbb{Q}_p(\sqrt[n]{\omega})$ is inertial of degree n, the algebra $(a, \omega)_{\omega,\mathbb{Q}_p} = (a, \omega)_{\omega,F} \otimes_F \mathbb{Q}_p$ is a division algebra by [7, §17.10]. Thus, $(a, \omega)_{\omega,F}$ is a division algebra. It has an anti-automorphism extending τ but no involution, since a satisfies all the conditions of Corollary 3.6.

[1] Draxl uses the notation $(a, b; n, F, \omega)$ and the term "power norm residue algebra."

For instance, let $n = 5$. We may then choose $p = 31$ since $31 \equiv 1 + 5 \bmod 5^2$. Let τ be a generator of $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ and let $x = 6 + \sqrt{5}$. We have

$$x\tau(x) = (6 + \sqrt{5})(6 - \sqrt{5}) = 31,$$

and x is integral over $\mathbb{Z}$, so there is an extension v of the 31-adic valuation to $\mathbb{Q}(\sqrt{5})$ such that

$$v(x) = 1 \qquad \text{and} \qquad v\big(\tau(x)\big) = 0.$$

Scalar extension to $\mathbb{Q}_{31}$ shows that the symbol algebra

$$\Big(\frac{6 + \sqrt{5}}{6 - \sqrt{5}}, \omega\Big)_{\omega, F}$$

is a division algebra, and Corollary 3.6 shows that this division algebra has an anti-automorphism extending τ, but no involution.

4. Twisted Laurent series examples

Our last examples are division rings which are complete for a discrete valuation. We start by recalling a few facts on this topic, and refer to [7, Chapter 17] for a more detailed account.

A *valuation* on a division ring D is a surjective map

$$v\colon\ D \to \mathbb{Z} \cup \{\infty\}$$

such that for all x, $y \in D$,

(a) $v(x + y) \geq \min\{v(x), v(y)\}$,
(b) $v(xy) = v(x) + v(y)$,
(c) $v(x) = \infty$ if and only if $x = 0$.

More precisely, the definition above describes a *normalized*, *discrete* valuation. We shall not use any other type of valuation in this work.

Choosing a real number $\delta > 1$, we may associate a norm to v by the formula

$$\|x\| = \delta^{-v(x)} \qquad \text{for } x \in D.$$

Note that in [7, Chapter 17] (and in many other references), valuations are defined as norm maps rather than by the properties (a)–(c) above. If D is a complete metric space for the norm, we refer to (D, v) as a *complete valued division ring*.

For any valuation v on D, let

$$\mathcal{O}_v = \{x \in D \mid v(x) \geq 0\} \quad \text{and} \quad \mathcal{M}_v = \{x \in D \mid v(x) > 0\}.$$

The set $\mathcal{O}_v$ is the valuation ring of v and $\mathcal{M}_v$ is its unique maximal left ideal and also its unique maximal right ideal, hence the factor ring

$$\overline{D} = \mathcal{O}_v/\mathcal{M}_v$$

is a division ring, called the *residue* division ring. The image of any $u \in \mathcal{O}_v$ in $\overline{D}$ is denoted by $\overline{u}$. The map $u \mapsto \overline{u}$ is the *residue map*.

The following result is probably well-known. We include a proof for lack of a convenient reference.

Proposition 4.1. *Let (D, v) be a complete valued division ring. Every automorphism and anti-automorphism of D preserves v.*

Proof. Let f be an automorphism or an anti-automorphism of D. We need to prove that $v\big(f(x)\big) = v(x)$ for all $x \in D$.

Step 1: *If $v(x) > 0$, then $v\big(f(x)\big) \geq 0$.* Let $E \subset D$ be the closure of the subfield generated by x (for the topology induced by the norm). The field E is complete since D is complete. For any integer n prime to the characteristic of $\overline{D}$, the residue of the polynomial $X^n - (1+x)$ has 1 as a simple root, hence Hensel's lemma [7, p. 324] yields an element $y \in E$ such that $y^n = 1 + x$. Taking the image of both sides under f, we obtain

$$f(y)^n = 1 + f(x).$$

If $v\big(f(x)\big) < 0$, it follows that $v\big(f(x)\big) = n\, v\big(f(y)\big) \in n\mathbb{Z}$, which cannot hold for infinitely many n. This contradiction proves the claim.

Step 2: *If $v(x) = 0$, then $v(f(x)) = 0$.* Suppose instead that $v\big(f(x)\big) \neq 0$. Replacing x by x^{-1}, if necessary, we may assume that $v\big(f(x)\big) < 0$. Let $\pi \in D$ have $v(\pi) = 1$. By Step 1, we have $v\big(f(\pi)\big) \geq 0$. Pick an integer n with $n\, v\big(f(x)\big) < -v\big(f(\pi)\big)$. Then $v(x^n\pi) = 1$ and

$$v\big(f(x^n\pi)\big) = n\, v\big(f(x)\big) + v\big(f(\pi)\big) < 0,$$

a contradiction to Step 1.

Step 3: *If $v(\pi) = 1$, then $v\big(f(x)\big) = v(x)v\big(f(\pi)\big)$ for all nonzero $x \in D$.* Let $n = v(x)$. Then $v(x^{-1}\pi^n) = 0$, hence Step 2 yields $v\big(f(x^{-1}\pi^n)\big) = 0$. Since $f(x^{-1}\pi^n) = f(x)^{-1}f(\pi)^n$ or $f(\pi)^n f(x)^{-1}$, it follows that $v\big(f(x)\big) = n\, v\big(f(\pi)\big)$.

To conclude the proof, observe that if $v(\pi) = 1$, then $v\big(f(\pi)\big) \geq 0$ by Step 1, and $v\big(f(\pi)\big)$ divides $v\big(f(x)\big)$ for all nonzero $x \in D$ by Step 3. Since f is onto, it follows that $v\big(f(\pi)\big) = 1$. Then Step 3 shows that f preserves v. □

Corollary 4.2. *(See, e.g.,* [8, p. 102]*.) The field $\mathbb{Q}_p$ of p-adic numbers has no nontrivial automorphism.*

Proof. The proposition shows that every automorphism of $\mathbb{Q}_p$ preserves the p-adic valuation, hence also the induced metric. Since $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$, which has no nontrivial automorphism, the corollary follows. □

The proposition also shows that every automorphism or anti-automorphism f of D preserves $\mathcal{O}_v$ and $\mathcal{M}_v$, and therefore induces a map $\overline{f}\colon\ \overline{D} \to \overline{D}$ defined by

$$\overline{f}(\overline{u}) = \overline{f(u)} \qquad \text{for } u \in \mathcal{O}_v.$$

Clearly, $\overline{f}$ is an automorphism if f is an automorphism, and an anti-automorphism if f is an anti-automorphism. Moreover, $\overline{f}^n = \overline{f^n}$ for all integer n, so $\overline{f}^2 = \mathrm{Id}$ if f is an involution.

To construct specific examples, consider a field K with an automorphism σ, and let $K((t;\sigma))$ be the division ring of twisted Laurent series in the indeterminate t with usual addition, but with multiplication twisted by $ta = \sigma(a)t$ for all $a \in K$ (see [7, Section 19.7]). There is a canonical discrete valuation on $K((t;\sigma))$, defined by

$$v\Big(\sum_n a_n t^n\Big) = \min\{n \mid a_n \neq 0\},$$

and $(K((t;\sigma)), v)$ is a complete valued division ring with valuation ring $\mathcal{O}_v = K[[t;\sigma]]$, the ring of twisted powers series over K, and residue field $\overline{K((t;\sigma))} = K$.

Proposition 4.3. *If f is an anti-automorphism of $K((t;\sigma))$, then the automorphism $\overline{f}$ of K satisfies $\overline{f}\circ\sigma = \sigma^{-1}\circ\overline{f}$.*

Note that the residue division ring is commutative, hence $\overline{f}$ is an automorphism for every anti-automorphism f.

Proof. The equation $ta = \sigma(a)t$ for $a \in K$ implies

$$\overline{txt^{-1}} = \sigma(\overline{x}) \quad \text{and} \quad \overline{t^{-1}xt} = \sigma^{-1}(\overline{x}) \quad \text{for all } x \in K[[t;\sigma]].$$

Therefore,

$$(\overline{f}\circ\sigma)(\overline{x}) = \overline{f(txt^{-1})} = \overline{f(t)^{-1}f(x)f(t)} \quad \text{for all } x \in K[[t;\sigma]]. \tag{1}$$

Since f preserves v by Proposition 4.1, we have $f(t) = tu$ for some $u \in K((t;\sigma))$ with $v(u) = 0$, hence

$$\overline{f(t)^{-1}f(x)f(t)} = \overline{u^{-1}t^{-1}f(x)tu} = \overline{u}^{-1}\sigma^{-1}\big(\overline{f}(\overline{x})\big)\overline{u} \quad \text{for all } x \in K[[t;\sigma]]. \tag{2}$$

The right side simplifies to $(\sigma^{-1}\circ\overline{f})(\overline{x})$ since the residue division ring is commutative, and the proposition then follows from (1) and (2). □

As a kind of converse to Proposition 4.3, observe that every automorphism τ of K such that $\tau\sigma = \sigma^{-1}\tau$ extends to an anti-automorphism f of $K((t;\sigma))$ defined by

$$f\Big(\sum_n a_n t^n\Big) = \sum_n \sigma^n\tau(a_n)t^n.$$

Theorem 4.4. *Let n, m be integers, $n > 2$, and let G be the group defined by generators and relations*

$$G = \langle \sigma, \tau \mid \sigma^n = \tau^{4m} = 1,\ \tau\sigma = \sigma^{-1}\tau\rangle.$$

If K/F_0 is a Galois extension of fields with Galois group G, then $K((t;\sigma))$ has an anti-automorphism but no involution f such that $\overline{f}(x) = x$ for all $x \in F_0$. In particular, if F_0 has no non-trivial automorphism (e.g. $F_0 = \mathbb{Q}$ or $\mathbb{Q}_p$, see Corollary 4.2), then $K((t;\sigma))$ has no involution at all.

Proof. As observed above, the automorphism τ extends to an anti-automorphism of $K((t;\sigma))$ leaving t invariant. On the other hand, if f is an involution of $K((t;\sigma))$ such that $\overline{f}$ is the identity on F_0, then $\overline{f} \in G$ satisfies $\overline{f}^2 = 1$ and $\overline{f}\sigma = \sigma^{-1}\overline{f}$, by Proposition 4.3. But G does not contain any such element. □

Theorem 4.4 applies for instance to the extension K/F_0 constructed at the end of Section 3.2, with $F_0 = \mathbb{Q}$, $n = 3$, $m = 1$. Here is another specific example, with $F_0 = \mathbb{Q}_p$ and arbitrary integers $n > 2$, $m \geq 1$. Dirichlet's theorem on primes in an arithmetic progression yields an odd prime p with $p \equiv -1 \bmod n$. Let $m \geq 1$, and let F be the inertial extension of $\mathbb{Q}_p$ of degree $4m$. Set $L = \mathbb{Q}_p(\sqrt[n]{p})$, and $K = FL$. We note that $L/\mathbb{Q}_p$ is totally ramified, so F and L are linearly disjoint over $\mathbb{Q}_p$. Since $p^{4m} \equiv 1 \bmod n$, the field $\mathbb{F}_{p^{4m}}$ contains a primitive n-th root of unity. Therefore, by Hensel's lemma, F contains a primitive n-th root of unity ω. Note that $\omega \notin \mathbb{Q}_p$ since n does not divide $p-1$. The generator of $\mathrm{Gal}(F/\mathbb{Q}_p)$ which induces the Frobenius automorphism on $\overline{F}$ sends ω to $\omega^p = \omega^{-1}$. Since F and L are linearly disjoint over $\mathbb{Q}_p$, this generator extends to an automorphism τ of K/F. On the other hand, there is an automorphism σ of K fixing F, which sends $\sqrt[n]{p}$ to $\omega\sqrt[n]{p}$. Then

$$\tau\sigma(\sqrt[n]{p}) = \omega^{-1}\sqrt[n]{p} = \sigma^{-1}\tau(\sqrt[n]{p}),$$

hence $\tau\sigma = \sigma^{-1}\tau$ and it follows that $\mathrm{Gal}(K/\mathbb{Q}_p) = \langle\sigma, \tau\rangle = G$.

Consider for instance $n = 3$, $m = 1$. We may then choose $p = 5$. Since $\mathbb{F}_5^\times$ is cyclic of order 4, generated by 2, there is a primitive 4-th root of unity $\zeta \in \mathbb{Q}_5$ with $\overline{\zeta} = 2$. Therefore, the cyclic extension $F/\mathbb{Q}_5$ is a Kummer extension; it can be represented as

$$F = \mathbb{Q}_5(\sqrt[4]{-3})$$

since -3 has order 4 in $\mathbb{F}_5^\times/\mathbb{F}_5^{\times 4} = \mathbb{F}_5^\times$. The construction above then yields

$$K = \mathbb{Q}_5(\sqrt[4]{-3}, \sqrt[3]{5}).$$

In order to describe σ and τ, fix some elements α, $\beta \in K$ with $\alpha^4 = -3$, $\beta^3 = 5$. We have $\overline{\alpha}^5 = 2\overline{\alpha} = \overline{\zeta\alpha}$ in $\mathbb{F}_5$, so we define τ by

$$\tau(\alpha) = \zeta\alpha, \qquad \tau(\beta) = \beta.$$

On the other hand, we may let $\omega = \frac{-1+\alpha^2}{2}$, which is a primitive 3-rd root of unity by the choice of α, and define σ by

$$\sigma(\alpha) = \alpha, \qquad \sigma(\beta) = \omega\beta.$$

Remark 4.5. The degree of $K((t;\sigma))$ over its center is the order of σ, see [7, p. 385]. Moreover, the anti-automorphism constructed in the proof of Theorem 4.4 has the same order $4m$ as τ. Thus, the construction above yields for any $n > 2$ and $m \geq 1$ an example of a central division algebra of degree $n > 2$ which has an anti-automorphism of order $4m$, but no involution.

References

[1] A.A. Albert, *Structure of Algebras*, Colloq. Pub. 24, Amer. Math. Soc., Providence, RI, 1939.
[2] R. Baer, *Linear Algebra and Projective Geometry*, Academic Press Inc., New York, 1952.
[3] P.K. Draxl, *Skew Fields*, Cambridge Univ. Press, Cambridge, 1983.
[4] O. Endler, *Valuation Theory*, Springer-Verlag, Berlin Heidelberg New York, 1972.
[5] I.N. Herstein, On a theorem of A.A. Albert, *Scripta Math.* **29** (1973), 391–394.
[6] P.J. Morandi, *Field and Galois Theory*, Springer-Verlag, New York, 1996.
[7] R.S. Pierce. *Associative Algebras*, Graduate Texts in Math. **88**, Springer-Verlag, New York Heidelberg Berlin, 1982.
[8] P. Ribenboim, *The Theory of Classical Valuations*, Springer Monographs in Math., Springer-Verlag, New York, 1999.
[9] I. Reiner, *Maximal Orders*, Academic Press, London New York, 1975.
[10] W. Scharlau, *Quadratic and Hermitian Forms*, Springer-Verlag, Berlin Heidelberg New York Tokyo, 1985.

Department of Mathematical Sciences, New Mexico State University, Las Cruces, NM 88003, USA
E-mail address: pmorandi@nmsu.edu
URL: http://math.nmsu.edu/morandi

Department of Mathematics, California State University, Northridge, Northridge, CA 91330, USA
E-mail address: al.sethuraman@csun.edu
URL: http://www.csun.edu/~asethura

Institut de Mathématique Pure et Appliquée, Université catholique de Louvain, B-1348 Louvain-la-Neuve, Belgium
E-mail address: tignol@math.ucl.ac.be
URL: http://www.math.ucl.ac.be/membres/tignol