QUARTIC EXERCISES

MAX-ALBERT KNUS AND JEAN-PIERRE TIGNOL

ABSTRACT. A correspondence between quartic étale algebras over a field and quadratic étale extensions of cubic étale algebras is set up and investigated. The basic constructions are laid out in general for sets with a profinite group action and for torsors, and translated in terms of étale algebras and Galois algebras. In the final section, a parametrization of cyclic quartic algebras is given.

It is known since the XVIth century that the solution of quartic equations can be obtained by means of auxiliary equations of degree 3, called cubic resolvents. The situation is easily understood in terms of Galois theory. For any integer $n \geq 1$, let $\mathfrak{S}_n$ denote the symmetric group on $\{1, \ldots, n\}$. The symmetric group $\mathfrak{S}_4$ contains a normal subgroup of order 4, Klein's Vierergruppe

$$\mathfrak{V} = \{I, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\},$$

which is the kernel of the action of $\mathfrak{S}_4$ on its three Sylow 2-subgroups. Numbering from 1 to 3 these Sylow subgroups, we get an exact sequence of groups

$$1 \to \mathfrak{V} \to \mathfrak{S}_4 \xrightarrow{\rho} \mathfrak{S}_3 \to 1. \tag{1}$$

Let F be an arbitrary field and $P \in F[X]$ be a separable polynomial of degree 4. Let also F_s be a separable closure of F and $Q \subset F_s$ be the subfield generated by the roots of P. The Galois group $\mathrm{Gal}(Q/F)$ can be viewed as a subgroup of $\mathfrak{S}_4$ through its action on the roots of P. The subfield L of Q fixed under $\mathrm{Gal}(Q/F) \cap \mathfrak{V}$ is generated by the roots of a cubic resolvent, as was shown by Lagrange. For a given quartic polynomial P, there are actually many polynomials of degree 3 which qualify as cubic resolvents; only the extension L/F is an invariant of P (or of Q).

Galois cohomology provides another viewpoint on this construction. Since $\mathfrak{S}_n$ is the automorphism group of the étale F-algebra $F^n = F \times \cdots \times F$, it is well-known that the Galois cohomology set $H^1(F, \mathfrak{S}_n)$ is in canonical one-to-one correspondence with the isomorphism classes of étale F-algebras of degree n, see [3, (29.9)]. The map ρ in (1) induces a map

$$\rho^1 \colon H^1(F, \mathfrak{S}_4) \to H^1(F, \mathfrak{S}_3)$$

which associates to every quartic étale F-algebra Q a cubic étale F-algebra $\mathcal{R}(Q)$ uniquely determined up to isomorphism. If $P \in F[X]$ is a separable polynomial of degree 4 with cubic resolvent R, and if Q is the factor algebra $Q = F[X]/P$, then $\mathcal{R}(Q) \simeq F[X]/R$, see §4.3.

Our first aim is to make explicit the construction of $\mathcal{R}(Q)$ from Q. But this construction can be further extended. Each of the three Sylow 2-subgroups of $\mathfrak{S}_4$

The authors gratefully acknowledge support from the RT Network "K-theory, Linear Algebraic Groups and Related Structures" (contract HPRN-CT-2002-00287). The first author is partially supported by the Swiss National Foundation under grant 21-064712.01. The second author is partially supported by the National Fund for Scientific Research (Belgium).

contains two transpositions, and each transposition is in one and only one Sylow subgroup, hence the set of transpositions can be viewed as a double covering of the set of Sylow 2-subgroups. Therefore, the conjugation action of $\mathfrak{S}_4$ on its six transpositions defines a map

$$\lambda\colon \mathfrak{S}_4 \to \mathfrak{S}_2 \wr \mathfrak{S}_3,$$

where the wreath product $\mathfrak{S}_2 \wr \mathfrak{S}_3$ is viewed as the group of automorphisms of a double covering of a set of three elements (see §3.1). The map λ extends to an isomorphism of groups

$$\hat{\lambda}\colon \mathfrak{S}_2 \times \mathfrak{S}_4 \xrightarrow{\sim} \mathfrak{S}_2 \wr \mathfrak{S}_3,$$

see §4.2. The set $H^1(F, \mathfrak{S}_2 \wr \mathfrak{S}_3)$ classifies the quadratic étale extensions of cubic étale F-algebras (see §3.2), and the induced bijection

$$\hat{\lambda}^1\colon H^1(F, \mathfrak{S}_2) \times H^1(F, \mathfrak{S}_4) \xrightarrow{\sim} H^1(F, \mathfrak{S}_2 \wr \mathfrak{S}_3)$$

associates to every pair consisting of a quartic étale F-algebra Q and a quadratic étale F-algebra a quadratic étale extension of the cubic resolvent $\mathcal{R}(Q)$. In §4.3, we give an explicit construction of this quadratic extension, and we describe in §4.4 the inverse of $\hat{\lambda}^1$, attaching a quartic étale F-algebra and a quadratic étale F-algebra to any quadratic étale extension of a cubic étale F-algebra.

In the final sections, we classify quartic étale algebras and their associated quadratic extensions of cubic algebras according to their decomposition into direct products of fields (see §5.3) and we parametrize cyclic quartic extensions.

Contents

> La recherche des extensions d'un corps k dont le groupe de Galois sur k est $\mathfrak{S}_4$ ou $\mathfrak{A}_4$ n'est pas autre chose, du point de vue des algébristes du XIX[e] siècle, que la théorie de l'équation du 4[e] degré. C'est un problème pour lequel ces algébristes n'avaient que du mépris. (A. Weil)

1. Γ-sets and coverings

1.1. Basic constructions on Γ-sets. Let Γ be a profinite group, which will be fixed throughout this section. Finite sets with a continuous action of Γ are called Γ-sets. We let $|X|$ denote the number of elements in a Γ-set X. If X is a Γ-set with n elements, and k is a positive integer, $k \leq n$, we let $\Sigma_k(X)$ denote the set of k-tuples of pairwise distinct elements of X and $\Lambda_k(X)$ the set of k-element subsets of X; thus

$$\Sigma_k(X) = \bigl\{(\xi_1, \dots, \xi_k) \in X^k \mid \xi_i \neq \xi_j \text{ for } i \neq j\bigr\},$$
$$\Lambda_k(X) = \bigl\{\{\xi_1, \dots, \xi_k\} \subset X \mid \xi_i \neq \xi_j \text{ for } i \neq j\bigr\}.$$

The action of Γ on X induces actions on $\Sigma_k(X)$ and $\Lambda_k(X)$, hence $\Sigma_k(X)$ and $\Lambda_k(X)$ are Γ-sets, and we have

$$|\Sigma_k(X)| = k!\binom{n}{k}, \qquad |\Lambda_k(X)| = \binom{n}{k}.$$

The symmetric group $\mathfrak{S}_k$ acts on $\Sigma_k(X)$ by permutation of the entries, and we may consider $\Lambda_k(X)$ as the set of orbits of $\Sigma_k(X)$ under this action, i.e. as the quotient Γ-set

$$\Lambda_k(X) = \Sigma_k(X)/\mathfrak{S}_k.$$

For $k = n$, we may also consider the action of the alternating group $\mathfrak{A}_n$ on $\Sigma_n(X)$. The quotient is called the *discriminant* of X and denoted by $\Delta(X)$,

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

see [3, p. 291]. This is a Γ-set with $|\Delta(X)| = 2$ if $n \geq 2$.

If n is even, $n = 2m$, let

$$\gamma_X\colon \Lambda_m(X) \to \Lambda_m(X)$$

be the map which associates to every m-element subset of X its complementary subset. Since $\gamma_X^2 = \mathrm{Id}$, this map defines an action of $\mathfrak{S}_2$ on $\Lambda_m(X)$. The map γ_X is Γ-equivariant (i.e. compatible with the action of Γ), hence the quotient

$$\mathcal{R}(X) = \Lambda_m(X)/\mathfrak{S}_2$$

is a Γ-set. It is the set of partitions of X into m-element subsets.

Example 1.1. If $X = \{1,2,3,4\}$, then

$$\Lambda_2(X) = \bigl\{\{1,2\},\{3,4\},\{1,3\},\{2,4\},\{1,4\},\{2,3\}\bigr\}$$

and

$$\mathcal{R}(X) = \Bigl\{\bigl\{\{1,2\},\{3,4\}\bigr\},\bigl\{\{1,3\},\{2,4\}\bigr\},\bigl\{\{1,4\},\{2,3\}\bigr\}\Bigr\}.$$

If $|X| = 2$, the map

$$\gamma_X\colon\ X = \Lambda_1(X) \to \Lambda_1(X) = X$$

interchanges the two elements of X. For X, X' two Γ-sets with $|X| = |X'| = 2$, the map

$$\gamma_X \times \gamma_{X'}\colon\ X \times X' \to X \times X'$$

defines an action of $\mathfrak{S}_2$ compatible with the Γ-action. Let

$$X * X' = (X \times X')/\mathfrak{S}_2,$$

a Γ-set with $|X * X'| = 2$. Thus, if $X = \{x_1, x_2\}$ and $X' = \{x'_1, x'_2\}$, then

$$X * X' = \big\{\{(x_1, x'_1), (x_2, x'_2)\}, \{(x_1, x'_2), (x_2, x'_1)\}\big\}.$$

The following observations are clear:

Proposition 1.2. *Let X, X', be Γ-sets of two elements.*

(a) *The Γ-action on $X * X$ is trivial.*
(b) *If the Γ-action on X' is trivial, then $X * X' \simeq X$. (Note that the isomorphism is* not *canonical.)*
(c) *The operation $*$ defines a group structure on the set of isomorphism classes of Γ-sets of two elements.*

See §3.2 for a cohomological interpretation of the group structure induced by $*$.

1.2. **Coverings.** A morphism $Y \xleftarrow{\pi} Z$ of Γ-sets (i.e. a Γ-equivariant map) is called a *covering* if the number of elements in each fiber $\pi^{-1}(\eta) \subset Z$ does not depend on $\eta \in Y$. This number is called the *degree* of the covering. Coverings of degree 2 are called *double* coverings. A *morphism of coverings*

$$(Y_1 \xleftarrow{\pi_1} Z_1) \to (Y_2 \xleftarrow{\pi_2} Z_2)$$

is a pair $(\sigma\colon\ Y_1 \to Y_2, \tau\colon\ Z_1 \to Z_2)$ of morphisms such that $\sigma \circ \pi_1 = \pi_2 \circ \tau$. Given two coverings $Y \xleftarrow{\pi_1} Z_1$ and $Y \xleftarrow{\pi_2} Z_2$ of the same Γ-set Y, an *isomorphism over Y* is an isomorphism $\tau\colon\ Z_1 \to Z_2$ such that $\pi_1 = \pi_2 \circ \tau$.

For any covering $Y \xleftarrow{\pi} Z$ let $\Omega(Z/Y)$ be the set of sections of π,

$$\Omega(Z/Y) = \big\{\{\zeta_1, \dots, \zeta_n\} \subset Z \mid \{\pi(\zeta_1), \dots, \pi(\zeta_n)\} = Y\big\} \subset \Lambda_n(Z).$$

This is a Γ-set with $|\Omega(Z/Y)| = d^n$. If $d = 2$, the morphism

$$\gamma_Z\colon \Lambda_n(Z) \to \Lambda_n(Z)$$

preserves $\Omega(Z/Y)$ and induces a $\mathfrak{S}_2$-action compatible with the action of Γ. Define

$$\mathcal{S}(Z/Y) = \Omega(Z/Y)/\mathfrak{S}_2.$$

Note that every double covering $Y \xleftarrow{\pi} Z$ has an involutive automorphism $\gamma_{Z/Y}$ which is the identity on Y and interchanges the two elements in each fiber of π. Thus, for $\{\zeta_1, \dots, \zeta_n\} \in \Omega(Z/Y)$,

$$\gamma_Z\big(\{\zeta_1, \dots, \zeta_m\}\big) = \big\{\gamma_{Z/Y}(\zeta_1), \dots, \gamma_{Z/Y}(\zeta_n)\big\}.$$

Example 1.3. Let $Z = \{z_1, z'_1, z_2, z'_2, z_3, z'_3\}$, $Y = \{1, 2, 3\}$, and let $Y \xleftarrow{\pi} Z$ be the map which carries z_i and z'_i to i for $i = 1, 2, 3$. Then

$$\Omega(Z/Y) = \big\{\{z_1, z_2, z_3\}, \{z_1, z'_2, z'_3\}, \{z'_1, z_2, z'_3\}, \{z'_1, z'_2, z_3\},$$
$$\{z'_1, z'_2, z'_3\}, \{z'_1, z_2, z_3\}, \{z_1, z'_2, z_3\}, \{z_1, z_2, z'_3\}\big\}$$

and

$$\mathcal{S}(Z/Y) = \Big\{\big\{\{z_1,z_2,z_3\},\{z_1',z_2',z_3'\}\big\},\big\{\{z_1,z_2',z_3'\},\{z_1',z_2,z_3\}\big\},$$
$$\big\{\{z_1',z_2,z_3'\},\{z_1,z_2',z_3\}\big\},\big\{\{z_1',z_2',z_3\},\{z_1,z_2,z_3'\}\big\}\Big\}.$$

Let $Y \xleftarrow{\pi} Z$ be an arbitrary double covering of a Γ-set Y of n elements, so $|Z| = 2n$, and let $\{\zeta_1,\dots,\zeta_n\} \in \Omega(Z/Y)$. Even though the n-tuple $(\zeta_1,\dots,\zeta_n)$ is not uniquely determined by the set $\{\zeta_1,\dots,\zeta_n\}$, it turns out that the orbit

$$\big(\zeta_1,\dots,\zeta_n,\gamma_{Z/Y}(\zeta_1),\dots,\gamma_{Z/Y}(\zeta_n)\big)^{\mathfrak{A}_{2n}}$$

is well-defined, since every permutation of $\zeta_1,\dots,\zeta_n$ induces a corresponding permutation of $\gamma_{Z/Y}(\zeta_1),\dots,\gamma_{Z/Y}(\zeta_n)$, and the resulting permutation of the $2n$ elements $\zeta_1,\dots,\gamma_{Z/Y}(\zeta_n)$ is necessarily even. Therefore, we may define

$$\delta\big(\{\zeta_1,\dots,\zeta_n\}\big) = \big(\zeta_1,\dots,\zeta_n,\gamma_{Z/Y}(\zeta_1),\dots,\gamma_{Z/Y}(\zeta_n)\big)^{\mathfrak{A}_{2n}} \in \Sigma_{2n}(Z)/\mathfrak{A}_{2n} = \Delta(Z)$$

and thus obtain a morphism of Γ-sets

$$\delta = \delta_Z\colon\ \Omega(Z/Y) \to \Delta(Z). \tag{2}$$

On the other hand, since $\mathcal{S}(Z/Y)$ is a quotient of $\Omega(Z/Y)$, there is a canonical map

$$\varepsilon\colon\ \Omega(Z/Y) \to \mathcal{S}(Z/Y).$$

Proposition 1.4. *For $Y \xleftarrow{\pi} Z$ a double covering with $|Y| = n$ odd, the map*

$$(\delta,\varepsilon)\colon\ \Omega(Z/Y) \to \Delta(Z) \times \mathcal{S}(Z/Y)$$

is an isomorphism of Γ-sets.

Proof. Since the map (δ,ε) is clearly Γ-equivariant, and since the sets $\Omega(Z/Y)$ and $\Delta(Z) \times \mathcal{S}(Z/Y)$ both have 2^n elements, it suffices to show that (δ,ε) is injective. Suppose $\{\zeta_1,\dots,\zeta_n\}$, $\{\zeta_1',\dots,\zeta_n'\} \in \Omega(Z/Y)$ are distinct elements such that $\varepsilon\big(\{\zeta_1,\dots,\zeta_n\}\big) = \varepsilon\big(\{\zeta_1',\dots,\zeta_n'\}\big)$; then $\{\zeta_1',\dots,\zeta_n'\} = \gamma_Z\big(\{\zeta_1,\dots,\zeta_n\}\big)$ and we may assume the elements are numbered in such a way that $\pi(\zeta_i') = \pi(\zeta_i)$ (i.e. $\zeta_i' = \gamma_{Z/Y}(\zeta_i)$) for $i = 1,\dots,n$. Since the permutation which interchanges ζ_i and ζ_i' for $i = 1,\dots,n$ is odd, we have

$$(\zeta_1,\dots,\zeta_n,\zeta_1',\dots,\zeta_n')^{\mathfrak{A}_{2n}} \neq (\zeta_1',\dots,\zeta_n',\zeta_1,\dots,\zeta_n)^{\mathfrak{A}_{2n}},$$

hence $\delta\big(\{\zeta_1,\dots,\zeta_n\}\big) \neq \delta\big(\{\zeta_1',\dots,\zeta_n'\}\big)$. $\square$

If $Y \xleftarrow{\pi} Z$ and $Y \xleftarrow{\pi'} Z'$ are two double coverings of the same Γ-set Y with n elements, consider the *fiber product*

$$Z \times_Y Z' = \big\{(\zeta,\zeta') \in Z \times Z' \mid \pi(\zeta) = \pi'(\zeta')\big\} \subset Z \times Z'.$$

The group $\mathfrak{S}_2$ acts on $Z \times_Y Z'$ by mapping (ζ,ζ') to $\big(\gamma_{Z/Y}(\zeta),\gamma_{Z'/Y}(\zeta')\big)$. Let

$$Z *_Y Z' = (Z \times_Y Z')/\mathfrak{S}_2.$$

The canonical map $Y \xleftarrow{\pi\times\pi'} Z \times_Y Z'$ induces a map

$$Y \xleftarrow{\pi*\pi'} Z *_Y Z'$$

which is a double covering. In particular, for any Γ-set X of two elements and any covering $Y \xleftarrow{\pi} Z$ of degree 2, we may consider

$$Y \xleftarrow{\pi_2*\pi} (X \times Y) *_Y Z$$

where $Y \xleftarrow{\pi_2} X \times Y$ is the projection map. Abusing notation, we write simply

$$Y \xleftarrow{\pi} X * Z$$

for this double covering. The proof of the following easy proposition is omitted:

Proposition 1.5. *Let X be a set of two elements with trivial Γ-action, and let $Y \xleftarrow{\pi} Z$ be a double covering.*

(a) *The covering $Y \xleftarrow{\pi * \pi} Z *_Y Z$ is isomorphic to $Y \xleftarrow{\pi_2} X \times Y$.*
(b) *The covering $Y \xleftarrow{\pi} X * Z$ is (non-canonically) isomorphic to $Y \xleftarrow{\pi} Z$.*
(c) *The operation $*_Y$ defines a group structure on the set of isomorphism classes over Y of double coverings of Y. The neutral element is the isomorphism class of $Y \xleftarrow{\pi_2} X \times Y$.*

Proposition 1.6. *Let $Y \xleftarrow{\pi} Z$ and $Y \xleftarrow{\pi} Z'$ be two double coverings. There is a canonical isomorphism $\Delta(Z *_Y Z') \simeq \Delta(Z) * \Delta(Z')$.*

Proof. Recall from (2) the map

$$\delta_Z\colon\ \Omega(Z/Y) \to \Delta(Z)$$

defined for any double covering $Y \xleftarrow{\pi} Z$ of a Γ-set Y with $|Y| = n$. In the sequel, we write simply $\delta_Z(z_1, \dots, z_n)$ for $\delta_Z(\{z_1, \dots, z_n\})$. For ω, $\omega' \in \Omega(Z/Y)$, we have $\delta_Z(\omega) = \delta_Z(\omega')$ if and only if $|\omega \cap \omega'| \equiv n \bmod 2$. In particular, the map δ_Z is onto. Let $Y \xleftarrow{\pi} Z$ and $Y \xleftarrow{\pi'} Z'$ be two double coverings of Y. Denote simply by $\bar{}$ the canonical automorphisms $\gamma_{Z/Y}$ and $\gamma_{Z'/Y}$ and also the canonical automorphisms of $\Delta(Z)$ and $\Delta(Z')$. For $\{z_1, \dots, z_n\} \in \Omega(Z/Y)$ and $\{z'_1, \dots, z'_n\} \in \Omega(Z'/Y)$, we have

$$\delta_Z(\overline{z_1}, z_2, \dots, z_n) = \overline{\delta_Z(z_1, z_2, \dots, z_n)}$$

and, similarly,

$$\delta_{Z'}(\overline{z'_1}, z'_2, \dots, z'_n) = \overline{\delta_{Z'}(z'_1, z'_2, \dots, z'_n)}.$$

Therefore, the element

$$\Big\{\big(\delta_Z(z_1, \dots, z_n), \delta_{Z'}(z'_1, \dots, z'_n)\big), \big(\overline{\delta_Z(z_1, \dots, z_n)}, \overline{\delta_{Z'}(z'_1, \dots, z'_n)}\big)\Big\} \in \Delta(Z) * \Delta(Z')$$

depends only on

$$\omega = \Big\{\big\{(z_1, z'_1), (\overline{z_1}, \overline{z'_1})\big\}, \dots, \big\{(z_n, z'_n), (\overline{z_n}, \overline{z'_n})\big\}\Big\} \in \Omega(Z *_Y Z'/Y).$$

We thus have a canonical map

$$\psi\colon\ \Omega(Z *_Y Z'/Y) \to \Delta(Z) * \Delta(Z').$$

If $\omega' \in \Omega(Z *_Y Z'/Y)$ is obtained from ω by substituting

$$\big\{(z_1, \overline{z'_1}), (\overline{z_1}, z'_1)\big\} \quad \text{for} \quad \big\{(z_1, z'_1), (\overline{z_1}, \overline{z'_1})\big\},$$

then $\psi(\omega) \neq \psi(\omega')$, hence ψ is onto. On the other hand, if ω' is obtained from ω by an even number of changes as above, then $\psi(\omega) = \psi(\omega')$. Therefore, $\psi(\omega) = \psi(\omega')$ if $|\omega \cap \omega'| \equiv n \bmod 2$, and it follows that ψ factors through the map

$$\delta_{Z *_Y Z'}\colon\ \Omega(Z *_Y Z'/Y) \to \Delta(Z *_Y Z').$$

This completes the proof. $\square$

For later use, we record another case where the map δ of (2) can be used in the computation of a discriminant. Let X be a Γ-set of two elements. For any Γ-set Y, we may consider the double covering $Y \xleftarrow{\pi_2} X \times Y$ given by the projection.

Proposition 1.7. *If $|X| = 2$ and $|Y|$ is odd, the composition of the Γ-equivariant map*

$$\iota\colon X \to \Omega(X \times Y/Y), \qquad \iota(x) = \bigl\{(x,y) \mid y \in Y\bigr\}$$

and

$$\delta_{X\times Y}\colon \Omega(X \times Y/Y) \to \Delta(X \times Y)$$

defines an isomorphism

$$\delta \circ \iota\colon X \xrightarrow{\sim} \Delta(X \times Y).$$

Proof. Since $|Y|$ is odd, we have

$$\delta \circ \iota\bigl(\gamma_X(x)\bigr) = \gamma_{\Delta(X\times Y)}\bigl(\delta \circ \iota(x)\bigr) \qquad \text{for } x \in X.$$

Therefore, $\delta \circ \iota$ is surjective, hence bijective. □

Proposition 1.8. *Let X be a Γ-set of two elements, and let $Y \xleftarrow{\pi} Z$ be a double covering. There is a canonical isomorphism*

$$\mathcal{S}(Z/Y) \simeq \mathcal{S}(X * Z/Y).$$

Proof. For simplicity of notation, let $X = \{+,-\}$ and denote by $\bar{\ }$ the canonical automorphism $\gamma_{Z/Y}$. We may then identify $X*Z$ with the set of formal polynomials $\zeta - \overline{\zeta}$, for $\zeta \in Z$. Note however that the Γ-action on these polynomials is not linear, since Γ may act non trivially on $\{+,-\}$. The structure map $Y \leftarrow X * Z$ carries $\zeta - \overline{\zeta}$ to $\pi(\zeta) = \pi(\overline{\zeta})$. Therefore,

$$\Omega(X * Z/Y) = \bigl\{\{\zeta_1 - \overline{\zeta_1}, \dots, \zeta_n - \overline{\zeta_n}\} \mid \{\pi(\zeta_1), \dots, \pi(\zeta_n)\} = Y\bigr\}$$

and

$$\mathcal{S}(X * Z/Y) = \bigl\{\bigl\{\{\zeta_1 - \overline{\zeta_1}, \dots, \zeta_n - \overline{\zeta_n}\}, \{\overline{\zeta_1} - \zeta_1, \dots, \overline{\zeta_n} - \zeta_n\}\bigr\} \mid \{\pi(\zeta_1), \dots, \pi(\zeta_n)\} = Y\bigr\}.$$

On the other hand,

$$\mathcal{S}(Z/Y) = \bigl\{\bigl\{\{\zeta_1, \dots, \zeta_n\}, \{\overline{\zeta_1}, \dots, \overline{\zeta_n}\}\bigr\} \mid \{\pi(\zeta_1), \dots, \pi(\zeta_n)\} = Y\bigr\}.$$

The map

$$\bigl\{\{\zeta_1, \dots, \zeta_n\}, \{\overline{\zeta_1}, \dots, \overline{\zeta_n}\}\bigr\} \mapsto \bigl\{\{\zeta_1 - \overline{\zeta_1}, \dots, \zeta_n - \overline{\zeta_n}\}, \{\overline{\zeta_1} - \zeta_1, \dots, \overline{\zeta_n} - \zeta_n\}\bigr\}$$

is a Γ-isomorphism $\mathcal{S}(Z/Y) \xrightarrow{\sim} \mathcal{S}(X * Z/Y)$, whatever the action of Γ on $\{+,-\}$ is. □

2. Étale algebras and extensions

In this section, F is an arbitrary field. We denote by F_s a separable closure of F and let $\Gamma = \mathrm{Gal}(F_s/F)$. A finite-dimensional F-algebra E is called *étale* if $E \otimes_F F_s$ is isomorphic to a split F_s-algebra $F_s \times \cdots \times F_s$. For any étale F-algebra E of dimension n, the set of F-algebra homomorphisms

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

is a Γ-set of n elements since Γ acts on F_s.

Conversely, starting from a Γ-set X with $|X| = n$, we may let Γ act by semi-linear automorphisms on the F_s-algebra of maps $\mathrm{Map}(X, F_s)$. The fixed F-algebra

$$\mathbf{M}(X) = \mathrm{Map}(X, F_s)^\Gamma = \{f\colon X \to F_s \mid \gamma f(\xi) = f({}^\gamma\xi) \text{ for } \gamma \in \Gamma,\, \xi \in X\}$$

is étale of dimension n. Moreover, there are canonical isomorphisms

$$\mathbf{M}\bigl(\mathbf{X}(E)\bigr) \simeq E, \qquad \mathbf{X}\bigl(\mathbf{M}(X)\bigr) \simeq X$$

(see [3, (18.19)]), so that the functors $\mathbf{M}$ and $\mathbf{X}$ define an anti-equivalence between the category $\acute{\mathsf{E}}\mathsf{t}_F$ of étale F-algebras (with F-algebra homomorphisms) and the category Set_Γ of Γ-sets. Under this anti-equivalence, the direct product (resp. tensor product) of F-algebras corresponds to the disjoint union (resp. direct product) of Γ-sets: for E_1, E_2 étale F-algebras, there are obvious identifications

$$\mathbf{X}(E_1 \otimes E_2) = \mathbf{X}(E_1) \times \mathbf{X}(E_2) \quad \text{and} \quad \mathbf{X}(E_1 \times E_2) = \mathbf{X}(E_1) \amalg \mathbf{X}(E_2).$$

Moreover, if G is a group acting on an étale F-algebra E by F-automorphisms, then for the fixed subalgebra E^G we have

$$\mathbf{X}(E^G) = \mathbf{X}(E)/G$$

since E^G is the equalizer of the automorphisms $\sigma\colon E \to E$ for $\sigma \in G$, and $\mathbf{X}(E)/G$ is the co-equalizer of the corresponding automorphisms of $\mathbf{X}(E)$. Through the anti-equivalence $\acute{\mathsf{E}}\mathsf{t}_F \equiv \mathsf{Set}_\Gamma$, the constructions on Γ-sets defined in §1.1 therefore have counterparts in the category of étale F-algebras. The aim of this section is to make them explicit.

2.1. **Basic constructions on étale algebras.** Let E be an étale F-algebra of dimension n. Under the canonical isomorphism $E \simeq \mathbf{M}\bigl(\mathbf{X}(E)\bigr)$, the idempotents of E correspond to the characteristic functions of Γ-subsets of $\mathbf{X}(E)$. If $e \in E$ is the characteristic function of a subset $Y \subset \mathbf{X}(E)$, then multiplication by e defines an isomorphism $E/(1-e)E \xrightarrow{\sim} eE$. Moreover, $\mathbf{X}(eE) = Y$ and under the anti-equivalence $\acute{\mathsf{E}}\mathsf{t}_F \equiv \mathsf{Set}_\Gamma$, the map $E \to eE$ corresponds to the inclusion $\mathbf{X}(E) \leftarrow Y$.

Example 2.1. If E is the split étale F-algebra $E = F^n$, then $\mathbf{X}(E)$ is in duality with the set $e_1, \ldots, e_n$ of minimal idempotents of E, namely $\mathbf{X}(E) = \{\xi_1, \ldots, \xi_n\}$ where

$$\xi_i(e_j) = \begin{cases} 0 & \text{if } i \neq j, \\ 1 & \text{if } i = j. \end{cases}$$

The idempotent corresponding to a subset $Y = \{\xi_i \mid i \in I\} \subset \mathbf{X}(E)$ is $\sum_{i \in I} e_i$.

Let E be an arbitrary étale F-algebra of dimension n. For any integer k with $1 \leq k \leq n$, we let $s_k \in E^{\otimes k}$ be the idempotent corresponding to the characteristic function of the subset

$$\Sigma_k\bigl(\mathbf{X}(E)\bigr) = \bigl\{(\xi_1, \ldots, \xi_k) \mid \xi_i \neq \xi_j \text{ for } i \neq j\bigr\} \subset \mathbf{X}(E)^k = \mathbf{X}(E^{\otimes k}).$$

Therefore, letting $\Sigma_k(E) = s_k E^{\otimes k}$, we have

$$\mathbf{X}\bigl(\Sigma_k(E)\bigr) = \Sigma_k\bigl(\mathbf{X}(E)\bigr).$$

In particular, for $k = 2$ the idempotent $1 - s_2$ is the characteristic function of the diagonal of $\mathbf{X}(E) \times \mathbf{X}(E) = \mathbf{X}(E \otimes E)$. It is the *separability idempotent* of E, see [3, p. 285]. For $k \geq 3$, the idempotent s_k can also be defined in terms of the separability idempotent of E, see [8, p. 42], [3, p. 320].

The symmetric group $\mathfrak{S}_k$ acts on $E^{\otimes k}$ by permutation of the factors, and the idempotent s_k is fixed under this action, so $\mathfrak{S}_k$ also acts on $\Sigma_k(E)$. We consider the fixed subalgebra

$$\Lambda_k(E) = \Sigma_k(E)^{\mathfrak{S}_k} = s_k(E^{\otimes k})^{\mathfrak{S}_k}.$$

We have

$$\mathbf{X}\big(\Lambda_k(E)\big) = \Lambda_k\big(\mathbf{X}(E)\big)$$

since under the anti-equivalence $\acute{\mathit{E}}\mathit{t}_F \equiv \mathit{Set}_\Gamma$ the fixed algebra under $\mathfrak{S}_k$ corresponds to the factor set under the $\mathfrak{S}_k$-action.

The *discriminant* of E is defined by

$$\Delta(E) = \Sigma_n(E)^{\mathfrak{A}_n},$$

and we have

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

Example 2.2. If $E = F^n$ is split with minimal idempotents $e_1, \ldots, e_n$, then

$$s_k = \sum_{(i_1,\ldots,i_k)} e_{i_1} \otimes \cdots \otimes e_{i_k}$$

where $(i_1, \ldots, i_k)$ ranges over the k-tuples of pairwise distinct integers from 1 to n (i.e. $(i_1, \ldots, i_k) \in \Sigma_k\big(\{1, \ldots, n\}\big)$). The algebra $\Sigma_k(E)$ is then split, with minimal idempotents

$$e_{i_1} \otimes \cdots \otimes e_{i_k}$$

for $(i_1, \ldots, i_k) \in \Sigma_k\big(\{1, \ldots, n\}\big)$. Similarly, the algebra $\Lambda_k(E)$ is split, with minimal idempotents

$$e_{\{i_1,\ldots,i_k\}} = \sum_{\sigma\in\mathfrak{S}_k} e_{i_{\sigma(1)}} \otimes \cdots \otimes e_{i_{\sigma(k)}}$$

for $\{i_1, \ldots, i_k\}$ a subset of k elements of $\{1, \ldots, n\}$, i.e. $\{i_1, \ldots, i_k\} \in \Lambda_k\big(\{1, \ldots, n\}\big)$.

We also have $\Delta(E) \simeq F \times F$ if $n \geq 2$, with minimal idempotents

$$\sum_{\sigma\in\mathfrak{A}_n} e_{\sigma(1)} \otimes \cdots \otimes e_{\sigma(n)} \qquad \text{and} \qquad \sum_{\sigma\notin\mathfrak{A}_n} e_{\sigma(1)} \otimes \cdots \otimes e_{\sigma(n)}.$$

For an arbitrary étale F-algebra E of dimension n, the algebra $\Lambda_k(E)$ can also be viewed as an algebra of linear transformations of the exterior power $\bigwedge^k E$ (where E is just regarded as a vector space), as we now show.

Multiplication on the left defines an F-algebra homomorphism (the regular representation)

$$E^{\otimes k} \to \operatorname{End}_F(E^{\otimes k}).$$

As pointed out by Saltman [7, Lemma 1.1], the image of $(E^{\otimes k})^{\mathfrak{S}_k}$ in $\operatorname{End}_F(E^{\otimes k})$ preserves the kernel of the canonical map $E^{\otimes k} \to \bigwedge^k E$. Therefore, there is an induced F-algebra homomorphism

$$(E^{\otimes k})^{\mathfrak{S}_k} \to \operatorname{End}_F(\textstyle\bigwedge^k E). \tag{3}$$

Lemma 2.3. *The homomorphism* (3) *maps s_k to the identity map on $\bigwedge^k E$.*

Proof. It suffices to check the assertion over an extension of F. We may thus assume that E is split, $E = F^n$. Let $e_1, \dots, e_n$ be the minimal idempotents of E; then s_k is as in Example 2.2 and its image in $\operatorname{End}_F(\bigwedge^k E)$ maps $e_{j_1} \wedge \ldots \wedge e_{j_k}$ to

$$\sum_{(i_1,\dots,i_k)} e_{i_1}e_{j_1} \wedge \ldots \wedge e_{i_k}e_{j_k} = e_{j_1} \wedge \ldots \wedge e_{j_k}.$$

□

In view of the lemma, the homomorphism (3) induces an F-algebra homomorphism

$$\varphi_k\colon\ (E^{\otimes k})^{\mathfrak{S}_k}/(1-s_k)(E^{\otimes k})^{\mathfrak{S}_k} = \Lambda_k(E) \to \operatorname{End}_F(\textstyle\bigwedge^k E).$$

Saltman [7, Lemma 1.3] has shown that the image of this map has dimension $\binom{n}{k} = \dim \Lambda_k(E)$, hence φ_k is injective.

For instance, for $a, x_1, \dots, x_k \in E$,

$$\varphi_k\big(s_k(a\otimes\cdots\otimes a)\big)(x_1\wedge\ldots\wedge x_k) = ax_1 \wedge \ldots \wedge ax_k,$$

and

$$\begin{aligned}\varphi_k\big(s_k(a\otimes 1\otimes\cdots\otimes 1 + 1\otimes a\otimes\cdots\otimes 1 + \cdots + 1\otimes\cdots\otimes 1\otimes a)\big)(x_1\wedge\ldots\wedge x_k) =\\ (ax_1\wedge x_2\wedge\ldots\wedge x_k) + (x_1\wedge ax_2\wedge\ldots\wedge x_k) + \cdots + (x_1\wedge x_2\wedge\ldots\wedge ax_k).\end{aligned}$$

Now, consider the case where n is even, $n = 2m$. Since $\dim \bigwedge^n E = 1$, and the exterior product $\bigwedge^m E \times \bigwedge^m E \to \bigwedge^n E$ is a nonsingular bilinear pairing, there is an adjoint involution γ on $\operatorname{End}_F(\bigwedge^m E)$, defined by the equation

$$f(x)\wedge y = x \wedge \gamma(f)(y) \qquad \text{for } x,\, y \in \textstyle\bigwedge^m E,\ f \in \operatorname{End}_F(\bigwedge^m E).$$

Proposition 2.4. *The involution γ preserves the image of φ_k. Therefore, there is an induced involutive automorphism γ_E on $\Lambda_m(E)$ defined by $\varphi_m \circ \gamma_E = \gamma \circ \varphi_m$.*

Proof. Extending scalars to a separable closure, we may assume E is split. It is then spanned by its minimal idempotents $e_1, \dots, e_n$, and $\Lambda_m(E)$ is spanned by the minimal idempotents $e_{\{i_1,\dots,i_m\}}$ defined in Example 2.2 for $\{i_1,\dots,i_m\} \in \Lambda_m\big(\{1,\dots,n\}\big)$.

Computation shows that for $\{i_1,\dots,i_m\}$, $\{j_1,\dots,j_m\} \in \Lambda_m\big(\{1,\dots,n\}\big)$,

$$\varphi_m(e_{\{i_1,\dots,i_m\}})(e_{j_1}\wedge\ldots\wedge e_{j_m}) = \begin{cases} e_{j_1}\wedge\ldots\wedge e_{j_m} & \text{if } \{i_1,\dots,i_m\} = \{j_1,\dots,j_m\},\\ 0 & \text{if } \{i_1,\dots,i_m\} \neq \{j_1,\dots,j_m\}.\end{cases}$$

It is then easily verified that

$$\gamma\circ\varphi_m(e_{\{i_1,\dots,i_m\}}) = e_{\{k_1,\dots,k_m\}}, \tag{4}$$

where $\{k_1,\dots,k_m\}$ is the complementary subset of $\{i_1,\dots,i_m\}$ in $\{1,\dots,n\}$. □

We may now define

$$\mathcal{R}(E) = \Lambda_m(E)^{\mathfrak{S}_2} = \{x \in \Lambda_m(E) \mid \gamma_E(x) = x\}.$$

Theorem 2.5. $\mathbf{X}\big(\mathcal{R}(E)\big) = \mathcal{R}\big(\mathbf{X}(E)\big)$.

Proof. It suffices to see that under the anti-equivalence $\mathit{\acute{E}t}_F \equiv \mathit{Set}_\Gamma$, the automorphism γ_E of $\Lambda_m(E)$ corresponds to the permutation $\gamma_{\mathbf{X}(E)}$ of $\mathbf{X}\big(\Lambda_m(E)\big) = \Lambda_m\big(\mathbf{X}(E)\big)$. Again, we may extend scalars to a separable closure of F and assume E is split. Using the same notation as in the preceding proof, we may identify $\mathbf{X}(E)$ with the dual basis of $e_1, \ldots, e_n$. Equation (4) shows that

$$\gamma_E(e_{\{i_1,\ldots,i_m\}}) = e_{\{k_1,\ldots,k_m\}},$$

where $\{k_1,\ldots,k_m\}$ is the complementary subset of $\{i_1,\ldots,i_m\}$ in $\{1,\ldots,n\}$, and the proof is complete. □

When $\dim E = 2$, the algebra E is called a *quadratic* étale F-algebra. In the notation above, we then have $m = 1$, so $\Lambda_m(E) = E$, hence E carries a canonical involutive automorphism γ_E. Let E, E' be two quadratic étale F-algebras, with canonical involutive automorphisms γ_E, $\gamma_{E'}$. The tensor product $\gamma_E \otimes \gamma_{E'}$ defines a $\mathfrak{S}_2$-action on $E \otimes_F E'$, and we let

$$E * E' = (E \otimes_F E')^{\mathfrak{S}_2}.$$

Proposition 2.6. $\mathbf{X}(E * E') = \mathbf{X}(E) * \mathbf{X}(E')$.

Proof.

$$\mathbf{X}\big((E \otimes_F E')^{\mathfrak{S}_2}\big) = \mathbf{X}(E \otimes_F E')/\mathfrak{S}_2 = \big(\mathbf{X}(E) \times \mathbf{X}(E')\big)/\mathfrak{S}_2.$$

□

Let $\mathrm{Quad}(F)$ be the set of isomorphism classes of quadratic étale F-algebras, which is in bijection under $\mathbf{X}$ with the set of isomorphism classes of Γ-sets of two elements. The following analogue of Proposition 1.2 is easily proved, either directly or by reduction to Proposition 1.2 under the anti-equivalence $\mathit{\acute{E}t}_F \equiv \mathit{Set}_\Gamma$:

Proposition 2.7. *Let E, E' be two quadratic étale F-algebras.*

(a) *The F-algebra $E * E$ is split: $E * E \simeq F \times F$.*
(b) *If the algebra E' is split, then $E * E' \simeq E$ (not canonically).*
(c) *The operation $*$ defines a group structure on the set* $\mathrm{Quad}(F)$.

2.2. **Extensions of étale algebras.** An étale F-algebra B containing an F-algebra A (necessarily étale) is called an *extension of degree d* of A if it is a free A-module of rank d. Equivalently, this condition means that the inclusion $A \xrightarrow{i} B$ corresponds under the anti-equivalence $\mathit{\acute{E}t}_F \equiv \mathit{Set}_\Gamma$ to a map $\mathbf{X}(A) \xleftarrow{i^*} \mathbf{X}(B)$ which is a covering of degree d. Extensions of degree 2 are called *quadratic* extensions.

Suppose B/A is an extension of degree d. Let $\dim_F A = n$ (hence $\dim_F B = nd$), and let $s_n^A \in (A^{\otimes n})^{\mathfrak{S}_n}$ be the idempotent defining $\Sigma_n(A)$, see §2.1. Then $i^{\otimes n}(s_n^A)$ is an idempotent of $(B^{\otimes n})^{\mathfrak{S}_n}$. Define

$$\Omega(B/A) = i^{\otimes n}(s_n^A) \cdot (B^{\otimes n})^{\mathfrak{S}_n}.$$

Proposition 2.8. *There is a canonical surjective map $\Lambda_n(B) \to \Omega(B/A)$, and*

$$\mathbf{X}\big(\Omega(B/A)\big) = \Omega\big(\mathbf{X}(B)/\,\mathbf{X}(A)\big).$$

Therefore, $\dim_F \Omega(B/A) = d^n$.

Proof. The set $\mathbf{X}\big(\Omega(B/A)\big)$ is the set of F-algebra homomorphisms $(B^{\otimes n})^{\mathfrak{S}_n} \to F_s$ which map $i^{\otimes n}(s_n^A)$ to 1. Since

$$\mathbf{X}\big((B^{\otimes n})^{\mathfrak{S}_n}\big) = \mathbf{X}(B)^n/\mathfrak{S}_n,$$

every such homomorphism is the orbit of an n-tuple $(\xi_1,\dots,\xi_n)$ of elements of $\mathbf{X}(B)$; the condition that the homomorphism maps $i^{\otimes n}(s_n^A)$ to 1 is equivalent to the following: the homomorphism $(A^{\otimes n})^{\mathfrak{S}_n} \to F_s$ associated to the n-tuple $\big(i^*(\xi_1),\dots,i^*(\xi_n)\big)$ maps s_n^A to 1. In view of the definition of s_n^A, this means that $i^*(\xi_1)$, ..., $i^*(\xi_n)$ are pairwise distinct, hence

$$\{i^*(\xi_1),\dots,i^*(\xi_n)\} = \mathbf{X}(A)$$

since $|\,\mathbf{X}(A)| = n$. Of course, this condition implies that ξ_1, ..., ξ_n are pairwise distinct, hence $\{\xi_1,\dots,\xi_n\} \in \Lambda_n\big(\mathbf{X}(B)\big)$. Thus,

$$\begin{aligned}\mathbf{X}\big(\Omega(B/A)\big) = \big\{\{\xi_1,\dots,\xi_n\} \subset \mathbf{X}(B) \mid \{i^*(\xi_1),\dots,i^*(\xi_n)\} = \mathbf{X}(A)\big\}\\ = \Omega\big(\mathbf{X}(B)/\,\mathbf{X}(A)\big).\end{aligned}$$

The inclusion $\Omega\big(\mathbf{X}(B)/\,\mathbf{X}(A)\big) \subset \Lambda_n\big(\mathbf{X}(B)\big)$ yields the canonical surjective map $\Lambda_n(B) \to \Omega(B/A)$ under the anti-equivalence $\mathit{Ét}_F \equiv \mathit{Set}_\Gamma$. □

Now, suppose $d = 2$, so that $\dim_F B = 2n$. The canonical involutive automorphism $\gamma_{\mathbf{X}(B)/\,\mathbf{X}(A)}$ on $\mathbf{X}(B)$ corresponds to a canonical involutive automorphism $\gamma_{B/A}$ of B such that

$$A = \{x \in B \mid \gamma_{B/A}(x) = x\}.$$

On the other hand, there is also a "complementary subset" map

$$\gamma_{\mathbf{X}(B)}\colon\ \Lambda_n\big(\mathbf{X}(B)\big) \to \Lambda_n\big(\mathbf{X}(B)\big).$$

Since this map preserves $\Omega\big(\mathbf{X}(B)/\,\mathbf{X}(A)\big)$, the corresponding map $\gamma_B\colon\ \Lambda_n(B) \to \Lambda_n(B)$ induces an involutive automorphism on $\Omega(B/A)$, which we also denote by γ_B, and we may consider the subalgebra of fixed points

$$\mathcal{S}(B/A) = \Omega(B/A)^{\mathfrak{S}_2} = \{x \in \Omega(B/A) \mid \gamma_B(x) = x\}.$$

By definition, it is clear that

$$\mathbf{X}\big(\mathcal{S}(B/A)\big) = \mathcal{S}\big(\mathbf{X}(B)/\,\mathbf{X}(A)\big),$$

hence $\dim_F \mathcal{S}(B/A) = 2^{n-1}$.

Example 2.9. Suppose A and B are split of dimensions 3 and 6 respectively, with minimal idempotents e_1, e_2, e_3 and f_1, f_1', f_2, f_2', f_3, f_3' such that

$$e_i = f_i + f_i' \qquad \text{for } i = 1,\, 2,\, 3.$$

As observed in Example 2.2,

$$s_3^A = \sum_{\sigma\in\mathfrak{S}_3} e_{\sigma(1)} \otimes e_{\sigma(2)} \otimes e_{\sigma(3)},$$

and $\{e_{\sigma(1)} \otimes e_{\sigma(2)} \otimes e_{\sigma(3)} \mid \sigma \in \mathfrak{S}_3\}$ is the set of minimal idempotents of $\Sigma_3(A)$. Denoting in general by $\sum u \otimes v \otimes w$ the sum of the six products obtained by permuting the factors u, v, w (so

$$\sum u \otimes v \otimes w = \sum_{\sigma\in\mathfrak{S}_3} u_{\sigma(1)} \otimes u_{\sigma(2)} \otimes u_{\sigma(3)}$$

where $u_1 = u$, $u_2 = v$, $u_3 = w$), the minimal idempotents of $\Omega(B/A)$ are

$$\begin{aligned} g_0 &= \sum f_1 \otimes f_2 \otimes f_3, & g_0' &= \sum f_1' \otimes f_2' \otimes f_3', \\ g_1 &= \sum f_1 \otimes f_2' \otimes f_3', & g_1' &= \sum f_1' \otimes f_2 \otimes f_3, \\ g_2 &= \sum f_1' \otimes f_2 \otimes f_3', & g_2' &= \sum f_1 \otimes f_2' \otimes f_3, \\ g_3 &= \sum f_1' \otimes f_2' \otimes f_3, & g_3' &= \sum f_1 \otimes f_2 \otimes f_3'. \end{aligned}$$

The involution γ_B interchanges g_i and g_i' for $i = 0, \ldots, 3$, hence the minimal idempotents of $\mathcal{S}(B/A)$ are

$$g_0 + g_0', \qquad g_1 + g_1', \qquad g_2 + g_2', \qquad g_3 + g_3'.$$

Let B, B' be quadratic extensions of an étale F-algebra A. The canonical map $B \otimes_F B' \to B \otimes_A B'$ induces an injective map

$$\mathbf{X}(B) \times \mathbf{X}(B') = \mathbf{X}(B \otimes_F B') \leftarrow \mathbf{X}(B \otimes_A B')$$

which identifies $\mathbf{X}(B \otimes_A B')$ to the fiber product $\mathbf{X}(B) \times_{\mathbf{X}(A)} \mathbf{X}(B')$. The tensor product $\gamma_{B/A} \otimes \gamma_{B'/A}$ defines an action of $\mathfrak{S}_2$ on $B \otimes_A B'$ by A-automorphisms, and we let

$$B *_A B' = (B \otimes_A B')^{\mathfrak{S}_2}.$$

The following result is clear:

Proposition 2.10. $\mathbf{X}(B *_A B') = \mathbf{X}(B) *_{\mathbf{X}(A)} \mathbf{X}(B')$.

If E is an étale F-algebra of dimension 2, then $E \otimes_F A$ is a quadratic extension of A. For any quadratic extension B/A, we have $E \otimes_F B = (E \otimes_F A) \otimes_A B$ and we write simply

$$E * B \qquad \text{for} \qquad (E \otimes_F A) *_A B.$$

Let $\operatorname{Quad}(A)$ be the set of isomorphism classes *over* A of quadratic extensions of A. The following proposition is the analogue of Proposition 1.5:

Proposition 2.11. *Let E be a split étale F-algebra of dimension 2 (i.e. $E \simeq F \times F$), and let B/A be a quadratic extension of étale F-algebras.*

(a) *The extension $(B *_A B)/A$ is isomorphic to $(E \otimes_F A)/A$ (hence also to $(A \times A)/A$).*
(b) *The extension $(E * B)/A$ is (non-canonically) isomorphic to B/A.*
(c) *The operation $*_A$ defines a group structure on $\operatorname{Quad}(A)$. The neutral element is the isomorphism class of $(A \times A)/A$.*

It is clear that Propositions 1.4, 1.6 and 1.8 have analogues for étale algebras. We record them below.

Proposition 2.12. *Let E be an étale F-algebra of dimension 2, and let B/A and B'/A be quadratic extensions of an étale F-algebra A. There are canonical isomorphisms:*

(a) $\Delta(B) \otimes \mathcal{S}(B/A) \simeq \Omega(B/A)$ *(if $\dim A$ is odd);*
(b) $\Delta(B *_A B') \simeq \Delta(B) * \Delta(B')$*;*
(c) $\mathcal{S}(E * B/A) \simeq \mathcal{S}(B/A)$.

3. Cohomology of permutation groups

3.1. **Permutations.** For any finite set X, let $\mathfrak{S}_X$ be the symmetric group of X, i.e. the group of all permutations of X. Thus, $\mathfrak{S}_X = \mathfrak{S}_n$ for $X = \{1, \ldots, n\}$. Every permutation of a set X of n elements induces a permutation of the sets $\Sigma_k(X)$, $\Lambda_k(X)$ (for $k \leq n$), $\Delta(X)$, and of $\mathcal{R}(X)$ if n is even. There are therefore canonical group homomorphisms

$$\mathfrak{S}_X \to \mathfrak{S}_{\Sigma_k(X)}, \quad \mathfrak{S}_X \to \mathfrak{S}_{\Lambda_k(X)}, \quad \mathfrak{S}_X \to \mathfrak{S}_{\Delta(X)}, \quad \mathfrak{S}_X \to \mathfrak{S}_{\mathcal{R}(X)} \text{ (if } n \text{ is even).}$$

(If $n \geq 2$, the map $\mathfrak{S}_X \xrightarrow{\text{sgn}} \mathfrak{S}_{\Delta(X)} = \mathfrak{S}_2$ is the *signature* map.)

If $Y \xleftarrow{\pi} Z$ is a covering of degree d of a set of n elements, let

$$\mathfrak{S}_{Z/Y} = \big\{(\sigma, \tau) \in \mathfrak{S}_Y \times \mathfrak{S}_Z \mid \pi \circ \tau = \sigma \circ \pi\big\}$$

be the group of automorphisms of the covering. The map $(\sigma, \tau) \mapsto \tau$ identifies $\mathfrak{S}_{Z/Y}$ to a subgroup of $\mathfrak{S}_Z$. On the other hand, the map $(\sigma, \tau) \mapsto \sigma$ defines a surjective homomorphism

$$\beta_{Z/Y} \colon \mathfrak{S}_{Z/Y} \to \mathfrak{S}_Y$$

whose kernel is isomorphic to $\mathfrak{S}_d^n$ upon identifying each fiber of π with $\{1, \ldots, d\}$. Therefore, the group $\mathfrak{S}_{Z/Y}$ has order $(d!)^n n!$ and can be identified to a wreath product

$$\mathfrak{S}_{Z/Y} \simeq \mathfrak{S}_d \wr \mathfrak{S}_n.$$

Automorphisms of the covering $Y \leftarrow Z$ induce permutations of $\Omega(Z/Y)$, and of $\mathcal{S}(Z/Y)$ if $d = 2$, hence there are canonical group homomorphisms

$$\omega_{Z/Y} \colon \mathfrak{S}_{Z/Y} \to \mathfrak{S}_{\Omega(Z/Y)}, \qquad s_{Z/Y} \colon \mathfrak{S}_{Z/Y} \to \mathfrak{S}_{\mathcal{S}(Z/Y)} \text{ if } d = 2.$$

For later use, note that the kernel of $s_{Z/Y}$ is the "diagonal" subgroup $\mathfrak{S}_2$ of $\mathfrak{S}_{Z/Y}$, whose nontrivial element is $\gamma_{Z/Y}$. This diagonal subgroup is central in $\mathfrak{S}_{Z/Y}$.

On the other hand, every permutation of a set X with $n = 2m$ elements induces an automorphism of the covering $\mathcal{R}(X) \xleftarrow{\varepsilon} \Lambda_m(X)$, hence there is a canonical group homomorphism

$$\lambda_X \colon \mathfrak{S}_X \to \mathfrak{S}_{\Lambda_m(X)/\mathcal{R}(X)} \subset \mathfrak{S}_{\Lambda_m(X)}.$$

Proposition 3.1. *If $m \geq 2$, the image of λ_X is in the kernel of the signature map*

$$\text{sgn} \colon \mathfrak{S}_{\Lambda_m(X)} \to \mathfrak{S}_{\Delta(\Lambda_m(X))}.$$

Moreover, the composition of λ_X and the canonical homomorphism $s_{\Lambda_m(X)/\mathcal{R}(X)}$ is an injective map

$$\mathfrak{S}_X \hookrightarrow \mathfrak{S}_{\mathcal{S}(\Lambda_m(X)/\mathcal{R}(X))}.$$

The proof is left to the reader.

3.2. **Cohomology and Γ-sets.** As in §1, we denote by Γ a profinite group, which will be fixed throughout this subsection. The action of Γ on a set X with $|X| = n$ can be viewed as a group homomorphism

$$\Gamma \to \mathfrak{S}_X \simeq \mathfrak{S}_n.$$

Since the isomorphism $\mathfrak{S}_X \simeq \mathfrak{S}_n$ depends on the indexing of the elements in X, the homomorphism $\Gamma \to \mathfrak{S}_n$ is defined by X up to conjugation by an element in $\mathfrak{S}_n$. Therefore, there is a canonical one-to-one correspondence between isomorphism classes of Γ-sets of n elements and the cohomology set $H^1(\Gamma, \mathfrak{S}_n)$ (with the trivial action of Γ on $\mathfrak{S}_n$), by definition of this cohomology set. Under this correspondence, the distinguished element of $H^1(\Gamma, \mathfrak{S}_n)$ is mapped to the set with trivial Γ-action.

Since the symmetric group $\mathfrak{S}_2$ is abelian, there is an abelian group structure on $H^1(\Gamma, \mathfrak{S}_2)$. We leave it to the reader to verify that the product of the isomorphism classes of the Γ-sets X, X' with $|X| = |X'| = 2$ is the isomorphism class of $X * X'$.

Similarly, every covering $Y \xleftarrow{\pi} Z$ of degree d of a Γ-set Y with $|Y| = n$ yields a group homomorphism

$$\Gamma \to \mathfrak{S}_{Z/Y} \simeq \mathfrak{S}_d \wr \mathfrak{S}_n,$$

and there is a canonical one-to-one correspondence between isomorphism classes of coverings of degree d of Γ-sets of n elements and the cohomology set $H^1(\Gamma, \mathfrak{S}_d \wr \mathfrak{S}_n)$, which maps the distinguished element of the cohomology set to the covering with trivial Γ-action.

The basic constructions in subsections 1.1 and 1.2 yield canonical maps of cohomology sets through the induced homomorphisms of permutation groups (see §3.1). For instance, if X is a Γ-set of n elements and $k \leq n$, the canonical homomorphism $\sigma_k \colon \mathfrak{S}_X \to \mathfrak{S}_{\Sigma_k(X)}$ induces a morphism of pointed sets

$$\sigma_k^1 \colon H^1(\Gamma, \mathfrak{S}_X) \to H^1(\Gamma, \mathfrak{S}_{\Sigma_k(X)}).$$

Since the Γ-action on $\Sigma_k(X)$ is induced by the Γ-action on X through σ_k, the morphism σ_k^1 maps the isomorphism class of X to the isomorphism class of $\Sigma_k(X)$. A similar statement obviously holds for the morphisms

$$\begin{aligned} &H^1(\Gamma, \mathfrak{S}_X) \to H^1(\Gamma, \mathfrak{S}_{\Lambda_k(X)}),\\ &H^1(\Gamma, \mathfrak{S}_X) \to H^1(\Gamma, \mathfrak{S}_{\Delta(X)}),\\ &H^1(\Gamma, \mathfrak{S}_X) \to H^1(\Gamma, \mathfrak{S}_{\mathcal{R}(X)}) \text{ if } n \text{ is even.} \end{aligned}$$

Similarly, if $Y \xleftarrow{\pi} Z$ is a covering of degree d of Γ-sets, the canonical homomorphisms $\omega_{Z/Y}$ and $s_{Z/Y}$ of §3.1 induce morphisms of pointed sets

$$\begin{aligned} &\omega_{Z/Y}^1 \colon H^1(\Gamma, \mathfrak{S}_{Z/Y}) \to H^1(\Gamma, \mathfrak{S}_{\Omega(Z/Y)}),\\ &s_{Z/Y}^1 \colon H^1(\Gamma, \mathfrak{S}_{Z/Y}) \to H^1(\Gamma, \mathfrak{S}_{\mathcal{S}(Z/Y)}) \text{ if } d = 2. \end{aligned}$$

Since the Γ-action on $\Omega(Z/Y)$ and $\mathcal{S}(Z/Y)$ (if $d = 2$) are induced by the Γ-action on Z/Y through $\omega_{Z/Y}$ and $\sigma_{Z/Y}$ respectively, the morphisms $\omega_{Z/Y}^1$ and $s_{Z/Y}^1$ map the isomorphism class of the covering Z/Y to the isomorphism class of the Γ-sets $\Omega(Z/Y)$ and $\mathcal{S}(Z/Y)$, respectively.

Recall also from §3.1 the canonical homomorphism $\beta_{Z/Y} \colon \mathfrak{S}_{Z/Y} \to \mathfrak{S}_Y$ which maps every permutation of a covering to the induced permutation of the base. Let $\mathfrak{T}_{Z/Y} = \ker \beta_{Z/Y}$. This is the group of automorphisms over Y of the covering Z/Y, hence $H^1(\Gamma, \mathfrak{T}_{Z/Y})$ is in one-to-one correspondence with the set of isomorphism classes over Y of coverings of degree d of Y, where the Γ-action on Y is trivial.

The case of non-trivial Γ-action can be taken into account by twisting, see [3, §28.C]. If Z/Y is a covering of degree d, we define a non-trivial action of Γ on $\mathfrak{S}_{Z/Y}$ by conjugation: the action of Γ on Z/Y is a group homomorphism

$$\alpha \colon \Gamma \to \mathfrak{S}_{Z/Y},$$

and we define, for $\gamma \in \Gamma$ and $f \in \mathfrak{S}_{Z/Y}$,

$$\gamma * f = \alpha(\gamma) \circ f \circ \alpha(\gamma)^{-1}.$$

Let $\mathfrak{S}'_{Z/Y}$ be the group $\mathfrak{S}_{Z/Y}$ with this action of Γ, and define $\mathfrak{S}'_Y$ similarly. By [3, (28.8)], there are canonical bijections

$$H^1(\Gamma, \mathfrak{S}'_{Z/Y}) \xrightarrow{\sim} H^1(\Gamma, \mathfrak{S}_{Z/Y}) \qquad \text{and} \qquad H^1(\Gamma, \mathfrak{S}'_Y) \xrightarrow{\sim} H^1(\Gamma, \mathfrak{S}_Y)$$

which map the distinguished element of $H^1(\Gamma, \mathfrak{S}'_{Z/Y})$, $H^1(\Gamma, \mathfrak{S}'_Y)$ to the isomorphism class of the covering Z/Y and to the isomorphism class of Y, respectively. The map $\beta_{Z/Y}$ is also a Γ-group homomorphism $\beta_{Z/Y}\colon \mathfrak{S}'_{Z/Y} \to \mathfrak{S}'_Y$. Let $\mathfrak{T}'_{Z/Y} \subset \mathfrak{S}'_{Z/Y}$ be the kernel of $\beta_{Z/Y}$. Then $H^1(\Gamma, \mathfrak{T}'_{Z/Y})$ is in natural one-to-one correspondence with the set $C^d(Y)$ of isomorphism classes *over* Y of coverings of degree d of Y. (The distinguished element of $H^1(\Gamma, \mathfrak{T}'_{Z/Y})$ corresponds to the isomorphism class of Z/Y.)

The exact sequence of Γ-groups

$$1 \to \mathfrak{T}'_{Z/Y} \to \mathfrak{S}'_{Z/Y} \xrightarrow{\beta_{Z/Y}} \mathfrak{S}'_Y \to 1$$

yields an exact sequence in cohomology

$$H^0(\Gamma, \mathfrak{S}'_Y) \to H^1(\Gamma, \mathfrak{T}'_{Z/Y}) \to H^1(\Gamma, \mathfrak{S}'_{Z/Y}) \xrightarrow{\beta^1_{Z/Y}} H^1(\Gamma, \mathfrak{S}'_Y).$$

The kernel of $\beta^1_{Z/Y}$ is the set of isomorphism classes of coverings of degree d of Y. By [3, (28.4)], this kernel is in canonical bijection with the orbit space of $H^1(\Gamma, \mathfrak{T}'_{Z/Y})$ under the fixed-point group $H^0(\Gamma, \mathfrak{S}'_Y)$. Note that $H^0(\Gamma, \mathfrak{S}'_Y)$ is the group of permutations of Y which commute with the action of Γ; in other words, it is the group of automorphisms of the Γ-set Y,

$$H^0(\Gamma, \mathfrak{S}'_Y) = \operatorname{Aut}_\Gamma(Y).$$

This group acts naturally on $C^d(Y)$, and

$$\ker \beta^1_{Z/Y} \simeq C^d(Y)/\operatorname{Aut}_\Gamma(Y).$$

When the Γ-action on Y is transitive, let $\Gamma_0 \subset \Gamma$ be the stabilizer of an arbitrary (but fixed) element of Y, so that $Y \simeq \Gamma/\Gamma_0$. Then we may identify $\mathfrak{T}'_{Z/Y}$ with $\operatorname{Map}(\Gamma/\Gamma_0, \mathfrak{S}_d)$ and get a canonical bijection in the spirit of Shapiro's lemma

$$H^1(\Gamma, \mathfrak{T}'_{Z/Y}) \simeq H^1(\Gamma_0, \mathfrak{S}_d),$$

see [3, (28.20)].

Whatever the action of Γ on Y, when $d = 2$ the group $\mathfrak{T}'_{Z/Y}$ ($\simeq \mathfrak{S}_d^n$ where $n = |Y|$) is abelian, hence the set $H^1(\Gamma, \mathfrak{T}'_{Z/Y})$ is an abelian group. When Z/Y is the projection covering $\big(\{1,2\} \times Y\big)/Y$, the bijection $H^1(\Gamma, \mathfrak{T}'_{Z/Y}) \simeq C^2(Y)$ is a group isomorphism for the group structure induced on $C^2(Y)$ by the operation $*_Y$ of §1.2. Note that this operation is generally *not* defined on the orbit set $\ker \beta^1_{Z/Y} \simeq C^2(Y)/\operatorname{Aut}_\Gamma(Y)$.

3.3. **Torsors.** As in the preceding subsection, we fix a profinite group Γ. Besides the correspondence between $H^1(\Gamma, \mathfrak{S}_n)$ and the isomorphism classes of Γ-sets of n elements explained in the preceding subsection, there is also a one-to-one correspondence between $H^1(\Gamma, \mathfrak{S}_n)$ and isomorphism classes of $\mathfrak{S}_n$-torsors, i.e. of Γ-sets of $n! = |\mathfrak{S}_n|$ elements with a free action of $\mathfrak{S}_n$ (on the right) compatible with the Γ-action (on the left), see [3, (28.14)]. Combining the correspondences, we obtain a bijection between isomorphism classes of Γ-sets of n elements and $\mathfrak{S}_n$-torsors. To the isomorphism class of the Γ-set X with $|X| = n$ corresponds the class of $\Sigma_n(X)$, which clearly is an $\mathfrak{S}_n$-torsor. Conversely, we associate to an $\mathfrak{S}_n$-torsor Σ the class of $\Sigma/\mathfrak{S}_{n-1}$. The n projections

$$\pi_i\colon \Sigma_n(X) \to X, \qquad (\xi_1, \dots, \xi_n) \mapsto \xi_i \text{ for } i = 1, \dots, 2$$

are Γ-equivariant maps and satisfy

$$\pi_i\big((\xi_1, \dots, \xi_n)^\sigma\big) = \pi_{\sigma(i)}(\xi_1, \dots, \xi_n) \qquad \text{for } \sigma \in \mathfrak{S}_n.$$

Definition 3.2. An $\mathfrak{S}_n$*-Galois closure* of a Γ-set X of n elements is a pair (Σ, π) where Σ is an $\mathfrak{S}_n$-torsor and $X \xleftarrow{\pi} \Sigma$ is a covering (necessarily of degree $(n-1)!$) such that $\pi(x^\sigma) = \pi(x)$ for $x \in \Sigma$ and $\sigma \in \mathfrak{S}_{n-1}$.

Every $\mathfrak{S}_n$-Galois closure of X is isomorphic to $(\Sigma_n(X), \pi_n)$.

A similar construction can be given for coverings, since the set $H^1(\Gamma, \mathfrak{S}_d \wr \mathfrak{S}_n)$ classifies $\mathfrak{S}_d \wr \mathfrak{S}_n$-torsors as well as coverings of degree d of Γ-sets of n elements. If $Y \xleftarrow{\pi} Z$ is a covering of degree d of a Γ-set Y of n elements (so $|Z| = nd$), let $\Sigma(Z/Y)$ be the set of arrays

$$(\zeta_{ij})_{\substack{1\le i\le d\\ 1\le j\le n}}$$

of pairwise distinct elements of Z such that $\pi(\zeta_{ij})$ depends only on j for $i = 1, \dots, n$. The set $\Sigma(Z/Y)$ is a $\mathfrak{S}_d \wr \mathfrak{S}_n$-torsor. Its isomorphism class, viewed as an element of $H^1(\Gamma, \mathfrak{S}_d \wr \mathfrak{S}_n)$, corresponds to the isomorphism class of the covering $Y \xleftarrow{\pi} Z$. The nd projections

$$\pi_{k\ell}\colon \Sigma(Z/Y) \to Z, \quad (\zeta_{ij})_{\substack{1\le i\le d\\ 1\le j\le n}} \mapsto \zeta_{k\ell}$$

are Γ-equivariant maps. The projection $\pi\colon Z \to Y$ induces a $\mathfrak{S}_n$-equivariant projection

$$\Sigma(\pi)\colon \Sigma(Z/Y) \to \Sigma_n(Y), \quad (\zeta_{ij}) \mapsto \big(\pi(\zeta_{i1}), \dots, \pi(\zeta_{in})\big)$$

and $\Sigma_n(Y) \xleftarrow{\Sigma(\pi)} \Sigma(Z/Y)$ is a covering of degree $(d!)^n$. Moreover the diagram

$$\begin{array}{ccc}
\Sigma_n(Y) & \xleftarrow{\Sigma(\pi)} & \Sigma(Z/Y) \\
{\scriptstyle \pi_j}\big\downarrow & & \big\downarrow{\scriptstyle \pi_{ij}} \\
Y & \xleftarrow{\pi} & Z
\end{array}$$

is commutative. We say that $\Sigma_n(Y) \xleftarrow{\Sigma(\pi)} \Sigma(Z/Y)$ is an $\mathfrak{S}_d \wr \mathfrak{S}_n$*-Galois closure of* $Y \xleftarrow{\pi} Z$. (We leave it to the reader to formalize the definition of a $\mathfrak{S}_d \wr \mathfrak{S}_n$-Galois closure of $Y \xleftarrow{\pi} Z$.)

Note that the set $\Omega(Z/Y)$ of sections of Z/Y (see §1.2) can be identified with the set $\Sigma(Z/Y)/(\mathfrak{S}_{d-1} \wr \mathfrak{S}_n)$.

3.4. **Cohomology and étale algebras.** In this section, F is an arbitrary field, F_s is a separable closure of F and $\Gamma = \mathrm{Gal}(F_s/F)$ is the absolute Galois group of F. The anti-equivalence $\textit{Ét}_F \equiv \textit{Set}_\Gamma$ induces a canonical bijection between the set of isomorphism classes of étale F-algebras of dimension n and the set of isomorphism classes of Γ-sets of n elements. Since the latter set is in one-to-one correspondence with the cohomology set $H^1(\Gamma, \mathfrak{S}_n)$ (see §3.2), there is also a canonical bijection between $H^1(\Gamma, \mathfrak{S}_n)$ and isomorphism classes of étale F-algebras of dimension n.

This bijection can be set up directly, by identifying $\mathfrak{S}_n$ with the group of automorphisms of the split algebra F_s^n. More precisely, given an étale algebra A and an isomorphism $\alpha\colon F^n \otimes F_s \xrightarrow{\sim} A \otimes F_s$, the corresponding cocycle is $(f_\gamma)_{\gamma\in\Gamma}$, where

$$f_\gamma = \alpha^{-1} \circ (1 \otimes \gamma) \circ \alpha \circ (1 \otimes \gamma^{-1}) \in \operatorname{Aut}_{F_s}(F^n \otimes F_s) = \mathfrak{S}_n.$$

Conversely, given a cocycle $(f_\gamma)_{\gamma\in\Gamma}$ in $\mathfrak{S}_n$, the corresponding étale algebra is

$$A_\gamma = \{x \in F_s^n \mid \gamma f_\gamma(x) = x\}$$

where Γ acts on F_s^n entrywise.

As in §3.2, the basic constructions on étale algebras of §2.1 can be interpreted in terms of morphisms of cohomology sets. Details are left to the reader, as well as the analogues for extensions of étale algebras and the cohomology of wreath products. We simply note for later use the canonical isomorphism

$$\operatorname{Quad}(F) \simeq H^1(F, \mathfrak{S}_2)$$

where $\operatorname{Quad}(F)$ is the group of isomorphism classes of quadratic étale F-algebras (see Proposition 2.7). For any étale F-algebra A, we also have canonical isomorphisms

$$\operatorname{Quad}(A) \simeq C^2\big(\mathbf{X}(A)\big) \simeq H^1(\Gamma, \mathfrak{T}'_{\mathbf{X}(A\times A)/\mathbf{X}(A)}),$$

see §3.2. The set of isomorphism classes *over* F of quadratic extensions of A is $\operatorname{Quad}(A)/\operatorname{Aut}_F(A)$. The operation $*_A$ is generally *not* defined on this set.

3.5. **Galois algebras.** As in the preceding subsection, F is an arbitrary field and Γ is the absolute Galois group of F. Let G be a finite group. A G-Galois F-algebra is an étale F-algebra of dimension $|G|$ with an action of G by F-algebra automorphisms such that the algebra of fixed points is F (see [3, (18.15)]). Equivalently, an étale F-algebra E of dimension $|G|$ with an action of G is G-Galois if and only if the Γ-set $\mathbf{X}(E)$ is a G-torsor for the induced action of G. Therefore, the discussion of torsors in §3.3 has an analogue in terms of Galois algebras, and the set $H^1(\Gamma, \mathfrak{S}_n)$ is also in one-to-one correspondence with the set of isomorphism classes of $\mathfrak{S}_n$-Galois F-algebras.

If E is an étale F-algebra of dimension n, the algebra $\Sigma_n(E)$ has a natural action of $\mathfrak{S}_n$, for which it is an $\mathfrak{S}_n$-Galois algebra. There are n embeddings $\varepsilon_i\colon E \to \Sigma_n(E)$ corresponding to the projections $\pi_i\colon \Sigma_n\big(\mathbf{X}(E)\big) \to \mathbf{X}(E)$. They are defined explicitly as follows: for $x \in E$,

$$\varepsilon_i(x) = s_n \cdot 1 \otimes \cdots \otimes x \otimes \cdots \otimes 1 \qquad (x \text{ in } i\text{-th position})$$

where $s_n \in E^{\otimes n}$ is the idempotent such that $\Sigma_n(E) = s_n E^{\otimes n}$. Clearly, for $\sigma \in \mathfrak{S}_n$ and $x \in E$,

$$\varepsilon_{\sigma(i)}(x) = \sigma\big(\varepsilon_i(x)\big).$$

Definition 3.3. An $\mathfrak{S}_n$*-Galois closure* of an étale F-algebra E of dimension n is a pair (σ, ε) where Σ is an $\mathfrak{S}_n$-Galois F-algebra and $\varepsilon\colon E \to \Sigma$ is an embedding such that $\sigma\big(\varepsilon(x)\big) = \varepsilon(x)$ for $\sigma \in \mathfrak{S}_n$ and $x \in E$.

Every $\mathfrak{S}_n$-Galois closure of E is isomorphic to $(\Sigma_n(E), \varepsilon_n)$. This construction was suggested by Saltman, see [8, p. 42].

Example 3.4. Let A be a *cubic étale F-algebra*, i.e., $\dim A = 3$. The choice of any of the three canonical embeddings $\varepsilon_i\colon A \to \Sigma_3(A)$ induces an isomorphism

$$A \otimes \Delta(A) \simeq \Sigma_3(A).$$

This follows from the fact that the corresponding map $\Sigma_3(X) \to X \times \Delta(X)$ is bijective if $|X| = 3$, see [3, (18.27)].

We next sketch an analogue of the Galois closure for extensions of étale algebras, on the model of the corresponding construction for coverings in §3.3.

Let B/A be an extension of degree d of an étale F-algebra A of degree n. Viewing B as an étale A-algebra of degree d, we have an $\mathfrak{S}_d$-Galois closure $\Sigma_d^A(B)$ of B which is étale of degree $d!$ over A,

$$\Sigma_d^A(B) = s_d^{B/A} \cdot B^{\otimes_A d}$$

where $s_d^{B/A}$ is the idempotent corresponding to the characteristic function of the subset $\{(\xi_1, \dots, \xi_d) \mid \xi_i \neq \xi_j \text{ for } i \neq j, \text{ and } \pi(\xi_i) = \pi(\xi_j) \text{ for } i = 1, \dots, d\}$ in

$$\mathbf{X}(B) \times_{\mathbf{X}(A)} \cdots \times_{\mathbf{X}(A)} \mathbf{X}(B) = \mathbf{X}(B \otimes_A \cdots \otimes_A B).$$

There are d canonical embeddings $\varepsilon_i^A \colon B \to \Sigma_d^A(B)$ and a canonical embedding $j \colon A \to \Sigma_d^A(B)$ corresponding to the A-algebra structure on $\Sigma_d^A(B)$. Define

$$\Sigma(B/A) = j^{\otimes n}(s_n^A) \cdot \Sigma_d^A(B)^{\otimes n}.$$

As for Proposition 2.8 we have

Proposition 3.5. $\mathbf{X}\big(\Sigma(B/A)\big) = \Sigma\big(\mathbf{X}(B)/\mathbf{X}(A)\big)$.

The algebra $\Sigma(B/A)$ is an extension of $\Sigma_n(A)$ of degree $(d!)^n$ and there exist nd canonical embeddings

$$\varepsilon_{ij} \colon B \to \Sigma(B/A),\ 1 \leq i \leq d,\ 1 \leq j \leq n \tag{5}$$

such that the diagram

$$\begin{array}{ccc} \Sigma_n(A) & \longrightarrow & \Sigma(B/A) \\ {\scriptstyle \varepsilon_i}\uparrow & & \uparrow{\scriptstyle \varepsilon_{ij}} \\ A & \longrightarrow & B \end{array}$$

is commutative for all i and j. We say that the extension $\Sigma(B/A)/\Sigma_n(A)$ is an $\mathfrak{S}_d \wr \mathfrak{S}_n$-*Galois closure* of the extension B/A. Since $\Sigma_d^A(B)^{\mathfrak{S}_{d-1}} = B$, we have

$$\Sigma(B/A)^{\mathfrak{S}_{d-1} \wr \mathfrak{S}_n} = \Omega(B/A).$$

If $d = 2$, each of the canonical embeddings $\varepsilon_1^A, \varepsilon_2^A \colon B \to \Sigma_2^A(B)$ is an isomorphism (and $\varepsilon_2^A = \varepsilon_1^A \circ \gamma_{B/A}$), and $j \colon A \to \Sigma_2^A(B) = B$ is the inclusion. The algebra

$$\Sigma(B/A) = j^{\otimes n}(s_n^A) \cdot B^{\otimes n}$$

is an extension of degree 2^n of $\Sigma_n(A)$, and

$$\Omega(B/A) \simeq \Sigma(B/A)^{\mathfrak{S}_n}.$$

Example 3.6. Suppose, as in Example 2.9, that A and B are split of dimensions 3 and 6 respectively, with minimal idempotents e_1, e_2, e_3 and $f_1, f_1', f_2, f_2', f_3, f_3'$ such that

$$e_i = f_i + f_i' \qquad \text{for } i = 1, 2, 3.$$

The algebra $\Sigma(B/A)$ is split. Its 48 minimal idempotents are

$$\begin{array}{ll} f_{\sigma(1)} \otimes f_{\sigma(2)} \otimes f_{\sigma(3)}, & f'_{\sigma(1)} \otimes f'_{\sigma(2)} \otimes f'_{\sigma(3)}, \\ f_{\sigma(1)} \otimes f'_{\sigma(2)} \otimes f'_{\sigma(3)}, & f'_{\sigma(1)} \otimes f_{\sigma(2)} \otimes f_{\sigma(3)}, \\ f'_{\sigma(1)} \otimes f_{\sigma(2)} \otimes f'_{\sigma(3)}, & f_{\sigma(1)} \otimes f'_{\sigma(2)} \otimes f_{\sigma(3)}, \\ f'_{\sigma(1)} \otimes f'_{\sigma(2)} \otimes f_{\sigma(3)}, & f_{\sigma(1)} \otimes f_{\sigma(2)} \otimes f'_{\sigma(3)}, \end{array}$$

where σ varies in $\mathfrak{S}_3$. The action of $\mathfrak{S}_3$ on these idempotents is clear, and the fixed subalgebra is $\Omega(B/A)$ as described in Example 2.9.

Proposition 3.7. *Let B/A be an extension of étale algebras of degree d and let $n = \dim_F A$. If $b \in B$ is a generator of B as F-algebra, then the nd elements $\varepsilon_{ij}(b)$ generate $\Sigma(B/A)$ over $\Sigma_n(A)$.*

Proof. Let Σ' be the subalgebra of $\Sigma(B/A)$ generated over $\Sigma(A)$ by the $\varepsilon_{ij}(b)$. We show that $\Sigma' = \Sigma(B/A)$. We may assume that A and B are split and we assume for simplicity that $n = 3$ and $d = 2$. We use the notations of Example 2.9. Let

$$b = \beta_1 f_1 + \beta'_1 f'_1 + \beta_2 f_2 + \beta'_2 f'_2 + \beta_3 f_3 + \beta'_3 f'_3$$

with $\beta_1, \ldots, \beta'_3 \in F$, hence

$$\overline{b} = \beta'_1 f_1 + \beta_1 f'_1 + \beta'_2 f_2 + \beta_2 f'_2 + \beta'_3 f_3 + \beta_3 f'_3.$$

Since b generates B, the 6 elements β_i, β'_j are pairwise different. We have

$$\varepsilon_{11}(b) = s_3^A \cdot b \otimes 1 \otimes 1 \text{ and } \varepsilon_{21}(b) = s_3^A \cdot \overline{b} \otimes 1 \otimes 1.$$

Thus

$$\begin{array}{rcll} \varepsilon_{11}(b)(e_1 \otimes e_2 \otimes e_3) & = & (\beta_1 f_1 + \beta'_1 f'_1) \otimes e_2 \otimes e_3 & \text{and} \\ \varepsilon_{21}(b)(e_1 \otimes e_2 \otimes e_3) & = & (\beta'_1 f_1 + \beta_1 f'_1) \otimes e_2 \otimes e_3 & \end{array}$$

are elements of Σ'. It follows that $f_1 \otimes e_2 \otimes e_3$ and $f'_1 \otimes e_2 \otimes e_3$ are in Σ'. Hence all the minimal idempotents of $\Sigma(B/A)$ are in Σ' and $\Sigma' = \Sigma(B/A)$. □

4. The symmetric group on four elements

In the rest of this paper, we focus on various aspects of étale algebras of dimension 4 (called *quartic* étale algebras) which, as explained in the preceding sections, can be viewed from the perspective of Γ-sets of 4 elements, or of the cohomology of $\mathfrak{S}_4$, or of $\mathfrak{S}_4$-torsors, or of $\mathfrak{S}_4$-Galois algebras. It turns out that there is a group isomorphism

$$\mathfrak{S}_2 \times \mathfrak{S}_4 \simeq \mathfrak{S}_2 \wr \mathfrak{S}_3$$

which relates the various "quartic" notions listed above to those associated with the cohomology of $\mathfrak{S}_2 \wr \mathfrak{S}_3$: quadratic extensions of cubic étale algebras, double coverings of sets of 3 elements, $\mathfrak{S}_2 \wr \mathfrak{S}_3$-torsors and $\mathfrak{S}_2 \wr \mathfrak{S}_3$-Galois algebras. We explain this relation in the simplest case, namely Γ-sets and coverings, and then give the cohomological viewpoint in the next subsection. In the last two subsections, we give explicit constructions of $\mathcal{R}(Q)$ for a quartic algebra Q, making clear that this algebra is related to the resolvent cubic of quartic equations, and of $\Omega(B/A)$ and $\mathcal{S}(B/A)$ for a quadratic extension of a cubic algebra A.

4.1. **Sets of four elements and double coverings.** In this subsection, Γ is an arbitrary profinite group. Suppose X is a Γ-set with $|X|=4$, as in Example 1.1, where the constructions of $\Lambda_2(X)$ and $\mathcal{R}(X)$ are made explicit. Our first observation concerns the discriminants of $\Lambda_2(X)$ and $\mathcal{R}(X)$:

Proposition 4.1. *The map which carries* $(\xi_1,\xi_2,\xi_3,\xi_4)\in\Sigma_4(X)$ *to*

$$\big(\{\{\xi_1,\xi_2\},\{\xi_3,\xi_4\}\},\{\{\xi_1,\xi_3\},\{\xi_2,\xi_4\}\},\{\{\xi_1,\xi_4\},\{\xi_2,\xi_3\}\}\big)\in\Sigma_3\big(\mathcal{R}(X)\big)$$

induces a canonical isomorphism of Γ*-sets*

$$\Delta(X)\xrightarrow{\sim}\Delta\big(\mathcal{R}(X)\big).$$

Moreover, the Γ*-action on* $\Delta\big(\Lambda_2(X)\big)$ *is trivial.*

The proof is a straightforward verification. To see that the Γ-action on $\Delta\big(\Lambda_2(X)\big)$ is trivial, it suffices to observe that every transposition on X —hence every permutation of X— induces an even permutation of $\Lambda_2(X)$. For another approach, see Proposition 4.7.

To get a better grasp of the various constructions associated with X, it is useful to think of X as the set of diagonals of a cube.[1] Each pair of diagonals determines a diagonal plane (passing through an edge and its opposite), hence $\Lambda_2(X)$ is identified with the set of diagonal planes of the cube. The map γ_X carries each diagonal plane to the plane through parallel edges, and $\mathcal{R}(X)$ can therefore be identified with the set of directions of the edges. The canonical map $\mathcal{R}(X)\xleftarrow{\varepsilon}\Lambda_2(X)$ maps each diagonal plane to the direction of the edges it contains. The set $\Omega\big(\Lambda_2(X)/\mathcal{R}(X)\big)$ consists of (unordered) triples of diagonal planes with different edge directions. For each such triple τ, either the intersection of the planes is a diagonal, or the intersection is just the center of the cube. However, if the intersection is a diagonal, then the intersection of the complementary triple $\overline{\tau}=\gamma_{\Lambda_2(X)/\mathcal{R}(X)}(\tau)$ is the center. Therefore, we may associate to the pair $\{\tau,\overline{\tau}\}\in\mathcal{S}\big(\Lambda_2(X)/\mathcal{R}(X)\big)$ a unique diagonal in X, and obtain a map

$$\Phi\colon\ \mathcal{S}\big(\Lambda_2(X)/\mathcal{R}(X)\big)\to X.$$

Proposition 4.2. *For* $|X|=4$*, the map*

$$\Phi\colon\ \mathcal{S}\big(\Lambda_2(X)/\mathcal{R}(X)\big)\to X$$

is a canonical isomorphism of Γ*-sets.*

Proof. From the definition, it is clear that Φ is Γ-equivariant. Bijectivity of Φ is checked by direct inspection. $\square$

To put this result into perspective, consider the full subcategory Set_Γ^4 of Set_Γ whose objects are the Γ-sets of four elements, and the category $\mathsf{Cov}_\Gamma^{2\wr 3}$ of double coverings of Γ-sets of three elements, with morphisms of coverings. There are functors

$$\mathbf{\Lambda}\colon\ \mathsf{Set}_\Gamma^4\to\mathsf{Cov}_\Gamma^{2\wr 3}\qquad\text{and}\qquad\boldsymbol{\mathcal{S}}\colon\ \mathsf{Cov}_\Gamma^{2\wr 3}\to\mathsf{Set}_\Gamma^4$$

defined by

$$\mathbf{\Lambda}(X)=\Lambda_2(X)/\mathcal{R}(X)\qquad\text{and}\qquad\boldsymbol{\mathcal{S}}(Y\xleftarrow{\pi}Z)=\mathcal{S}(Z/Y).$$

Proposition 4.2 yields a natural equivalence between $\boldsymbol{\mathcal{S}}\circ\mathbf{\Lambda}$ and the identity on Set_Γ^4.

[1] We are indebted to F. Buekenhout for his suggestion to use geometric language in this context.

To investigate the composition $\boldsymbol{\Lambda}\circ\boldsymbol{\mathcal{S}}$, suppose $Y \xleftarrow{\pi} Z$ is a double covering of a Γ-set Y with $|Y| = 3$. (See Example 1.3 for an explicit description of $\Omega(Z/Y)$ and $\mathcal{S}(Z/Y)$.) We may consider Z as the set of faces of a cube, Y as the set of directions of edges, and π as the map which carries each face to the orthogonal direction. Then $\Omega(Z/Y)$ is the set of (unordered) triples of faces which are not pairwise parallel. Since the faces in each such triple meet at one vertex, we may view $\Omega(Z/Y)$ as the set of vertices of the cube. The map $\gamma_{Z/Y}$ carries each vertex to its opposite, hence $\mathcal{S}(Z/Y)$ is the set of diagonals of the cube. As in the discussion before Proposition 4.2, we may then identify $\Lambda_2\big(\mathcal{S}(Z/Y)\big)$ with the set of diagonal planes and $\mathcal{R}\big(\mathcal{S}(Z/Y)\big)$ with the set of edge directions. It is then clear that $\mathcal{R}\big(\mathcal{S}(Z/Y)\big)$ is canonically identified with Y, but there is no canonical identification of $\Lambda_2\big(\mathcal{S}(Z/Y)\big)$ with Z.

As we now show, we may however define a canonical bijection

$$\Delta(Z) * \Lambda_2\big(\mathcal{S}(Z/Y)\big) \xrightarrow{\sim} Z,$$

hence an isomorphism of coverings between $Y \xleftarrow{\pi} Z$ and the covering $\mathcal{R}\big(\mathcal{S}(Z/Y)\big) \xleftarrow{\varepsilon} \Delta(Z)*\Lambda_2\big(\mathcal{S}(Z/Y)\big)$ induced by the canonical covering $\mathcal{R}\big(\mathcal{S}(Z/Y)\big) \xleftarrow{\varepsilon} \Lambda_2\big(\mathcal{S}(Z/Y)\big)$. (We denote both coverings by ε.)

Our first goal is to give a geometrical interpretation of the set $\Delta(Z)$. Recall the map

$$\delta_Z\colon\ \Omega(Z/Y) \to \Delta(Z)$$

of (2). By Proposition 1.4, this map is onto. It may therefore be used to consider $\Delta(Z)$ as a quotient of $\Omega(Z/Y)$, the set of vertices of the cube. It is easily checked that the four vertices which have the same image under δ_Z are the vertices of a regular tetrahedron whose edges are the diagonals of the faces of the cube. Therefore, we may identify $\Delta(Z)$ with the set $\{T_1, T_2\}$ of such tetrahedra. Given a diagonal plane $\lambda \in \Lambda_2\big(\mathcal{S}(Z/Y)\big)$ and a tetrahedron $T \in \Delta(Z)$, there is a unique face $z \in Z$ whose intersection with λ is an edge of T. The same face z intersects the "complementary" plane $\overline{\lambda}$ following an edge of the "complementary" tetrahedron $\overline{T}$. Therefore, the map $(T,\lambda) \mapsto z$ induces a well-defined map

$$\Psi\colon\ \Delta(Z) * \Lambda_2\big(\mathcal{S}(Z/Y)\big) \to Z.$$

Proposition 4.3. *The map Ψ defines an isomorphism of coverings between*

$$\mathcal{R}\big(\mathcal{S}(Z/Y)\big) \xleftarrow{\varepsilon} \Delta(Z) * \Lambda_2\big(\mathcal{S}(Z/Y)\big) \qquad \textit{and} \qquad Y \xleftarrow{\pi} Z.$$

Proof. The map Ψ is clearly equivariant. The other properties are checked by direct inspection. $\square$

This proposition shows that $\boldsymbol{\Lambda}\circ\boldsymbol{\mathcal{S}}$ is *not* equivalent to the identity. However, when $\Delta(Z)$ is a trivial Γ-set the proposition yields an isomorphism between Z/Y and $\boldsymbol{\Lambda}\circ\boldsymbol{\mathcal{S}}(Z/Y)$:

Corollary 4.4. *If the Γ-action on $\Delta(Z)$ is trivial, then there is an isomorphism of coverings between*

$$\mathcal{R}\big(\mathcal{S}(Z/Y)\big) \xleftarrow{\varepsilon} \Lambda_2\big(\mathcal{S}(Z/Y)\big) \qquad \textit{and} \qquad Y \xleftarrow{\pi} Z.$$

Proof. This readily follows from Proposition 4.3 and Proposition 1.5(b). $\square$

Corollary 4.4 applies in particular to double coverings of the form $\Lambda_2(X)/\,\mathcal{R}(X)$, for X a Γ-set with $|X| = 4$, by Proposition 4.1. Therefore, $\boldsymbol{\Lambda}\circ\boldsymbol{\mathcal{S}}(X) \simeq X$.

Theorem 4.5. *The functors $\mathbf{\Lambda}$ and $\boldsymbol{\mathcal{S}}$ define a canonical one-to-one correspondence between the set of isomorphism classes of Γ-sets of 4 elements and the set of isomorphism classes of double coverings Z/Y of Γ-sets Y of 3 elements with trivial action on $\Delta(Z)$.*

Remark. [2] For X, $X' \in \mathsf{Set}_\Gamma^4$, every morphism of coverings $f\colon \Lambda_2(X)/\mathcal{R}(X) \to \Lambda_2(X')/\mathcal{R}(X')$ induces a morphism $\mathcal{S}\big(\Lambda_2(X)/\mathcal{R}(X)\big) \to \mathcal{S}\big(\Lambda_2(X')/\mathcal{R}(X')\big)$, hence, by Proposition 4.2, a morphism $\tilde{f}\colon X \to X'$. The functor $\mathbf{\Lambda}$ carries $\tilde{f}$ to f, hence it is full. Since $\boldsymbol{\mathcal{S}} \circ \mathbf{\Lambda}$ is equivalent to the identity, the functor $\mathbf{\Lambda}$ is also faithful. Moreover, Corollary 4.4 shows that every covering $Z/Y \in \mathsf{Cov}_\Gamma^{2\wr 3}$ such that the Γ-action on $\Delta(Z)$ is trivial is isomorphic to a covering of the form $\mathbf{\Lambda}(X)$. Therefore, it follows from [6, Theorem 1, p. 93] that $\mathbf{\Lambda}$ is an equivalence of categories from Set_Γ^4 to the full subcategory of $\mathsf{Cov}_\Gamma^{2\wr 3}$ whose objects are the coverings Z/Y with trivial Γ-action on $\Delta(Z)$.

In order to take into account the double coverings of Γ-sets of three elements which have non-trivial action on the discriminant, we consider the product category $\mathsf{Set}_\Gamma^2 \times \mathsf{Set}_\Gamma^4$ whose objects are pairs (U, X) of Γ-sets with $|U| = 2$ and $|X| = 4$, and extend $\mathbf{\Lambda}$ and $\boldsymbol{\mathcal{S}}$ to functors

$$\hat{\mathbf{\Lambda}}\colon\ \mathsf{Set}_\Gamma^2 \times \mathsf{Set}_\Gamma^4 \to \mathsf{Cov}_\Gamma^{2\wr 3} \qquad \text{and} \qquad \hat{\boldsymbol{\mathcal{S}}}\colon\ \mathsf{Cov}_\Gamma^{2\wr 3} \to \mathsf{Set}_\Gamma^2 \times \mathsf{Set}_\Gamma^4$$

defined by

$$\hat{\mathbf{\Lambda}}(U,X) = \big(U * \Lambda_2(X)\big)/\mathcal{R}(X) \qquad \text{and} \qquad \hat{\boldsymbol{\mathcal{S}}}(Y \xleftarrow{\pi} Z) = \big(\Delta(Z), \mathcal{S}(Z/Y)\big).$$

Proposition 4.3 yields a natural equivalence between $\hat{\mathbf{\Lambda}} \circ \hat{\boldsymbol{\mathcal{S}}}$ and the identity on $\mathsf{Cov}_\Gamma^{2\wr 3}$.

On the other hand, for U, X with $|U| = 2$ and $|X| = 4$, we have canonical isomorphisms

$$\mathcal{S}\big(U * \Lambda_2(X)/\mathcal{R}(X)\big) \simeq \mathcal{S}\big(\Lambda_2(X)/\mathcal{R}(X)\big) \simeq X$$

by Propositions 1.8 and 4.2, and

$$\Delta\big(U * \Lambda_2(X)\big) \simeq \Delta\big(U \times \mathcal{R}(X)\big) * \Delta\big(\Lambda_2(X)\big) \simeq U * \Delta\big(\Lambda_2(X)\big), \tag{6}$$

by Propositions 1.6 and 1.7. The Γ-action on $\Delta\big(\Lambda_2(X)\big)$ is trivial by Proposition 4.1, hence the right-most Γ-set in (6) is isomorphic to U by Proposition 1.2(b). Note that the latter isomorphism is *not* canonical, hence $\hat{\boldsymbol{\mathcal{S}}} \circ \hat{\mathbf{\Lambda}}$ is not naturally equivalent to the identity on $\mathsf{Set}_\Gamma^2 \times \mathsf{Set}_\Gamma^4$. However, since $\hat{\boldsymbol{\mathcal{S}}} \circ \hat{\mathbf{\Lambda}}(U,X) \simeq (U,X)$, we have an isomorphism between sets of isomorphism classes.

Theorem 4.6. *The functors $\hat{\mathbf{\Lambda}}$ and $\hat{\boldsymbol{\mathcal{S}}}$ define a canonical one-to-one correspondence between the set of isomorphism classes of pairs of Γ-sets (U,X) with $|U| = 2$ and $|X| = 4$ and the set of isomorphism classes of double coverings of Γ-sets with three elements.*

An alternative proof in cohomology can be derived from Diagram (10). Theorems 4.5 and 4.6 have analogues in terms of quartic étale algebras and double coverings of cubic algebras, whose statements are left to the reader.

---

[2] The authors are indebted to F. Borceux for enlightening comments about this remark.

Remark. The functor $\hat{\mathcal{S}}$ is faithful since $\hat{\mathbf{\Lambda}} \circ \hat{\mathcal{S}}$ is equivalent to the identity. Moreover, every $(U, X) \in \mathit{Set}_\Gamma^2 \times \mathit{Set}_\Gamma^4$ is isomorphic to an object of the form $\hat{\mathcal{S}}(Z/Y)$ (namely, $Z/Y = \hat{\mathbf{\Lambda}}(U, X)$). Furthermore, every morphism $f\colon\ \hat{\mathcal{S}}(Z/Y) \to \hat{\mathcal{S}}(Z'/Y')$ induces a morphism $\hat{\mathbf{\Lambda}}(f)\colon\ \hat{\mathbf{\Lambda}} \circ \hat{\mathcal{S}}(Z/Y) \to \hat{\mathbf{\Lambda}} \circ \hat{\mathcal{S}}(Z'/Y')$, hence by Proposition 4.3 a morphism $\tilde{f}\colon\ Z/Y \to Z'/Y'$. We may check that $f = \hat{\mathcal{S}}(\tilde{f})$, hence the functor $\hat{\mathcal{S}}$ is full. By [6, Theorem 1, p. 93], it defines an equivalence of categories $\mathit{Cov}_\Gamma^{2\wr 3} \equiv \mathit{Set}_\Gamma^2 \times \mathit{Set}_\Gamma^4$.

4.2. **Cohomology.** This subsection presents the cohomological perspective on Theorem 4.6. We use the same notation as in the preceding subsection.

Let $U = \{1, 2\}$ and $X = \{1, 2, 3, 4\}$ with trivial Γ-action. The group of automorphisms of (U, X) in the category $\mathit{Set}_\Gamma^2 \times \mathit{Set}_\Gamma^4$ is $\mathfrak{S}_2 \times \mathfrak{S}_4$, and since $\hat{\mathcal{S}} \circ \hat{\mathbf{\Lambda}}(U, X) \simeq (U, X)$, the functor $\hat{\mathbf{\Lambda}}$ yields an isomorphism

$$\hat{\lambda}\colon\ \mathfrak{S}_2 \times \mathfrak{S}_4 \xrightarrow{\sim} \operatorname{Aut}\bigl(U * \Lambda_2(X)/\,\mathcal{R}(X)\bigr) \simeq \mathfrak{S}_2 \wr \mathfrak{S}_3. \tag{7}$$

For definiteness, consider $\mathfrak{S}_2 \wr \mathfrak{S}_3$ as the group of automorphisms of the covering

$$Y = \{1, 2, 3\} \xleftarrow{\pi_2} \{1, 2\} \times \{1, 2, 3\} = Z,$$

where Γ acts trivially on Y and Z. The right isomorphism in (7) depends on the choice of an isomorphism $U * \Lambda_2(X)/\,\mathcal{R}(X) \simeq Z/Y$.

Similarly, the functor $\hat{\mathcal{S}}$ yields an isomorphism

$$\hat{s}\colon\ \mathfrak{S}_2 \wr \mathfrak{S}_3 \xrightarrow{\sim} \operatorname{Aut}\bigl(\Delta(Z), \mathcal{S}(Z/Y)\bigr) \simeq \mathfrak{S}_2 \times \mathfrak{S}_4 \tag{8}$$

where again the latter isomorphism is given by identifications $\Delta(Z) \simeq \{1, 2\}$ and $\mathcal{S}(Z/Y) \simeq \{1, 2, 3, 4\}$. The isomorphisms $\hat{\lambda}$ and $\hat{s}$ induce bijections

$$H^1(\Gamma, \mathfrak{S}_2 \times \mathfrak{S}_4) \simeq H^1(\Gamma, \mathfrak{S}_2 \wr \mathfrak{S}_3).$$

Since these cohomology sets are in one-to-one correspondence with the sets of isomorphism classes in $\mathit{Set}_\Gamma^2 \times \mathit{Set}_\Gamma^4$ and $\mathit{Cov}_\Gamma^{2\wr 3}$ respectively (see §3.2), we thus recover Theorem 4.6.

The isomorphisms $\hat{\lambda}$ and $\hat{s}$ can also be described in purely group-theoretical terms. The subgroup $\mathfrak{S}_2 = \mathfrak{S}_2 \times \{1\} \subset \mathfrak{S}_2 \times \mathfrak{S}_4$ is mapped to the "diagonal" subgroup $\mathfrak{S}_2 \subset \mathfrak{S}_2 \wr \mathfrak{S}_3$, which is the center of $\mathfrak{S}_2 \wr \mathfrak{S}_3$. On the other hand, the restriction of $\hat{\lambda}$ to $\mathfrak{S}_4 = \{1\} \times \mathfrak{S}_4$ is a homomorphism

$$\lambda\colon\ \mathfrak{S}_4 \to \mathfrak{S}_2 \wr \mathfrak{S}_3$$

which may be described as the action of $\mathfrak{S}_4$ by conjugation on its transpositions. Indeed, $\mathfrak{S}_4$ contains six transpositions, which sit by pairs in the three Sylow 2-subgroups of $\mathfrak{S}_4$. The map which carries each transposition to the unique Sylow 2-subgroup which contains it is a double covering of a set of three elements. Note that the composition of λ and the canonical homomorphism $\beta\colon\ \mathfrak{S}_2 \wr \mathfrak{S}_3 \to \mathfrak{S}_3$ is the surjective homomorphism

$$\rho\colon\ \mathfrak{S}_4 \to \mathfrak{S}_3$$

which is the action of $\mathfrak{S}_4$ on its three Sylow 2-subgroups. (Alternately, the map ρ may be identified with the canonical homomorphism $\mathfrak{S}_X \to \mathfrak{S}_{\mathcal{R}(X)}$ for $X = \{1, 2, 3, 4\}$, since there is a canonical one-to-one correspondence between $\mathcal{R}(X)$ and the Sylow 2-subgroups of $\mathfrak{S}_X$.) The kernel of ρ is the Vierergruppe $\mathfrak{V}$.

By definition, it is clear that the first component of $\hat{s}$ is the signature map

$$\operatorname{sgn}\colon\ \mathfrak{S}_2 \wr \mathfrak{S}_3 \subset \mathfrak{S}_6 \to \mathfrak{S}_2,$$

since the map $\mathfrak{S}_{Z/Y} \to \mathfrak{S}_{\Delta(Z)}$ is the signature. The second component is a homomorphism

$$s\colon\ \mathfrak{S}_2 \wr \mathfrak{S}_3 \to \mathfrak{S}_4$$

which is the action of $\mathfrak{S}_2 \wr \mathfrak{S}_3$ on its four Sylow 3-subgroups. (There is a natural one-to-one correspondence between the Sylow 3-subgroups of $\mathfrak{S}_{Z/Y}$ and $\mathcal{S}(Z/Y)$.) The image of λ is the kernel of sgn, by Proposition 4.1 or by Proposition 3.1, and the map s splits λ (if the Sylow 3-subgroups of $\mathfrak{S}_2 \wr \mathfrak{S}_3$ are suitably indexed). The maps ρ, λ and β, and the inclusions ι, η, are part of the following commutative diagram with exact rows and columns:

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & & \\
1 \arrow[r] & \mathfrak{V} \arrow[r, "\iota"] \arrow[d] & \mathfrak{S}_4 \arrow[r, "\rho"] \arrow[d, "\lambda"] & \mathfrak{S}_3 \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \mathfrak{S}_2^3 \arrow[r, "\eta"] \arrow[d, "\sigma"'] & \mathfrak{S}_2 \wr \mathfrak{S}_3 \arrow[r, "\beta"] \arrow[d, "\mathrm{sgn}"] & \mathfrak{S}_3 \arrow[r] & 1 \\
 & \mathfrak{S}_2 \arrow[r, equal] \arrow[d] & \mathfrak{S}_2 \arrow[d] & & \\
 & 1 & 1 & &
\end{tikzcd} \tag{9}$$

where σ is the sum. Since the exact sequences in this diagram are split, there is a corresponding commutative diagram of exact sequences in cohomology:

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & & \\
1 \arrow[r] & H^1(\Gamma, \mathfrak{V}) \arrow[r, "\iota^1"] \arrow[d] & H^1(\Gamma, \mathfrak{S}_4) \arrow[r, "\rho^1"] \arrow[d, "\lambda^1"] & H^1(\Gamma, \mathfrak{S}_3) \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & H^1(\Gamma, \mathfrak{S}_2^3) \arrow[r, "\eta^1"] \arrow[d, "\sigma^1"'] & H^1(\Gamma, \mathfrak{S}_2 \wr \mathfrak{S}_3) \arrow[r, "\beta^1"] \arrow[d, "\mathrm{sgn}^1"] & H^1(\Gamma, \mathfrak{S}_3) \arrow[r] & 1 \\
 & H^1(\Gamma, \mathfrak{S}_2) \arrow[r, equal] \arrow[d] & H^1(\Gamma, \mathfrak{S}_2) \arrow[d] & & \\
 & 1 & 1. & &
\end{tikzcd} \tag{10}$$

Cohomology yields an alternative proof of Proposition 4.1:

Proposition 4.7. *For any* Γ*-set* X *with* $|X| = 4$*,*

$$\Delta(X) \simeq \Delta\big(\mathcal{R}(X)\big).$$

Moreover, the Γ*-action on* $\Delta\big(\Lambda_2(X)\big)$ *is trivial.*

Proof. The commutative diagram

$$\begin{array}{ccc}\mathfrak{S}_4 & \xrightarrow{\rho} & \mathfrak{S}_3\\ {\scriptstyle\mathrm{sgn}}\downarrow & & \downarrow{\scriptstyle\mathrm{sgn}}\\ \mathfrak{S}_2 & = & \mathfrak{S}_2\end{array}$$

induces a commutative diagram in cohomology

$$\begin{array}{ccc}H^1(\Gamma,\mathfrak{S}_4) & \xrightarrow{\rho^1} & H^1(\Gamma,\mathfrak{S}_3)\\ {\scriptstyle\mathrm{sgn}^1}\downarrow & & \downarrow{\scriptstyle\mathrm{sgn}^1}\\ H^1(\Gamma,\mathfrak{S}_2) & = & H^1(\Gamma,\mathfrak{S}_2).\end{array}$$

The first part of the proposition follows since ρ^1 maps the isomorphism class of X to the isomorphism class of $\mathcal{R}(X)$, and sgn^1 maps the isomorphism class of any Γ-set to the isomorphism class of its discriminant. The second part follows from the fact that

$$H^1(\Gamma,\mathfrak{S}_4)\xrightarrow{\lambda^1}H^1(\Gamma,\mathfrak{S}_2\wr\mathfrak{S}_3)\xrightarrow{\mathrm{sgn}^1}H^1(\Gamma,\mathfrak{S}_2)$$

is a zero-sequence. □

As another application of cohomology, we describe the quartic étale algebras which have a given resolvent cubic.

Let R be a Γ-set of three elements, and let $X_0 = R\amalg\{0\}$ be the Γ-set of four elements obtained by adjoining to R a fixed point 0. To each partition of X_0 into 2-element subsets, we may associate the unique element $r\in R$ such that $\{0,r\}$ is in the partition, and thus identify

$$\mathcal{R}(X_0)=R.$$

As in §3.2, we let Γ act by conjugation on the groups $\mathfrak{S}_{X_0}$, $\mathfrak{S}_R$, and denote by $\mathfrak{S}'_{X_0}$, $\mathfrak{S}'_R$ the Γ-groups thus defined. The inclusion $R\hookrightarrow X_0$ yields a Γ-equivariant embedding $\mathfrak{S}'_R\hookrightarrow\mathfrak{S}'_{X_0}$ which splits the map $\rho\colon\mathfrak{S}'_{X_0}\to\mathfrak{S}'_R$. The split exact sequence

$$1\to\mathfrak{V}'_{X_0}\xrightarrow{\iota}\mathfrak{S}'_{X_0}\xrightarrow{\rho}\mathfrak{S}'_R\to 1$$

yields an exact sequence in cohomology

$$1\to H^1(\Gamma,\mathfrak{V}'_{X_0})\xrightarrow{\iota^1}H^1(\Gamma,\mathfrak{S}'_{X_0})\xrightarrow{\rho^1}H^1(\Gamma,\mathfrak{S}'_R)\to 1, \tag{11}$$

and the isomorphism classes of $X\in\mathit{Set}^4_\Gamma$ such that $\mathcal{R}(X)\simeq R$ are in one-to-one correspondence with $\ker\rho^1=\operatorname{im}\iota^1$. They form a pointed set with the isomorphism class of X_0 as distinguished element. Note that exactness of the sequence (11) does *not* mean that ι^1 is injective. In fact, the group $\mathrm{Aut}_\Gamma(R)=H^0(\Gamma,\mathfrak{S}'_R)$ acts on $H^1(\Gamma,\mathfrak{V}'_{X_0})$, and $\operatorname{im}\iota^1$ is in canonical bijection with the orbit set $H^1(\Gamma,\mathfrak{V}'_{X_0})/\mathrm{Aut}_\Gamma(R)$, by [3, (28.4)].

To give a more explicit description, we use a variant of Diagram (10). First, observe that we may identify $\Lambda_2(X_0)$ to $\{1,2\}\times R$, as follows: we map a 2-element subset $U\subset X_0$ to $(1,r)$ if $0\notin U$ and $r\notin U$, to $(2,r)$ if $U=\{0,r\}$. We may then identify the double covering $\Lambda_2(X_0)/\mathcal{R}(X_0)$ to

$$R\xleftarrow{\pi_2}\{1,2\}\times R.$$

Let $Z_0 = \{1,2\} \times R$. As above, we let Γ act by conjugation on $\mathfrak{S}_{Z_0/R}$, and denote by $\mathfrak{S}'_{Z_0/R}$ the corresponding Γ-group. As in §3.2, let $\mathfrak{T}'_{Z_0/R}$ be the kernel of the canonical map $\beta_{Z_0/R}\colon \mathfrak{S}'_{Z_0/R} \to \mathfrak{S}'_R$. The exact sequence

$$1 \to \mathfrak{T}'_{Z_0/R} \xrightarrow{\eta} \mathfrak{S}'_{Z_0/R} \xrightarrow{\beta_{Z_0/R}} \mathfrak{S}'_R \to 1$$

is split, and induces an exact sequence in cohomology

$$1 \to H^1(\Gamma, \mathfrak{T}'_{Z_0/R}) \xrightarrow{\eta^1} H^1(\Gamma, \mathfrak{S}'_{Z_0/R}) \xrightarrow{\beta^1} H^1(\Gamma, \mathfrak{S}'_R) \to 1.$$

As above, there is a canonical bijection

$$\operatorname{im} \eta^1 = \ker \beta^1 \simeq H^1(\Gamma, \mathfrak{T}'_{Z_0/R}) / \operatorname{Aut}_\Gamma(R).$$

The orbit set on the right side may therefore be identified with the set of isomorphism classes of double coverings of R, see §3.2. Consider the commutative diagram analogous to (10),

$$\begin{tikzcd}
1 \arrow[d] & 1 \arrow[d] & \\
H^1(\Gamma, \mathfrak{V}'_{X_0}) \arrow[r, "\iota^1"] \arrow[d] & H^1(\Gamma, \mathfrak{S}'_{X_0}) \arrow[r, "\rho^1"] \arrow[d, "\lambda^1"] & H^1(\Gamma, \mathfrak{S}'_R) \arrow[d, equal] \\
H^1(\Gamma, \mathfrak{T}'_{Z_0/R}) \arrow[r, "\eta^1"] \arrow[d, "\sigma^1"'] & H^1(\Gamma, \mathfrak{S}'_{Z_0/R}) \arrow[r, "\beta^1"] \arrow[d, "\operatorname{sgn}^1"] & H^1(\Gamma, \mathfrak{S}'_R) \\
H^1(\Gamma, \mathfrak{S}_2) \arrow[r, equal] \arrow[d] & H^1(\Gamma, \mathfrak{S}_2) \arrow[d] & \\
1 & 1. &
\end{tikzcd} \tag{12}$$

The left vertical sequence is an exact sequence of groups. It shows that $H^1(\Gamma, \mathfrak{V}'_{X_0})$ can be identified with the kernel of σ^1. Recall from §3.2 that $H^1(\Gamma, \mathfrak{T}'_{Z_0/R})$ is in canonical bijection with the set $C^2(R)$ of isomorphism classes over R of double coverings of R, and that $H^1(\Gamma, \mathfrak{S}_2)$ classifies Γ-sets of two elements up to isomorphism. By commutativity of the lower square in (12), the map σ^1 carries every double covering to the isomorphism class of its discriminant. Therefore, we may identify $H^1(\Gamma, \mathfrak{V}'_{X_0})$ with the group $C_0^2(R)$ of isomorphism classes over R of double coverings of R with trivial discriminant,

$$H^1(\Gamma, \mathfrak{V}'_{X_0}) = C_0^2(R).$$

We have thus shown:

Proposition 4.8. *The set of isomorphism classes of sets X of four elements such that $\mathcal{R}(X) \simeq R$ is in canonical bijection with the set $C_0^2(R)/\operatorname{Aut}_\Gamma(R)$ of isomorphism classes of double coverings of R with trivial discriminant.*

Suppose now Γ is the absolute Galois group of a field F with separable closure F_s, and let A be a cubic étale F-algebra. Using the anti-equivalence $\mathsf{Set}_\Gamma \equiv \acute{\mathsf{E}}\mathsf{t}_F$, we may translate Proposition 4.8 into the following statement, where we denote by

$\mathrm{Quad}_0(A)$ the set of isomorphism classes over A of quadratic extensions of A whose discriminant (as F-algebra) is trivial:

Proposition 4.9. *The set of isomorphism classes of quartic étale F-algebras Q with $\mathcal{R}(Q) \simeq A$ is in canonical bijection with the set $\mathrm{Quad}_0(A)/\mathrm{Aut}_F(A)$ of F-isomorphism classes of quadratic extensions of A with trivial discriminant.*

The next proposition gives an explicit description of the group $\mathrm{Quad}_0(A)$.

Proposition 4.10. *Let $N^1(A)$ be the (multiplicative) group of elements of A of norm 1 and let $T^0(A)$ be the (additive) group of elements of A of trace 0.*

(a) *If $\mathrm{char}\, F \neq 2$, $\mathrm{Quad}_0(A) \simeq N^1(A)/N^1(A)^2$.*
(b) *If $\mathrm{char}\, F = 2$, $\mathrm{Quad}_0(A) \simeq T^0(A)/\wp\big(T^0(A)\big)$, where $\wp$ is the Artin-Schreier map $\wp(x) = x^2 - x$.*

Proof. If A is a field, the action of Γ on $\mathbf{X}(A)$ is transitive. Letting $\Gamma_0 \subset \Gamma$ be the absolute Galois group of a copy of A in F_s, we have $\mathrm{Quad}(A) \simeq H^1(\Gamma_0, \mathfrak{S}_2)$ as observed in §3.2, and the map σ^1 can be interpreted as the corestriction

$$H^1(\Gamma_0, \mathfrak{S}_2) \to H^1(\Gamma, \mathfrak{S}_2).$$

If $\mathrm{char}\, F \neq 2$, we identify $\mathfrak{S}_2$ with $\{1, -1\} \subset F_s^\times$. The exact sequence

$$1 \to \mathfrak{S}_2 \to F_s^\times \xrightarrow{2} F_s^\times \to 1$$

yields isomorphisms

$$H^1(\Gamma, \mathfrak{S}_2) \simeq F^\times/F^{\times 2} \qquad \text{and} \qquad H^1(\Gamma_0, \mathfrak{S}_2) \simeq A^\times/A^{\times 2}$$

under which the corestriction corresponds to a map induced by the norm. Its kernel is $N^1(A)/N^1(A)^2$ since if $y \in A^\times$ is such that $N_{A/F}(y) = z^2 \in F^{\times 2}$, then $N_{A/F}(y^3 z^{-2}) = 1$.

If $\mathrm{char}\, F = 2$, we identify $\mathfrak{S}_2$ with $\{0, 1\} \subset F_s$. The exact sequence

$$0 \to \mathfrak{S}_2 \to F_s \xrightarrow{\wp} F_s \to 0$$

yields isomorphisms

$$H^1(\Gamma, \mathfrak{S}_2) \simeq F/\wp(F) \qquad \text{and} \qquad H^1(\Gamma_0, \mathfrak{S}_2) \simeq A/\wp(A)$$

under which the corestriction corresponds to a map induced by the trace. Its kernel is $T^0(A)/\wp\big(T^0(A)\big)$ since if $T_{A/F}(y) = z^2 - z$, then $T_{A/F}(y - z^2 + z) = 0$.

If A is not a field, it decomposes into a direct product of fields,

$$A \simeq F \times K \qquad \text{or} \qquad A \simeq F \times F \times F.$$

In the first case,

$$\mathrm{Quad}(A) \simeq \mathrm{Quad}(F) \times \mathrm{Quad}(K) \simeq \begin{cases} (F^\times/F^{\times 2}) \times (K^\times/K^{\times 2}) & \text{if } \mathrm{char}\, F \neq 2, \\ \big(F/\wp(F)\big) \times \big(K/\wp(K)\big) & \text{if } \mathrm{char}\, F = 2, \end{cases}$$

and the map σ^1 can be again interpreted as induced by the norm or the trace. We may then use the same arguments as above. The case where $A \simeq F \times F \times F$ is left to the reader. □

Following §3.5, the set $H^1(\Gamma, \mathfrak{S}'_R)$ for $R = \mathbf{X}(A)$ is also in one-to-one correspondence with the set of isomorphism classes of $\mathfrak{S}_3$-Galois F-algebras, where the distinguished element corresponds to the isomorphism class of the $\mathfrak{S}_3$-Galois closure $\Sigma_3(A)$. Likewise, the set $H^1(\Gamma, \mathfrak{S}'_{X_0})$ classifies $\mathfrak{S}_4$-Galois F-algebras up to isomorphism, with the class of $\Sigma_4(F \times A)$ as distinguished element. The upper exact sequence of Diagram (12) shows that the $\mathfrak{S}_4$-Galois F-algebras M which are the $\mathfrak{S}_4$-Galois closure of an étale quartic F-algebra Q with $\mathcal{R}(Q) \simeq A$ are in one-to-one correspondence with $\operatorname{Quad}_0(A)/\operatorname{Aut}_F(A)$. Using Proposition 4.10, we may make this correspondence explicit as follows:

Proposition 4.11. *Let A be a cubic étale F-algebra, identified with a subalgebra of its $\mathfrak{S}_3$-Galois closure $\Sigma_3(A)$, and let $\rho \in \mathfrak{S}_3$ be an element of order 3.*

(a) *If $\operatorname{char} F \neq 2$, let $a \in A^\times$ be such that $N_{A/F}(a) = 1$, and set*

$$M = \Sigma_3(A)[\sqrt{a}, \sqrt{\rho(a)}, \sqrt{\rho^2(a)}].$$

(b) *If $\operatorname{char} F = 2$, let $a \in A$ be such that $T_{A/F}(a) = 0$, and set*

$$M = \Sigma_3(A)\big[\wp^{-1}(a), \wp^{-1}\big(\rho(a)\big), \wp^{-1}\big(\rho^2(a)\big)\big].$$

In each case, there is a $\mathfrak{S}_4$-action on M which endows it with the structure of an $\mathfrak{S}_4$-Galois algebra. The quartic subalgebra $Q = M^{\mathfrak{S}_3}$ satisfies $\mathcal{R}(Q) \simeq A$. Moreover, every $\mathfrak{S}_4$-Galois F-algebra which is the $\mathfrak{S}_4$-Galois closure of a quartic étale F-algebra Q with $\mathcal{R}(Q) \simeq A$ is of this form.

Remark. Similar constructions are described by Serre (see [10][3]) and by Weil (for the construction of dyadic field extensions with Galois group $\mathfrak{S}_4$, see [13, Section 31]).

4.3. **Quartic étale algebras.** In this subsection, our goal is to make explicit the relation between resolvent cubics of quartic polynomials and the construction of $\mathcal{R}(Q)$ for Q a quartic étale F-algebra. Our first observation is a direct consequence of Proposition 4.1 (see also Proposition 4.7).

Proposition 4.12. *Let Q be a quartic étale F-algebra. There is a canonical isomorphism*

$$\Delta\big(\mathcal{R}(Q)\big) \xrightarrow{\sim} \Delta(Q).$$

Moreover, $\Delta\big(\Lambda_2(Q)\big) \simeq F \times F$.

Proof. The proposition readily follows from Proposition 4.1 under the anti-equivalence $\mathsf{\acute{E}t}_F \equiv \mathsf{Set}_\Gamma$, since the Δ, $\mathcal{R}$ and Λ_2 construction commute with the functor $\mathbf{X}$. □

Recall from [12] that "the" resolvent cubic of a quartic polynomial

$$f(u) = u^4 - \alpha_1 u^3 + \alpha_2 u^2 - \alpha_3 u + \alpha_4 \tag{13}$$

with roots u_1, u_2, u_3, u_4 in an algebraic closure, is the polynomial $g(v)$ with roots

$$v_1 = (u_1 + u_2)(u_3 + u_4), \quad v_2 = (u_1 + u_3)(u_2 + u_4), \quad v_3 = (u_1 + u_4)(u_2 + u_3).$$

This polynomial has the form

$$g(v) = v^3 - \beta_1 v^2 + \beta_2 v - \beta_3 \tag{14}$$

where

$$\begin{aligned} \beta_1 &= 2\alpha_2, \\ \beta_2 &= \alpha_1\alpha_3 + \alpha_2^2 - 4\alpha_4, \\ \beta_3 &= \alpha_1\alpha_2\alpha_3 - \alpha_1^2\alpha_4 - \alpha_3^2. \end{aligned} \tag{15}$$

[3]We are indebted to J-P. Serre for calling our attention to this reference.

An alternative resolvent cubic suggested by Lagrange [4, (32), p. 266] in characteristic different from 2 has roots

$$w_1 = (u_1+u_2-u_3-u_4)^2, \qquad w_2 = (u_1-u_2+u_3-u_4)^2, \qquad w_3 = (u_1-u_2-u_3+u_4)^2.$$

Since $w_i = \alpha_1^2 - 4v_i$ for $i = 1, 2, 3$, this polynomial has the form

$$h(w) = -4^3 g\Big(\frac{\alpha_1^2 - w}{4}\Big) = w^3 - \varkappa_1 w^2 + \varkappa_2 w - \varkappa_3, \tag{16}$$

where

$$\begin{aligned} \varkappa_1 &= 3\alpha_1^2 - 8\alpha_2, \\ \varkappa_2 &= 3\alpha_1^4 - 16\alpha_1^2\alpha_2 + 16\alpha_1\alpha_3 + 16\alpha_2^2 - 64\alpha_4, \\ \varkappa_3 &= (\alpha_1^3 - 4\alpha_1\alpha_2 + 8\alpha_3)^2. \end{aligned} \tag{17}$$

Now, let Q be a quartic étale algebra over a field F of arbitrary characteristic. For $x \in Q$, let

$$\lambda_x = s_2 \cdot (x \otimes 1 + 1 \otimes x) \in \Lambda_2(Q). \tag{18}$$

Proposition 4.13. *Suppose $x \in Q$ is a generating element with minimal polynomial $f(u)$ as in* (13)*, so that the coefficient α_1 is the* trace $T_{Q/F}(x)$ *of x. Then*

(a) $\lambda_x + \gamma_Q(\lambda_x) = T_{Q/F}(x)$.

(b) $\gamma_Q(\lambda_x)\lambda_x \in \mathcal{R}(Q)$ *is a generating element with minimal polynomial $g(v)$ as in* (14)*. Moreover, if the characteristic of F is different from* 2*, then $\big(\lambda_x - \gamma_Q(\lambda_x)\big)^2 \in \mathcal{R}(Q)$ is a generating element with minimal polynomial $h(w)$ as in* (16)*.*

In arbitrary characteristic, if the element $\varkappa_3$ of (17) *is not zero,*[4] *then $\lambda_x \in \Lambda_2(Q)$ is a generating element over $\mathcal{R}(Q)$, with minimal polynomial*

$$t^2 - T_{Q/F}(x)t + \gamma_Q(\lambda_x)\lambda_x \in \mathcal{R}(Q)[t].$$

Proof. Extending scalars, we may assume that Q is split, with a basis (e_1, e_2, e_3, e_4) consisting of minimal (orthogonal) idempotents. Then $\mathcal{R}(Q)$ is split and $e_1 \otimes e_2 + e_2 \otimes e_1 + e_3 \otimes e_4 + e_4 \otimes e_3$, $e_1 \otimes e_3 + e_3 \otimes e_1 + e_2 \otimes e_4 + e_4 \otimes e_2$ and $e_1 \otimes e_4 + e_4 \otimes e_1 + e_2 \otimes e_3 + e_3 \otimes e_2$ is a basis of $\mathcal{R}(Q)$ consisting of minimal idempotents. Let

$$x = x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4$$

with x_1, x_2, x_3, $x_4 \in F$. Since x generates Q, the coefficients x_i are pairwise distinct. Computation shows that

$$\lambda_x = \sum_{1\le i<j\le 4} (x_i + x_j)(e_i \otimes e_j + e_j \otimes e_i),$$

hence

$$\gamma_Q(\lambda_x) = \sum_{1\le i<j\le 4} (x_i + x_j)(e_{i'} \otimes e_{j'} + e_{j'} \otimes e_{i'})$$

where $\{i, j, i', j'\} = \{1, 2, 3, 4\}$. It follows that

$$\lambda_x + \gamma_Q(\lambda_x) = (x_1 + x_2 + x_3 + x_4) \sum_{1\le i<j\le 4} (e_i \otimes e_j + e_j \otimes e_i) = T_{Q/F}(x).$$

[4] In characteristic 2, the condition is thus $T_{Q/F}(x) \neq 0$.

Similarly

$$\begin{aligned}\gamma_Q(\lambda_x)\lambda_x &= (x_1+x_2)(x_3+x_4)(e_1\otimes e_2+e_2\otimes e_1+e_3\otimes e_4+e_4\otimes e_3)\\ &\quad+(x_1+x_3)(x_2+x_4)(e_1\otimes e_3+e_3\otimes e_1+e_2\otimes e_4+e_4\otimes e_2)\\ &\quad+(x_1+x_4)(x_2+x_3)(e_1\otimes e_4+e_4\otimes e_1+e_2\otimes e_3+e_3\otimes e_2).\end{aligned}$$

This shows that $\gamma_Q(\lambda_x)\lambda_x$ is a root of a polynomial g whose roots in F are

$$y_1=(x_1+x_2)(x_3+x_4),\quad y_2=(x_1+x_3)(x_2+x_4),\quad y_3=(x_1+x_4)(x_2+x_3).$$

These roots are distinct since an easy computation yields

$$(y_1-y_2)(y_1-y_3)(y_2-y_3)=-\prod_{i<j}(x_i-x_j).$$

Therefore, $\gamma_Q(\lambda_x)\lambda_x$ is a generator of $\mathcal{R}(Q)$ and g is its minimal polynomial.

Similarly,

$$\begin{aligned}\big(\lambda_x-\gamma_Q(\lambda_x)\big)^2 &= (x_1+x_2-x_3-x_4)^2(e_1\otimes e_2+e_2\otimes e_1+e_3\otimes e_4+e_4\otimes e_3)\\ &\quad+(x_1-x_2+x_3-x_4)^2(e_1\otimes e_3+e_3\otimes e_1+e_2\otimes e_4+e_4\otimes e_2)\\ &\quad+(x_1-x_2-x_3+x_4)^2(e_1\otimes e_4+e_4\otimes e_1+e_2\otimes e_3+e_3\otimes e_2),\end{aligned}$$

and the same arguments show that $\big(\lambda_x-\gamma_Q(\lambda_x)\big)^2$ is a generating element of $\mathcal{R}(Q)$ with minimal polynomial h as in (16) if the characteristic of F is different from 2.

Since

$$\varkappa_3=(x_1+x_2-x_3-x_4)^2(x_1-x_2+x_3-x_4)^2(x_1-x_2-x_3+x_4)^2,$$

the condition $\varkappa_3\neq 0$ implies that the elements x_i+x_j for $1\le i<j\le 4$ are pairwise distinct, hence λ_x generates $\Lambda_2(Q)$. Since $\lambda_x+\gamma_Q(\lambda_x)=T_{E/F}(x)$, the minimal polynomial of λ_x over $\mathcal{R}(Q)$ is as stated in the proposition. □

Remark. Allison gives in [1, §6] another description of the algebra $\mathcal{R}(Q)$, for Q a quartic étale F-algebra. For $x\in Q$, he considers the image

$$f_x=\varphi_2(\lambda_x)\in\operatorname{End}_F(\textstyle\bigwedge^2 Q)$$

of $\lambda_x\in\Lambda_2(Q)$ under the map φ_2 induced by the homomorphism in (3) (see Lemma 2.3); thus

$$f_x(a\wedge b)=xa\wedge b+a\wedge xb\qquad\text{for } a,\, b\in Q.$$

Assuming that the characteristic of F is different from 2, Allison defines $\mathcal{R}(Q)$ as the span of the products $f_x\circ f_y$, for x, $y\in Q$ of trace zero. This definition coincides with the definition in §2.1 under an isomorphism induced by φ_2.

4.4. **Quadratic extensions of cubic étale algebras.** Let A be an étale F-algebra of dimension 3, and let B be an extension of degree 2 of A. In the same spirit as the preceding subsection, we proceed to give explicit equations for generating elements of $\mathcal{S}(B/A)$.

Our first observation is the analogue of Proposition 1.4 through the anti-equivalence between coverings of Γ-sets and extensions of étale F-algebras.

Proposition 4.14. *There is a canonical embedding $\Delta(B)\hookrightarrow\Omega(B/A)$ such that*

$$\Omega(B/A)\simeq\Delta(B)\otimes_F\mathcal{S}(B/A).$$

In the case where B (and therefore A) is split, the image of $\Delta(B)$ in $\Omega(B/A)$ is spanned by the idempotents

$$d = g_0 + g_1 + g_2 + g_3 \qquad \text{and} \qquad d' = g_0' + g_1' + g_2' + g_3',$$

in the notation of Example 2.9.

In the general case, for $b \in B$ we set for brevity $\overline{b} = \gamma_{B/A}(b)$, and

$$\begin{array}{lll} & b_1 = s_3^A \cdot (b \otimes 1 \otimes 1) = \varepsilon_{11}(b), & b_1' = s_3^A \cdot (\overline{b} \otimes 1 \otimes 1) = \varepsilon_{21}(b) \\ (19) & b_2 = s_3^A \cdot (1 \otimes b \otimes 1) = \varepsilon_{12}(b), & b_2' = s_3^A \cdot (1 \otimes \overline{b} \otimes 1) = \varepsilon_{22}(b) \\ & b_3 = s_3^A \cdot (1 \otimes 1 \otimes b) = \varepsilon_{13}(b), & b_3' = s_3^A \cdot (1 \otimes 1 \otimes \overline{b}) = \varepsilon_{23}(b) \end{array}$$

where $\varepsilon_{ij} \colon B \to \Sigma(B/A)$ are the embeddings of (5). Hence we have $\Sigma(B/A) = \Sigma_3(A)[b_1, b_1', \dots, b_3, b_3']$, by Proposition 3.7, and $\mathfrak{S}_3$ acts on $\Sigma(B/A)$ through the action on $\Sigma_3(A)$ and by permuting the b_i and the b_j'. The algebra $\Omega(B/A)$ is generated over F by all the polynomials in the b_i and the b_j' which are symmetric under $\mathfrak{S}_3$. In particular

$$\begin{array}{rcl} \delta_b & = & b_1 b_2 b_3 + b_1' b_2' b_3 + b_1' b_2 b_3' + b_1 b_2' b_3' \\ \omega_b & = & b_1 + b_2 + b_2 \end{array}$$

are elements of $\Omega(B/A)$.

Proposition 4.15. *The element δ_b lies in the image of $\Delta(B)$ in $\Omega(B/A)$, and*

$$\gamma_B(\delta_b) = \delta_{\overline{b}}.$$

Moreover, the following conditions are equivalent:

(a) *b generates B over A;*
(b) *δ_b generates $\Delta(B)$;*

Similarly, the following conditions are equivalent:

(a') *ω_b generates $\Omega(B/A)$ over $\Delta(B)$;*
(b') *$(b - \overline{b})^2$ generates A.*

Proof. It suffices to prove the assertions after scalar extension. We may therefore assume B is split, and use the same notation as in Example 2.9. Let

$$b = \beta_1 f_1 + \beta_1' f_1' + \beta_2 f_2 + \beta_2' f_2' + \beta_3 f_3 + \beta_3' f_3'$$

with $\beta_1, \dots, \beta_3' \in F$, hence

$$\overline{b} = \beta_1' f_1 + \beta_1 f_1' + \beta_2' f_2 + \beta_2 f_2' + \beta_3' f_3 + \beta_3 f_3'.$$

Computation yields

$$\begin{aligned} \delta_b = {} & (\beta_1\beta_2\beta_3 + \beta_1\beta_2'\beta_3' + \beta_1'\beta_2\beta_3' + \beta_1'\beta_2'\beta_3)(g_0 + g_1 + g_2 + g_3) \\ & + (\beta_1'\beta_2'\beta_3' + \beta_1'\beta_2\beta_3 + \beta_1\beta_2'\beta_3 + \beta_1\beta_2\beta_3')(g_0' + g_1' + g_2' + g_3'), \end{aligned} \tag{20}$$

proving $\delta_b \in \Delta_B$. Since $\overline{\gamma}_B$ interchanges $g_0 + \dots + g_3$ and $g_0' + \dots + g_3'$, it is clear that

$$\overline{\gamma}_B(\delta_b) = \delta_{\overline{b}}.$$

We have $\delta_b \in F$ if and only if the coefficients of $g_0 + \dots + g_3$ and $g_0' + \dots + g_3'$ in (20) above are equal, and this condition is equivalent to $\delta_b = \delta_{\overline{b}}$. On the other hand, b generates B over A if and only if $\beta_i \neq \beta_i'$ for $i = 1, 2, 3$. Since

$$\delta_b - \delta_{\overline{b}} = (\beta_1 - \beta_1')(\beta_2 - \beta_2')(\beta_3 - \beta_3')(g_0 + g_1 + g_2 + g_3 - g_0' - g_1' - g_2' - g_3'),$$

this condition holds if and only if $\delta_b \neq \delta_{\overline{b}}$. The equivalence of (a) and (b) is thus proved.

To complete the proof, let

$$\omega_b = u_0 g_0 + u_1 g_1 + u_2 g_2 + u_3 g_3 + u_0' g_0' + u_1' g_1' + u_2' g_2' + u_3' g_3'.$$

This element generates $\Omega(B/A)$ over $\Delta(B)$ if and only if $u_0, \dots, u_3$ are pairwise distinct and $u_0', \dots, u_3'$ are pairwise distinct. Computation yields

$$u_0 = \beta_1 + \beta_2 + \beta_3,\ u_1 = \beta_1 + \beta_2' + \beta_3',\ u_2 = \beta_1' + \beta_2 + \beta_3',\ u_3 = \beta_1' + \beta_2' + \beta_3,$$
$$u_0' = \beta_1' + \beta_2' + \beta_3',\ u_1' = \beta_1' + \beta_2 + \beta_3,\ u_2' = \beta_1 + \beta_2' + \beta_3,\ u_3' = \beta_1 + \beta_2 + \beta_3',$$

and

$$\begin{aligned}(u_0 - u_1)(u_0 - u_2)(u_0 - u_3)(u_1 - u_2)(u_1 - u_3)(u_2 - u_3) = \\ \big((\beta_2 - \beta_2')^2 - (\beta_3 - \beta_3')^2\big)\big((\beta_1 - \beta_1')^2 - (\beta_2 - \beta_2')^2\big)\big((\beta_1 - \beta_1')^2 - (\beta_3 - \beta_3')^2\big) = \\ (u_0' - u_1')(u_0' - u_2')(u_0' - u_3')(u_1' - u_2')(u_1' - u_3')(u_2' - u_3').\end{aligned}$$

Therefore, ω_b generates $\Omega(B/A)$ over $\Delta(B)$ if and only if $(\beta_1 - \beta_1')^2$, $(\beta_2 - \beta_2')^2$ and $(\beta_3 - \beta_3')^2$ are pairwise distinct. Since

$$(b - \overline{b})^2 = (\beta_1 - \beta_1')^2 e_1 + (\beta_2 - \beta_2')^2 e_2 + (\beta_3 - \beta_3')^2 e_3,$$

this proves the equivalence of (a') and (b'). □

Recall from [3, p. xviii] the forms $T = T_{A/F}$, $S = S_{A/F}$ and $N = N_{A/F}$ of degrees 1, 2 and 3 respectively on A, such that the generic polynomial of every element $a \in A$ has the form

$$X^3 - T(a)X^2 + S(a)X - N(a) \in F[X].$$

(The form T is the *trace*, and N is the *norm*.) For $a \in A$, let $a_i = \varepsilon_i(A) \in \Sigma_3(A)$. One has $T(a) = a_1 + a_2 + a_3$, $S(a) = a_1 a_2 + a_1 a_3 + a_2 a_3$ and $N(a) = a_1 a_2 a_3$.

Fix $b \in B$, and let

$$\alpha_1 = b + \overline{b} \in A, \qquad \alpha_2 = b\overline{b} \in A.$$

Computation yields

$$\begin{aligned}\delta_b + \delta_{\overline{b}} &= N(\alpha_1), \\ \delta_b \delta_{\overline{b}} &= S(\alpha_1^2 - 2\alpha_2)T(\alpha_2) - T(\alpha_1^2 - 2\alpha_2)T\big((\alpha_1^2 - 2\alpha_2)\alpha_2\big) \\ &\quad + T\big((\alpha_1^2 - 2\alpha_2)^2\alpha_2\big) + 4N(\alpha_2).\end{aligned} \tag{21}$$

Proposition 4.16. *If ω_b generates $\Omega(B/A)$ over $\Delta(B)$, its minimal polynomial is*

$$\begin{aligned}X^4 - 2T(\alpha_1)X^3 + \big(T(\alpha_1^2) + 2T(\alpha_2) + 3S(\alpha_1)\big)X^2 \\ - \big(4\alpha_b + 2\alpha_{\overline{b}} + 2T(\alpha_1)T(\alpha_2) + S(\alpha_1)T(\alpha_1) - 3N(\alpha_1)\big)X \\ + (2\delta_b + \delta_{\overline{b}})T(\alpha_1) + T(a_1)^2 T(\alpha_2) - S(\alpha_1)T(\alpha_2) \\ - T(\alpha_1^2\alpha_2) + T(\alpha_2^2) - T(\alpha_1)N(\alpha_1) - 2S(\alpha_2).\end{aligned}$$

Proof. Use that in the split case, the four roots of the minimal polynomial of ω_b over $\Delta(A)$ are (with the notations of the proof of Proposition 4.15) the elements u_i, $i = 0, \dots, 3$. □

If char $F \neq 2$, we may simplify the results above by a specific choice of generating element b. Let $b \in B$ be such that $\overline{b} = -b$ and assume that $a = b^2 \in A$ generates A.

Proposition 4.17. ($\operatorname{char} F \neq 2$) *With the notation above,*

$$\Delta(B) = F[\delta_b] \qquad \textit{and} \qquad \Omega(B/A) = F[\delta_b, \omega_b] = \Delta(B)[\omega_b].$$

Moreover, the minimal polynomial of δ_b over F is

$$X^2 - 16N(a),$$

and the minimal polynomial of ω_b over $\Delta(B)$ is

$$X^4 - 2T(a)X^2 - 2\delta_b X + T(a^2) - 2S(a).$$

Proof. Proposition 4.15 shows that δ_b generates $\Delta(B)$ and that ω_b generates $\Omega(B/A)$ over $\Delta(B)$. This last fact can also be seen directly: the algebra $\Omega(B/A)$ is generated over F by the elementary symmetric functions in the b_i; since

$$2(b_1b_2 + b_1b_3 + b_2b_3) = \omega_b^2 - (b_1^2 + b_2^2 + b_3^2) = \omega_b^2 - T(a)$$

we have $\Omega(B/A) = F[\delta_b, \omega_b] = \Delta(B)[\omega_b]$. The formula for the minimal polynomial of δ_b (resp. ω_b) follows from (21) (resp. Proposition 4.16). One can also repeat the proof of Proposition 4.16 with the special choice of b. □

Corollary 4.18. ($\operatorname{char} F \neq 2$) *The discriminant $\Delta(B)$ is split if and only if $N(a) \in F^{\times 2}$. If $N(a) = \nu^2$ for some $\nu \in F^\times$, then $\mathcal{S}(B/A)$ is generated over F by an element whose minimal polynomial is*

$$X^4 - 2T(a)X^2 - 8\nu X + T(a^2) - 2S(a).$$

Proof. The first part readily follows from Proposition 4.17. If $N(a) = \nu^2$, then $\Delta(B) \simeq F \times F$. Let d, d' be the minimal idempotents of $\Delta(B)$. By Proposition 4.14, we have

$$\Omega(B/A) \simeq \mathcal{S}(B/A) \times \mathcal{S}(B/A),$$

and we may identify $d\Omega(B/A)$ and $d'\Omega(B/A)$ with $\mathcal{S}(B/A)$. Since

$$d\delta_b = \pm 4\nu d \qquad \text{and} \qquad d'\delta_b = \mp 4\nu d',$$

the minimal polynomials of $d\omega_b$ and $d'\lambda_b$ are

$$X^4 - 2T(a)X^2 \pm 8\nu X + T(a^2) - 2S(a).$$

□

Assume now $\operatorname{char} F = 2$. Let b be a generating element for B over A with $\overline{b} = b + 1$, hence $b^2 + b \in A$. Let $a = b^2 + b$, i.e., using the notation $\wp$ for the map $x \mapsto x^2 + x$,

$$a = \wp(b) \in A.$$

Assume moreover a generates A, hence

$$A = F[a] \qquad \text{and} \qquad B = F[\wp^{-1}(a)].$$

In contrast with Proposition 4.17, ω_b does not generate $\Omega(B/A)$ since $(b - \overline{b})^2 = 1$ does not generate A (see Proposition 4.15). One could take for example ω_{ab} as a generator of $\Omega(B/A)$, since $(ab - \overline{ab})^2 = a^2$ (assuming that a^2 also generates A, which for a cubic étale algebra is in general the case). However a simpler minimal polynomial is obtained for the element

$$\mu_b = b_1b_2 + b_1b_3 + b_2b_3$$

(with the notations of Equation 19). Moreover we have

$$\delta_b = b_1 + b_2 + b_3.$$

if $\operatorname{char} F = 2$ and $\overline{b} + b = 1$.

Proposition 4.19. ($\operatorname{char} F = 2$) *With the notation above,*

$$\Delta(B) = F[\delta_b] \qquad \textit{and} \qquad \Omega(B/A) = F[\delta_b, \mu_b] = \Delta(B)[\mu_b].$$

Moreover, the minimal polynomial of δ_b over F is

$$X^2 + X + T(a),$$

and the minimal polynomial of μ_b over $\Delta(B)$ is

$$X^4 + X^3 + (\delta_b^2 + 1)X^2 + (\delta_b^2 + S(a) + 1)X + (\delta_b + S(a) + 1)S(a) + N(a).$$

Proof. Since b generates B over A, Proposition 4.15 shows that $\Delta(B) = F[\delta_b]$, and Equations (21) yield the minimal polynomial of δ_b.

To prove the rest, we extend scalars and assume B is split. Using the same notation as in Example 2.9, we have

$$b = \beta_1 f_1 + (\beta_1 + 1)f_1' + \beta_2 f_2 + (\beta_2 + 1)f_2' + \beta_3 f_3 + (\beta_3 + 1)f_3'$$

for some β_1, β_2, $\beta_3 \in F$. Then, letting

$$d = g_0 + g_1 + g_2 + g_3 \qquad \text{and} \qquad d' = g_0' + g_1' + g_2' + g_3'$$

be the minimal idempotents of $\Delta(B) \subset \Omega(B/A)$, we have

$$\delta_b = (\beta_1 + \beta_2 + \beta_3)d + (\beta_1 + \beta_2 + \beta_3 + 1)d',$$

and

$$\mu_b = v_0 g_0 + v_0' g_0' + v_1 g_1 + v_1' g_1' + v_2 g_2 + v_2' g_2' + v_3 g_3 + v_3' g_3'$$

where

$$\begin{aligned}
v_0 &= \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3, & v_0' &= v_0 + 1,\\
v_1 &= \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 + \beta_2 + \beta_3 + 1, & v_1' &= v_1 + 1,\\
v_2 &= \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 + \beta_1 + \beta_3 + 1, & v_2' &= v_2 + 1,\\
v_3 &= \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 + \beta_1 + \beta_2 + 1, & v_3' &= v_3 + 1.
\end{aligned}$$

Then

$$\prod_{0 \le i < j \le 3} (v_i - v_i) = \prod_{1 \le i < j \le 3} (\beta_i - \beta_j)^2.$$

Since b generates B over A, the elements β_1, β_2, β_3 are pairwise distinct, hence this equality shows that $v_0, \dots, v_3$ are pairwise distinct. Similarly, $v_0', \dots, v_3'$ are pairwise distinct, hence μ_b generates $\Omega(B/A)$ over $\Delta(B)$. We have

$$\begin{aligned}
T(a) &= (\beta_1^2 + \beta_1) + (\beta_2^2 + \beta_2) + (\beta_3^2 + \beta_3),\\
S(a) &= (\beta_1^2 + \beta_1)(\beta_2^2 + \beta_2) + (\beta_1^2 + \beta_1)(\beta_3^2 + \beta_3) + (\beta_2^2 + \beta_2)(\beta_3^2 + \beta_3),\\
N(a) &= (\beta_1^2 + \beta_1)(\beta_2^2 + \beta_2)(\beta_3^2 + \beta_3),
\end{aligned}$$

and brute force computation shows that v_0, v_1, v_2 and v_3 are roots of

$$\begin{aligned}
X^4 + X^3 + (\beta_1^2 + \beta_2^2 + \beta_3^2 + 1)X^2 + (\beta_1^2 + \beta_2^2 + \beta_3^2 + S(a) + 1)X&\\
+ (\beta_1 + \beta_2 + \beta_3 + S(a) + 1)S(a) + N(a)&.
\end{aligned}$$

Similarly, v_0', v_1', v_2' and v_3' are roots of

$$\begin{aligned}
X^4 + X^3 + (\beta_1^2 + \beta_2^2 + \beta_3^2)X^2 + \big(\beta_1^2 + \beta_2^2 + \beta_3^2 + S(a)\big)X&\\
+ \big(\beta_1 + \beta_2 + \beta_3 + S(a)\big)S(a) + N(a)&,
\end{aligned}$$

hence the proof is complete. $\square$

Corollary 4.20. ($\operatorname{char} F = 2$) *With the same notation as in Proposition 4.19, the discriminant $\Delta(B)$ is split if and only if $T(a) \in \wp(F)$. If $T(a) = \wp(\nu)$ for some $\nu \in F$, then $\mathcal{S}(B/A)$ is generated over F by an element whose minimal polynomial is*

$$X^4 + X^3 + \nu^2 X^2 + \big(\nu^2 + S(a)\big)X + \big(\nu + S(a)\big)S(a) + N(a).$$

Proof. The first part readily follows from Proposition 4.19. If $T(a) = \wp(\nu)$, then $\Delta(B) = F \times F$. Let d, d' be the minimal idempotents of $\Delta(B) \subset \Omega(B/A)$. We may assume $d = \delta_b + \nu$ and $d' = \delta_b + \nu + 1$, hence

$$d\delta_b = (\nu + 1)d.$$

As in the proof of Corollary 4.18, we may identify $d\Omega(B/A)$ and $d'\Omega(B/A)$ with $\mathcal{S}(B/A)$, and it follows from Proposition 4.19 that the minimal polynomial of $d\mu_b$ is as stated. $\square$

Combining the results of subsections 4.3 and 4.4 we get:

Proposition 4.21. *Let Q be a quartic étale algebra.*

(a) *If $\operatorname{char} F \neq 2$, let $x \in Q$ be a generator such that $T_{Q/F}(x) = 0$. There exists an isomorphism $\phi_1 \colon Q \xrightarrow{\sim} \mathcal{S}\big(\Lambda_2(Q)/\mathcal{R}(Q)\big)$ such that $\phi_1(x) = \omega_{\lambda_x}$.*

(b) *If $\operatorname{char} F = 2$, let $x \in Q$ be a generator such that $T_{Q/F}(x) = 1$. There exists an isomorphism $\phi_2 \colon Q \xrightarrow{\sim} \mathcal{S}\big(\Lambda_2(Q)/\mathcal{R}(Q)\big)$ such that $\phi_2(x) = \mu_{\lambda_x}$.*

5. Special actions on four elements

As in the preceding sections, Γ denotes a profinite group. The constructions on Γ-sets given in §1.1 take a special form when the Γ-action has some particular properties. For instance, if the action on a set X is not transitive, then the orbits $X_1, \ldots, X_r$ under Γ yield a Γ-set decomposition

$$X = X_1 \amalg \ldots \amalg X_r.$$

Even if the Γ-action on X is transitive, the induced action on $\Sigma_n(X)$ may not be transitive.

Proposition 5.1. *Let X be a Γ-set with $|X| = n$, and let $\alpha \colon \Gamma \to \mathfrak{S}_X$ be the action of Γ. If $\big(\mathfrak{S}_X : \alpha(\Gamma)\big) = r$, there is a Γ-set decomposition*

$$\Sigma_n(X) = \Omega_1 \amalg \ldots \amalg \Omega_r. \tag{22}$$

Each Γ-set Ω_i is a G_i-torsor for some subgroup $G_i \subset \mathfrak{S}_n$ isomorphic to $\alpha(\Gamma)$, and the subgroups G_i are conjugate in $\mathfrak{S}_n$. Moreover, the Γ-sets $\Omega_1, \ldots, \Omega_r$ are isomorphic.

Proof. The Γ-orbits of $\Sigma_n(X)$ yield the decomposition (22). To see that each Ω_i is a G_i-torsor, recall that for $(x_1, \ldots, x_n) \in \Sigma_n(X)$, $\gamma \in \Gamma$ and $\sigma \in \mathfrak{S}_n$, we have by definition

$$\gamma(x_1, \ldots, x_n) = \big(\alpha(\gamma)(x_1), \ldots, \alpha(\gamma)(x_n)\big) \text{ and } (x_1, \ldots, x_n)^\sigma = (x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

For each $\gamma \in \Gamma$, there is a unique $\sigma \in \mathfrak{S}_n$ such that

$$\gamma(x_1, \ldots, x_n) = (x_1, \ldots, x_n)^\sigma,$$

and the map $\gamma \mapsto \sigma$ defines a homomorphism $\Gamma \to \mathfrak{S}_n$ which depends on the choice of $(x_1, \dots, x_n)$ and factors through α to yield an injection $\alpha(\Gamma) \hookrightarrow \mathfrak{S}_n$. If $(x_1, \dots, x_n) \in \Omega_i$, let $G_i \subset \mathfrak{S}_n$ be the image of this map. Then Ω_i is a G_i-torsor. Moreover, if $(x_1, \dots, x_n) \in \Omega_i$ and $(y_1, \dots, y_n) \in \Omega_j$, there exists $\sigma \in \mathfrak{S}_n$ such that

$$(y_1, \dots, y_n) = (x_1, \dots, x_n)^\sigma.$$

Conjugation by σ maps G_j to G_i and the action of σ defines an isomorphism of Γ-sets $\Omega_i \xrightarrow{\sim} \Omega_j$. □

Remark. The $\mathfrak{S}_n$-torsor $\Sigma_n(X)$ can be obtained as the induced torsor $\operatorname{Ind}_{G_1}^{\mathfrak{S}_n} \Omega_1$, by mimicking the construction in [3, (18.17)].

Note that if the Γ-action on X is transitive, then the map $X \xleftarrow{\pi_n} \Sigma_n(X)$ restricts to each Ω_i to define a covering $X \leftarrow \Omega_i$. Extending Definition 3.2, this covering may be regarded as a G_i-Galois closure of X.

Taking for Γ the absolute Galois group of a field F, and using the anti-equivalence $\acute{\mathit{E}}t_F \equiv \mathit{Set}_\Gamma$ of Section 2, we may adapt the construction above to étale algebras. Disjoint unions of Γ-sets correspond to direct product decompositions of algebras, hence an étale F-algebra is a field if and only if the Γ-action on $\mathbf{X}(E)$ is transitive. If $\dim E = n$, Proposition 5.1 thus yields a direct product decomposition of the $\mathfrak{S}_n$-Galois closure $\Sigma_n(E)$ into isomorphic fields

$$\Sigma_n(E) \simeq L_1 \times \cdots \times L_r.$$

Each L_i is a Galois extension of F with Galois group $G_i \subset \mathfrak{S}_n$ isomorphic to the image of the action $\Gamma \to \mathfrak{S}_{\mathbf{X}(E)}$. If E is a field, each L_i can be regarded as a Galois closure of E/F, see [3, (18.22)].

In the rest of this section, we consider the particular case where $n = 4$. To determine the various possibilities for the image of the action $\Gamma \to \mathfrak{S}_4$, we list the subgroups of $\mathfrak{S}_4$.

Proposition 5.2. *In the symmetric group $\mathfrak{S}_4$,*

- *the alternating group $\mathfrak{A}_4$ is the unique subgroup of order 12;*
- *there are four subgroups of order 6; they are conjugate to $\mathfrak{S}_3$;*
- *there are three subgroups of order 8; they are pairwise conjugate and isomorphic to the dihedral group D_4.*

Moreover, every proper subgroup of $\mathfrak{S}_4$ is contained in at least one of the subgroups listed above.

Proof. Any subgroup of index 2 in $\mathfrak{S}_4$ must contain all the Sylow 3-subgroups of $\mathfrak{S}_4$. Since these Sylow subgroups are generated by the cycles of length 3, the first claim is clear.

A subgroup of order 6 in $\mathfrak{S}_4$ cannot be transitive on $\{1, 2, 3, 4\}$. On the other hand, it has an orbit of 3 elements since it contains a Sylow 3-subgroup, hence it must be the isotropy group of one of 1, 2, 3, or 4.

The dihedral group D_4 acts on the four vertices of a square, hence it may be considered as a subgroup of $\mathfrak{S}_4$. It is then identified with a 2-Sylow subgroup of $\mathfrak{S}_4$, and all the 2-Sylow subgroups are conjugate.

Finally, let $G \subset \mathfrak{S}_4$ be a subgroup. If its order is divisible by 3, then it is 3, 6 or 12, hence G is contained in $\mathfrak{A}_4$ or in a conjugate of $\mathfrak{S}_3$. If its order is a power of 2, then G is contained in a 2-Sylow subgroup. □

In the following subsections, we examine the additional information on a Γ-set X with $|X| = 4$ (or on a quartic étale F-algebra Q) when the Γ-action factors through a subgroup $\mathfrak{S}_3$ or D_4. We then collect the information to obtain a classification of quartic étale F-algebras in §5.3.

5.1. **Action through $\mathfrak{S}_3$.** Suppose first the action of Γ leaves an element $x \in X$ invariant. It then preserves a disjoint union decomposition

$$X = \{x\} \amalg R,$$

where $|R| = 3$. The 2-element subsets of X containing x are in one-to-one correspondence with R, hence $\Lambda_2(X)$ decomposes as

$$\Lambda_2(X) = R \amalg \Lambda_2(R).$$

Moreover, the "complementary subset" involution γ_X on $\Lambda_2(X)$ interchanges R and $\Lambda_2(R)$ and defines an isomorphism $R \simeq \Lambda_2(R)$. Therefore, we have canonical isomorphisms

$$\Lambda_2(X) \simeq R \amalg R \quad \text{and} \quad \mathcal{R}(X) \simeq R.$$

(See also §4.2.)

Assuming Γ is the absolute Galois group of a field F, we may translate the results above in the framework of étale F-algebras.

Proposition 5.3. *Let Q be a quartic étale F-algebra. If the Γ-action on $\mathbf{X}(Q)$ factors through a subgroup $\mathfrak{S}_3 \subset \mathfrak{S}_{\mathbf{X}(Q)}$, then there is a cubic field extension L/F such that*

$$Q \simeq F \times L, \qquad \Lambda_2(Q) \simeq L \times L, \quad \text{and} \quad \mathcal{R}(Q) \simeq L.$$

Moreover, the following conditions are equivalent:

(a) *the Γ-action factors through a cyclic subgroup C_3;*
(b) *the extension L/F is Galois (hence cyclic);*
(c) $\Delta(Q) \simeq F \times F$.

5.2. **Action through D_4.** Suppose now that the action of Γ factors through a Sylow 2-subgroup of $\mathfrak{S}_X$, i.e. through a dihedral subgroup D_4. Since the Sylow 2-subgroups of $\mathfrak{S}_X$ are the isotropy groups of partitions of X into 2-element subsets, there is such a partition which is invariant under Γ. This observation characterizes the case where Γ acts through D_4:

Proposition 5.4. *For a set $X \in \mathsf{Set}_\Gamma^4$, the following conditions are equivalent:*

(a) *the Γ-action factors through a Sylow 2-subgroup of $\mathfrak{S}_X$;*
(b) *the Γ-action leaves a point of $\mathcal{R}(X)$ fixed;*
(c) $\mathcal{R}(X) \simeq \{*\} \amalg \Delta(X)$;
(d) *X is a double covering of a set of two elements, i.e. there exists a map $(D \leftarrow X) \in \mathsf{Cov}_\Gamma^{2\wr 2}$.*

Proof. The points of $\mathcal{R}(X)$ are the partitions of X into 2-element subsets, hence (a) $\iff$ (b). The implication (c)$\Rightarrow$(b) is clear, and (b)$\Rightarrow$(c) follows from Proposition 4.1. If $D = \big\{\{x_1, x_2\}, \{x_3, x_4\}\big\} \in \mathcal{R}(X)$ is fixed under Γ, then the canonical map $D \leftarrow X$ which carries x_1, x_2 to $\{x_1, x_2\}$ and x_3, x_4 to $\{x_3, x_4\}$ is a double covering, hence (b)$\Rightarrow$(d). Finally, (d)$\Rightarrow$(a) follows from $\mathfrak{S}_2 \wr \mathfrak{S}_2 \simeq D_4$. $\square$

The following proposition establishes the existence of a "dual" Γ-set $\check{X}$:

Proposition 5.5. *If the equivalent conditions of Proposition 5.4 hold, then there exists a* Γ*-set* $\check{X} \in \mathsf{Set}^4_\Gamma$*, with* Γ*-action through a Sylow* 2*-subgroup of* $\mathfrak{S}_{\check{X}}$*, such that*

$$\Lambda_2(X) \simeq \Delta(\check{X}) \amalg \check{X}, \qquad \Lambda_2(\check{X}) \simeq \Delta(X) \amalg X,$$
$$\mathcal{R}(X) \simeq \{\Delta(\check{X})\} \amalg \Delta(X), \qquad \mathcal{R}(\check{X}) \simeq \{\Delta(X)\} \amalg \Delta(\check{X}).$$

Moreover, X *is a double covering of* $\Delta(\check{X})$*, and* $\check{X}$ *is a double covering of* $\Delta(X)$*.*

If the Γ*-action on* $\Delta(X)$ *is not trivial, the* Γ*-set* $\check{X}$ *is canonically determined. If the* Γ*-actions on* $\Delta(X)$ *and* $\Delta(\check{X})$ *are not trivial, then there is a canonical isomorphism*

$$\check{\check{X}} = X.$$

Proof. Let $D \in \mathcal{R}(X)$ be a fixed point of Γ. Define $\check{X}$ as the complementary subset in $\Lambda_2(X)$ of the fiber $\varepsilon^{-1}(D)$ under the canonical map $\mathcal{R}(X) \xleftarrow{\varepsilon} \Lambda_2(X)$. The set $\check{X}$ is thus canonically determined if Γ has a unique fixed point $D \in \mathcal{R}(X)$, or, equivalently by Proposition 5.4, if the Γ-action on $\Delta(X)$ is not trivial.

We proceed to prove that $\check{X}$ satisfies the stated properties. To clarify the discussion, we use geometric language. If $D = \big\{\{x_1,x_2\},\{x_3,x_4\}\big\}$, we identify X with the set of vertices of a square, letting $\{x_1,x_2\}$ and $\{x_3,x_4\}$ be the pairs of opposite vertices. We may thus identify D to the set of diagonals of the square, and we have a decomposition

$$\Lambda_2(X) = D \amalg \check{X} \tag{23}$$

where $\check{X}$ is the set of pairs of adjacent vertices, which may be identified with the set of edges of the square. (Note that $\check{X}$ may also be viewed as the *dual square* of X in the sense of polytope theory.) There is a “dual” decomposition

$$\Lambda_2(\check{X}) = M \amalg X, \tag{24}$$

where X is identified with the set of pairs of adjacent edges (by mapping every such pair to their common vertex) and M is the set of pairs of parallel edges, which may be identified with the medians of the square. The “complementary subset” involutions γ_X and $\gamma_{\check{X}}$ preserve the decompositions (23) and (24), and the set of orbits of $\check{X}$ (resp. X) under γ_X (resp. $\gamma_{\check{X}}$) can be identified with M (resp. D), hence

$$\mathcal{R}(X) = \{D\} \amalg M \qquad \text{and} \qquad \mathcal{R}(\check{X}) = \{M\} \amalg D, \tag{25}$$

and there are natural maps $D \leftarrow X$ and $M \leftarrow \check{X}$ which show X and $\check{X}$ are double coverings of D and M respectively. By Proposition 4.1, Equations (25) yield canonical isomorphisms

$$M = \Delta(X) \qquad \text{and} \qquad D = \Delta(\check{X}).$$

If the Γ-action on $\Delta(\check{X})$ is not trivial, then M is the unique fixed point of $\mathcal{R}(\check{X})$, and $X \subset \Lambda_2(\check{X})$ is the complementary subset of the fiber of M under the canonical map $\mathcal{R}(\check{X}) \leftarrow \Lambda_2(\check{X})$, hence $\check{\check{X}} = X$. This completes the proof. □

We may use the Γ-set $\check{X}$ to obtain information on the Γ-action on X, as follows:

Proposition 5.6. *Let* $X \in \mathsf{Set}^4_\Gamma$ *be a* Γ*-set satisfying the equivalent properties of Proposition 5.4, and suppose the* Γ*-action on* $\Delta(X)$ *is not trivial, so the dual set* $\check{X}$ *is uniquely determined. The following properties are equivalent:*

(a) *the* Γ*-action on* X *factors through a cyclic subgroup* C_4*;*
(b) $\check{X} \simeq X$*;*
(c) $\Delta(\check{X}) \simeq \Delta(X)$.

Proof. If the action of Γ factors through C_4, we may regard X as the set of vertices of an *oriented* square, and use the orientation to define a canonical isomorphism $X \xrightarrow{\sim} \check{X}$, proving (a)$\Rightarrow$(b). Since the implication (b)$\Rightarrow$(c) is clear, it only remains to prove (c)$\Rightarrow$(a). If the image of Γ under the action contains the Vierergruppe $\mathfrak{V}_X$, then there is an element in Γ which acts trivially on M and non-trivially on D, hence $\Delta(X) \not\simeq \Delta(\check{X})$. Similarly, if some element of Γ acts by a single transposition on X, then it acts trivially on D and non-trivially on M, hence $\Delta(X) \not\simeq \Delta(\check{X})$. Therefore, (c) implies that the image of the action of Γ contains at most cycles of length 4 and one element of $\mathfrak{V}_X$. $\square$

Remark. The Γ-set $D * M = \Delta(X) * \Delta(\check{X})$ can be identified with the set of orientations of the square.

For the following proposition, recall that the dihedral group D_4 contains two non-conjugate elementary abelian subgroups $C_2 \times C_2$. Viewing D_4 as a subgroup of $\mathfrak{S}_4$, one of these subgroups is $\mathfrak{V}$ $(= D_4 \cap \mathfrak{A}_4)$. The other one is generated by two disjoint transpositions; it is not transitive on $\{1, 2, 3, 4\}$.

Proposition 5.7. *Let* $X \in \mathsf{Set}^4_\Gamma$ *be a* Γ*-set satisfying the equivalent properties of Proposition 5.4, and suppose the* Γ*-action on* $\Delta(X)$ *is not trivial, so the dual set* $\check{X}$ *is uniquely determined. The following properties are equivalent:*

(a) *the* Γ*-action on* X *factors through an elementary abelian subgroup* $C_2 \times C_2 \neq \mathfrak{V}_X$*;*
(b) *the* Γ*-action on* $\check{X}$ *factors through* $\mathfrak{V}_{\check{X}}$*;*
(c) *the* Γ*-action on* $\Delta(\check{X})$ *is trivial.*

The proof is left to the reader.

Finally, we consider the case where the Γ-action on X factors through $\mathfrak{V}_X$.

Proposition 5.8. *For a* Γ*-set* $X \in \mathsf{Set}^4_\Gamma$*, the following conditions are equivalent:*

(a) *the* Γ*-action on* X *factors through the Vierergruppe* $\mathfrak{V}_X$*;*
(b) *the* Γ*-action on* $\mathcal{R}(X)$ *is trivial;*
(c) *the* Γ*-set* $\Lambda_2(X)$ *has a decomposition into 2-element subsets stable under the canonical involution of* $\Lambda_2(X)/\mathcal{R}(X)$*,*

$$\Lambda_2(X) = D_1 \amalg D_2 \amalg D_3;$$

(d) X *satisfies the equivalent conditions of Proposition 5.4 and* Γ *acts trivially on* $\Delta(X)$.

Moreover, if these conditions hold, then the Γ*-action on* $D_1 * D_2 * D_3$ *is trivial.*

Proof. The Vierergruppe can be defined as the subgroup of $\mathfrak{S}_X$ which leaves invariant all the partitions of X into 2-element subsets, hence (a) $\Longleftrightarrow$ (b). The equivalence of (b) and (c) is clear: take for D_1, D_2 and D_3 the fibers of the canonical map $\mathcal{R}(X) \leftarrow \Lambda_2(X)$. The equivalence (b) $\Longleftrightarrow$ (d) readily follows from Proposition 5.4.

If the equivalent conditions of the proposition hold, then the set $\check{X}$ of Proposition 5.5 can be arbitrarily chosen as $D_1 \amalg D_2$, $D_1 \amalg D_3$ or $D_2 \amalg D_3$. If we choose

$\check{X} = D_1 \amalg D_2$, Proposition 5.5 yields $\Delta(\check{X}) = D_3$. On the other hand, it is easily checked that

$$\Delta(D_1 \amalg D_2) \simeq D_1 * D_2,$$

hence $D_1 * D_2 \simeq D_3$ and therefore the Γ-action on $D_1 * D_2 * D_3$ is trivial. $\square$

Taking for Γ the absolute Galois group of a field F, we may translate in terms of étale F-algebras the results of this subsection, by using the anti-equivalence $\mathsf{\acute{E}t}_F \equiv \mathsf{Set}_\Gamma$ of §2. By a *quartic 2-algebra* we mean an étale algebra which is a quadratic extension of a quadratic étale algebra. These algebras can be characterized through Proposition 5.4:

Proposition 5.9. *For a quartic F-algebra Q, the following conditions are equivalent:*

(a) *the Γ-action on $\mathbf{X}(Q)$ factors through a Sylow 2-subgroup of $\mathfrak{S}_{\mathbf{X}(Q)}$;*
(b) *$\mathcal{R}(Q)$ is not a field;*
(c) *$\mathcal{R}(Q) \simeq F \times \Delta(Q)$;*
(d) *Q is a quartic 2-algebra.*

Proposition 5.5 proves for every quartic 2-algebra Q the existence of a "dual" quartic 2-algebra $\check{Q}$, which is canonically determined if $\Delta(Q)$ is not split. This algebra is a quadratic extension of $\Delta(Q)$, and Q is a quadratic extension of $\Delta(\check{Q})$. Moreover, Q and $\check{Q}$ satisfy the following relations:

$$\Lambda_2(Q) \simeq \Delta(\check{Q}) \times \check{Q}, \qquad \Lambda_2(\check{Q}) \simeq \Delta(Q) \times Q,$$
$$\mathcal{R}(Q) \simeq F \times \Delta(Q), \qquad \mathcal{R}(\check{Q}) \simeq F \times \Delta(\check{Q}).$$

We record a few special cases:

Proposition 5.10. *Let Q be a quartic 2-algebra over F.*

(1) *If Q is a cyclic field extension of F, then $\check{Q} \simeq Q$, hence Q is a quadratic extension of $\Delta(Q)$, and*

$$\Lambda_2(Q) \simeq \Delta(Q) \times Q, \qquad \mathcal{R}(Q) \simeq F \times \Delta(Q).$$

(2) *If $Q = K_1 \times K_2$, where K_1 and K_2 are non-isomorphic quadratic F-algebras, then $\check{Q} \simeq K_1 \otimes_F K_2$, $\Delta(Q) \simeq K_1 * K_2$, and*

$$\Lambda_2(Q) \simeq F \times F \times (K_1 \otimes_F K_2), \qquad \mathcal{R}(Q) \simeq F \times (K_1 * K_2).$$

(3) *If $Q = K_1 \otimes_F K_2$, where K_1 and K_2 are quadratic field extensions of F, then one may take $\check{Q} = K_1 \times K_2$, or $K_1 \times (K_1 * K_2)$, or $K_2 \times (K_1 * K_2)$. Moreover, $\Delta(Q)$ is split, and*

$$\Lambda_2(Q) \simeq K_1 \times K_2 \times (K_1 * K_2), \qquad \mathcal{R}(Q) \simeq F \times F \times F.$$

These results are easily derived from Propositions 5.6, 5.7 and 5.8. Note that split quadratic algebras are allowed in (2), and that the case where $Q = K \times K$ for some quadratic field extension K of F is covered by (3) since $K \times K \simeq K \otimes_F K$.

Since $\Lambda_2(Q) \simeq \Delta(\check{Q}) \times \check{Q}$, we may use the computations of §4.3 to give an explicit description of $\check{Q}$.

Proposition 5.11. *Let Q be a quartic 2-algebra over F, and let $K \subset Q$ be a quadratic étale F-algebra. Denote by $\bar{\ }$ the canonical involution of K over F.*

(1) *Suppose* $\operatorname{char} F \neq 2$ *and* $Q = K(\sqrt{y})$ *where* $y \in K$ *generates* K*. Then*

$$\Delta(Q) \simeq F\big(\sqrt{N_{K/F}(y)}\big) \quad \textit{and} \quad \check{Q} \simeq F(\sqrt{y} + \sqrt{\overline{y}}) \quad (\textit{and } \Delta(\check{Q}) \simeq K).$$

(2) *Suppose* $\operatorname{char} F = 2$ *and* $Q = K\big(\wp^{-1}(y)\big)$ *where* $y \in K$ *generates* K*. Then*

$$\Delta(Q) \simeq F\big(\wp^{-1}(T_{K/F}(y))\big) \quad \textit{and} \quad \check{Q} \simeq F\big(\wp^{-1}(y)\wp^{-1}(\overline{y})\big) \quad (\textit{and } \Delta(\check{Q}) \simeq K).$$

In the proof below, we write simply $T(y)$, $N(y)$ for $T_{K/F}(y)$ and $N_{K/F}(y)$.

Proof. (1) By hypothesis, the element $x = \sqrt{y}$ generates Q over F. Its minimal polynomial is

$$u^4 - T(y)u^2 + N(y) \in F[u]. \tag{26}$$

Let $\lambda_x \in \Lambda_2(Q)$ be defined as in (18). By Proposition 4.13, $\gamma_Q(\lambda_x)\lambda_x$ generates $\mathcal{R}(Q)$ and its minimal polynomial is

$$t\big((t + T(y))^2 - 4N(y)\big).$$

Therefore,

$$\mathcal{R}(Q) \simeq F \times F\big(\sqrt{N(y)}\big), \tag{27}$$

determining $\Delta(Q)$. Moreover, Proposition 4.13 also shows that $\gamma_Q(\lambda_x) = -\lambda_x$, hence regarding (27) as an identification,

$$\lambda_x^2 = \big(0, T(y) - 2\sqrt{N(y)}\big).$$

Therefore, the projection $\check{\lambda}_x$ of λ_x to $\check{Q}$ under the isomorphism $\Lambda_2(Q) \simeq \Delta(\check{Q}) \times \check{Q}$ satisfies

$$\check{\lambda}_x^2 = T(y) - 2\sqrt{N(y)} = y + \overline{y} - 2\sqrt{y\overline{y}}. \tag{28}$$

If the minimal polynomial (26) of x has no root in F, computation shows that $T(y) - 2\sqrt{N(y)}$ is not a square in $\Delta(Q)$, hence

$$\check{Q} = F(\check{\lambda}_x).$$

The proof is complete, since (28) shows that we may identify $\check{\lambda}_x$ with $\sqrt{y} + \sqrt{\overline{y}}$, determining the square roots in such a way that $\sqrt{y}\sqrt{\overline{y}} = -\sqrt{N(y)}$.

If the minimal polynomial (26) has a root in F, then Q has a factor F and we are in the situation of Proposition 5.10(2) with K_1 or K_2 split. This case is left to the reader.

(2) Suppose now $\operatorname{char} F = 2$. The element $x = y\wp^{-1}(y)$ generates Q with minimal polynomial

$$u^4 + T(y)u^3 + \big(T(y)^3 + T(y)N(y) + N(y)\big)u^2 + T(y)^2N(y)u + N(y)^3 \in F[u].$$

Consider again the element $\lambda_x \in \Lambda_2(Q)$ defined in (18). By Proposition 4.13, $\gamma_Q(\lambda_x)\lambda_x$ generates $\mathcal{R}(Q)$ and has minimal polynomial

$$\big(t - N(y)\big)\big(t^2 - N(y)t + T(y)^6 + T(y)^2N(y) + T(y)N(y)^2\big).$$

If w is a root of the quadratic factor, then

$$\wp\big(N(y)^{-1}(w - T(y)^3 - T(y)N(y))\big) = T(y),$$

hence

$$\mathcal{R}(Q) \simeq F \times F\big(\wp^{-1}(T(y))\big).$$

Proposition 4.13 also shows that the projection $\check{\lambda}_x$ of λ_x onto $\check{Q}$ satisfies

$$\check{\lambda}_x^2 + T(y)\check{\lambda}_x + w = 0. \tag{29}$$

If $\wp^{-1}(y)$ and $\wp^{-1}(\overline{y})$ are determined in such a way that $\wp^{-1}(y) + \wp^{-1}(\overline{y}) = \wp^{-1}(T(y))$, computation shows that $\wp^{-1}(T(y))\big(T(y) + \wp^{-1}(y)\wp^{-1}(\overline{y})\big)$ also satisfies (29), hence we may identify $\check{Q}$ with $F\big(\wp^{-1}(y)\wp^{-1}(\overline{y})\big)$. □

We refer to [5] for a description of quartic 2-extensions of fields in characteristic different from 2.

5.3. **Classification of quartic algebras.** Combining the results of §§5.1 and 5.2, we obtain a classification of quartic étale F-algebras Q based on the action of the absolute Galois group Γ of F on $\mathbf{X}(Q)$. We summarize the various possibilities for Q, $\Delta(Q)$, $\mathcal{R}(Q)$ and $\Lambda_2(Q)$ in the table below. In this table, $\alpha(\Gamma) \subset \mathfrak{S}_{\mathbf{X}(Q)} \simeq \mathfrak{S}_4$ is the image of the Γ-action. The letters N and L are used for sextic and cubic separable field extensions of F, and K, $\check{K}$, K_1, K_2 for quadratic separable field extensions of F. A quartic separable field extension is called an $\mathfrak{S}_4$-quartic (resp. $\mathfrak{A}_4$-quartic) if its Galois closure has Galois group isomorphic to $\mathfrak{S}_4$ (resp. $\mathfrak{A}_4$).

$\alpha(\Gamma)$	Q	$\Delta(Q)$	$\mathcal{R}(Q)$	$\Lambda_2(Q)$
$\{1\}$	F^4	F^2	F^3	F^6
$C_2 \not\subset \mathfrak{V}$	$F^2 \times K$	K	$F \times K$	$F^2 \times K^2$
$C_2 \subset \mathfrak{V}$	$K \times K$	F^2	F^3	$F^2 \times K^2$
C_3	$F \times L, L\,\text{cyclic}$	F^2	L	$L \times L$
$C_2 \times C_2 \not\subset \mathfrak{V}$	$K_1 \times K_2$	$K_1 * K_2$	$F \times K_1 * K_2$	$F^2 \times (K_1 \otimes K_2)$
$\mathfrak{V}$	$K_1 \otimes K_2$	F^2	F^3	$K_1 \times K_1 \times K_1 * K_2$
C_4	cyclic	$K \subset Q$	$F \times K$	$K \times Q$
S_3	$F \times L$	K	L	$L \times L$
D_4	$Q \supset \check{K}$	K	$F \times K$	$\check{K} \times \check{Q}$, $\check{Q} \supset K$
$\mathfrak{A}_4$	$\mathfrak{A}_4$-quartic	F^2	$L\,\text{cyclic}$	$N \supset L$
$\mathfrak{S}_4$	$\mathfrak{S}_4$-quartic	K	$L\,S_3$-cubic	$N \supset L$

6. Cyclic quartic algebras

Let F be an arbitrary field with absolute Galois group $\Gamma = \mathrm{Gal}(F_s/F)$. Quartic étale F-algebras Q such that the Γ-action on $\mathbf{X}(Q)$ factors through a cyclic group C_4 can be endowed with the structure of a C_4-Galois algebra. (In the table of §5.3, they can be found in the lines $\alpha(\Gamma) = \{1\}$, $\alpha(\Gamma) = C_2 \subset \mathfrak{V}$ and $\alpha(\Gamma) = C_4$.) Fixing a generator of C_4 (or, equivalently, choosing an isomorphism $C_4 \simeq \mathbb{Z}/4\mathbb{Z}$), we may consider a C_4-Galois F-algebra as a pair (Q,ν) where Q is a quartic étale F-algebra and ν is an F-algebra automorphism of Q such that

$$\{x \in Q \mid \nu(x) = x\} = F.$$

The automorphism ν then satisfies $\nu^4 = \mathrm{Id}$, and it yields the action on Q of the generator of C_4. An isomorphism of C_4-Galois F-algebras $\beta\colon (Q,\nu) \to (Q',\nu')$ is an isomorphism $\beta\colon Q \xrightarrow{\sim} Q'$ such that $\nu' \circ \beta = \beta \circ \nu$. Let $\mathrm{Cycl}_4(F)$ be the set of isomorphism classes of C_4-Galois F-algebras. As observed in §3.5, there is a canonical bijection

$$\mathrm{Cycl}_4(F) \simeq H^1(\Gamma, C_4).$$

If C_4 is embedded in $\mathfrak{S}_4$, the corresponding map in cohomology $H^1(\Gamma, C_4) \to H^1(\Gamma, \mathfrak{S}_4)$ maps the isomorphism class of (Q, ν) to the isomorphism class of Q.

Since C_4 is an abelian group, the set $H^1(\Gamma, C_4)$ is an abelian group. The group structure on $\mathrm{Cycl}_4(F)$ is induced by the following composition law (see [2]):

$$(Q, \nu) \star (Q', \nu') = \big((Q \otimes Q')^{\nu^{-1} \otimes \nu'}, \nu \otimes \mathrm{Id}\big).$$

The class of the split algebra F^4 with the cyclic permutation of factors is the neutral element. The squaring map $\rho \colon C_4 \to \mathfrak{S}_2$ fits into an exact sequence

$$1 \to \mathfrak{S}_2 \xrightarrow{\iota} C_4 \xrightarrow{\rho} \mathfrak{S}_2 \to 1.$$

Since $H^1(\Gamma, \mathfrak{S}_2) \simeq \mathrm{Quad}(F)$ (see §3.4), the induced exact sequence in cohomology takes the form

$$1 \to \mathrm{Quad}(F) \xrightarrow{\iota^1} \mathrm{Cycl}_4(F) \xrightarrow{\rho^1} \mathrm{Quad}(F). \tag{30}$$

The map ι^1 is induced by $K \mapsto (K \times K, \nu)$ where $\nu(x, y) = \big(y, \gamma_K(x)\big)$, and the map ρ^1 carries every C_4-Galois algebra (Q, ν) to its discriminant $\Delta(Q)$ (which is isomorphic to the quadratic subalgebra Q^{ν^2}, see Proposition 5.10).

Remark. The algebra $K \times K$ contains K and $F \times F$ as quadratic subalgebras. However, Galois theory shows that if (Q, ν) is a C_4-Galois algebra and Q is a field, then Q contains a unique quadratic extension of F.

In the rest of this section, we give an explicit description of $H^1(\Gamma, C_4)$ and use it to parametrize C_4-Galois algebras up to isomorphism. The description depends in an essential way on whether the characteristic is 2 or not.

6.1. **Characteristic not 2.** If $\operatorname{char} F \neq 2$, the group $\mu_4(F_s) \subset F_s$ of fourth roots of unity is cyclic of order 4. Let $S = F[X]/(X^2 + 1)$. Twisting the Γ-action on $\mu_4(F_s)$ by a cocycle whose image in $H^1(\Gamma, \mathfrak{S}_2)$ defines S, we obtain a Γ-module $\mu_{4[S]}$ with trivial Γ-action. Thus, $\mu_{4[S]} \simeq C_4$, and C_4-Galois F-algebras are also classified by $H^1(\Gamma, \mu_{4[S]})$. To give an explicit description of this group, consider the homomorphism

$$\Upsilon \colon F^\times \times S^\times \to F^\times \times S^\times$$

defined by

$$\Upsilon(\ell, z) = (N_{S/F}(z), \ell z^2).$$

Proposition 6.1. *There is a canonical isomorphism*

$$H^1(\Gamma, \mu_{4[S]}) \simeq (F^\times \times S^\times)/\Upsilon(F^\times \times S^\times).$$

Proof. Let $i = \sqrt{-1} \in S$ be the image of X. We may identify $\mu_{4[S]}$ with

$$\big\{(1,1), (1,-1), (-1, 1 \otimes i), (-1, -1 \otimes i)\big\} \subset F_s^\times \times (F_s \otimes S)^\times,$$

which is the kernel of the map Υ extended to F_s. The proposition follows from the cohomology exact sequence associated with

$$1 \to \mu_{4[S]} \to F_s^\times \times (F_s \otimes S)^\times \xrightarrow{\Upsilon} F_s^\times \times (F_s \otimes S)^\times \to 1,$$

since Hilbert's Theorem 90 and Shapiro's lemma yield $H^1(\Gamma, F_s^\times \times (F_s \otimes S)^\times) = 1$. □

Remark. Another description of $H^1(\Gamma, \mu_{4[S]})$ is given in [3, (30.13)].

It follows from Proposition 6.1 that C_4-Galois algebras are classified by the group

$$(F^\times \times S^\times)/\Upsilon(F^\times \times S^\times).$$

(See [2] for a proof without cohomology and, more generally for a class of commutative rings in which 2 is invertible.) We give an explicit description of this correspondence.

Let $i = \sqrt{-1} \in S$. For $\lambda \in F^\times$ and $s = s_1 + is_2 \in S^\times$, let $d = N_{S/F}(s) = s_1^2 + s_2^2$ and let

$$Q_{\lambda,s} = F[W,X,Y]/I_{\lambda,s}$$

where $I_{\lambda,s}$ is the ideal generated by

$$W^2 - d, \quad X^2 - \frac{\lambda}{2}(d + s_1W), \quad Y^2 - \frac{\lambda}{2}(d - s_1W), \quad XY - \frac{\lambda}{2}s_2W.$$

The automorphism ν of $F[W,X,Y]$ defined by

$$\nu(W) = -W, \quad \nu(X) = Y, \quad \nu(Y) = -X$$

preserves $I_{\lambda,s}$ and induces an automorphism of $Q_{\lambda,s}$ which we denote by $\nu_{\lambda,s}$.

Proposition 6.2. *For any $\lambda \in F^\times$ and $s \in S^\times$, the pair $(Q_{\lambda,s}, \nu_{\lambda,s})$ is a C_4-Galois F-algebra. The map $(\lambda, s) \mapsto (Q_{\lambda,s}, \nu_{\lambda,s})$ induces a group isomorphism*

$$\Phi\colon\ F^\times \times S^\times/\big\{(N_{S/F}(z), \ell z^2) \mid \ell \in F^\times, z \in S^\times\big\} \xrightarrow{\sim} \mathrm{Cycl}_4(F).$$

Proof. We first show that $Q_{\lambda,s}$ is a quartic étale F-algebra. Let ω, ξ, $\eta \in Q_{\lambda,s}$ be the images of W, X, Y respectively. The algebra $F[\omega]$ is quadratic, $F[\omega] \simeq F[\sqrt{d}]$.

If $s_2 \neq 0$, then $d \neq s_1^2$, hence $d + s_1\omega$ is invertible. Computation shows $(\xi^{-1}\frac{\lambda}{2}s_2\omega)^2 = \frac{\lambda}{2}(d - s_1\omega)$, so

$$Q_{\lambda,s} = F[\omega,\xi] \simeq F[\sqrt{d}]\left[\sqrt{\frac{\lambda}{2}(d + s_1\sqrt{d})}\right].$$

If $s_2 = 0$, then $d = s_1^2$, hence $F[\omega] \simeq F \times F$ and we may identify ξ and η to $s_1(\sqrt{\lambda}, 0)$ and $s_1(0, \sqrt{\lambda})$ in

$$Q_{\lambda,s} \simeq F[\sqrt{\lambda}] \times F[\sqrt{\lambda}].$$

Therefore, in each case $Q_{\lambda,s}$ is a quartic étale F-algebra, and the fact that the subalgebra fixed under $\nu_{\lambda,s}$ is F is easily verified.

To prove that Φ is a group homomorphism, consider (λ, s), $(\lambda', s') \in F^\times \times S^\times$ with $s = s_1 + is_2$, $s' = s_1' + is_2'$. Let $d = N_{S/F}(s)$, $d' = N_{S/F}(s')$ and let ω, ξ, $\eta \in Q_{\lambda,s}$ and ω', ξ', $\eta' \in Q_{\lambda',s'}$ be defined as above. The elements

$$\omega_\star = \omega \otimes \omega', \quad \xi_\star = \xi \otimes \xi' - \eta \otimes \eta', \quad \eta_\star = \xi \otimes \eta' + \eta \otimes \xi'$$

are in $(Q_{\lambda,s} \otimes Q_{\lambda',s'})^{\nu_{\lambda,s}^{-1} \otimes \nu_{\lambda',s'}}$ and satisfy

$$\begin{aligned}
\omega_\star^2 &= dd', \\
\xi_\star^2 &= \frac{\lambda\lambda'}{2}\big[dd' + (s_1s_1' - s_2s_2')\omega_\star\big], \\
\xi_\star\eta_\star &= \frac{\lambda\lambda'}{2}(s_1s_2' + s_2s_1')\omega_\star, \\
\eta_\star^2 &= \frac{\lambda\lambda'}{2}\big[dd' - (s_1s_1' - s_2s_2')\omega_\star\big].
\end{aligned}$$

Moreover,

$$(\nu_{\lambda,s}\otimes \mathrm{Id})(\omega_\star)=-\omega_\star,\quad (\nu_{\lambda,s}\otimes \mathrm{Id})(\xi_\star)=\eta_\star,\quad (\nu_{\lambda,s}\otimes \mathrm{Id})(\eta_\star)=-\xi_\star.$$

Therefore,

$$(Q_{\lambda,s},\nu_{\lambda,s})\star(Q_{\lambda',s'},\nu_{\lambda',s'})\simeq(Q_{\lambda\lambda',ss'},\nu_{\lambda\lambda',ss'}).$$

If $(\lambda,s)=(N_{S/F}(z),\ell z^2)$ for some $\ell\in F^\times$, $z=z_1+iz_2\in S^\times$, then the homomorphism $F[W,X,Y]\to F^4$ defined by

$$\begin{aligned}W&\mapsto \ell N_{S/F}(z)(1,-1,1,-1),\\ X&\mapsto \ell N_{S/F}(z)(z_1,z_2,-z_1,-z_2),\\ Y&\mapsto \ell N_{S/F}(z)(z_2,-z_1,-z_2,z_1)\end{aligned}$$

induces an isomorphism $(Q_{\lambda,s},\nu_{\lambda,s})\xrightarrow{\sim}(F^4,\sigma)$ where σ is the cyclic permutation.

Conversely, suppose that for some $(\lambda,s)\in F^\times\times S^\times$ there is an isomorphism $Q_{\lambda,s}\simeq F^4$, and let $(\omega_i)_{1\le i\le 4}$, $(\xi_i)_{1\le i\le 4}$, $(\eta_i)_{1\le i\le 4}$ be the images of ω, ξ and η respectively in F^4. Then from the relations between ω, ξ and η it follows that $z=\omega_1^{-1}(\xi_1+i\eta_1)\in S$ and $\ell=(\xi_1^2+\eta_1^2)^{-1}\omega_1^3$ satisfy

$$\lambda=N_{S/F}(z)\qquad\text{and}\qquad s=\ell z^2.$$

Therefore, the homomorphism Φ is injective, and it only remains to prove its surjectivity.

Let (Q,ν) be a C_4-Galois F-algebra. If $Q\simeq F[\sqrt{\mu}]\times F[\sqrt{\mu}]$ for some $\mu\in F^\times$, then $Q\simeq Q_{\mu,1}$, as was observed at the beginning of the proof. Therefore, for the rest of the proof we may assume Q is a field. Let $K=Q^{\nu^2}\subset Q$ be the subfield fixed under ν^2, let $K=F(\omega)$ with $\omega^2=d$ for some $d\in F^\times$, and let $Q=K(\xi)$ with $\xi^2=y$ for some $y\in K^\times$. We have $y\notin F$ since Q/F is cyclic. Let $y=a+b\omega$ with a, $b\in F$, $b\neq 0$. Substituting for y an element of the form u^2y with $u\in K$, we may assume $a\neq 0$. Letting $\lambda=2ad^{-1}$ and $s_1=a^{-1}bd$, we may then write y in the form

$$y=\frac{\lambda}{2}(d+s_1\omega).$$

Let $\eta=\nu(\xi)$. Since $\xi^2\in K$ and $\xi\notin K$, we have $\nu^2(\xi^2)=\xi^2$ and $\nu^2(\xi)\neq\xi$, hence $\nu^2(\xi)=-\xi$. Therefore, $\nu(\xi\eta)=-\xi\eta$, and it follows that $\xi\eta\in\omega F^\times$. Let

$$\xi\eta=\frac{\lambda}{2}s_2\omega\qquad\text{for some } s_2\in F^\times. \tag{31}$$

From the equation $\xi^2=\frac{\lambda}{2}(d+s_1\omega)$, we obtain

$$\eta^2=\frac{\lambda}{2}(d-s_1\omega).$$

Therefore, (31) yields

$$\frac{\lambda^2}{4}s_2^2d=\frac{\lambda^2}{4}(d+s_1\omega)(d-s_1\omega),$$

hence $d=s_1^2+s_2^2$. It is then clear that $(Q,\nu)\simeq(Q_{\lambda,s},\nu_{\lambda,s})$ with $s=s_1+is_2$. □

Corollary 6.3. *A quadratic étale F-algebra $F[\sqrt{d}]$ can be embedded in a C_4-Galois algebra (Q,ν) as $F[\sqrt{d}]\simeq Q^{\nu^2}$ if and only if d is a sum of two squares in F.*

Proof. The "only if" part was shown in the last lines of the proof of Proposition 6.2. (Alternately, it follows from Propositions 5.10 and 5.11.) The "if" part follows from the observation that $F[\sqrt{d}] \simeq Q_{\lambda,s}^{\nu_{\lambda,s}^2}$ whenever $N_{S/F}(s) = d$. □

In other words, this corollary shows that the exact sequence (30) can be extended to

$$1 \to \mathrm{Quad}(F) \xrightarrow{\iota^1} \mathrm{Cycl}_4(F) \xrightarrow{\rho^1} \mathrm{Quad}(F) \xrightarrow{\delta} \mathrm{Br}(F),$$

where $\mathrm{Br}(F)$ is the Brauer group of F and δ maps $K = F[\sqrt{d}]$ to the Brauer class of the quaternion algebra $(-1, d)_F$. Of course, this result is well-known and has an easy cohomological proof.

6.2. **Characteristic 2.** Cyclic Galois C_{p^n}-algebras over fields over characteristic p were constructed by Witt [14, Satz 13], using Witt vectors. The group $H^1(F, C_{p^n})$ over a field of characteristic p was computed by Serre in [9, Chap. X, §3], also in terms of Witt vectors. We recall explicitly the results of Serre and Witt for the group C_4 over a field F of characteristic 2.

Let $W_2(F)$ be the additive group of Witt vectors of length 2. By definition we have $W_2(F) = \{(t, s) \mid t, s \in F\}$ with the addition

$$(t_1, s_1) \dotplus (t_2, s_2) = (t_1 + t_2, s_1 + s_2 + t_1 t_2).$$

Alternately,

$$W_2(F) = \left\{ \begin{pmatrix} 1 & t & s \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix} \middle| \, s, t \in F \right\} \subset \mathrm{GL}_2(F).$$

The neutral element is $(0, 0)$ and $\dot{-}(t, s) = (t, s + t^2)$. The map

$$\wp_2 \colon W_2(F) \to W_2(F), \; (t, s) \mapsto (t^2, s^2) \;\dot{-}\; (t, s) = (t^2 + t, s^2 + s + t^2 + t^3)$$

is a group homomorphism and there is an exact sequence of Γ-modules:

$$0 \to C_4 \to W_2(F_s) \xrightarrow{\wp_2} W_2(F_s) \to 0, \tag{32}$$

where C_4 is identified with the subgroup of $W_2(F_s)$ generated by $(1, 0)$.

Proposition 6.4. *$H^1\big(\Gamma, W_2(F_s)\big) = 0$ and $H^1(\Gamma, C_4) \simeq W_2(F)/\wp_2\big(W_2(F)\big)$.*

Proof. The first claim follows from the exact sequence of (additive) Γ-modules:

$$0 \to F_s \xrightarrow{\iota} W_2(F_s) \xrightarrow{\pi} F_s \to 0$$

where $\iota(s) = (0, s)$ and $\pi(t, s) = t$, and the fact that $H^1(\Gamma, F_s) = 0$ (by the additive version of Hilbert's Theorem 90). The last claim follows from the exactness of (32) and from the first claim. □

For $(t, s) \in W_2(F)$, let $I_{(t,s)} \subset F[W, X]$ be the ideal generated by the polynomials $f_1(W)$, $f_2(W, X)$ such that

$$\big(f_1(W), f_2(W, X)\big) = \wp_2(W, X) \;\dot{-}\; (t, s),$$

and let

$$Q_{(t,s)} = F[W, X]/I_{(t,s)}.$$

Letting ω, ξ be the images of W, X in $Q_{(t,s)}$, the relations defining $Q_{(t,s)}$ can be rewritten as

$$\omega^2 + \omega = t, \qquad \xi^2 + \xi = t\omega + s.$$

It is therefore clear that $Q_{(t,s)}$ is a quartic 2-algebra over F. The automorphism of $F[W,X]$ given by

$$(W,X) \mapsto (W,X) \dotplus (1,0)$$

induces an automorphism $\nu_{(t,s)}$ of $Q_{(t,s)}$; we have by definition $\nu_{(t,s)}(\omega) = \omega + 1$ and $\nu_{(t,s)}(\xi) = \xi + \omega$, hence the fixed subalgebra of $Q_{(t,s)}$ is F. Thus, $(Q_{(t,s)}, \nu_{(t,s)})$ is a C_4-Galois F-algebra.

Proposition 6.5. *The map* $(t,s) \mapsto (Q_{(t,s)}, \nu_{(t,s)})$ *induces a group isomorphism*

$$\Psi\colon W_2(F)/\wp_2\bigl(W_2(F)\bigr) \xrightarrow{\sim} \mathrm{Cycl}_4(F).$$

Proof. Let (t,s), $(t',s') \in W_2(F)$, and let ω, $\xi \in Q_{(s,t)}$ and ω', $\xi' \in Q_{(s',t')}$ be the elements defined as above. In $Q_{(t,s)} \otimes Q_{(t',s')}$, consider the elements

$$\omega_\star = \omega \otimes 1 + 1 \otimes \omega', \qquad \xi_\star = \xi \otimes 1 + 1 \otimes \xi' + \omega \otimes \omega'.$$

Computation shows that $\omega_\star$ and $\xi_\star$ are invariant under $\nu_{(t,s)}^{-1} \otimes \nu_{(t',s')}$ and satisfy

$$\omega_\star^2 + \omega_\star = t + t', \qquad \xi_\star^2 + \xi_\star = (t+t')\omega_\star + s + s' + tt'.$$

Moreover, $(\nu_{(t,s)} \otimes \mathrm{Id})(\omega_\star) = \omega_\star + 1$ and $(\nu_{(t,s)} \otimes \mathrm{Id})(\xi_\star) = \xi_\star + \omega_\star$. Therefore,

$$(Q_{(t,s)}, \nu_{(t,s)}) \star (Q_{(t',s')}, \nu_{(t',s')}) \simeq (Q_{(t,s) \dotplus (t',s')}, \nu_{(t,s) \dotplus (t',s')}).$$

If $(t,s) = \wp_2(x,y) = (x^2 + x, y^2 + y + x^3 + x^2)$ for some x, $y \in F$, then the map $F[W,X] \to F$ defined by

$$W \mapsto (x, x+1, x, x+1), \qquad X \mapsto (y, x+y, y+1, x+y+1)$$

induces an isomorphism $(Q_{(t,s)}, \nu_{(t,s)}) \xrightarrow{\sim} (F^4, \sigma)$ where σ is the cyclic permutation of factors.

Conversely, if $Q_{(t,s)} \simeq F^4$ for some t, $s \in F$, then letting $(\omega_i)_{1 \le i \le 4}$ and $(\xi_i)_{1 \le i \le 4}$ denote the images of ω and ξ in F^4, it is readily verified that

$$t = \omega_1^2 + \omega_1 \qquad \text{and} \qquad s = \xi_1^2 + \xi_1 + \omega_1^3 + \omega_1^2,$$

hence $(t,s) = \wp_2(\omega_1, \xi_1)$. This shows that the map Ψ is an injective homomorphism of groups, and it only remains to prove its surjectivity.

Let (Q,ν) be a C_4-Galois algebra. If $Q \simeq F[\wp^{-1}(u)] \times F[\wp^{-1}(u)]$ for some $u \in F$, then $(Q,\nu) \simeq (Q_{(0,u)}, \nu_{(0,u)})$. For the rest of the proof, we may thus assume Q is a field. Let $K = Q^{\nu^2} \subset Q$ be the subfield fixed under ν^2 and let $Q = K(\xi)$ with $\xi^2 + \xi \in K$. Then $\nu^2(\xi) = \xi + 1$, and it follows that the element $\omega = \xi + \nu(\xi)$ satisfies

$$\nu^2(\omega), \qquad \nu(\omega) = \omega + 1,$$

hence $K = F(\omega)$. We then have $\xi^2 + \xi = t\omega + s$ for some t, $s \in F$, and

$$\omega^2 + \omega = (\xi^2 + \xi) + \nu(\xi^2 + \xi) = t.$$

Therefore, $(Q,\nu) \simeq (Q_{(t,s)}, \nu_{(t,s)})$. $\square$

Corollary 6.6. *Every quadratic étale* F*-algebra can be embedded in a* C_4*-Galois* F*-algebra* (Q,ν) *as* $Q^{\nu^2} \simeq \Delta(Q)$.

Proof. For any $t \in F$, we have $F[\wp^{-1}(t)] \simeq Q_{(t,s)}^{\nu_{(t,s)}^2}$ for all $s \in F$. $\square$

The corollary shows that the last map in the exact sequence (30) is onto when $\mathrm{char}\, F = 2$. This is clear from a cohomological viewpoint, since the cohomological 2-dimension of Γ is at most 1, see [11, p. 86].

References

[1] B.N. Allison. Construction of 3×3-matrix algebras and some Lie algebras of type D_4. *J. Algebra.* 143:63–92, 1991.

[2] M. Ferrero, A Paques, and A. Solecki. On cyclic quartic extensions with normal basis. *Bull. Sci. Math.*, 116:487–500, 1992.

[3] M.-A. Knus, A.S. Merkurjev, M. Rost, J.-P. Tignol, *The Book of Involutions*, Amer. Math. Soc. Coll. Pub. 44, AMS, Providence, RI, 1998.

[4] J.-L. Lagrange, *Œuvres, tome 3.* (Publiées par J.-A. Serret), Gauthier-Villars, Paris, 1869.

[5] T. Y. Lam, D. B. Leep, and J.-P. Tignol. Biquaternion algebras and quartic extensions *Inst. Hautes Études Sci. Publ. Math.*, 77:63–102, 1993.

[6] S. Mac Lane, *Categories for the Working Mathematician*, 2d edition, Graduate Texts Math. 5, Springer-Verlag, New York Berlin Heidelberg, 1998.

[7] D.J. Saltman. Exterior powers of fields and subfields. *Nagoya Math. J.*, 89:119–127, 1983.

[8] D.J. Saltman. *Lectures on Division Algebras.* CBMS Regional Conference Series in Math. **94**, Amer. Math. Soc., Providence, RI, 1999.

[9] J.-P. Serre. *Corps Locaux*, Deuxième édition, *Publications de l'Université de Nancago*, No VIII. Hermann, Paris, 1968.

[10] J.-P. Serre. Corps quartiques associés à un corps cubique donné (Compléments au cours du 29/10/1984, Janvier 1985).

[11] J.-P. Serre. *Cohomologie galoisienne*, Cinquième édition, révisée et complétée, Lecture Notes in Math. **5**, Springer-Verlag Berline-Heidelberg-New York, 1994.

[12] B.L. van der Waerden, *Algebra I*, Grundlehren der Math. Wiss. 33, Springer-Verlag, Berlin, 1930.

[13] A. Weil. Exercices dyadiques. *Invent. Math.*, 27:1–22, 1974.

[14] E. Witt. Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. *J. reine angew. Math.*, 176: 126–140, 1937.

Departement 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: tignol@math.ucl.ac.be