TRIALITY AND ÉTALE ALGEBRAS

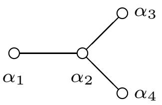
MAX-ALBERT KNUS AND JEAN-PIERRE TIGNOL

Dedicated with great friendship to R. Parimala at the occasion of her 60^{th} *birthday*

Abstract. Trialitarian automorphisms are related to automorphisms of order 3 of the Dynkin diagram of type D_4. Octic étale algebras with trivial discriminant, containing quartic subalgebras, are classified by Galois cohomology with value in the Weyl group of type D_4. This paper discusses triality for such étale extensions.

1. Introduction

All Dynkin diagrams but one admit at most automorphisms of order two, which are related to duality in algebra and geometry. The Dynkin diagram of D_4



is special, in the sense that it admits automorphisms of order 3. Algebraic and geometric objects related to D_4 are of particular interest as they also usually admit exceptional automorphisms of order 3, which are called trialitarian. For example the special projective orthogonal group PGO_8^+ or the simply connected group Spin_8 admit outer automorphisms of order 3. As already observed by E. Cartan, [5], the Weyl group $W(D_4) = \mathfrak{S}_2^3 \rtimes \mathfrak{S}_4$ of Spin_8 or of PGO_8^+ similarly admits trialitarian automorphisms. Let F be a field and let F_s be a separable closure of F. The Galois cohomology set $H^1\big(\Gamma, W(D_4)\big)$, where Γ is the absolute Galois group $\mathrm{Gal}(F_s/F)$, classifies isomorphism classes of étale extensions S/S_0 where S has dimension 8, S_0 dimension 4 and S has trivial discriminant (see §3). There is an induced trialitarian action on $H^1\big(\Gamma, W(D_4)\big)$, which associates to the isomorphism class of an extension S/S_0 as above, two extensions S'/S'_0 and S''/S''_0, of the same kind, so that the triple $(S/S_0, S'/S'_0, S''/S''_0)$ is cyclically permuted by triality. This paper is devoted to the study of such triples of étale algebras. It grew out of a study, in the spirit of [16], of Severi-Brauer varieties over the "field of one element", [13], which is in preparation (see also [17] and [18]).

In Part 2 we describe some basic constructions on finite Γ-sets and étale algebras. Some results are well-known, others were taken from [13], like the Clifford construction. In Section 3 we recall how Γ-sets and étale algebras are related to Galois cohomology. Section 4 is devoted to triality in connection with Γ-sets and in Section 5 we discuss trialitarian automorphisms of the Weyl group $W(D_4)$. In Section 6 we consider triality at the level of étale algebras. We give in Table 1 a list of isomorphism classes of étale algebras corresponding to the conjugacy classes

The second author is supported in part by the F.R.S.–FNRS (Belgium).

of subgroups of $W(D_4)$, together with a description of the triality action. We also consider étale algebras associated to subgroups of $W(D_4)$ which are fixed under triality. We then view in Section 7 triality as a way to create resolvents and give explicit formulae for polynomials defining étale algebras. Finally we give in the last section results of Serre on Witt invariants of $W(D_4)$.

We are grateful to Parimala for her unshakable interest in triality, in particular for many discussions at earlier stages of this work and we specially thank J-P. Serre for communicating to us his results on Witt and cohomological invariants of the group $W(D_4)$. We also thank Emmanuel Kowalski who introduced us to Magma [2] with much patience, Jean Barge for his help with Galois cohomology and J. E. Humphreys and B. Mühlherr for the reference to the paper [8]. The paper [10] on octic fields was a very useful source of inspiration. Finally we are highly thankful to the referee for many improvements.

2. Étale algebras and Γ-sets

Throughout most of this work, F is an arbitrary field. We denote by F_s a separable closure of F and by Γ the absolute Galois group $\Gamma = \mathrm{Gal}(F_s/F)$, which is a profinite group.

A finite-dimensional commutative F-algebra S is called *étale* (over F) if $S \otimes_F F_s$ is isomorphic to the F_s-algebra $F_s^n = F_s \times \cdots \times F_s$ (n factors) for some $n \geq 1$. Étale F-algebras are the direct products of finite separable field extensions of F. We refer to [11, §18.A] for various equivalent characterizations. Étale algebras (with F-algebra homomorphisms) form a category $\mathsf{Ét}_F$ in which finite direct products and finite direct sums (= tensor products) are defined.

Finite sets with a continuous left action of Γ (for the discrete topology) are called (finite) Γ-sets. They form a category Set_Γ whose morphisms are the Γ-equivariant maps. Finite direct products and direct sums (= disjoint unions) are defined in this category. We denote by $|X|$ the cardinality of any finite set X.

For any étale F-algebra S of dimension n, the set of F-algebra homomorphisms

$$\mathbf{X}(S) = \mathrm{Hom}_{F\text{-alg}}(S, F_s)$$

is a Γ-set of n elements since Γ acts on F_s. Conversely, if X is a Γ-set of n elements, the F-algebra $\mathbf{M}(X)$ of Γ-equivariant maps $X \to F_s$ is an étale F-algebra of dimension n,

$$\mathbf{M}(X) = \{f\colon X \to F_s \mid \gamma\big(f(x)\big) = f({}^\gamma x) \text{ for } \gamma \in \Gamma,\, x \in X\}.$$

As first observed by Grothendieck, there are canonical isomorphisms

$$\mathbf{M}\big(\mathbf{X}(S)\big) \cong S, \qquad \mathbf{X}\big(\mathbf{M}(X)\big) \cong X,$$

so that the functors $\mathbf{M}$ and $\mathbf{X}$ define an anti-equivalence of categories

$$\mathsf{Set}_\Gamma \equiv \mathsf{Ét}_F \tag{2.1}$$

(see [6, Proposition (4.3), p. 25] or [11, (18.4)]). Under this anti-equivalence, the cardinality of Γ-sets corresponds to the dimension of étale F-algebras, the disjoint union $\sqcup$ in Set_Γ corresponds to the product $\times$ in $\mathsf{Ét}_F$, and the product $\times$ in Set_Γ to the tensor product $\otimes$ in $\mathsf{Ét}_F$. For any integer $n \geq 1$, we let $\mathsf{Ét}_F^n$ denote the groupoid[1] whose objects are n-dimensional étale F-algebras and whose morphisms

[1] A groupoid is a category in which all morphisms are isomorphisms.

are F-algebra isomorphisms, and Set_Γ^n the groupoid of Γ-sets with n elements. The anti-equivalence (2.1) restricts to an anti-equivalence $\mathsf{Set}_\Gamma^n \equiv \acute{\mathsf{E}}\mathsf{t}_F^n$. The split étale algebra F^n corresponds to the Γ-set $\boldsymbol{n}$ of n elements with trivial Γ-action. Étale algebras of dimension 2 are also called *quadratic* étale algebras.

A morphism[2] of Γ-sets $Y \xleftarrow{\pi} Z$ is called a Γ-*covering* if the number of elements in each fiber $y^{\pi^{-1}} \subset Z$ does not depend on $y \in Y$. This number is called the *degree* of the covering. For n, $d \geq 1$ we let $\mathsf{Cov}_\Gamma^{d/n}$ denote the groupoid whose objects are coverings of degree d of a Γ-set of n elements and whose morphisms are isomorphisms of Γ-coverings.

A homomorphism $S \xrightarrow{\varepsilon} T$ of étale F-algebras is said to be an *extension of degree d of étale algebras* if ε endows T with a structure of a free S-module of rank d. This corresponds under the anti-equivalence (2.1) to a *covering of degree d*:

$$\mathbf{X}(S) \xleftarrow{\mathbf{X}(\varepsilon)} \mathbf{X}(T)$$

(see [13]). Let $\acute{\mathsf{E}}\mathsf{tex}_F^{d/n}$ denote the groupoid of étale extensions $S \xrightarrow{\varepsilon} T$ of degree d of F-algebras with $\dim_F S = n$ (hence $\dim_F T = dn$). From (2.1) we obtain an anti-equivalence of groupoids

$$\acute{\mathsf{E}}\mathsf{tex}_F^{d/n} \equiv \mathsf{Cov}_\Gamma^{d/n}.$$

The Γ-covering with trivial Γ-action

$$\boldsymbol{d}/\boldsymbol{n}: \quad \boldsymbol{n} \xleftarrow{p_1} \boldsymbol{n} \times \boldsymbol{d} \tag{2.2}$$

where p_1 is the first projection corresponds to the extension $F^n \to (F^d)^n$.

Of particular importance in the sequel are coverings of degree 2, which are also called *double coverings*. Each such covering $Y \xleftarrow{\pi} Z$ defines a canonical automorphism $Z \xleftarrow{\sigma} Z$ of order 2, which interchanges the elements in each fiber of π. Clearly, this automorphism has no fixed points. Conversely, if Z is any Γ-set and $Z \xleftarrow{\sigma} Z$ is an automorphism of order 2 without fixed points, the set of orbits

$$Z/\sigma = \big\{\{z, z^\sigma\} \mid z \in Z\}$$

is a Γ-set and the canonical map $(Z/\sigma) \leftarrow Z$ is a double covering. An *involution* of a Γ-set with an even number of elements is any automorphism of order 2 without fixed points.

Let $\sigma\colon S \to S$ be an automorphism of order 2 of an étale F-algebra S, and let $S^\sigma \subset S$ denote the F-sub-algebra of fixed elements, which is necessarily étale. The following conditions are equivalent (see [13]):

(a) the inclusion $S^\sigma \to S$ is a quadratic étale extension of F-algebras;
(b) the automorphism $\mathbf{X}(\sigma)$ is an involution on $\mathbf{X}(S)$.

We say under these equivalent conditions that the automorphism σ is an *involution* of the étale F-algebra S.

[2]We let morphisms of Γ-sets act on the right of the arguments (with the exponential notation) and use the usual function notation for morphisms in the anti-equivalent category of étale algebras.

Basic constructions on Γ-sets. We recall from [11, §18] and [12, §2.1] the construction of the discriminant $\Delta(X)$ of a Γ-set X with $|X| = n \geq 2$. Consider the set of n-tuples of elements in X:

$$\Sigma_n(X) = \{(x_1, \dots, x_n) \mid X = \{x_1, \dots, x_n\}\}.$$

This Γ-set carries an obvious transitive (right) action of the symmetric group $\mathfrak{S}_n$. The *discriminant* $\Delta(X)$ is the set of orbits under the alternating group $\mathfrak{A}_n$:

$$\Delta(X) = \Sigma_n(X)/\mathfrak{A}_n.$$

It is a Γ-set of two elements, so Δ is a functor

$$\Delta\colon \mathsf{Set}_\Gamma^n \to \mathsf{Set}_\Gamma^2.$$

For any covering $Z_0 \xleftarrow{\pi} Z$ of degree 2 with $|Z_0| = n$, (hence $|Z| = 2n$), we consider the set of (not necessarily Γ-equivariant) sections of π:

$$C(Z/Z_0) = \big\{\{z_1, \dots, z_n\} \subset Z \mid \{z_1^\pi, \dots, z_n^\pi\} = Z_0\big\}.$$

It is a Γ-set with 2^n elements, so C is a functor

$$C\colon \mathsf{Cov}_\Gamma^{2/n} \to \mathsf{Set}_\Gamma^{2^n},$$

called the *Clifford functor* (see [13]). The Γ-set $C(Z/Z_0)$ is equipped with a canonical surjective morphism

$$\Delta(Z) \xleftarrow{\delta} C(Z/Z_0), \tag{2.3}$$

which is defined in [12, §2.2] as follows: let $\sigma\colon Z \to Z$ be the involution canonically associated to the double covering $Z_0 \xleftarrow{\pi} Z$, so the fiber of z^π is $\{z, z^\sigma\}$ for each $z \in Z$; then δ maps each section $\{z_1, \dots, z_n\}$ to the $\mathfrak{A}_{2n}$-orbit of the $2n$-tuple $(z_1, \dots, z_n, z_1^\sigma, \dots, z_n^\sigma)$,

$$\{z_1, \dots, z_n\}^\delta = (z_1, \dots, z_n, z_1^\sigma, \dots, z_n^\sigma)^{\mathfrak{A}_{2n}}.$$

Note that the canonical involution σ induces an involution $\underline{\sigma}$ on $C(Z/Z_0)$, which maps each section ω to its complement $Z \backslash \omega$. We may view $C(Z/Z_0)$ as a covering of degree 2 of the set of orbits $C(Z/Z_0)/\underline{\sigma}$, and thus consider the Clifford construction as a functor

$$C\colon \mathsf{Cov}_\Gamma^{2/n} \to \mathsf{Cov}_\Gamma^{2/2^{n-1}}. \tag{2.4}$$

Proposition 2.5. *For sections ω, $\omega' \in C(Z/Z_0)$, we have $\omega^\delta = (\omega')^\delta$ if and only if $|\omega \cap \omega'| \equiv n \bmod 2$. Moreover, denoting by ι the nontrivial automorphism of $\Delta(Z)$, we have*

$$\underline{\sigma} \circ \delta = \begin{cases} \delta & \text{if } n \text{ is even,} \\ \delta \circ \iota & \text{if } n \text{ is odd.} \end{cases}$$

Proof. Let $\omega = \{z_1, \dots, z_n\}$ and $\omega' = \{z_1, \dots, z_r, z_{r+1}^\sigma, \dots, z_n^\sigma\}$, so $r = |\omega \cap \omega'|$,

$$\omega^\delta = (z_1, \dots, z_n, z_1^\sigma, \dots, z_n^\sigma)^{\mathfrak{A}_{2n}}$$

and

$$(\omega')^\delta = (z_1, \dots, z_r, z_{r+1}^\sigma, \dots, z_n^\sigma, z_1^\sigma, \dots, z_r^\sigma, z_{r+1}, \dots, z_n)^{\mathfrak{A}_{2n}}.$$

The permutation σ' that interchanges z_i and z_i^σ for $i = r+1, \dots, n$ satisfies

$$(z_1, \dots, z_n, z_1^\sigma, \dots, z_n^\sigma)^{\sigma'} = (z_1, \dots, z_r, z_{r+1}^\sigma, \dots, z_n^\sigma, z_1^\sigma, \dots, z_r^\sigma, z_{r+1}, \dots, z_n);$$

it is in $\mathfrak{A}_{2n}$ if and only if $n-r$ is even, which means $|\omega \cap \omega'| \equiv n \bmod 2$. For $\omega' = \omega^{\underline{\sigma}}$ the complement of ω we have $|\omega \cap \omega^{\underline{\sigma}}| = 0$, hence $\omega^{\underline{\sigma}\delta} = \omega^{\delta}$ if and only if $n \equiv 0 \bmod 2$. □

Oriented Γ-sets. An *oriented* Γ*-set* is a pair (Z, ∂_Z) where Z is a Γ-set and ∂_Z is a fixed isomorphism of Γ-sets $\mathbf{2} \xleftarrow{\sim} \Delta(Z)$. In particular the Γ-action on $\Delta(Z)$ is trivial. There are two possible choices for ∂_Z. A choice is an *orientation of* Z. Oriented Γ-sets with n elements form a groupoid $(\mathsf{Set}^n_\Gamma)^+$ whose morphisms are isomorphisms $Z_2 \xleftarrow{f} Z_1$ such that $\Delta(f) \circ \partial_{Z_2} = \partial_{Z_1}$. Similarly *oriented coverings* are pairs $(Z/Z_0, \partial_Z)$ where $Z_0 \leftarrow Z$ is a Γ-covering and ∂_Z is an orientation of Z. We denote by $(\mathsf{Cov}^{d/n}_\Gamma)^+$ the groupoid of oriented coverings of degree d of Γ-sets with n elements. Changing the orientation through the twist $\mathbf{2} \xleftarrow{\iota} \mathbf{2}$ defines an involutive functor

$$\kappa\colon (\mathsf{Cov}^{d/n}_\Gamma)^+ \to (\mathsf{Cov}^{d/n}_\Gamma)^+.$$

Proposition 2.6. *If n is even the functor $C\colon \mathsf{Cov}^{2/n}_\Gamma \to \mathsf{Cov}^{2/2^{n-1}}_\Gamma$ of* (2.4) *restricts to a pair of functors*

$$C_1,\, C_2\colon (\mathsf{Cov}^{2/n}_\Gamma)^+ \to \mathsf{Cov}^{2/2^{n-2}}_\Gamma.$$

Moreover two sections ω and ω' of the oriented Γ-covering $(Z/Z_0, \partial_Z)$ lie in the same set $C_1(Z/Z_0, \partial_Z)$ or $C_2(Z/Z_0, \partial_Z)$ if and only if $|\omega \cap \omega'| \equiv 0 \mod 2$.

Proof. Let Z/Z_0 be a $2/n$-covering. Proposition 2.5 implies that the covering $\Delta(Z) \xleftarrow{\delta} C(Z/Z_0)$ factors through $C(Z/Z_0)/\underline{\sigma}$, where $\underline{\sigma}$ is the canonical involution of $C(Z/Z_0)$:

$$\Delta(Z) \leftarrow C(Z/Z_0)/\underline{\sigma} \leftarrow C(Z/Z_0).$$

Thus, if Z/Z_0 is oriented, we may use the given isomorphism $\mathbf{2} \xleftarrow{\partial_Z} \Delta(Z)$ to define the Γ-sets

$$C_1(Z/Z_0, \partial_Z) = \{\omega \in C(Z/Z_0) \mid \omega^{\delta\partial_Z} = 1\}$$

and

$$C_2(Z/Z_0, \partial_Z) = \{\omega \in C(Z/Z_0) \mid \omega^{\delta\partial_Z} = 2\}.$$

Obviously, we have $C(Z/Z_0) = C_1(Z/Z_0, \partial_Z) \sqcup C_2(Z/Z_0, \partial_Z)$, and Proposition 2.5 shows that $\underline{\sigma}$ restricts to involutions on $C_1(Z/Z_0, \partial_Z)$ and $C_2(Z/Z_0, \partial_Z)$. The last claim also follows from Proposition 2.5. □

We call the two functors C_1 and C_2 the *spinor functors.* Note that when n is even an orientation ∂_Z on Z/Z_0 can also be defined by specifying whether a given section $\omega \in C(Z/Z_0)$ lies in $C_1(Z/Z_0, \partial_Z)$ or $C_2(Z/Z_0, \partial_Z)$. Indeed, $\omega \in C_1(Z/Z_0, \partial_Z)$ if and only if $\omega^\delta \in \Delta(Z)$ is mapped to 1, which determines ∂_Z uniquely. We shall avail ourselves of this possibility to define orientations on coverings in $\mathsf{Cov}^{2/4}_\Gamma$ in §4.

Basic constructions on étale algebras. We now consider analogues of the functors Δ and C for étale algebras and étale extensions.

For S an étale F-algebra of dimension $n \geq 2$, the discriminant $\Delta(S)$ is a quadratic étale F-algebra such that

$$\mathbf{X}\big(\Delta(S)\big) = \Delta\big(\mathbf{X}(S)\big).$$

We thus have a functor

$$\Delta\colon \mathsf{\acute{E}t}_F^n \to \mathsf{\acute{E}t}_F^2 \qquad \text{for } n \geq 2.$$

If the field F has characteristic different from 2, it is usual to represent $\Delta(S)$ as $F[x]/\big(x^2 - \operatorname{Disc}(S)\big)$, $\operatorname{Disc}(S) \in F^\times$, and the class of $\operatorname{Disc}(S)$ in $F^\times/(F^\times)^2$ is the usual discriminant. We refer to [11, p. 291–293] and [12, §3.1] for details.
Let $S \xrightarrow{\varepsilon} T$ be an étale extension of degree 2 of (étale) F-algebras, with $\dim_F S = n$, $\dim_F T = 2n$. In [12, §3.2][3] we define an étale F-algebra $C(T/S)$ such that

$$\mathbf{X}\big(C(T/S)\big) = C\big(\mathbf{X}(T)/\,\mathbf{X}(S)\big).$$

Example 2.7. If $\dim_F T = 2$ and $S = F$, we have $C(T/S) = T$.
For S_1, S_2 étale algebras of arbitrary dimension, and for arbitrary étale extensions T_1/S_1 and T_2/S_2 of degree 2, there is a canonical isomorphism

$$P\colon C\big((T_1 \times T_2)/(S_1 \times S_2)\big) \;\xrightarrow{\sim}\; C(T_1/S_1) \otimes C(T_2/S_2).$$

We call the 2^n-dimensional algebra $C(T/S)$ the *Clifford algebra* of T/S. It admits a canonical involution $\underline{\sigma}$. If $\dim_F S$ is even $\underline{\sigma}$ is the identity on $\Delta(T)$. The canonical morphism δ of (2.3)

$$\Delta\big(\mathbf{X}(T)\big) \xleftarrow{\delta} C\big(\mathbf{X}(T)/\,\mathbf{X}(S)\big)$$

yields a canonical F-algebra homomorphism which we again denote by δ,

$$\Delta(T) \xrightarrow{\delta} C(T/S),$$

so that $C(T/S)$ is an étale extension of degree 2^{n-1} of a quadratic étale F-algebra.

Oriented étale algebras. As for oriented Γ-sets we define *oriented étale algebras* as pairs (S, ∂_S) where S is an étale algebra and $\partial_S\colon \Delta(S) \xrightarrow{\sim} F \times F$ is an isomorphism of F-algebras. *Oriented extensions of étale algebras* are pairs $(S/S_0, \partial_S)$ where S/S_0 is an extension of étale algebras and $\partial_S\colon \Delta(S) \xrightarrow{\sim} F \times F$ is an isomorphism of F-algebras. We have corresponding groupoids $(\mathsf{\acute{E}t}_F^n)^+$, $(\mathsf{\acute{E}tex}_F^{d/n})^+$ and anti-equivalences

$$(\mathsf{Set}_\Gamma^n)^+ \equiv (\mathsf{\acute{E}t}_F^n)^+ \text{ and } (\mathsf{Cov}_\Gamma^{d/n})^+ \equiv (\mathsf{\acute{E}tex}_F^{d/n})^+.$$

Switching the orientation induces an involutive functor κ on these groupoids.
The Clifford functor C restricts to a pair of *spinor functors*

$$C_1, C_2\colon (\mathsf{\acute{E}tex}_F^{2/n})^+ \to \mathsf{\acute{E}tex}_F^{2/2^{n-2}} \tag{2.8}$$

if n is even.

Remark 2.9. The terminology used above owes its origin to the fact that the Clifford functor is related to the theory of Clifford algebras in the framework of quadratic forms and central simple algebras with involution. We refer to [13] for details and more properties of the Clifford construction.

[3]The notation Ω is used for C in [12].

3. Cohomology

For any integer $n \geq 1$, we consider the Γ-set $\boldsymbol{n} = \{1, \dots, n\}$ with the trivial Γ-action and let $\mathfrak{S}_n$ denote the symmetric group on $\boldsymbol{n}$, i.e., the automorphism group of $\boldsymbol{n}$,

$$\mathfrak{S}_n = \mathrm{Aut}(\boldsymbol{n}).$$

Recall from [11, §28.A] that the cohomology set $H^1(\Gamma, \mathfrak{S}_n)$ (for the trivial action of Γ on $\mathfrak{S}_n$) is the set of continuous group homomorphisms $\Gamma \to \mathfrak{S}_n$ ("cocycles") up to conjugation.
Letting $\mathrm{Iso}(\mathsf{Set}_\Gamma^n)$ denote the set of isomorphism classes in Set_Γ^n, we have a canonical bijection of pointed sets

$$\mathrm{Iso}(\mathsf{Set}_\Gamma^n) \xrightarrow{\sim} H^1(\Gamma, \mathfrak{S}_n). \tag{3.1}$$

Cohomology sets can also be used to describe isomorphism classes of Γ-coverings: for any integers n, $d \geq 1$, the group of automorphisms of the Γ-covering with trivial Γ-action $\boldsymbol{d}/\boldsymbol{n}$ is the wreath product (of order $(d!)^n n!$)

$$\mathrm{Aut}(\boldsymbol{d}/\boldsymbol{n}) = \mathfrak{S}_d \wr \mathfrak{S}_n \quad (= \mathfrak{S}_d^n \rtimes \mathfrak{S}_n).$$

The same construction as above yields a canonical bijection

$$\mathrm{Iso}(\mathsf{Cov}_\Gamma^{d/n}) \xrightarrow{\sim} H^1(\Gamma, \mathfrak{S}_d \wr \mathfrak{S}_n), \tag{3.2}$$

where the Γ-action on $\mathfrak{S}_d \wr \mathfrak{S}_n$ is trivial; see [12, §4.2]. The automorphism group of the oriented Γ-covering $(\boldsymbol{d}/\boldsymbol{n}, \partial_{\boldsymbol{n}\times\boldsymbol{d}})$ is the group

$$(\mathfrak{S}_d \wr \mathfrak{S}_n)^+ = (\mathfrak{S}_d \wr \mathfrak{S}_n) \cap \mathfrak{A}_{dn}$$

so that

$$\mathrm{Iso}\big((\mathsf{Cov}_\Gamma^{d/n})^+\big) \xrightarrow{\sim} H^1\big(\Gamma, (\mathfrak{S}_d \wr \mathfrak{S}_n)^+\big). \tag{3.3}$$

We now assume that Γ is the absolute Galois group $\Gamma = \mathrm{Gal}(F_s/F)$ of a field F and use the notation $H^1(F, \mathfrak{S}_n)$ for $H^1(\Gamma, \mathfrak{S}_n)$. The anti-equivalence $\mathsf{Set}_\Gamma^n \equiv \mathsf{\acute{E}t}_F^n$ and the bijection (3.1) induce canonical bijections

$$\mathrm{Iso}(\mathsf{\acute{E}t}_F^n) \cong \mathrm{Iso}(\mathsf{Set}_\Gamma^n) \cong H^1(F, \mathfrak{S}_n)$$

The bijection $\mathrm{Iso}(\mathsf{\acute{E}t}_F^n) \cong H^1(F, \mathfrak{S}_n)$ may of course also be defined directly since

$$\mathrm{Aut}_{F\text{-alg}}(F^n) \cong \mathfrak{S}_n,$$

see [11, (29.9)]. Similarly, it follows from (3.2), (3.3), and the anti-equivalence of groupoids $\mathsf{\acute{E}tex}_F^{d/n} \equiv \mathsf{Cov}_\Gamma^{d/n}$, $(\mathsf{\acute{E}tex}_F^{d/n})^+ \equiv (\mathsf{Cov}_\Gamma^{d/n})^+$, that we have canonical bijections of pointed sets:

$$\mathrm{Iso}(\mathsf{\acute{E}tex}_\Gamma^{d/n}) \cong \mathrm{Iso}(\mathsf{Cov}_\Gamma^{d/n}) \cong H^1(F, \mathfrak{S}_d \wr \mathfrak{S}_n) \tag{3.4}$$

and

$$\mathrm{Iso}\big((\mathsf{\acute{E}tex}_\Gamma^{d/n})^+\big) \cong \mathrm{Iso}\big((\mathsf{Cov}_\Gamma^{d/n})^+\big) \cong H^1\big(F, (\mathfrak{S}_d \wr \mathfrak{S}_n)^+\big). \tag{3.5}$$

Remark 3.6. Any group homomorphism $\varphi\colon G \to H$, where G and H are automorphism groups of finite sets or of finite double coverings, induces a map on the level of cocycles $\varphi_*\colon (\gamma\colon \Gamma \to G) \mapsto (\varphi \circ \gamma\colon \Gamma \to H)$. Thus φ associates in a "canonical way" an étale algebra (or an étale algebra with involution) E_φ, whose isomorphism class belongs to $H^1(F, H)$, to an étale algebra E (or an étale algebra E with involution), whose class belongs to $H^1(F, G)$. We say that the algebra E_φ is a *resolvent* of E. For example the discriminant $\Delta(E)$ is the resolvent of E associated to the parity map $\mathfrak{S}_n \to \mathfrak{S}_2$. Other examples of resolvents will be discussed in relation with triality.

4. Triality and Γ-coverings

Recall the functor C, which associates to any double covering its set of sections. For oriented 2/4-coverings of Γ-sets, it leads to two functors

$$C_1,\ C_2\colon (\mathsf{Cov}_\Gamma^{2/4})^+ \to \mathsf{Cov}_\Gamma^{2/4},$$

see Proposition 2.6. The functors C_1 and C_2 together with the functor κ, which changes the orientation, give an explicit description of an action of the group $\mathfrak{S}_3$ on the pointed set $\mathrm{Iso}\big((\mathsf{Cov}_\Gamma^{2/4})^+\big)$.

Theorem 4.1. *The functors C_1, $C_2\colon (\mathsf{Cov}_\Gamma^{2/4})^+ \to \mathsf{Cov}_\Gamma^{2/4}$ factor through the forgetful functor $\mathcal{F}\colon (\mathsf{Cov}_\Gamma^{2/4})^+ \to \mathsf{Cov}_\Gamma^{2/4}$, i.e., there are functors*

$$C_1^+,\ C_2^+\colon (\mathsf{Cov}_\Gamma^{2/4})^+ \to (\mathsf{Cov}_\Gamma^{2/4})^+$$

such that $\mathcal{F}\circ C_i^+ = C_i$ for $i=1$, 2. These functors satisfy natural equivalences:

$$(C_1^+)^3 = \mathrm{Id}, \qquad (C_1^+)^2 = C_2, \qquad C_1^+\kappa = \kappa C_2^+.$$

Proof. Let $(Z/Z_0,\partial)$ be an object in $(\mathsf{Cov}_\Gamma^{2/4})^+$ and let σ denote the involution of Z/Z_0. Consider a real vector space V with basis (e_1,e_2,e_3,e_4). Fixing a bijection φ between a section $\omega\in C_1(Z/Z_0,\partial)$ and $\{e_1,\dots,e_4\}$, we identify Z with a subset of V by

$$z\mapsto \begin{cases} z^\varphi & \text{if } z\in\omega,\\ -z^{\sigma\varphi} & \text{if } z\notin\omega.\end{cases}$$

Thus, $Z=\{\pm e_1,\pm e_2,\pm e_3,\pm e_4\}$ and σ acts on Z by mapping each element to its opposite. The action of Γ on Z extends to a linear action on V since it commutes with σ. We also identify $C(Z/Z_0)$ with a subset of V by the map

$$\omega'\mapsto \tfrac12\sum_{z\in\omega'} z.$$

The set $C(Z/Z_0)$ then consists of the following vectors and their opposite:

$$\begin{aligned}
f_1 &= \tfrac12(e_1+e_2+e_3+e_4) & g_1 &= \tfrac12(e_1+e_2+e_3-e_4),\\
f_2 &= \tfrac12(e_1+e_2-e_3-e_4) & g_2 &= \tfrac12(e_1+e_2-e_3+e_4),\\
f_3 &= \tfrac12(e_1-e_2+e_3-e_4) & g_3 &= \tfrac12(e_1-e_2+e_3+e_4),\\
f_4 &= \tfrac12(-e_1+e_2+e_3-e_4) & g_4 &= \tfrac12(e_1-e_2-e_3-e_4).
\end{aligned}$$

Since $\omega\in C_1(Z/Z_0,\partial)$, we have (see Proposition 2.6

$$C_1(Z/Z_0,\partial)=\{\pm f_1,\pm f_2,\pm f_3,\pm f_4\}$$

and

$$C_2(Z/Z_0,\partial)=\{\pm g_1,\pm g_2,\pm g_3,\pm g_4\}.$$

The canonical involutions on $C_1(Z/Z_0,\partial)$ and $C_2(Z/Z_0,\partial)$ map each vector to its opposite. Note that these identifications are independent of the choice of the section ω in $C_1(Z/Z_0,\partial)$ and of the bijection φ.

Let ∂_1 be the orientation of $C_1(Z/Z_0,\partial)$ such that $C_1(C_1(Z/Z_0,\partial),\partial_1)$ contains the section $\{f_1,f_2,f_3,f_4\}$. Thus, by Proposition 2.6, $C_1(C_1(Z/Z_0,\partial),\partial_1)$ consists of the following sections:

$$\pm\{f_1,f_2,f_3,f_4\},\ \pm\{f_1,f_2,-f_3,-f_4\},\ \pm\{f_1,-f_2,f_3,-f_4\},\ \pm\{-f_1,f_2,f_3,-f_4\}.$$

They are characterized by the property that for each $i=1,\ldots,4$ they contain a section $\pm f_j$ containing e_i and a section $\pm f_k$ containing $-e_i$. Identifying these sections to vectors in V as above, we obtain

$$\begin{aligned}C_1(C_1(Z/Z_0,\partial),\partial_1)=\{&\pm\tfrac{1}{2}(f_1+f_2+f_3+f_4),\pm\tfrac{1}{2}(f_1+f_2-f_3-f_4),\\ &\pm\tfrac{1}{2}(f_1-f_2+f_3-f_4),\pm\tfrac{1}{2}(-f_1+f_2+f_3-f_4)\}.\end{aligned}$$

Likewise, let ∂_2 be the orientation of $C_2(Z/Z_0,\partial)$ such that

$$\begin{aligned}C_1(C_2(Z/Z_0,\partial),\partial_2)=\{&\pm\tfrac{1}{2}(g_1+g_2+g_3+g_4),\pm\tfrac{1}{2}(g_1+g_2-g_3-g_4),\\ &\pm\tfrac{1}{2}(g_1-g_2+g_3-g_4),\pm\tfrac{1}{2}(-g_1+g_2+g_3-g_4)\}.\end{aligned}$$

Define the functors C_1^+, $C_2^+\colon (\mathsf{Cov}_\Gamma^{2/4})^+\to(\mathsf{Cov}_\Gamma^{2/4})^+$ by

$$C_1^+(Z/Z_0,\partial)=(C_1(Z/Z_0),\partial_1)\qquad\text{and}\qquad C_2^+(Z/Z_0,\partial)=(C_2(Z/Z_0),\partial_2).$$

By definition, it is clear that $\mathcal{F}\circ C_i^+=C_i$ for $i=1$, 2. To establish the natural equivalences, consider the linear map $\mu\colon V\to V$ defined by $\mu(e_i)=f_i$ for $i=1$, $\ldots$, 4. Using this map, we may rephrase the definition of C_1^+ as follows: for $Z=\{\pm e_1,\pm e_2,\pm e_3,\pm e_4\}$ with the orientation ∂ such that $C_1(Z/Z_0,\partial)\ni\mu(e_1)$, we have

$$C_1^+(Z/Z_0,\partial)=\{\pm\mu(e_1),\pm\mu(e_2),\pm\mu(e_3),\pm\mu(e_4)\}$$

with the orientation such that

$$C_1\big(C_1^+(Z/Z_0,\partial)\big)\ni\tfrac{1}{2}\big(\mu(e_1)+\mu(e_2)+\mu(e_3)+\mu(e_4)\big).$$

Note that $\frac{1}{2}\big(\mu(e_1)+\mu(e_2)+\mu(e_3)+\mu(e_4)\big)=\mu(f_1)=\mu^2(e_1)$. Therefore, substituting $\mu(e_i)$ for e_i, for $i=1,\ldots,4$, we obtain

$$(C_1^+)^2(Z/Z_0,\partial)=\{\pm\mu^2(e_1),\pm\mu^2(e_2),\pm\mu^2(e_3),\pm\mu^2(e_4)\},$$

endowed with an orientation such that

$$C_1\big((C_1^+)^2(Z/Z_0,\partial)\big)\ni\mu^3(e_1).$$

Computation shows that $\mu^2(e_i)=g_i$ for $i=1,\ldots,4$, and $\mu^3=\mathrm{Id}$. Since $\frac{1}{2}(g_1+g_2+g_3+g_4)=e_1$, it follows that $(C_1^+)^2(Z/Z_0,\partial)=C_2^+(Z/Z_0,\partial)$. Similarly, we have

$$(C_1^+)^3(Z/Z_0,\partial)=\{\pm\mu^3(e_1),\pm\mu^3(e_2),\pm\mu^3(e_3),\pm\mu^3(e_4)\}=Z,$$

endowed with an orientation such that

$$C_1\big((C_1^+)^3(Z/Z_0,\partial)\big)\ni\mu^4(e_1)=f_1,$$

hence $(C_1^+)^3(Z/Z_0,\partial)=(Z/Z_0,\partial)$. Finally, we have

$$\kappa(Z/Z_0,\partial)=\{\pm e_1,\pm e_2,\pm e_3,\pm e_4\}$$

with an orientation such that $C_1\kappa(Z/Z_0,\partial)\ni\mu^2(e_1)$, hence

$$C_1^+\kappa(Z/Z_0,\partial)=\{\pm\mu^2(e_1),\pm\mu^2(e_2),\pm\mu^2(e_3),\pm\mu^2(e_4)\}$$

endowed with an orientation such that

$$C_1\big(C_1^+\kappa(Z/Z_0,\partial)\big)\ni\mu^4(e_1)=f_1.$$

Therefore, $C_1^+\kappa(Z/Z_0,\partial) = \kappa C_2^+(Z/Z_0,\partial)$. □

Remark 4.2. The decomposition $C(Z/Z_0) = C_1(Z/Z_0,\partial) \sqcup C_2(Z/Z_0,\partial)$ can also be viewed geometrically on a hypercube: suppose $V = \mathbb{R}^4$ and let (e_1, e_2, e_3, e_4) be the standard basis. The set

$$C(Z/Z_0) = \{\tfrac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4)\}$$

is the set of vertices of a hypercube $\mathcal{K}$ (see Figure 1), and the set

$$Z = \{\pm e_1, \pm e_2, \pm e_3, \pm e_4\}$$

is in bijection with the set of 3-dimensional cells of $\mathcal{K}$.

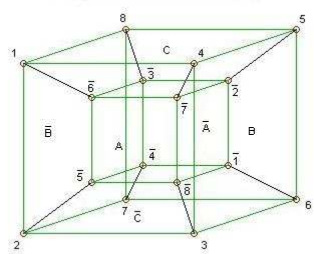


Figure 1

We identify

$$Z = \{A, \bar{A}, B, \bar{B}, C, \bar{C}, D, \bar{D}\}$$

where $A, \dots, \bar{C}$ are as in Figure 1, D is the big cell and $\bar{D}$ the small cell inside. The involution permutes a cell with its opposite cell and the set Z_0 is obtained by identifying pairs of opposite cells

$$Z_0 = \{\{A, \bar{A}\}, \{B, \bar{B}\}, \{C, \bar{C}\}, \{D, \bar{D}\}\}.$$

To obtain a corresponding identification of $C(Z/Z_0)$ with the set of vertices of $\mathcal{K}$, observe that a section of Z/Z_0 consists of a set of four cells which are pairwise not opposite. Four such cells intersect in exactly one vertex and conversely each vertex lies in four cells. With the notation in Figure 1 we have the following identification:

$$\begin{array}{llll}
1 = \{A, \bar{B}, C, D\} & \bar{1} = \{\bar{A}, B, \bar{C}, \bar{D}\} & 2 = \{A, \bar{B}, \bar{C}, D\} & \bar{2} = \{\bar{A}\ B, C, \bar{D}\} \\
3 = \{A, B, \bar{C}, D\} & \bar{3} = \{\bar{A}, \bar{B}, C, \bar{D}\} & 4 = \{A, B, C, D\} & \bar{4} = \{\bar{A}, \bar{B}, \bar{C}, \bar{D}\} \\
5 = \{\bar{A}, B, C, D\} & \bar{5} = \{A, \bar{B}, \bar{C}, \bar{D}\} & 6 = \{\bar{A}, B, \bar{C}, D\} & \bar{6} = \{A, \bar{B}, C, \bar{D}\} \\
7 = \{\bar{A}, \bar{B}, \bar{C}, D\} & \bar{7} = \{A, B, C, \bar{D}\} & 8 = \{\bar{A}, \bar{B}, C, D\} & \bar{8} = \{A, B, \bar{C}, \bar{D}\}
\end{array}$$

This set of vertices decomposes into two classes, two vertices being in the same class if the number of edges in any path connecting them is even. One class is

$$X = \{1, \bar{1}, 3, \bar{3}, 5, \bar{5}, 7, \bar{7}\}$$

and the other

$$Y = \{2, \bar{2}, 4, \bar{4}, 6, \bar{6}, 8, \bar{8}\}.$$

We get coverings X/X_0 and Y/Y_0 by identifying opposite vertices v and $\bar{v}$. If $\Delta(Z) \simeq \mathbf{2}$, the decomposition of $C(Z/Z_0)$ as the disjoint union $X/X_0 \sqcup Y/Y_0$ is Γ-compatible; the functors C_1 and C_2 are given (up to a possible permutation) by the rule

$$C_1(Z/Z_0,\partial) = X/X_0 \qquad \text{and} \qquad C_2(Z/Z_0,\partial) = Y/Y_0.$$

A section of X/X_0 is a set of four vertices in X which are pairwise not opposite. Four such vertices either lie on a 3-dimensional cell or are adjacent to exactly one vertex in the complementary set Y. A similar claim holds for a section of Y/Y_0. This leads to identifying:

$$\begin{array}{ll} A=\{1,3,\bar5,\bar7\}=\{2,4,\bar6,\bar8\} & \bar A=\{\bar1,\bar3,5,7\}=\{\bar2,\bar4,6,8\}\\ B=\{\bar1,3,5,\bar7\}=\{\bar2,4,6,\bar8\} & \bar B=\{1,\bar3,\bar5,7\}=\{2,\bar4,\bar6,8\}\\ C=\{1,\bar3,5,\bar7\}=\{\bar2,4,\bar6,8\} & \bar C=\{\bar1,3,\bar5,7\}=\{2,\bar4,6,\bar8\}\\ D=\{1,3,5,7\}=\{2,4,6,8\} & \bar D=\{\bar1,\bar3,\bar5,\bar7\}=\{\bar2,\bar4,\bar6,\bar8\} \end{array} \tag{4.3}$$

and

$$\begin{array}{ll} 1=\{A,\bar B,C,D\}=\{2,4,\bar6,8\} & \bar1=\{\bar A,B,\bar C,\bar D\}=\{\bar2,\bar4,6,\bar8\}\\ 3=\{A,B,\bar C,D\}=\{2,4,6,\bar8\} & \bar3=\{\bar A,\bar B,C,\bar D\}=\{\bar2,\bar4,\bar6,8\}\\ 5=\{\bar A,B,C,D\}=\{\bar2,4,6,8\} & \bar5=\{A,\bar B,\bar C,\bar D\}=\{2,\bar4,\bar6,\bar8\}\\ 7=\{\bar A,\bar B,\bar C,D\}=\{2,\bar4,6,8\} & \bar7=\{A,B,C,\bar D\}=\{\bar2,4,\bar6,\bar8\}\\[4pt] 2=\{A,\bar B,\bar C,D\}=\{1,3,\bar5,7\} & \bar2=\{\bar A,B,C,\bar D\}=\{\bar1,\bar3,5,\bar7\}\\ 4=\{A,B,C,D\}=\{1,3,5,\bar7\} & \bar4=\{\bar A,\bar B,\bar C,\bar D\}=\{\bar1,\bar3,\bar5,7\}\\ 6=\{\bar A,B,\bar C,D\}=\{\bar1,3,5,7\} & \bar6=\{A,\bar B,C,\bar D\}=\{1,\bar3,\bar5,\bar7\}\\ 8=\{\bar A,\bar B,C,D\}=\{1,\bar3,5,7\} & \bar8=\{A,B,\bar C,\bar D\}=\{\bar1,3,\bar5,\bar7\}, \end{array} \tag{4.4}$$

hence the existence of decompositions $C(X/X_0)=Y/Y_0\sqcup Z/Z_0$ and $C(Y/Y_0)=Z/Z_0\sqcup X/X_0$ which, in fact, are decompositions as Γ-sets.

Remark 4.5. In the proof of Theorem 4.1, μ is not the unique linear map that can be used to describe the C_1^+ and the C_2^+ construction. An alternative description uses Hurwitz' quaternions. Choosing for V the skew field of real quaternions $\mathbb{H}$ and for (e_1,e_2,e_3,e_4) the standard basis $(1,\, i,\, j,\, k)$, we have

$$Z=\{\pm1,\, \pm i,\, \pm j,\, \pm k\},\qquad C(Z/Z_0)=\{\tfrac12(\pm1\pm i\pm j\pm k)\},$$

so the union $Z\cup C(Z/Z_0)\subset\mathbb{H}$ is the group $\mathbb{H}^1$ of Hurwitz integral quaternions of norm 1. The element

$$\rho=-\tfrac12(1+i+j+k)$$

is of order 3 in $\mathbb{H}^1$ and conjugation by ρ permutes i, j and k cyclically. The set Z is in fact the underlying set of the quaternionic group $\mathfrak{Q}_8$ and

$$\mathbb{H}^1=\mathfrak{Q}_8\rtimes\mathfrak{C}_3$$

where the cyclic group of three elements $\mathfrak{C}_3$ operates on $\mathfrak{Q}_8$ via conjugation with ρ. If ∂ is the orientation of Z/Z_0 such that $\rho\in C_1(Z/Z_0,\partial)$, we have $C_1^+(Z/Z_0,\partial)=\rho\cdot Z$ with the orientation such that $\rho^2\in C_1\big(C_1^+(Z/Z_0,\partial)\big)$, and $C_2^+(Z/Z_0,\partial)=(C_1^+)^2(Z/Z_0,\partial)=\rho^2\cdot Z$ with the orientation such that $1\in C_1\big(C_2^+(Z/Z_0,\partial)\big)$. Note that, with respect to the standard basis, multiplication by ρ is given by the matrix

$$\rho=\frac12\begin{pmatrix}-1&1&1&1\\-1&-1&1&-1\\-1&-1&-1&1\\-1&1&-1&-1\end{pmatrix} \tag{4.6}$$

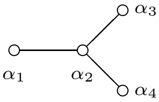
whereas the matrix of μ is

$$\mu=\frac12\begin{pmatrix}1&1&1&-1\\1&1&-1&1\\1&-1&1&1\\1&-1&-1&-1\end{pmatrix}. \tag{4.7}$$

5. The Weyl group of D_4

The Dynkin diagram D_4

(5.1)



has the permutation group $\mathfrak{S}_3$ as a group of automorphisms. The vertices of the diagram are labeled by the simple roots of the Lie algebra of type D_4. Let (e_1, e_2, e_3, e_4) be the standard orthonormal basis of the Euclidean space $\mathbb{R}^4$. The simple roots are

$$\alpha_1 = e_1 - e_2, \quad \alpha_2 = e_2 - e_3, \quad \alpha_3 = e_3 - e_4 \ \text{ and } \alpha_4 = e_3 + e_4$$

(see [3]). The permutation $\alpha_1 \mapsto \alpha_4,\ \alpha_4 \mapsto \alpha_3,\ \alpha_3 \mapsto \alpha_1,\ \alpha_2 \mapsto \alpha_2$ is an automorphism of order 3 of the Dynkin diagram. Its extension to a linear automorphism of $\mathbb{R}^4$ is given by the orthogonal matrix μ of (4.7). The matrix

$$\nu = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{5.2}$$

extends the automorphism $\alpha_1 \mapsto \alpha_1$, $\alpha_4 \mapsto \alpha_3$, $\alpha_3 \mapsto \alpha_4$, $\alpha_2 \mapsto \alpha_2$. The set $\{\mu, \nu\}$ generates a subgroup of O_4 isomorphic to $\mathfrak{S}_3$, which restricts to the automorphism group of the Dynkin diagram. The group

$$W(D_4) = (\mathfrak{S}_2 \wr \mathfrak{S}_4)^+ = \mathfrak{S}_2^3 \rtimes \mathfrak{S}_4$$

is the Weyl group of the split adjoint algebraic group PGO_8^+, which is of type D_4. The group $W(D_4) = \mathfrak{S}_2^3 \rtimes \mathfrak{S}_4$, as a subgroup of the orthogonal group O_4, is generated by the reflections with respect to the roots of the Lie algebra of PGO_8^+. Elements of $\mathfrak{S}_2 \wr \mathfrak{S}_4$ can be written as matrix products

$$w = D \cdot P(\pi), \tag{5.3}$$

where D is the diagonal matrix $\mathrm{Diag}(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$, $\varepsilon_i = \pm 1$, and $P(\pi)$ is the permutation matrix of $\pi \in \mathfrak{S}_4$. The group $\mathfrak{S}_2 \wr \mathfrak{S}_4$ fits into the exact sequence

$$1 \to \mathfrak{S}_2^4 \to \mathfrak{S}_2 \wr \mathfrak{S}_4 \xrightarrow{\beta} \mathfrak{S}_4 \to 1 \tag{5.4}$$

where β maps $w = D \cdot P(\pi)$ to π. Elements of $W(D_4)$ have a similar representation, with the supplementary condition $\prod_i \varepsilon_i = 1$.

In relation with the geometric description of C_1 and C_2 at the end of §4, note that the group $\mathfrak{S}_2 \wr \mathfrak{S}_4 = \mathfrak{S}_2^4 \rtimes \mathfrak{S}_4$ is the group of automorphisms of the hypercube $\mathcal{K}$. The subgroup $W(D_4) = (\mathfrak{S}_2 \wr \mathfrak{S}_4)^+ = \mathfrak{S}_2^3 \rtimes \mathfrak{S}_4$ consists of the automorphisms of $\mathcal{K}$ respecting the decomposition of the set of vertices as $X \sqcup Y$, i.e., automorphisms of the half-hypercube.

Automorphisms of $W(D_4)$. We view $W(D_4)$ as a subgroup of O_4 as in (5.3). Conjugation $x \mapsto \mu x \mu^{-1}$ with the matrices μ and ν on O_4 induce by restriction outer automorphisms $\tilde{\mu}$ and $\tilde{\nu}$ of $W(D_4)$. The set $\{\tilde{\mu}, \tilde{\nu}\}$ generates a group of automorphisms of $W(D_4)$ isomorphic to $\mathfrak{S}_3$ (see already [5, p. 368]). The center of $W(D_4)$ is isomorphic to $\mathfrak{S}_2$ and is generated by

$$w_0 = \mathrm{Diag}(-1, -1, -1, -1) = -1. \tag{5.5}$$

Thus $W(D_4)/\langle w_0\rangle$ acts on $W(D_4)$ as the group of inner automorphisms. Let ψ be the automorphism of order 2 of $W(D_4)$ given by

$$\psi\colon D\cdot P(\pi)\mapsto D\cdot P(\pi)\cdot (w_0)^{\mathrm{sgn}(\pi)},$$

or equivalently by $x\mapsto x\det(x)$, $x\in W(D_4)\subset \mathrm{O}_4$. A proof of the following result can be found in [8, Theorem 31,(5)] or in [7, Prop. 2.8,(e)]:

Proposition 5.6.

$$\mathrm{Aut}\big(W(D_4)\big)\simeq \big((W(D_4)/\langle w_0\rangle)\rtimes \mathfrak{S}_3\big)\times\langle\psi\rangle.$$

For any $w\in W(D_4)$, we let $\mathrm{Int}(w)\colon x\mapsto wxw^{-1}$ be the inner automorphism of $W(D_4)$ defined by conjugation by w, and by $\mathrm{Int}\big(W(D_4)\big)$ the group of inner automorphisms of $W(D_4)$. As an immediate consequence of Proposition 5.6, we have

Corollary 5.7.

$$\mathrm{Aut}\big(W(D_4)\big)/\,\mathrm{Int}\big(W(D_4)\big)\simeq \mathfrak{S}_3\times\langle\psi\rangle.$$

We call *trialitarian* the outer automorphisms of order 3 of $W(D_4)$. As observed above, the automorphisms $\tilde\mu$ and $\tilde\mu^2$ are trialitarian. Conjugation by the matrix ρ of (4.6) also yields a trialitarian automorphism $\tilde\rho$: indeed, we have $\rho^3=1$ and

$$\rho\mu^{-1}=-1\cdot\begin{pmatrix}0&0&0&1\\0&1&0&0\\1&0&0&0\\0&0&1&0\end{pmatrix}\in W(D_4);$$

hence, letting w be the matrix on the right side, we have $\tilde\rho=\mathrm{Int}(w)\circ\tilde\mu$.

Proposition 5.8. *Any trialitarian automorphism of $W(D_4)$ is conjugate in the group* $\mathrm{Aut}\big(W(D_4)\big)$ *to either $\tilde\mu$ or $\tilde\rho$.*

Proof. Explicit computation (with the help of the algebra computational system Magma [2]) shows that the conjugation class of $\tilde\rho$ contains 16 elements and the conjugation class of $\tilde\mu$ contains 32 elements. In view of Proposition 5.6 any trialitarian automorphism of $W(D_4)$ is the restriction to $W(D_4)$ of conjugation by an element $u\in\mathrm{O}_4$ of the form $u=\mu\cdot w$ or $u=\mu^2\cdot w$, with $w\in W(D_4)$ and $u^3=1$. There are 48 elements u of this form, hence the claim. □

Corollary 5.9. *There are up to isomorphism two types of subgroups of fixed points of trialitarian automorphisms of $W(D_4)$, those isomorphic to* $\mathrm{Fix}(\tilde\mu)$ *and those isomorphic to* $\mathrm{Fix}(\tilde\mu)$ *.*

Proof. Trialitarian automorphisms which are conjugate in $\mathrm{Aut}\big(W(D_4)\big)$ have isomorphic groups of fixed points. □

Proposition 5.10. *1) The 2-dimensional subspace of $\mathbb{R}^4$ generated by the set of elements $\{e_1+e_3,e_2-e_3\}$ is fixed under μ.*
2) The set $\{e_1+e_3,e_2-e_3\}$ generates a root system of type G_2 and the group $\mathrm{Fix}(\tilde\mu)$ *is the corresponding Weyl group, which is the dihedral group $\mathfrak{D}_6$ of order* 12.

Proof. By explicit computation. □

Proposition 5.11. *The group* $\mathrm{Fix}(\tilde\rho)$ *is isomorphic to the group of order* 24 *of Hurwitz quaternions $\mathbb{H}^1=\mathfrak{Q}_8\rtimes\mathfrak{C}_3$. This group is isomorphic to the double covering $\tilde{\mathfrak{A}}_4$ of $\mathfrak{A}_4$.*

Proof. Recall that the matrix ρ is obtained by choosing $(1, i, j, k)$ as basis of $\mathbb{R}^4$ and letting $-\frac{1}{2}(1+i+j+k)$ operate by left multiplication in $\mathbb{H}$. The group $\mathbb{H}^1$ has a representation in $W(D_4)$ by right multiplication which obviously commutes with the action of ρ. Hence $\mathrm{Fix}(\tilde{\rho})$ contains a copy of $\mathbb{H}^1$. The claim then follows from the fact that $\mathrm{Fix}(\tilde{\rho})$ has 24 elements. □

Cohomology with $W(D_4)$ coefficients. Each automorphism $\alpha \in \mathrm{Aut}\big(W(D_4)\big)$ acts on $H^1\big(\Gamma, W(D_4)\big)$ by

$$\alpha_*\colon [\varphi] \mapsto [\alpha \circ \varphi],$$

where $\varphi\colon \Gamma \to W(D_4)$ is a cocycle with values in $W(D_4)$. If $\alpha' = \mathrm{Int}(w) \circ \alpha$ for some $w \in W(D_4)$, then for all cocycles $\varphi\colon \Gamma \to W(D_4)$ we have

$$w \cdot \alpha\big(\varphi(\gamma)\big) \cdot w^{-1} = \alpha'\big(\varphi(\gamma)\big) \qquad \text{for all } \gamma \in \Gamma,$$

hence $[\alpha \circ \varphi] = [\alpha' \circ \varphi]$ and therefore $\alpha_* = \alpha'_*$. Thus, the action of $\mathrm{Aut}\big(W(D_4)\big)$ on $H^1\big(\Gamma, W(D_4)\big)$ factors through $\mathrm{Aut}\big(W(D_4)\big) / \mathrm{Int}\big(W(D_4)\big) \simeq \mathfrak{S}_3 \times \langle\psi\rangle$. In particular the symmetric group $\mathfrak{S}_3$ acts on $H^1\big(\Gamma, W(D_4)\big)$. Under the bijections (3.5), the symmetric group $\mathfrak{S}_3$ also acts on $\mathrm{Iso}\big((\mathsf{Cov}_\Gamma^{2/4})^+\big)$ and $\mathrm{Iso}\big((\mathsf{\acute{E}tex}_\Gamma^{2/4})^+\big)$. The action of the outer automorphism $\tilde{\nu}$ associates to the oriented 2/4-covering $(Z/Z_0, \partial_Z)$ the oriented covering $\kappa(Z/Z_0, \partial) = (Z/Z_0, \partial_Z \circ \iota)$ where $\mathbf{2} \xleftarrow{\iota} \mathbf{2}$ twists the orientation. The proof of Theorem 4.1 shows that the action of $\tilde{\mu}$ maps the class of an oriented covering $(Z/Z_0, \partial_Z)$ to the class of $C_1^+(Z/Z_0, \partial_Z)$.

6. Triality and étale algebras

We next investigate triality on isomorphism classes of étale algebras using Galois cohomology. Oriented extensions of étale algebras S/S_0 with $\dim_F S = 8$ and $\dim_F S_0 = 4$ correspond to cocycles, i.e., continuous homomorphisms $\Gamma \to W(D_4)$, and isomorphism classes of such algebras correspond to cocycles up to conjugation. If the cocycle factors through a subgroup G of $W(D_4)$, the conjugacy class of G in $W(D_4)$ is determined by the isomorphism class of the algebra. Thus it makes sense to classify isomorphism classes of algebras according to the conjugacy classes of the subgroups G of $W(D_4)$.

We give in Table 1 a list of all conjugacy classes of subgroups of $W(D_4)$. We still consider $W(D_4)$ as a subgroup of O_4 (see (5.3)) and use the following notation. The group $W(D_4)$ fits into the split exact sequence:

$$1 \to \mathfrak{S}_2^3 \to W(D_4) \xrightarrow{\beta} \mathfrak{S}_4 \to 1. \tag{6.1}$$

where β is as in (5.4). For each subgroup G of $W(D_4)$ we denote by G_1 the restriction $G \cap \mathfrak{S}_2^3$ and by G_0 the projection $\beta(G)$. The center of $W(D_4)$, generated by $w_0 = \mathrm{Diag}(-1,-1,-1,-1) = -1$ is denoted by C and we set $w_1 = \mathrm{Diag}(1,-1,1,-1)$, $w_2 = \mathrm{Diag}(1,-1,-1,1)$ and $w_3 = \mathrm{Diag}(-1,-1,1,1)$ for special elements of the subgroup $\mathfrak{S}_2^3 \subset W(D_4)$ given by diagonal matrices. We denote by $\mathfrak{S}_n$ the permutation group of n elements, $\mathfrak{A}_n$ is the alternating subgroup, $\mathfrak{C}_n$ is cyclic of order n, $\mathfrak{D}_n$ is the dihedral group of order $2n$, $\mathfrak{V}_4$ is the Klein 4-group, and $\mathfrak{Q}_8$ is the quaternionic group with eight elements. In Column S we summarize the various possibilities for étale algebras of dimension 8 associated to the class of a cocycle $\alpha\colon \Gamma \to W$ which factors through G and in Column S_0 étale algebras of dimension 4 associated to the class of the induced cocycle $\beta \circ \alpha\colon \Gamma \to \mathfrak{S}_4$ which

factors through G_0. The entry K in one of the columns S or S_0 denotes a quadratic separable field extension. We use symbols E, respectively E_0 for separable field extensions whose Galois closures have Galois groups G, respectively G_0. The symbol $R(E)$ stands for the cubic resolvent of E if E is a quartic separable field extension and $\lambda^2 E$ stands for the second lambda power of E (see [12], where it is denoted $\Lambda_2(E)$ or [9], where it is denoted $E(2)$[4]). If $\dim_F E = 4$, $\lambda^2 E$ admits an involution σ and for any quadratic étale algebra K with involution ι we set $K * \lambda^2 E = (K \otimes_F \lambda^2 E)^{\iota \otimes \sigma}$. We write $\overline{E}_0$ for the Galois closure of E_0. The symbol ℓ gives the number of subgroups in the conjugacy class of G, MS refers to the maximal subgroups of G and in column T we give the two conjugacy classes which are the images of the class of G under the trialitarian automorphisms $\tilde{\mu}$ and $\tilde{\mu}^2$.
Entries N, $|G|$, ℓ and MS in the table were generated with the help of the Magma algebra software [2]. The computation of the entry T, the explicit representation of the group G as an exact sequence and the decomposition of the étale algebras as products of fields were checked case by case.
Explicit computations of trialitarian triples were made in [1] and [19] using the description of the trialitarian action given in the proof of Theorem 4.1.

[4]The corresponding Γ-set $\lambda^2 X$ is obtained by removing the diagonal from $X \times X$ and dividing by the involution $(x, y) \mapsto (y, x)$.

N	S_0	S	$G_1 \to G \to G_0$	$\lvert G\rvert$	ℓ	MS	T
1	F^4	F^8	$1 \to 1 \to 1$	1	1	1	$1,1$
2	F^4	K^4	$C \to \mathfrak{S}_2 \to 1$	2	6	1	$2,2$
3	K^2	K^4	$1 \to \mathfrak{S}_2 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	2	6	1	$3,5$
4	K^2	K^4	$1 \to \mathfrak{S}_2 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	2	6	1	$4,3$
5	F^4	$F^2 \times K^2$	$\langle w_1\rangle \to \mathfrak{S}_2 \to 1$	2	6	1	$5,4$
6	$F^2 \times K$	$F^2 \times K^2$	$1 \to \mathfrak{S}_2 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	2	12	1	$6,6$
7	$F^2 \times K$	$F^2 \times K^2$	$1 \to \mathfrak{S}_2 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	2	12	1	$7,7$
8	$F \times E_0$	$F^2 \times S_0^2$	$1 \to \mathfrak{C}_3 \to \mathfrak{C}_3$	3	16	1	$8,8$
9	F^4	$K_1^2 \times K_2^2$	$\langle C, w_1\rangle \to \mathfrak{S}_2^2 \to 1$	4	3	2 5	$11,10$
10	K^2	$K \otimes K_1^2$	$C \to \mathfrak{S}_2^2 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	4	3	2 3	$9,11$
11	K^2	$K \otimes K_1^2$	$C \to \mathfrak{S}_2^2 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	4	3	2 4	$10,9$
12	$K_1 \otimes K_2$	$K_1 \otimes K_2^2$	$1 \to \mathfrak{S}_2^2 \to \mathfrak{V}_4$	4	4	4	$14,13$
13	F^4	$K_1^2 \times K_2^2$	$\langle w_1, w_2\rangle \to \mathfrak{S}_2^2 \to 1$	4	4	5	$12,14$
14	$K_1 \otimes K_2$	$K_1 \otimes K_2^2$	$1 \to \mathfrak{S}_2^2 \to \mathfrak{V}_4$	4	4	3	$13,12$
15	$F^2 \times K$	$F^4 \times K_1 \otimes K$	$\langle w_1\rangle \to \mathfrak{S}_2^2 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	4	6	5 6	$18,17$
16	$K_1 \times K_2$	$K_1 \otimes K_2^2$	$1 \to \mathfrak{S}_2^2 \to \mathfrak{S}_2^2$	4	6	4 7	$21,19$
17	$K_1 \times K_2$	$K_1^2 \times K_2^2$	$1 \to \mathfrak{S}_2^2 \to \mathfrak{S}_2^2$	4	6	3 6	$15,18$
18	$K_1 \times K_2$	$K_1^2 \times K_2^2$	$1 \to \mathfrak{S}_2^2 \to \mathfrak{S}_2^2$	4	6	4 6	$17,15$
19	$F^2 \times K$	$K_1^2 \times K_1 \times K$	$\langle w_1\rangle \to \mathfrak{S}_2^2 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	4	6	5 7	$16,21$
20	K^2	E^2	$C \to \mathfrak{C}_4 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	4	2	2	$20,20$
21	$K_1 \times K_2$	$K_1 \otimes K_2^2$	$1 \to \mathfrak{S}_2^2 \to \mathfrak{S}_2^2$	4	6	3 7	$19,16$
22	$K_1 \times K_2$	$K_1^2 \times K_1 \otimes K_2$	$1 \to \mathfrak{S}_2^2 \to \mathfrak{S}_2^2$	4	12	4 6 7	$23,27$
23	$K_1 \times K_2$	$K_1^2 \times K_1 \otimes K_2$	$1 \to \mathfrak{S}_2^2 \to \mathfrak{S}_2^2$	4	12	3 6 7	$27,22$
24	K^2	$K^2 \times K \otimes K_1$	$\langle w_1\rangle \to \mathfrak{S}_2^2 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	4	12	3 4 5	$24,24$
25	$F^2 \times K$	$F^4 \times E$	$\langle w_1\rangle \to \mathfrak{C}_4 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	4	12	5	$26,28$
26	E_0	E_0^2	$1 \to \mathfrak{C}_4 \to \mathfrak{C}_4$	4	12	4	$28,25$
27	$F^2 \times K$	$K_1^2 \times K_1 \otimes K$	$\langle -w_1\rangle \to \mathfrak{S}_2^2 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	4	12	5 6 7	$22,23$
28	E_0	$E_0 \times E_0$	$1 \to \mathfrak{C}_4 \to \mathfrak{C}_4$	4	12	3	$25,26$
29	$F^2 \times K$	$K^2 \times K \otimes K_1$	$C \to \mathfrak{S}_2^2 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	4	12	2 6 7	$29,29$
30	$F \times E_0$	$F^2 \times E_0 \otimes \Delta(E_0)$	$1 \to \mathfrak{S}_3 \to \mathfrak{S}_3$	6	16	7 8	$30,30$
31	$F \times E_0$	$F^2 \times E$	$C \to \mathfrak{C}_6 \to \mathfrak{C}_3$	6	16	2 8	$31,31$
32	$F \times E_0$	$F^2 \times E_0^2$	$1 \to \mathfrak{S}_3 \to \mathfrak{S}_3$	6	16	6 8	$32,32$
33	E_0	E	$C \to \mathfrak{S}_2^3 \to \mathfrak{V}_4$	8	1	11 12	$34,35$
34	E_0	E	$C \to \mathfrak{S}_2^3 \to \mathfrak{V}_4$	8	1	10 14	$35,33$
35	F^4	$K_1 \times K_2 \times K_3 \times K_{123}$	$\mathfrak{S}_2^3 \to \mathfrak{S}_2^3 \to 1$	8	1	9 13	$33,34$
36	E_0	E	$C \to \mathfrak{Q}_8 \to \mathfrak{V}_4$	8	2	20	$36,36$
37	K^2	$E_1 \times E_2$	$\langle C, w_1\rangle \to \mathfrak{S}_2 \times \mathfrak{C}_4 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	8	3	3 20	$38,40$
38	E_0	$E_0 \otimes K$	$C \to \mathfrak{S}_2 \times \mathfrak{C}_4 \to \mathfrak{C}_4$	8	3	11 20	$40,37$
39	K^2	$K \otimes K_1 \times K \otimes K_2$	$\langle C, w_1\rangle \to \mathfrak{S}_2^3 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	8	3	9 10 11 24	$39,39$
40	E_0	$E_0 \otimes K$	$C \to \mathfrak{S}_2 \times \mathfrak{C}_4 \to \mathfrak{C}_4$	8	3	10 20	$37,38$
41	K^2K	E^2	$\langle C, w_2\rangle \to \mathfrak{D}_4 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	8	6	9 11 20	$49,45$
42	$F^2 \times K$	$K_1 \times E$	$\langle C, w_1\rangle \to \mathfrak{S}_2 \times \mathfrak{C}_4 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	8	6	9 25	$44,47$
43	$K_1 \times K_2$	$K \otimes K_1 \times K \otimes K_2$	$C \to \mathfrak{S}_2^3 \to \mathfrak{S}_2^2$	8	6	10 17 21 23 29	$48,46$
44	E_0	E	$C \to \mathfrak{S}_2 \times \mathfrak{C}_4 \to \mathfrak{C}_4$	8	6	11 26	$47,42$
45	K^2	E^2	$\langle C, w_2\rangle \to \mathfrak{D}_4 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	8	6	9 10 20	$41,49$
46	$K_1 \times K_2$	$K \otimes K_1 \times K \otimes K_2$	$C \to \mathfrak{S}_2^3 \to \mathfrak{S}_2^2$	8	6	11 16 18 22 29	$43,48$
47	E_0	$E_0 \otimes K$	$C \to \mathfrak{S}_2 \times \mathfrak{C}_4 \to \mathfrak{C}_4$	8	6	10 28	$42,44$
48	$F^2 \times K$	$K_1^2 \times K \otimes K_2$	$\langle C, w_1\rangle \to \mathfrak{S}_2^3 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	8	6	9 15 19 27 29	$46,43$
49	E_0	E	$C \to \mathfrak{D}_4 \to \mathfrak{V}_4$	8	6	10 11 20	$45,41$

Table 1

N	S_0	S	$G_1 \to G \to G_0$	$\lvert G\rvert$	ℓ	MS	T
50	$F^2 \times K$	$K^2 \times E$	$\langle w_1, w_2\rangle \to \mathfrak{D}_4 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	8	6	13 19 25	$55, 51$
51	E_0	E	$1 \to \mathfrak{D}_4 \to \mathfrak{D}_4$	8	12	14 21 28	$50, 55$
52	E_0	E_0^2	$1 \to \mathfrak{D}_4 \to \mathfrak{D}_4$	8	12	14 17 28	$54, 57$
53	$K_1 \times K_2$	$K \otimes K_1 \times K \otimes K_2$	$\langle w_1\rangle \to \mathfrak{S}_2^3 \to \mathfrak{S}_2^2$	8	12	16 19 21 22 23 24 27	$53, 53$
54	$F^2 \times K$	$F^2 \times K \times E$	$\langle w_1, w_2\rangle \to \mathfrak{D}_4 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	8	12	13 15 25	$57, 52$
55	E_0	$\bar{E}_0$	$1 \to \mathfrak{D}_4 \to \mathfrak{D}_4$	8	12	12 16 26	$51, 50$
56	$K_1 \times K_2$	$K_1^2 \times E$	$\langle w_1\rangle \to \mathfrak{S}_2^3 \to \mathfrak{S}_2^2$	8	12	15 17 18 22 23 24 27	$56, 56$
57	E_0	E_0^2	$1 \to \mathfrak{D}_4 \to \mathfrak{D}_4$	8	12	12 18 26	$52, 54$
58	E_0	E_0^2	$1 \to \mathfrak{A}_4 \to \mathfrak{A}_4$	12	4	8 14	$59, 60$
59	$F \times E_0$	$F^2 \times E_0^2$	$\langle w_1, w_2\rangle \to \mathfrak{S}_2^2 \rtimes \mathfrak{C}_3 \to \mathfrak{C}_3$	12	4	8 13	$60, 58$
60	E_0	E_0^2	$1 \to \mathfrak{A}_4 \to \mathfrak{A}_4$	12	4	8 12	$58, 59$
61	$F \times E_0$	$K \times K \otimes E_0$	$C \to \mathfrak{S}_2 \times \mathfrak{S}_3 \to \mathfrak{S}_3$	12	4	$29, 30, 31, 32$	$61, 61$
62	$K_1 \times K_2$	E^2	$\langle C, w_1\rangle \to [2^2]4 \to \mathfrak{S}_2^2$	16	3	39 42	$66, 63$
63	E_0	E	$\langle C, w_1\rangle \to [2^2]4 \to \mathfrak{C}_4$	16	3	39 47	$62, 66$
64	K^2	$E_1 \times E_2$	$\mathfrak{S}_2^3 \to \mathfrak{S}_2 \times \mathfrak{D}_4 \to \mathfrak{S}_2 \subset \mathfrak{V}_4$	16	3	35 37 39 41 45	$68, 67$
65	$K_1 \times K_2$	$K_1 \otimes K_3 \times K_2 \otimes K_4$	$\langle C, w_1\rangle \to \mathfrak{S}_2^4 \to \mathfrak{S}_2^2$	16	3	39 43 46 48 53 56	$65, 65$
66	E_0	E	$\langle C, w_1\rangle \to [2^2]4 \to \mathfrak{C}_4$	16	3	39 44	$63, 62$
67	E_0	E	$\langle C, w_1\rangle \to \mathfrak{S}_2 \times \mathfrak{D}_4 \to \mathfrak{V}_4$	16	3	34 39 40 45 49	$64, 68$
68	E_0	E	$\langle C, w_2\rangle \to \mathfrak{S}_2 \times \mathfrak{D}_4 \to \mathfrak{V}_4$	16	3	33 38 39 41 49	$67, 64$
69	$K_1 \times K_2$	E^2	$\langle C, w_1\rangle \to [2^2]4 \to \mathfrak{S}_2^2$	16	6	37 42 48	$73, 72$
70	E_0	E	$\langle C, w_1\rangle \to \mathfrak{Q}_8 : 2 \to \mathfrak{V}_4$	16	6	36 37 38 40 41 45 49	$70, 70$
71	$F^2 \times K$	$K_1^2 \times E$	$\mathfrak{S}_2^3 \to \mathfrak{S}_2 \times \mathfrak{D}_4 \to \mathfrak{S}_2 \not\subset \mathfrak{V}_4$	16	6	35 42 48 50 54	$75, 74$
72	E_0	E	$\langle C, w_1\rangle \to [2^2]4 \to \mathfrak{V}_4$	16	6	40 43 47	$69, 73$
73	E_0	E	$C \to [2^2]4 \to \mathfrak{D}_4$	16	6	38 44 46	$72, 69$
74	E_0	$E_0 \otimes K$	$C \to \mathfrak{S}_2 \times \mathfrak{D}_4 \to \mathfrak{D}_4$	16	6	34 43 47 51 52	$71, 75$
75	E_0	$E_0 \otimes K$	$C \to \mathfrak{S}_2 \times \mathfrak{D}_4 \to \mathfrak{D}_4$	16	6	33 44 46 55 57	$74, 71$
76	E_0	E_0^2	$1 \to \mathfrak{S}_4 \to \mathfrak{S}_4$	24	4	32 52 58	$79, 81$
77	$F \times R(E)$	$\Delta(E) \times \lambda^2 E$	$\langle w_1, w_3\rangle \to \mathfrak{S}_2^2 \rtimes \mathfrak{S}_3 \to \mathfrak{S}_3$	24	4	30 50 59	$84, 82$
78	$F \times E_0$	$\Delta(E) \times \lambda^2 E$	$\mathfrak{S}_2^3 \to \mathfrak{S}_2^3 \rtimes \mathfrak{C}_3 \to \mathfrak{C}_3$	24	4	31 35 59	$83, 80$
79	$F \times R(E)$	$F^2 \times \lambda^2 E$	$\langle w_1, w_3\rangle \to \mathfrak{S}_2^2 \rtimes \mathfrak{S}_3 \to \mathfrak{S}_3$	24	4	32 54 59	$76, 81$
80	E_0	$E_0 \otimes K$	$C \to \mathfrak{S}_2 \times \mathfrak{A}_4 \to \mathfrak{A}_4$	24	4	31 34 58	$78, 83$
81	E_0	E_0^2	$1 \to \mathfrak{S}_4 \to \mathfrak{S}_4$	24	4	32 57 60	$76, 79$
82	E_0	$E_0 \otimes \Delta(E_0)$	$1 \to \mathfrak{S}_4 \to \mathfrak{S}_4$	24	4	30 51 58	$77, 84$
83	E_0	E	$C \to \mathfrak{S}_2 \times \mathfrak{A}_4 \to \mathfrak{A}_4$	24	4	31 33 60	$78, 80$
84	E_0	$E_0 \otimes \Delta(E_0)$	$1 \to \mathfrak{S}_4 \to \mathfrak{S}_4$	24	4	30 55 66	$82, 77$
85	E_0	E	$\mathfrak{S}_2 \to \tilde{\mathfrak{A}}_4 \to \mathfrak{A}_4$	24	4	31 36	$85, 85$
86	E_0	E	$\mathfrak{S}_2^3 \to \mathfrak{S}_2^3 \rtimes \mathfrak{V}_4 \to \mathfrak{V}_4$	32	1	64 67 68 70	$86, 86$
87	E_0	E	$\langle C, w_1\rangle \to \mathfrak{S}_2^2 \rtimes \mathfrak{D}_4 \to \mathfrak{D}_4$	32	3	63 65 67 72 74	$92, 90$
88	E_0	E	$\mathfrak{S}_2^3 \to \mathfrak{S}_2^3 \rtimes \mathfrak{C}_4 \to \mathfrak{C}_4$	32	3	63 64 66	$91, 89$
89	E_0	E	$\langle C, w_1\rangle \to \mathfrak{S}_2^3 \rtimes \mathfrak{C}_4 \to \mathfrak{D}_4$	32	3	62 66 67	$88, 91$
90	E_0	E	$\langle C, w_1\rangle \to \mathfrak{S}_2^2 \rtimes \mathfrak{D}_4 \to \mathfrak{D}_4$	32	3	65 66 68 73 75	$92, 87$
91	E_0	E	$\langle C, w_1\rangle \to \mathfrak{S}_2^3 \rtimes \mathfrak{C}_4 \to \mathfrak{D}_4$	32	3	62 63 68	$89, 88$
92	$K_1 \times K_2$	$E_1 \times E_2$	$\mathfrak{S}_2^3 \to \mathfrak{S}_2^2 \rtimes \mathfrak{D}_4 \to \mathfrak{S}_2^2$	32	3	62 64 65 69 71	$87, 90$
93	$F \times R(E)$	$\Delta(E) \times K * \lambda^2 E$	$\mathfrak{S}_2^3 \to \mathfrak{S}_2 \times \mathfrak{S}_4 \to \mathfrak{S}_3$	48	4	61 71 77 78 79	$94, 95$
94	E_0	$E_0 \otimes K$	$C \to \mathfrak{S}_2 \times \mathfrak{S}_4 \to \mathfrak{S}_4$	48	4	61 75 81 83 84	$95, 93$
95	E_0	$E_0 \otimes K$	$C \to \mathfrak{S}_2 \times \mathfrak{S}_4 \to \mathfrak{S}_4$	48	4	61 74 76 80 82	$93, 94$
96	E_0	E	$\mathfrak{S}_2^3 \to \mathfrak{S}_2^3 \rtimes \mathfrak{D}_4 \to \mathfrak{D}_4$	64	3	86 87 88 89 90 91 92	$96, 96$
97	E_0	E	$\mathfrak{S}_2^3 \to \mathfrak{S}_2^3 \rtimes \mathfrak{A}_4 \to \mathfrak{A}_4$	96	1	78 80 83 85 86	$97, 97$
98	E_0	E	$\mathfrak{S}_2^3 \to \mathfrak{S}_2^3 \rtimes \mathfrak{S}_4 \to \mathfrak{S}_4$	192	1	93 94 95 96 97	$98, 98$

Table 1

Trialitarian triples and fixed points. Let α be any trialitarian automorphism of $W(D_4)$. The subset $H^1\big(\Gamma, W(D_4)\big)^{C_3}$ of cohomology classes that are fixed under

α_* is independent of the particular choice of α. Clearly, the image in $H^1\big(\Gamma, W(D_4)\big)$ of any cohomology class in $H^1\big(\Gamma, \mathrm{Fix}(\alpha)\big)$ is fixed under α_*, hence this image lies in $H^1\big(\Gamma, W(D_4)\big)^{C_3}$. Thus, we have a canonical map

$$H^1\big(F, \mathrm{Fix}(\alpha)\big) \to H^1\big(F, W(D_4)\big)^{C_3} \tag{6.2}$$

for any trialitarian automorphism α of $W(D_4)$.

Theorem 6.3. *Any class in $H^1\big(F, W(D_4)\big)^{C_3}$ lies in the image of the map* (6.2) *for $\alpha = \tilde{\mu}$ or $\alpha = \tilde{\rho}$ as in* (5.8).

Proof. If the class $[\varphi]$ of a cocycle $\varphi\colon \Gamma \to W(D_4)$ belongs to $H^1\big(\Gamma, W(D_4)\big)^{C_3}$, the cocycle factors through a subgroup G whose conjugacy class is invariant under $\tilde{\mu}$. We get from Columns N and T of Table 1 a list of all triples of conjugate classes of subgroups $W(D_4)$ which are permuted by a trialitarian automorphism of $W(D_4)$. A triple consists of three identic labels (for example $(70, 70, 70)$) if there exists $a \in W(D_4)$ such that

$$\mu G \mu^{-1} = aGa^{-1},$$

where μ is as in (4.7). A cocycle factoring through such a group G does not necessarily correspond to a triple of isomorphism classes of étale algebras fixed under triality. For a triple consisting of isomorphic algebras we must have $a \in W(D_4)$ such that

$$\mu x \mu^{-1} = axa^{-1} \tag{6.4}$$

for all $x \in G$, since isomorphic classes of algebras are given by homomorphisms $\gamma\colon \Gamma \to G$ up to conjugation. Thus a necessary condition to get a triple of fixed isomorphism classes of algebras is that the conjugacy classes of all subgroups H of G are invariant under triality. Thus the conjugacy classes N = 24, 39, 53, 56, 65, 70, 86, 96, 97 and 98 do not correspond to triples of isomorphism classes of algebras invariant under triality. The conjugacy classes left over in Table are N= 1, 2, 6, 7, 8, 20, 29, 30, 31, 32, 36, 61 and 85. They give rise to triples of isomorphism classes of étale algebras fixed under triality, since they correspond to subgroups contained in $\mathrm{Fix}(\tilde{\mu})$ (N = 61) or contained in $\mathrm{Fix}(\tilde{\rho})$ (N=85). □

Observe that fixed étale algebras in class $N = 61$ are of the form $K \times (E_0 \otimes K)$, where K is quadratic and E_0 is cubic. Hence they are not fields over F, in contrast to algebras in class $N = 85$.

7. Trialitarian resolvents

Trialitarian triples of étale algebras can be viewed as one étale algebra with two attached resolvents (see Remark 3.6). For example, let E be a quartic separable field with Galois group $\mathfrak{S}_4$. The field $E \otimes \Delta(E)$ is octic with the same Galois group $\mathfrak{S}_4$ and the extension $E \otimes \Delta(E)/E$ corresponds to Class $N = 82$ in Table 1. Class $N = 77$ in the same trialitarian triple corresponds to the extension

$$\big(\Delta(E) \times \lambda^2 E\big)/\big(F \times R(E)\big),$$

where $\Delta(E)$ is the discriminant, $R(E)$ is the cubic resolvent of E and $\lambda^2 E$ is the second lambda power of E, as defined in [12].

In this section we consider the situation where one étale algebra in the triple is given by a separable polynomial and compute polynomials for the two other étale algebras. We assume that the base field F is infinite and has characteristic different from 2.

Proposition 7.1. *Let S/S_0 be an étale algebra with involution of dimension $2n$ over F.*
1) There exists an invertible element $x \in S$ such that x generates S and x^2 generates S_0.
2) There exists a polynomial

$$f_n(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

with coefficients in F such that $S_0 \xrightarrow{\sim} F[x]/\big(f_n(x)\big)$ and $S \xrightarrow{\sim} F[x]/\big(f_{2n}(x)\big)$, where $f_{2n}(x) = f_n(x^2)$.
3) The algebra S has trivial discriminant if and only if $(-1)^n a_0$ is a square in F.

Proof. To prove 1) we are looking for invertible elements x of S such that $\mathrm{Tr}_{S/S_0}(x) = 0$ and such that the discriminant of the characteristic polynomial of x^2 is not zero. Any such element generates S and $x^2 \in S_0$ generates S_0. These elements form an Zariski open subset of the space of trace zero elements. One checks that this open subspace is not empty by going to an algebraic closure of F.
2) follows from 1) and 3) follows from a discriminant formula (see [4, p. 51]) for the discriminant $D(f_{2n})$ of f_{2n}:

$$D(f_{2n}) = (-1)^n a_0 \cdot \big(2^n D(f_n)\big)^2$$

(recall that $\Delta(S) \xrightarrow{\sim} F[x]/\big(x^2 - D(f_{2n})\big)$). □

Theorem 7.2. *Let S/S_0, $\dim_F S = 8$, with trivial discriminant, be given as in Proposition 7.1, by a polynomial*

$$f_4(x) = x^4 + ax^3 + bx^2 + cx + e^2. \tag{7.3}$$

The polynomials

$$\begin{aligned} f_4'(x) &= x^4 + ax^3 + (\tfrac{3}{8}a^2 - \tfrac{1}{2}b + 3e)x^2 + \\ &\quad (\tfrac{1}{16}a^3 - \tfrac{1}{4}ab + c + \tfrac{1}{2}ae)x + \big(\tfrac{1}{16}a^2 - \tfrac{1}{4}b - \tfrac{1}{2}e\big)^2 \quad \textit{and} \\ f_4''(x) &= x^4 + ax^3 + (\tfrac{3}{8}a^2 - \tfrac{1}{2}b - 3e)x^2 + \\ &\quad (\tfrac{1}{16}a^3 - \tfrac{1}{4}ab + c - \tfrac{1}{2}ae)x + \big(\tfrac{1}{16}a^2 - \tfrac{1}{4}b + \tfrac{1}{2}e\big)^2 \end{aligned}$$

define extensions of étale algebras S'/S_0', S''/S_0'' such that the isomorphism classes of S/S_0, S'/S_0' and S''/S_0'' are in triality.

Proof. Let $\{y_1, y_2, y_3, y_4\}$ be the set of zeroes of f_4 in a separable closure F_s of F. The set $\{\pm x_i = \pm\sqrt{y}_i,\ i = 1, \ldots 4\}$ is the set of zeroes of f_8. Let ξ be the column vector $[x_1, x_2, x_3, x_4]^T$. If $\varphi : \Gamma \to W(D_4) \subset \mathrm{O}_4$ is the cocycle corresponding to S/S_0, the group $\varphi(\Gamma)$ permutes the elements $\pm x_i$ through left matrix multiplication on ξ. The cocycle corresponding to S'/S_0' is given by

$$\varphi' : \gamma \mapsto \mu\varphi(\gamma)\mu^{-1}, \gamma \in \Gamma,$$

where μ is as in 4.7. Thus $\varphi'(\Gamma)$ permutes the components of $\pm\xi' = \pm\mu\xi = \pm[x_1', x_2', x_3', x_4']^T$ and $\{\pm x_i', i = 1, \ldots, 4\}$ is the set of zeroes of f_8'. It follows that

$$f_8'(x) = f_4'(x^2) = \prod_i (x - x_i')(x + x_i') = \prod_i (x^2 - {x_i'}^2).$$

The x_i' are the components of $\xi' = \mu\xi$. Thus the coefficients of $f_8'(x)$ can be expressed as functions of the x_i. Using that the symmetric functions in the x_i can be expressed as functions of the coefficients of f_8 one gets (for example with Magma [2]) the expression given in Proposition 7.2 for f_i'. Similar computations with μ^2 instead of μ lead to the formula for f_4''. □

Remark 7.4. Observe that we move from f_8' to f_8'' by replacing e by $-e$, as it should be.

8. Triality and Witt invariants of étale algebras

The results of this section were communicated to us by J-P. Serre, [15]. They are based on results of [14] and [9]. Similar results can be obtained for cohomological invariants of étale algebras instead of Witt invariants. Let k be a fixed base field of characteristic not 2 and F/k be a field extension. Let $WGr(F)$ be the Witt-Grothendieck ring and $W(F)$ the Witt ring of F, viewed as functors of F. We recall that elements of $WGr(F)$ are formal differences $q - q'$ of isomorphism classes of nonsingular quadratic forms over F and that the sum and product are those induced by the orthogonal sum and the tensor product of quadratic forms. The Witt ring $W(F)$ is the quotient of $WGr(F)$ by the ideal consisting of integral multiples of the 2-dimensional diagonal form $\langle 1, -1\rangle$.

Some of the following considerations hold for oriented quadratic extensions S/S_0 of étale algebras of arbitrary dimension. To simplify notation we assume from now on that $\dim_F S = 8$.

Let $(\text{Étex}^{2/4})^+$ be the functor which associates to F the set $\left(\text{Étex}_F^{2/4}\right)^+$ of isomorphism classes of oriented quadratic extensions S/S_0 of étale algebras over F such that $\dim_F S = 8$. A *Witt invariant* on $(\text{Étex}^{2/4})^+$, more precisely on $W(D_4)$, is a map

$$H^1\big(F, W(D_4)\big) \to W(F)$$

for each F/k, subject to compatibility and specialization conditions (see [9]). The set of Witt invariants

$$\operatorname{Inv}\big(W(D_4), W\big) = \operatorname{Inv}\big((\text{Étex}^{2/4})^+, W\big)$$

is a module over $W(k)$. The aim of this section is to describe this module and how triality acts on it. A main tool is the following splitting principle, which is a special case of a variant of the splitting principle for étale algebras (see [9, Theorem 24.9]) and which can be proved following the same lines.

Theorem 8.1. *If $a \in \operatorname{Inv}\big((\text{Étex}^{2/4})^+, W\big)$ satisfies $a(S/S_0) = 0$ for every product of two biquadratic algebras*

$$S = F\big(\sqrt{x}, \sqrt{y}\big) \times F\big(\sqrt{z}, \sqrt{t}\big), \quad S_0 = F\big(\sqrt{xy}\big) \times F\big(\sqrt{zt}\big).$$

over every extension F of k, then $a = 0$.

Let G be an elementary abelian subgroup of $W(D_4)$ of type $(2, 2, 2, 2)$. It belongs to the conjugacy class $N = 65$ in Table 1. Theorem 8.1 can be restated in the following form:

Theorem 8.2. *The restriction map*

$$\operatorname{Res}\colon \operatorname{Inv}\big(W(D_4), W\big) \to \operatorname{Inv}\big(G, W\big)$$

is injective.

Proof. G-torsors correspond to products of two biquadratic algebras. □

A construction of Witt invariants is through trace forms. Let $S/S_0 \in (\mathsf{\acute{E}tex}^{2/4})^+$ and let σ be the involution of S. We may associate two nonsingular quadratic trace forms to the extension S/S_0:

$$\begin{array}{rcccl} Q(x) & = & Q_S(x) & = & \frac{1}{8}\operatorname{Tr}_{S/F}(x^2) \\ Q'(x) & = & Q'_S(x) & = & \frac{1}{8}\operatorname{Tr}_{S/F}\big(x\sigma(x)\big),\ x \in S \end{array}$$

The decomposition

$$S = \operatorname{Sym}(S,\sigma) \oplus \operatorname{Skew}(S,\sigma)$$

leads to orthogonal decompositions

$$Q = Q^+ \perp Q^-, \quad Q' = Q^+ \perp -Q^-,$$

hence the forms Q^+ and Q^- define two Witt invariants attached to S/S_0. The étale algebras associated to S/S_0 by triality lead to corresponding invariants. We introduce following notations: $S/S_0 = S_1/S_{0,1}$ and $S_i/S_{0,i},\ i = 2, 3$, for the associated étale algebras. We denote the corresponding Witt invariants by $Q_i^+ = Q_{S_i}^+$ and $Q_i^- = Q_{S_i}^-$, $i = 1$, 2 and 3.
Another construction of Witt invariants is through orthogonal representations. Let O_n be the orthogonal group of the n-dimensional form $\langle 1, \ldots, 1\rangle$. Quadratic forms over F of dimension n are classified by the cohomology set $H^1(F, \mathrm{O}_n)$. Thus any group homomorphism $W(D_4) \to \mathrm{O}_n$ gives rise to a Witt invariant. In particular we get a Witt invariant q associated with the orthogonal representation $W(D_4) \to \mathrm{O}_4$ described in (5.3). Moreover the group $W(D_4)$ has three normal subgroups H_i of type $(2, 2, 2)$ (i.e., isomorphic to $\mathfrak{S}_2^3$), corresponding to the classes $N = 33$, 34, 35 of Table 1. Since the factor groups are isomorphic to $\mathfrak{S}_4$, the canonical representation $\mathfrak{S}_4 \to \mathrm{O}_4$ through permutation matrices leads to three Witt invariants q_1, q_2, q_3.

Proposition 8.3. *1) The Witt invariant q is invariant under triality and coincides with Q_i^-, $i = 1, 2, 3$.*
2) We have $q_i = Q_i^+$, $i = 1$, 2, 3, and the three invariants q_1, q_2, q_3 are permuted by triality.

Proof. The fact that q is invariant under triality follows from the fact that triality acts on $W(D_4)$ by an inner automorphism of O_4. Moreover the trialitarian action on $W(D_4)$ permutes the normal subgroups H_i, hence the invariants q_i. For the other claims we may assume by the splitting principle that S_1 is a product of two biquadratic algebras

$$S_1 = F\big(\sqrt{x}, \sqrt{y}\big) \times F\big(\sqrt{z}, \sqrt{t}\big), \quad S_{0,1} = F\big(\sqrt{xy}\big) \times F\big(\sqrt{zt}\big). \tag{8.4}$$

An explicit computation, using for example the description of triality given in the proof of Theorem 4.1 (see [1] and [19]) shows that one can make the following identifications

$$S_2 = F\big(\sqrt{x}, \sqrt{z}\big) \times F\big(\sqrt{y}, \sqrt{t}\big), \quad S_{0,2} = F\big(\sqrt{xz}\big) \times F\big(\sqrt{yt}\big)$$

and

$$S_3 = F\big(\sqrt{x}, \sqrt{t}\big) \times F\big(\sqrt{y}, \sqrt{z}\big), \quad S_{0,3} = F\big(\sqrt{xt}\big) \times F\big(\sqrt{yz}\big).$$

Observe that, with this identification, the 3-cycle (y,z,t) permutes cyclically the algebras $S_i/S_{0,i}$. We get

$$Q_i^- = \langle x,y,z,t\rangle$$

for $i = 1, 2, 3$, and

$$Q_1^+ = \langle 1,1,xy,zt\rangle,\ Q_2^+ = \langle 1,1,xz,yt\rangle,\ Q_3^+ = \langle 1,1,xt,yz\rangle.$$

The equalities $q = Q_i^-$ and $q_i = Q_i^+$ follow from the fact that the corresponding cocycles are conjugate in O_4. □

Further basic invariants are the constant invariant $\langle 1\rangle$ and the discriminant

$$\langle d\rangle = \mathrm{Disc}(q) = \mathrm{Disc}(q_i),\ i = 1, 2, 3,$$

which corresponds to the 1-dimensional representation $\det\colon W(D_4) \to \mathrm{O}_1 = \pm 1$. Since $Q_i^+(1) = 1$, the quadratic forms $q_i = Q_i^+$ represent 1 and one can replace them by 3-dimensional invariants $\ell_i = (1)^\perp \subset q_i$, $i = 1,2,3$.
In the following result $\lambda^2 q$ denotes the second exterior power of the quadratic form q (see [9]). If $q = \langle \alpha_1,\dots,\alpha_n\rangle$ is diagonal, then $\lambda^2 q$ is the $n(n-1)/2$-dimensional form $\lambda^2 q = \langle \alpha_1\alpha_2,\dots,\alpha_{n-1}\alpha_n\rangle$.

Theorem 8.5. *1) The $W(k)$-module* $\mathrm{Inv}\big(W(D_4),W\big) = \mathrm{Inv}\big((\mathsf{\acute{E}tex}^{2/4})^+,W\big)$ *is free over $W(k)$ with basis*

$$\big(\langle 1\rangle,\ \langle d\rangle,\ q, \langle d\rangle\cdot q,\ \ell_1,\ell_2,\ \ell_3\big). \tag{8.6}$$

2) The elements $\langle 1\rangle$, $\langle d\rangle$, q, $\langle d\rangle\cdot q$ are fixed under triality and the elements ℓ_1,ℓ_2 and ℓ_3 are permuted.
3) The following nonlinear relations hold among elements of (8.6)*:*

$$\begin{array}{rcl} \langle d\rangle & = & \mathrm{Disc}(q) = \mathrm{Disc}(q_i),\\ \lambda^2 q & = & \ell_1+\ell_2+\ell_3 - \langle 1,1,1\rangle\\ \langle 1,d\rangle\cdot q & = & q\cdot(\ell_i - \langle 1\rangle),\ i = 1,\,2,\,3. \end{array}$$

Proof. 1) The proof follows the pattern of the proof of [9, Theorem 29.2]. Let G be an elementary subgroup of $W(D_4)$ of type $(2,2,2,2)$, i.e. isomorphic to $\mathfrak{S}_2^4$. An arbitrary element of $H^1(F,G)$ is given by a 4-tuple $(\alpha_1,\alpha_2,\alpha_3,\alpha_4) \in \big(F^\times/F^{\times 2}\big)^4$. For I a subset of $[1,4] = \{1,2,3,4\}$, we write α_I for the product of the α_i for $i \in I$. By [9, Theorem 27.15] the set $\mathrm{Inv}(G,W)$ is a free $W(k)$-module with basis $(\alpha_I)_{I\subset[1,4]}$. It then follows from Theorem 8.2 that the family of elements given in (8.6) is linearly independent over $W(k)$. Let a be an element of $\mathrm{Inv}\big((\mathsf{\acute{E}tex}^{2/4})^+,W\big)$ and let S_α be the algebra (8.4) for $\alpha_1 = x$, $\alpha_2 = y$, $\alpha_3 = z$, $\alpha_4 = t$. The map $\alpha \mapsto a(S_\alpha)$ is a Witt invariant of G, hence by [9, Theorem 27.15] can be uniquely written as a linear combination

$$\sum c_I\cdot\langle\alpha_I\rangle \text{ with } c_I \in W(k). \tag{8.7}$$

The claim will follow if we show that the invariant α is in fact a linear combination of the elements given in (8.6). By [9, Prop. 13.2], the image of the restriction map $\mathrm{Inv}\big(W(D_4),W\big) \to \mathrm{Inv}(G,W)$ is contained in the $W(k)$-submodule of $\mathrm{Inv}(G,W)$ fixed by the normalizer $N = \mathfrak{S}_2^3 \rtimes \mathfrak{D}_4$ of G in $W(D_4)$ (conjugacy class $N = 96$ in Table 1). The group N acts on the set of isomorphisms classes of algebras S_i by acting in the obvious way on the symbols $\pm\sqrt{x}$, $\pm\sqrt{y}$, $\pm\sqrt{z}$, $\pm\sqrt{t}$. It follows that

N acts trivially on this set of isomorphisms classes. This shows that only linear combinations of elements in the family

$$\begin{aligned}\mathcal{B} = \quad & \{\langle 1\rangle, \langle x\rangle + \langle y\rangle + \langle z\rangle + \langle t\rangle, \langle xy\rangle + \langle zt\rangle, \langle xz\rangle + \langle yt\rangle, \langle xt\rangle + \langle yz\rangle, \\ & \langle xyz\rangle + \langle xyt\rangle + \langle xzt\rangle + \langle yzt\rangle, \langle xyzt\rangle\}\end{aligned}$$

can occur in the sum (8.7). The family $\mathcal{B}$ and the family given in 8.6 are equivalent bases. This implies the first claim of Theorem 8.5. Claim 2) follows from Proposition 8.3 and 3) is easy to check for a product of biquadratic extensions. □

References

[1] L. Beltrametti. Über quadratische Erweiterungen étaler Algebren der Dimension vier. Diplomarbeit, Mathematikdepartement, ETH Zürich, 2006, http://www.math.ethz.ch/~knus.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, pages 235–265, 1997.

[3] Nicolas Bourbaki. *Éléments de mathématique*. Masson, Paris, 1981. Groupes et algèbres de Lie. Chapitres 4, 5 et 6.

[4] J. Brillhart. On the Euler and Bernoulli polynomials. *J.Reine Angew. Math.*, 234:45–64, 1969.

[5] E. Cartan. Le principe de dualité et la théorie des groupes simples et semi-simples. *Bull. Sci. Math*, 49:361–374, 1925.

[6] P. Deligne. *Séminaire de géométrie algébrique du Bois-Marie, SGA 4 1/2, Cohomologie étale, avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier*, volume 569 of *Lecture Notes in Mathematics*. Springer-Verlag, 1977.

[7] W. N. Franzsen. *Automorphisms of Coxeter Groups*. PhD thesis, School of Mathematics and Statistics, University of Sydney, 2001, http://www.maths.usyd.edu.au/u/PG/theses.html.

[8] W. N. Franzsen and R. B. Howlett. Automorphisms of nearly finite Coxeter groups. *Adv. Geom.*, 3(3):301–338, 2003.

[9] Skip Garibaldi, Alexander Merkurjev, and Jean-Pierre Serre. *Cohomological invariants in Galois cohomology*, volume 28 of *University Lecture Series*. American Mathematical Society, Providence, RI, 2003.

[10] J. W. Jones and D. P. Roberts. Octic 2-adic fields. *J. Number Theory*, 128:1410–1429, 2008.

[11] M-A. Knus, A. A. Merkurjev, M. Rost, and J-P. Tignol. *The Book of Involutions*. Number 44 in American Mathematical Society Colloquium Publications. American Mathematical Society, Providence, R.I., 1998. With a preface in French by J. Tits.

[12] M-A. Knus and J-P. Tignol. Quartic exercises. *Inter. J. Math. Math. Sci.*, 2003:4263–4323, 2003.

[13] M-A. Knus and J-P. Tignol. Severi-Brauer varieties over the field of one element. In preparation, 2009.

[14] J-P. Serre. Witt invariants and trace forms. Minicourse, Workshop "From quadratic forms to algebraic groups", Ascona, organized by Paul Balmer, Eva Bayer and Max-Albert Knus, February 18–23, 2007.

[15] J-P. Serre. Les invariants de $W(D_4)$. Emails. June 5, June 6, June 18, 2009.

[16] J. Tits. Sur les analogues algébriques des groupes semi-simples complexes. In *Colloque d'algèbre supérieure, tenu à Bruxelles du 19 au 22 décembre 1956*, pages 261–289. Centre Belge de Recherches Mathématiques, Établissements Ceuterick, Louvain; Librairie Gauthier-Villars, Paris, 1957.

[17] J. Tits. Sur la trialité et certain groupes qui s'en déduisent. *Publ. Math. IHES*, 2:14–60, 1959.

[18] J. Tits. Buildings of Spherical Type and Finite BN-Pairs. Lecture Notes in Mathematics vol. 386. (Springer-Verlag, 1974)

[19] S. Zweifel. Etale Algebren und Trialität. Diplomarbeit, Mathematikdepartement, ETH Zürich, 2006, http://www.math.ethz.ch/~knus

Department Mathematik, ETH Zentrum, CH-8092 Zürich, Switzerland
E-mail address: knus@math.ethz.ch

Institut de Mathématique Pure et Appliquée, Université catholique de Louvain, B-1348 Louvain-la-Neuve, Belgium
E-mail address: jean-pierre.tignol@uclouvain.be