



Deposited via The University of Sheffield.

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/id/eprint/241001/>

Version: Published Version

Article:

Szymik, M. (2026) Artin–Schreier quandles of involutions in absolute Galois groups.
Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg. ISSN: 0025-5858

<https://doi.org/10.1007/s12188-026-00297-z>

Reuse

This article is distributed under the terms of the Creative Commons Attribution (CC BY) licence. This licence allows you to distribute, remix, tweak, and build upon the work, even commercially, as long as you credit the authors for the original work. More information and the full terms of the licence here:

<https://creativecommons.org/licenses/>

Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.



Artin–Schreier quandles of involutions in absolute Galois groups

Markus Szymik^{1,2}

Received: 20 May 2024
© The Author(s) 2026

Abstract

We introduce a new invariant of fields that refines their real spectrum and is related to their absolute Galois group: the Artin–Schreier quandle. For totally real number fields, it is freely generated—in the variety of profinite involutory quandles—by a Cantor space of indeterminates. For Laurent series fields, we compute it in terms of the Artin–Schreier quandle of the coefficient field. This result, along with other examples, shows that, in general, there are relations.

Keywords Absolute Galois groups · Arithmetic topology · Artin–Schreier theory · Involutions · Quandles · Real spectra

1 Introduction

The real spectrum of a commutative ring is a topological space that enriches its Zariski spectrum by incorporating ideas from the theory of formally real fields. For a field, which has only one prime ideal, the Zariski spectrum is merely a singleton, whereas the real spectrum comprises the space of orderings of the field. From a group-theoretic perspective, we know that we can identify the real spectrum of a field with the space of conjugacy classes of involutions in the absolute Galois group (see Sect. 3 for a review). This observation allows us, in this paper, to further refine the real spectrum of a field F . Instead of working with equivalence classes in the form of conjugacy classes of involutions, we define the Artin–Schreier quandle $AS(F)$ directly, based on the set of all involutions within the absolute Galois group $\text{Gal}(F) = \text{Gal}(\overline{F}|F)$. A novel observation is that this set not only possesses

Communicated by Ingo Runkel.

✉ Markus Szymik
m.szymik@sheffield.ac.uk; markus.szymik@rub.de

¹ School of Mathematical and Physical Sciences, University of Sheffield, Hicks Building, Hounsfield Road, Sheffield S3 7RH, UK

² Fakultät für Mathematik, Ruhr-Universität Bochum, Universitätsstraße 150, 44801 Bochum, Germany

a topological structure as a subspace of a profinite group but also an algebraic one: Although it is not a subgroup, it is still closed under conjugation. The algebraic theory of quandles is a well-established axiomatic framework for modelling conjugation, and $\text{AS}(F)$, therefore, inherits the structure of an involutory quandle (see Sect. 2 for a review). One of our main results characterises the profinite involutory quandle $\text{AS}(F)$ in the most fundamental cases:

Theorem 1.1 *The Artin–Schreier quandle $\text{AS}(\mathbb{Q})$ of the rational number field $\mathbb{Q}$ is a free profinite involutory quandle. A Cantor space of involutions inside the absolute Galois group $\text{Gal}(\mathbb{Q})$ gives a basis. A similar statement holds for all totally real number fields.*

We prove this result as Theorems 4.1 and 4.4 in the text. Totally imaginary number fields have no involutions in their absolute Galois groups, and their Artin–Schreier quandles are empty.

For more context, recall that Hilbert’s 17th problem asked if we could write a real multivariate polynomial that only assumes non-negative values as a sum of squares of rational functions. This problem was solved affirmatively in 1927 by Artin [2] who, in collaboration with Schreier [1, 3, 4], founded the subject of real algebra. In 1979, Coste and Roy introduced the real spectrum of a commutative ring [13]. It plays the same role in real algebraic geometry as the ordinary prime spectrum in the usual algebraic geometry. For a field F , the real spectrum has various, seemingly different descriptions: If F is a number field, we can identify it with the (finite) set of embeddings of F into the field $\mathbb{R}$ of real numbers. In general, referring again to the review in Sect. 3 for more detail, it is better to think of it as the set of orderings of F , as the set of ring morphisms $W(F) \rightarrow \mathbb{Z}$, where $W(F)$ is the Witt ring of quadratic forms over F , or—for us—as the set of conjugacy classes of involutions in the absolute Galois group $\text{Gal}(F)$. The Artin–Schreier quandle replaces the set of conjugacy classes with the collection of all their representatives and non-judgementally embraces the algebraic structure that comes with it.

The thrust of this idea extends beyond real algebra to the many other contexts of conjugation in algebraic number theory, and it opens new avenues in the flourishing ‘arithmetic topology’ program initiated by Manin, Mazur, Mumford, and others. The connection to topology comes via an algebraic structure that codifies conjugation: quandles. We refer to Sect. 2 again for a review of the basic definition, but we point out here that we can think of quandles as generalisations of knots: first considered by Burde [12] in that context, Joyce [30] and Matveev [42], building on earlier work of Waldhausen, showed that knot quandles, a canonical refinement of knot groups, completely classify knots. The knot quandle of a prime knot is the conjugacy class of the meridian with the quandle structure given by conjugation. (For composite knots, the description is more subtle and not relevant here.) Meridians are generators of the fundamental groups of ‘small’ disks that are transversal to the knot and have been punctured by removing the intersection with the knot. Given the importance of meridians for understanding knot groups and quandles, we are urged to understand the function fields $F((t))$ of punctured formal disks. The following result is Theorem 5.1 in the main text.

Theorem 1.2 *For any field F , there is an isomorphism*

$$\text{AS}(F((t))) \cong \text{AS}(F) \times \text{FQ}_2^{\wedge} \{\sigma, \tau\} \cong \text{AS}(F) \times \widehat{\mathbb{Z}}$$

of profinite involutory quandles, where $\mathrm{FQ}_2^\wedge\{\sigma, \tau\}$ is the free profinite involutory quandle on a set $\{\sigma, \tau\}$ with two elements, and which, as a profinite space, is homeomorphic to $\widehat{\mathbb{Z}}$. The quandle structure is given by $a \triangleright b = 2a - b$ for $a, b \in \widehat{\mathbb{Z}}$.

We note that Takahashi [57] (see also Davis–Schlank [14]) has associated quandles with Galois covers of arithmetic schemes in a different way than here. We refer to Shusterman [53] for another framework that uses quandles and the more general racks in number theory.

This paper is written to be broadly accessible to number theorists and topologists. We discuss involutions and involutory quandles in Sect. 2, with the second half of that section describing the free models and covering the topological details needed for the profinite context. We specialise this general theory to Artin–Schreier quandles in Sect. 3. We describe the Artin–Schreier quandles of number fields and other global fields in Sect. 4. The final Sect. 5 contains Theorem 5.1 and discusses examples of Artin–Schreier quandles that have relations.

2 Involutions and quandles

We start with some necessary recollections and extensions to the profinite setting of the main algebraic structure that we are interested in: quandles, which describe symmetries in a way different from, but of course related to, groups. Suitable references are [10, 17, 30, 42]. The terminology and notation vary considerably among the various sources, and we shall stick to the following throughout:

Definition 2.1 Consider a pair $(R, \triangleright)$ consisting of a set R together with a binary operation $\triangleright$, a *magma*. A morphism of magmas is a map that is compatible with the operations $\triangleright$, and an automorphism is, of course, a bijective morphism. A *rack* is a magma such that, for all x in R , the left-multiplication $\lambda_x : y \mapsto x \triangleright y$ is an automorphism of the underlying magma. The corresponding equation says

$$x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z) \quad (2.1)$$

for all x, y , and z in R . A *profinite rack* is a profinite space R together with a rack structure $\triangleright : R \times R \rightarrow R$ that is continuous.

Recall that a profinite space is a totally disconnected compact Hausdorff space, where a compact Hausdorff space is totally disconnected if we can separate any two points by subsets that are both open and closed at the same time.

Remark 2.2 The choice of definition of a profinite rack here is more debatable than in the case of profinite groups. Rubinsztein [52, Def. 2.1], for instance, defined topological racks as racks R together with a rack structure $\triangleright : R \times R \rightarrow R$ that is continuous and such that all left-multiplication $\lambda_x : R \rightarrow R$ are homeomorphisms. Of course, for a compact Hausdorff space, such as a profinite space, continuous bijections are homeomorphisms, so this requirement is automatic. In fact, more is true. As the rack structure $\triangleright$ is continuous if and only its adjoint $R \rightarrow \mathrm{Top}(R)$ to the topological group $\mathrm{Top}(R)$ of self-homeomorphisms is continuous (see [36, Thm. 5.1.8] for instance) we can use the continuity of the inversion in the topological group $\mathrm{Top}(R)$, if R is compact Hausdorff, to deduce the continuity of the

inverted operation $\triangleright^{-1} : R \times R \rightarrow R$ given by $x \triangleright^{-1} y = \lambda_x^{-1}(y)$. This recovers that our profinite racks satisfy Takahashi's more restrictive definition [57, Def. 2.7] of a topological rack. Singh [54, Def. 3.6] defines profinite racks as inverse limits of finite racks, and these examples are profinite racks in our sense. Overall, we find the definition chosen above to be just right for the context of the present paper.

Remark 2.3 By definition, racks bring their own automorphisms, namely the left-multiplications, one for each element x . Still, there is also a *natural* automorphism, namely $x \mapsto x \triangleright x$, which is compatible with all rack morphisms and which generates all natural automorphisms [55, Thm. 5.4], and which does not necessarily have the form of a left-multiplication.

Definition 2.4 If all natural automorphisms of a rack are the identity, then the rack is called a *quandle*. In symbols, this property means

$$x \triangleright x = x \quad (2.2)$$

for all elements x . A *profinite quandle* is a profinite rack that is a quandle.

Examples 2.5 The underlying set of any group forms a quandle under conjugation, i.e., if we define $g \triangleright x = gxg^{-1}$. Any profinite group gives rise to a profinite quandle in this way.

Definition 2.6 A rack is called *involutory* if all left-multiplications have order at most two. It is equivalent to asking that the equation

$$x \triangleright (x \triangleright y) = y \quad (2.3)$$

holds for all x and y .

Remark 2.7 An involutory quandle is sometimes called a *kei*, following Takasaki [58]. The term *Takasaki quandle* is sometimes used in his honour. Our present terminology follows Joyce [30]. Fenn and Rourke [17, Sec. 1.3] call such structures *involutive*, but according to Brieskorn [10, Sec. 2], this term refers to a completely different property that we will not need here. We refer to [30, Sec. 10f.] for more information on involutory quandles.

Remark 2.8 If G is a group, the formula $g \triangleright x = gx^{-1}g$ defines a binary operation that turns the whole underlying set of G into an involutory quandle. This class of examples seems to originate in Loos' work [39] on the structure of symmetric spaces. As a particular case, if G is the Euclidean plane, with the group structure given by addition, then we have $g \triangleright x = 2g - x$, so that left-multiplication is reflection in the point g . Figure 1 illustrates the rack axiom. This particular rack is an involutory quandle. Bachmann [5, 6], building on earlier work of Hjelmslev, has used groups generated by involutions as a foundation for geometry in a way that is distinctly different from Coxeter's better-known work on reflection groups.

Examples 2.9 For any group G , the subset

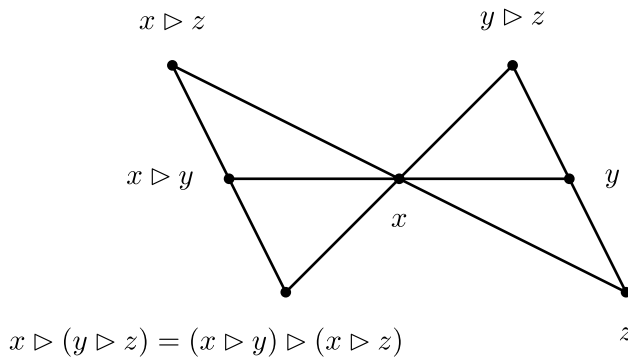


Fig. 1 The rack axiom (2.1) for symmetric spaces

$$\text{Inv}(G) = \{s \in G \mid s^2 = e \neq s\} \quad (2.4)$$

of *involutions* in G forms an involutory quandle with respect to conjugation. We emphasise that this convention excludes the identity from being an involution. If G is profinite, and $\text{Inv}(G)$ is a closed subset, then $\text{Inv}(G)$ will also be profinite. We shall see below, in Lemma 3.7, that this is always the case in the situations we are interested in.

To understand an algebraic structure, it is vital to understand its free models. In fact, any algebraic theory is determined by its free models (see Lawvere [38]), but we will not use the language of algebraic theories here except for in Remark 2.14 further down. However, we do need to discuss the free models in the relevant examples. For the theory of groups, for instance, we have the free groups $F(S)$ generated by sets S , and if S has n elements, then the elements of $F(S)$ are in bijection with the natural operations on groups of arity n . Specifically, if $S = \{x, y\}$, then the multiplication corresponds to the element $xy \in F\{x, y\}$, whereas $xyx^{-1} \in F\{x, y\}$ gives conjugation. For the theory of quandles, we can describe the free models as follows.

Proposition 2.10 *The free quandle $\text{FQ}(S)$ on a set S is the union of the conjugacy classes of the basis elements $S \subseteq F(S)$ inside the free group $F(S)$; the operation $\triangleright$ is given by conjugation.*

We refer to [30, Thm. 4.1] and [34, Satz 2.5] for proofs.

We can also describe free involutory quandles explicitly in a similar manner. We will have to replace the free groups $F(S)$, which we can think of as the universal Artin groups, with the universal Coxeter groups. Recall that an Artin group can be presented in the form $\langle S | R \rangle$, where S is a set of generators, and R is a set of relations of the form $sts\dots = tst\dots$ for $s \neq t$ in S . The *universal* Artin group corresponds to the case $R = \emptyset$, i.e., just the free group generated by the set S . Coxeter groups have the additional relations $s^2 = e$ for all generators s in S , so that the *universal* Coxeter group [45] on a set S of generators is the quotient

$$F_2(S) = \langle s \in S \mid s^2 = e \text{ for all } s \in S \rangle$$

of the free group $F(S)$ by the relations that say that the generating elements in S are involutions. When the set S has n elements, then the group $F_2(S) \cong (\mathbb{Z}/2)^{*n}$ is the coproduct of n copies of the group of order 2.

Proposition 2.11 *The free involutory quandle $\mathrm{FQ}_2(S)$ on a set S is the union of the conjugacy classes of the basis elements $S \subseteq F_2(S)$ inside the universal Coxeter group $F_2(S)$.*

We refer to [30, Cor. 10.3] and [34, Satz 2.5] once more.

Remark 2.12 We remark that the group $F_2(S)$ is not defined by universal identities or laws; the equation $s^2 = e$ is required for the generators s only. It does not necessarily hold for every group element. If we require $g^2 = e$ for all elements g in a group G , the group G must be abelian. In fact, this law defines the variety of elementary abelian 2-groups, and $F_2(S)$ is not abelian unless S has at most one element. So, while the functor F_2 from the category of sets to the category of groups is a left-adjoint, it is not left-adjoint to the canonical forgetful functor. In contrast, the involutory quandle $\mathrm{FQ}_2(S)$ is characterised as a left-adjoint to the forgetful functor from the category of involutory quandles; it is a free object among involutory quandles.

Proposition 2.13 *We have $\mathrm{FQ}_2(S) = \{g \in F_2(S) \mid g^2 = e \neq g\}$.*

Proof Clearly, every conjugate of a generator $s \in S$ in $F_2(S)$ is an involution. The converse also holds: Every involution is conjugate to a generator. This is elementary to verify, and it is also a consequence of the Kurosh subgroup theorem; see [41, Cor. 4.1.4], for instance. $\square$

Remark 2.14 We can rephrase the observation leading to Proposition 2.13 in more conceptual terms as follows. In any category with finite sums, we can take the full subcategory whose objects are the finite sums of any chosen object Z , and this will be an algebraic theory in the sense of Lawvere [38]. For instance, if we consider the category of models for an algebraic theory and choose for Z a free model on one generator, we recover that algebraic theory in this way. In particular, for the group $Z = \mathbb{Z}$, the free groups recover the algebraic theory of groups. More generally, we now see that any group Z defines an algebraic theory such that the sets $\mathrm{Mor}(Z, G)$ of group morphisms from Z into groups G are models for that theory. For the case $Z = \mathbb{Z}/2$ of interest to us here, we see that the sets $\mathrm{Mor}(\mathbb{Z}/2, G) \cong \mathrm{Inv}(G) \cup \{e\}$ support models for an algebraic theory: the theory of involutory quandles with unit, where a unit u is an element that is both fixed and fixing: $x \triangleright u = u$ and $u \triangleright y = y$ for all x, y (see [37, Def. 2.8] for this terminology). In fact, the theory defined by $Z = \mathbb{Z}/2$ is the theory of involutory quandles with unit. This insight goes back to Bergman (see his ICM talk [7] for general statements and his textbook [8, Sec. 10.11] for details).

For the Galois theory context, we also need the profinite versions $F^\wedge(S)$ and $F_2^\wedge(S)$ of the groups $F(S)$ and $F_2(S)$, respectively, where S can now be any profinite space. If the space S is finite, we can build the profinite groups $F^\wedge(S)$ as the profinite completions of the free groups $F(S)$, namely the limit $\lim_N F(S)/N$, where N ranges over the finite index normal subgroups of $F(S)$. If S is, more generally, profinite, we have two choices:

On the one hand, we can set $F^\wedge(S) = \lim_N F(S)/N$ as before, but require that $gN \cap S$ is open in S for the (finitely many) cosets gN of N in $F(S)$. On the other hand, we can set $F^\wedge(S) = \lim_R F^\wedge(S/R)$, where R ranges over the equivalence relations on S that have a finite discrete quotient. Both constructions give isomorphic results [24, Prop. 1.7]. This and other suitable references come from Gildenhuys et al. [24, 25], which build on earlier work of Neukirch et al. [9, 46, 47], Mac Lane [40], and the writings of Haran and Jarden [26, 27]. The last two are especially relevant because of the next result, Proposition 2.15, which they provide. They concern the groups $F_2^\wedge(S)$ that are characterised by the property that a continuous homomorphism $F_2^\wedge(S) \rightarrow G$ into a profinite group G is the same thing as a continuous map $S \rightarrow G$ such that the elements in the image square to the identity element e . To construct them, we can follow [27, §1 and Prop. 3.1] and use $F_2^\wedge(S) = \lim_N F(S)/N$ with the added requirement that N contains all squares of elements in S or work with $F_2^\wedge(S) = \lim_R F_2^\wedge(S/R)$. There are profinite versions of the Kurosh subgroup theorem:

Proposition 2.15 *Every involution in $F_2^\wedge(S)$ is conjugate to a unique element in S , and the centraliser of any involution consists of only that involution and the identity.*

Proof If S is a finite set of n elements, Haran–Jarden [26, Prop. 6.1] show that there are exactly n conjugacy classes of involutions in $F_2^\wedge(S)$, represented by the elements in S . In [27, Cor. 3.2], they extend this to the general case. $\square$

Proposition 2.16 *For every profinite space S , there is a profinite involutory quandle $\text{FQ}_2^\wedge(S)$ together with a continuous map $S \rightarrow \text{FQ}_2^\wedge(S)$ that satisfies the universal property: Restriction gives a bijection between the set of continuous homomorphism $\text{FQ}_2^\wedge(S) \rightarrow Q$ into a profinite involutory quandle Q and the set of continuous maps $S \rightarrow Q$. Furthermore, there is a continuous map $\text{FQ}_2^\wedge(S) \rightarrow S$ that identifies the target S with the orbit space of the $F_2^\wedge(S)$ –action on $\text{FQ}_2^\wedge(S)$ via conjugation.*

Proof Let us set

$$\text{FQ}_2^\wedge(S) = \text{Inv}(F_2^\wedge(S)). \quad (2.5)$$

This is a profinite quandle: the involutions form a closed subset of the topological space $F_2^\wedge(S)$ as they are the image of the continuous map $F_2^\wedge(S) \times S \rightarrow F_2^\wedge(S)$ that sends (g, s) to $gs g^{-1}$. The involutory quandle $\text{FQ}_2^\wedge(S)$ comes with a natural continuous map from S because the image of the canonical map $S \rightarrow F_2^\wedge(S)$ lies inside $\text{FQ}_2^\wedge(S)$. So, any continuous morphism $\text{FQ}_2^\wedge(S) \rightarrow Q$ from $\text{FQ}_2^\wedge(S)$ into a profinite involutory quandle Q restricts to a continuous map $S \rightarrow Q$.

Conversely, if $\varphi : S \rightarrow Q$ is any continuous map, we can extend it functorially to a continuous morphism $F_2^\wedge(\varphi) : F_2^\wedge(S) \rightarrow F_2^\wedge(Q)$ of groups, and this restricts to a continuous morphism $\text{FQ}_2^\wedge(\varphi) : \text{FQ}_2^\wedge(S) \rightarrow \text{FQ}_2^\wedge(Q)$ of involutory quandles. We get a continuous morphism $\text{FQ}_2^\wedge(S) \rightarrow Q$ by composition of this morphism $\text{FQ}_2^\wedge(\varphi)$ with the continuous orbit map $\text{FQ}_2^\wedge(Q) \rightarrow Q$, where Q is identified with the space of orbits in the subspace $\text{FQ}_2^\wedge(Q) = \text{Inv}(F_2^\wedge(Q))$ for the continuous action of the group $F_2^\wedge(Q)$ on itself via conjugation. The preceding two constructions are inverse to each other.

The final statement is immediate from what we have already used in the previous paragraph of the proof: The composition $S \longrightarrow \mathrm{FQ}_2^\wedge(S) \longrightarrow \mathrm{FQ}_2^\wedge(S)/\mathrm{F}_2^\wedge(S)$ is a homeomorphism, and we can use its inverse to obtain the desired map. $\square$

Remark 2.17 We remark that any free quandle generates a free group: Ignoring topologies for a moment, the *enveloping group* $\mathrm{Gr}(Q)$ of a quandle Q is, by definition, the value of the left-adjoint Gr to the forgetful functor from the category of groups to the category of quandles. To construct it, up to isomorphism, we can start with the free group $F(Q)$ on the set Q , with $f(q)$ the basis element corresponding to an element $q \in Q$, and pass to the quotient by the relations

$$f(x \triangleright y) = f(x)f(y)f(x)^{-1}. \quad (2.6)$$

As a left adjoint, the functor Gr preserves colimits, and this shows that we have an isomorphism $\mathrm{Gr}(FQ(S)) \cong F(S)$. The construction can be adapted to profinite quandles Q . Ignoring the quandle structure on Q for a moment, the profinite space Q freely generates the profinite group $F^\wedge(Q)$, and $\mathrm{Gr}^\wedge(Q)$ is the quotient of it by the closed normal subgroup generated by the relations (2.6). Similarly, the enveloping group of the quandle $\mathrm{FQ}_2^\wedge(S)$ is canonically isomorphic to the group $F_2^\wedge(S)$ for formal reasons; both sides satisfy the same universal property. All that is to point out that, in contrast, the proof of Theorem 4.1 will go the other way. We will argue for the freeness of a quandle from the freeness of its enveloping group, and such an implication is not just a categorical formality. Any argument to deduce the freeness of a quandle Q from the freeness of its enveloping group has to be non-formal.

Remark 2.18 We shall also use the fact that the map $\mathrm{FQ}_2^\wedge(S) \rightarrow F_2^\wedge(S)$ is injective. This is not automatic, either. There are quandles Q for which the canonical map from Q into the enveloping group is not injective. For example, if $Q = \{x, y, z\}$ is the involutory quandle with λ_x transposing y and z , and $\lambda_y = \lambda_z = \mathrm{id}_Q$, then $y \triangleright x = x$ implies that x commutes with y in the enveloping group, and $x \triangleright y = z$ implies that x conjugates y into z in the enveloping group. Therefore, the elements y and z must become equal in the enveloping group.

3 Artin–Schreier quandles

With this section, we turn our attention to fields. We start by establishing notation and context. Suitable references for this material are Lam [35] and Knebusch–Scheiderer [33].

We recall that an *ordering* of a field F is given by a subset $P \subset F$ of elements that is closed under addition and multiplication and satisfies $P \cap -P = \{0\}$ and $P \cup -P = F$, where $-P = \{a \in F \mid -a \in P\}$. It follows that all sums of squares are in P . A field is *formally real* if and only if we can order it. A *Euclidean field* is a field for which the set of squares is an ordering. In a Euclidean field, the ordering is necessarily unique. A field is *real closed* if, in addition, each polynomial of odd degree with coefficients in F has at least one root in F .

The *real spectrum* of a field F is the set $\mathrm{Ord}(F)$ of orderings of F equipped with the *Harrison topology*: given any element $a \neq 0$ in F , the set of orderings for which a is positive is a generating open set. With this topology, the real spectrum is a profinite space.

The *Grothendieck–Witt ring* $\mathrm{GW}(F)$ of a field F (of characteristic not 2) is the group completion of the semi-ring of non-degenerate quadratic forms. The dimension gives a well-defined homomorphism $\mathrm{GW}(F) \rightarrow \mathbb{Z}$. The *Witt ring* $W(F)$ is the quotient of the Grothendieck–Witt ring $\mathrm{GW}(F)$ by the ideal generated by the hyperbolic plane. The parity of the dimension gives a well-defined homomorphism $W(F) \rightarrow \mathbb{Z}/2$.

Proposition 3.1 *The real spectrum of a field F is in natural bijection with the set of ring morphisms $W(F) \rightarrow \mathbb{Z}$ from the Witt ring of F to the ring of integers.*

Sketch of proof Given any ordering P of F , the associated morphism sends a quadratic form to its P -signature—the difference of the numbers of positive and negative diagonal entries, where the meaning of ‘positive’ and ‘negative’ is determined by the ordering P . Another way to think about this: an ordering determines an embedding into a real closed field so that we can use functoriality and the fact that the Witt ring of a real closed field is canonically isomorphic to $\mathbb{Z}$ through the signature. We refer to [33, Thm. I.2.3] for more detail. $\square$

Remark 3.2 The kernel I of the parity homomorphism $W(F) \rightarrow \mathbb{Z}/2$ defines the I -adic filtration on the Witt ring $W(F)$, and the associated graded ring is then $\mathrm{gr} W(F) = W(F)/I \oplus I/I^2 \oplus I^2/I^3 \oplus \dots$. It is a fact that $\mathrm{gr} W(F)$ is a graded commutative algebra over $\mathbb{F}_2$, and it is isomorphic to mod 2 Milnor K-theory and mod 2 Galois cohomology via Milnor’s conjecture, which is now a theorem [48]. Therefore, we can recover $\mathrm{gr} W(F)$ from the absolute Galois group of F . Can we recover $W(F)$ itself from a refinement of the absolute Galois group? This was a non-trivial question because there are examples of fields with isomorphic $\mathrm{gr} W(F)$ ’s but non-isomorphic $W(F)$ ’s (see [49]); it has been answered in the affirmative by Mináč and Spira in [43, 44]. The authors show that the Witt ring determines and is determined (modulo a small restriction) by a specific quotient of the absolute Galois group (see [44, Thm. 3.8] in particular).

Remark 3.3 Half a century ago, Dress [15] found a relation between Witt rings and Burnside rings: If E/F is a Galois extension with Galois group G , then there is a map $A(G) \rightarrow W(F)$ from the Burnside ring $A(G)$ of the Galois group to the Witt ring of the ground field that sends G/H to (E^H, tr) , where tr is the usual trace form $(a, b) \mapsto \mathrm{tr}_{E|F}(ab)$.

Proposition 3.4 *There is an identification between the real spectrum of a field F and the set of conjugacy classes of involutions in its absolute Galois group $\mathrm{Gal}(F)$.*

Sketch of proof Given a conjugacy class $[\sigma]$ of an involution σ in $\mathrm{Gal}(F)$, we have the ordering $P[\sigma] = \{a \in F \mid \sigma(\sqrt{a}) = \sqrt{a}\}$. Note that the condition $\sigma(\sqrt{a}) = \sqrt{a}$ does not depend on the choice of the square root $\sqrt{a}$ of a . We refer to [33, Thm. I.11.3] for more detail. $\square$

We take this observation as an incentive to turn our attention towards involutions.

Let F be a field and $\mathrm{Gal}(F)$ be its absolute Galois group. From the work of Artin and Schreier cited in the introduction, see [4, Satz 4] in particular, it is known that the group $\mathrm{Gal}(F)$, even though profinite, can only have non-trivial elements of finite order if $\mathrm{char}(F) = 0$, and all of these elements necessarily have order 2, i.e., they are involu-

tions. We refer to [29] for an interesting discussion of torsion in absolute Galois groups from a different angle. The following lemma collects useful group-theoretic statements about involutions in absolute Galois groups.

Lemma 3.5 *Let F be a field and let $\sigma \in \text{Gal}(F)$ be an involution with fixed field $\text{Fix}(\sigma)$. Then $\text{Aut}(\text{Fix}(\sigma)|F) = \{\text{id}\}$. The centraliser of the involution σ within $\text{Gal}(F)$ is the subgroup $\langle \sigma \rangle$ generated by σ . The normaliser of $\text{Gal}(\text{Fix}(\sigma))$ within $\text{Gal}(F)$ is $\text{Gal}(\text{Fix}(\sigma))$ itself.*

Proof We first observe that $\text{Fix}(\sigma)$ is real closed and, therefore, has a unique ordering consisting of its squares. This means every field automorphism of $\text{Fix}(\sigma)$ preserves the ordering.

If τ is a field automorphism of $\text{Fix}(\sigma)$ that fixes F , and $a \in \text{Fix}(\sigma)$ with $\tau(a) \neq a$, we have $a < \tau(a)$, say. Then $a < \tau(a) < \tau^2(a) < \tau^3(a) < \dots$, contradicting the algebraicity of a : the τ -orbit of a must be finite. The argument for $a > \tau(a)$ is similar, and we deduce $\tau(a) = a$ for all $a \in \text{Fix}(\sigma)$. This shows $\text{Aut}(\text{Fix}(\sigma)|F) = \{\text{id}\}$.

If an element $\tau \in \text{Gal}(F)$ lies in the centraliser of σ , then τ sends $\text{Fix}(\sigma)$ into itself. From what we have shown before, it follows that τ is the identity on $\text{Fix}(\sigma)$ and lies in $\text{Gal}(\text{Fix}(\sigma)) = \langle \sigma \rangle$. The last statement is simply yet another reformulation of the preceding statement. $\square$

Later, we shall need the following stronger statement about involutions in absolute Galois groups.

Lemma 3.6 *A finite subgroup of an absolute Galois group has order at most 2.*

Proof By Artin–Schreier, we already know that every element of the finite subgroup G must have order 1 or 2. It follows from group theory that G is an elementary abelian 2-group, that is $G \cong (\mathbb{Z}/2)^n$ for some n . We show $n = 1$ by showing that $\text{Gal}(F)$ cannot contain a subgroup of the form $\mathbb{Z}/2 \times \mathbb{Z}/2$: Given an involution $\sigma \neq \text{id}$, Lemma 3.5 says that its centraliser within $\text{Gal}(F)$ is the subgroup $\langle \sigma \rangle$ generated by σ . Therefore, there can be no other element in the group $\text{Gal}(F)$ that commutes with σ . $\square$

With these preliminaries out of our way, we can now define a new invariant of fields F . Recall that we have defined, in (2.4), the subset $\text{Inv}(G)$ of involutions of a group G .

Lemma 3.7 *For any field F , the set $\text{Inv}(\text{Gal}(F))$ is a closed subspace of the absolute Galois group $\text{Gal}(F)$. Therefore, it is profinite as well.*

Proof The subset $\text{Inv}(\text{Gal}(F)) \cup \{\text{id}\}$ is closed, as this subset is defined by the equation $\sigma^2 = \text{id}$. It remains for us to show that the identity is an isolated point. To see that, we consider two cases. First, if $F(\sqrt{-1}) = F$, then $\text{Gal}(F)$ contains no involution, and we are talking about the empty set. Else, the field $F(\sqrt{-1})$ is a quadratic extension, so that $U = \text{Gal}(F(\sqrt{-1}))$ is an index 2 subgroup of $\text{Gal}(F)$, hence open and containing the identity. But $F(\sqrt{-1})$ is not formally real, so that U contains no involution. $\square$

Definition 3.8 Let F be a field. The *Artin–Schreier quandle* $\text{AS}(F)$ of F is the profinite involutory quandle

$$\text{AS}(F) = \text{Inv}(\text{Gal}(F)). \quad (3.1)$$

It consists of the set of involutions inside the absolute Galois group $\text{Gal}(F)$ of F together with the operation $\triangleright$ given by conjugation and its topology inherited from $\text{Gal}(F)$.

Remark 3.9 The Artin–Schreier quandle $\text{AS}(F)$ of a field F , just as its absolute Galois group $\text{Gal}(F)$, depends on the choice of an algebraic closure of F . If $\omega : \Omega_1 \rightarrow \Omega_2$ is an F –isomorphism of algebraic closures of F , then $\sigma \mapsto \omega\sigma\omega^{-1}$ is an isomorphism $\text{Aut}(\Omega_1|F) \rightarrow \text{Aut}(\Omega_2|F)$ and this isomorphism restricts to an isomorphism between the Artin–Schreier quandles computed using Ω_1 and Ω_2 , respectively. As usual, we will suppress the choice of an algebraic closure from the notation.

Remark 3.10 It is usually a bad idea to forget everything from a group except its conjugation. In [56], the authors argue that it is more reasonable to keep at least the group operations of arity 0 and 1 as well, which are the unit e and the power operations $g \mapsto g^n$ for all integers n . In the present situation, it is easy to recover this more refined structure from the knowledge of only the operation $\triangleright$ on $\text{AS}(F)$: By our definition of an involution, the unit $e = \text{id}$ of $\text{Gal}(F)$ is disjoint from $\text{AS}(F)$, and the power operations on the disjoint union $\text{AS}(F) \cup \{\text{id}\}$ are determined by $\sigma^n = \text{id}$ if n is even, as all elements g considered have order at most 2, and $\sigma^n = \sigma$ if n is odd, for the same reason. This suggests that we are not missing out on something obvious when considering the set $\text{AS}(F)$ together with only the conjugation $\triangleright$ on it as an algebraic invariant of F .

Before we come to examples, let us note the following algebraic result about a particular property of Artin–Schreier quandles.

Proposition 3.11 Let $\text{AS}(F)$ be the Artin–Schreier quandle of a field F . For σ and τ in $\text{AS}(F)$ we have $\sigma \triangleright \tau = \tau$ if and only if $\sigma = \tau$.

Proof The ‘if’ direction is part of the quandle axioms, which are evident by now. For the ‘only if’ direction, note that $\sigma \triangleright \tau = \tau$ is equivalent to $\sigma\tau = \tau\sigma$, so that τ must be in the centraliser of σ . It cannot be the identity, by definition of $\text{AS}(F)$, so the result follows from Lemma 3.5. $\square$

Unlike groups, which always have a neutral element, quandles can be empty. The following result characterises when this happens for Artin–Schreier quandles.

Proposition 3.12 Let F be a field. Then $\text{AS}(F)$ is non-empty if and only if F is formally real. This can only happen if $\text{char}(F) = 0$.

Proof A field F is known to be formally real if and only if its absolute Galois group $\text{Gal}(F)$ contains an involution (see [33, Kor. I.6.2], for instance). $\square$

Example 3.13 The field $\mathbb{C}$ of complex numbers is not formally real, and the Artin–Schreier quandle $\text{AS}(\mathbb{C})$ is empty. The same holds for all finite fields and the cyclotomic fields $\mathbb{Q}(\zeta_n)$ as soon as we are in the non-trivial range $n \geq 3$.

Proposition 3.12 implies that it is not interesting—for our purposes—to consider fields that are not formally real. Therefore, unless otherwise stated, we can assume we are dealing with formally real fields.

Proposition 3.14 *Let F be a field. Then $\text{AS}(F)$ is a singleton if and only if F is real closed.*

Proof We know from the work of Artin and Schreier (see again [4, Satz 4]) that a field F is real closed if and only if its absolute Galois group has order 2. $\square$

Example 3.15 The field $\mathbb{R}$ of real numbers is real closed, and the unique element in the involutory quandle $\text{AS}(\mathbb{R}) = \{\gamma\}$ is complex conjugation $\gamma : z \mapsto \bar{z}$ inside the absolute Galois group $\text{Gal}(\mathbb{R}) = \text{Aut}(\mathbb{C}|\mathbb{R}) = \{\text{id}, \gamma\}$ of order 2.

Remark 3.16 A bijection exists between the set $\text{AS}(F)$ and the set of real closed subfields containing F of the algebraic closure of F used to define the absolute Galois group. An involution σ corresponds to its fixed field $\text{Fix}(\sigma)$.

The following result shows that the examples characterised in Propositions 3.12 and 3.14 are the only ones where the Artin–Schreier quandle is finite.

Proposition 3.17 *If $\text{AS}(F)$ contains more than one element, it is infinite.*

Proof When the Artin–Schreier quandle $\text{AS}(F)$ contains more than one element, the absolute Galois group $\text{Gal}(F)$ contains two different involutions, say $\sigma \neq \tau$. Consider the morphism $F_2\{s, t\} \rightarrow \text{Gal}(F)$ of groups that sends the generator s to σ and t to τ , and suppose there was a non-trivial kernel. Recall that the group $F_2\{s, t\}$ is the infinite dihedral group, which contains an infinite cyclic subgroup generated by the product st of the generators, with inverse ts , and all other elements are alternating products $ststs\ldots$ and $tstst\ldots$ of odd length, which are conjugate to their ‘middle’ factor, either s or t . The kernel of the morphism above cannot contain s or t by definition, and it cannot contain any other involution, as these are each conjugate to either s or t inside $F_2\{s, t\}$. It follows that the kernel is a subgroup of the infinite cyclic subgroup generated by st , so that the image is a finite (dihedral) subgroup of $\text{Gal}(F)$, and it contains two different involutions $\sigma \neq \tau$. But the finite subgroups of $\text{Gal}(F)$ have order at most 2 by Lemma 3.6—a contradiction. Hence, the morphism $F_2\{s, t\} \rightarrow \text{Gal}(F)$ is injective, and $\text{Gal}(F)$ contains infinitely many involutions because this already holds for the infinite dihedral group $F_2\{s, t\}$, and these lie in $\text{AS}(F)$. $\square$

4 Number fields

The prime field $F = \mathbb{Q}$ of rational numbers is formally real but not real closed. It has a unique ordering. In other words, the real spectrum $\text{Ord}(\mathbb{Q})$ is a singleton, and all involutions in the absolute Galois group $\text{Gal}(\mathbb{Q})$ form one conjugacy class. If we choose any involution $\sigma \in \text{AS}(\mathbb{Q})$, then conjugation induces a homeomorphism $\text{Gal}(\mathbb{Q})/\langle\sigma\rangle \cong \text{AS}(\mathbb{Q})$, via $g \mapsto g\sigma g^{-1}$, where the subgroup $\langle\sigma\rangle$ is the centraliser of the involution σ (see Lemma 3.5). In particular, there are uncountably many involutions inside $\text{Gal}(\mathbb{Q})$, and the topology is reasonably well understood. In contrast, the algebraic structure of the Artin–Schreier quandle $\text{AS}(\mathbb{Q})$ supported on it is much more interesting:

Theorem 4.1 *The Artin–Schreier quandle $\text{AS}(\mathbb{Q})$ of the rational number field $\mathbb{Q}$ is a free profinite involutory quandle. A basis is given by a Cantor space of involutions inside $\text{Gal}(\mathbb{Q})$.*

This result indicates that the Artin–Schreier quandle $\text{AS}(\mathbb{Q})$ is algebraically as complicated as possible, given the constraints of being an involutory quandle. Unfortunately, the proof will not display an explicit Cantor space inside $\text{Gal}(\mathbb{Q})$ that is a basis for it. Instead, it implicitly uses Brouwer’s characterisation [11] of the Cantor space: Every profinite space that meets the minimum requirements (i.e., it has to be non-empty, second countable, and does not have an isolated point) is homeomorphic to it.

Proof of Theorem 4.1 Our goal is to show that there is a subspace $S \subseteq \text{Gal}(\mathbb{Q})$ homeomorphic to Cantor space and consisting of involutions so that the canonical extension

$$\text{FQ}_2^\wedge(S) \longrightarrow \text{AS}(\mathbb{Q}) \quad (4.1)$$

of the inclusion is an isomorphism of profinite quandles. As it is always a continuous morphism of profinite quandles, it will suffice to show that it is bijective.

The subset $\text{AS}(\mathbb{Q})$ of involutions generates a normal subgroup of $\text{Gal}(\mathbb{Q})$. Its closure N is a closed normal subgroup with fixed field an infinite Galois extension $\mathbb{Q}^{\text{tr}}$ of $\mathbb{Q}$, the field of totally real numbers, and the group N can be identified with the absolute Galois group $\text{Gal}(\mathbb{Q}^{\text{tr}})$ of $\mathbb{Q}^{\text{tr}}$. Fried–Haran–Völklein [18, 19] and (independently) Pop [50] have shown that this absolute Galois group $\text{Gal}(\mathbb{Q}^{\text{tr}})$ of the field $\mathbb{Q}^{\text{tr}}$ is isomorphic to the free profinite Coxeter group $\text{F}_2^\wedge(S)$ generated by a Cantor space S . In other words, we can choose a subspace S as above so that the canonical morphism

$$\text{F}_2^\wedge(S) \longrightarrow \text{Gal}(\mathbb{Q}^{\text{tr}}) \quad (4.2)$$

is an isomorphism of profinite groups. Restriction to the subset of involutions gives an isomorphism

$$\text{Inv}(\text{F}_2^\wedge(S)) \longrightarrow \text{Inv}(\text{Gal}(\mathbb{Q}^{\text{tr}}))$$

of profinite involutory quandles. The left hand side is $\text{FQ}_2^\wedge(S)$ by definition (2.5). The right hand side is $\text{Inv}(\text{Gal}(\mathbb{Q}))$ by our choice of $\text{Gal}(\mathbb{Q}^{\text{tr}})$ inside $\text{Gal}(\mathbb{Q})$: it contains all invo-

lutions. The result then follows from the definition $\text{AS}(\mathbb{Q}) = \text{Inv}(\text{Gal}(\mathbb{Q}))$ of the Artin–Schreier quandle. $\square$

Remark 4.2 For any field F of characteristic zero, passage to conjugacy classes gives a surjection $\text{AS}(F) \rightarrow \text{Ord}(F)$ of profinite spaces from the Artin–Schreier quandle onto the real spectrum. This surjection should *not* suggest, however, that we can compute the real spectrum $\text{Ord}(F)$ from the Artin–Schreier quandle $\text{AS}(F)$ alone. In particular, the reader may have wondered if we can recover the real spectrum of a field from its Artin–Schreier quandle as the space of orbits. To make perfect sense of this question, one would first have to exercise some care to define spaces of orbits for all profinite quandles. Any reasonable definition, however, would yield the following for Artin–Schreier quandles: the group $\text{Gal}(F)$ acts on the space $\text{AS}(F)$ via conjugation, and $\text{Orb}(\text{AS}(F))$ is the space of orbits for the restriction of this action to the closed subgroup generated by $\text{AS}(F)$. Yet, we still cannot recover the real spectrum of a field from its Artin–Schreier quandle as the space of orbits in this sense (see the following Example 4.3). Instead, we have two surjections.

$$\text{AS}(F) \longrightarrow \text{Orb}(\text{AS}(F)) \longrightarrow \text{Ord}(F), \quad (4.3)$$

and neither of them has to be injective. The Artin–Schreier quandle $\text{AS}(F)$ is contained inside $\text{Gal}(F)$, of course, and we can identify the real spectrum $\text{Ord}(F)$ with the orbits of the involutions under conjugation with $\text{Gal}(F)$. In contrast, the elements in $\text{Orb}(\text{AS}(F))$ are the orbits under conjugation with respect to the closed subgroup generated by the involutions.

Example 4.3 We give an example showing that we cannot recover the real spectrum of a field from its Artin–Schreier quandle as the set of orbits. First, note that we have an equality $\text{AS}(\mathbb{Q}(\sqrt{2})) = \text{AS}(\mathbb{Q})$ of involutory quandles: every involution in $\text{Gal}(\mathbb{Q})$ lies in the normal subgroup $\text{Gal}(\mathbb{Q}(\sqrt{2}))$ (see Theorem 4.4 below for a more general statement.) Therefore, the Artin–Schreier quandles of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}$ are free on a Cantor space, and the space of orbits is the Cantor space in both cases. However, the rational number field $\mathbb{Q}$ has a unique ordering, whereas the real quadratic extension $\mathbb{Q}(\sqrt{2})$ has two. Some involutions in $\text{Gal}(\mathbb{Q}(\sqrt{2}))$ that are not conjugate in $\text{Gal}(\mathbb{Q}(\sqrt{2}))$ become conjugate in $\text{Gal}(\mathbb{Q})$.

Let us finally look at other examples of ‘small’ fields. The other prime fields, finite fields, and all fields of positive characteristic are uninteresting to us, as their absolute Galois groups contain no involutions. We have already discussed $\mathbb{R}$ and $\mathbb{C}$, and the other local fields of characteristic 0 (i.e., the p -adic fields $\mathbb{Q}_p$ and their finite extensions) contain no involutions either: each $\mathbb{Q}_p$ contains a square root of $1 - p^n$ for sufficiently large n . This leaves us with the problem of extending Theorem 4.1 to other number fields.

We first establish some more notation. Let F be a number field. We write $d = \dim_{\mathbb{Q}}(F)$ for its degree. Then there are isomorphisms $\mathbb{C} \otimes_{\mathbb{Q}} F \cong \mathbb{C}^d$ and $\mathbb{R} \otimes_{\mathbb{Q}} F \cong \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$ with $d = r_1 + 2r_2$. The r_1 -element set $\text{Mor}(F, \mathbb{R})$ of real embeddings $F \rightarrow \mathbb{R}$, which we can identify with its real spectrum, sits inside the d -element set $\text{Mor}(F, \mathbb{C})$ of complex embeddings as the fixed points under the action of the Galois group $\text{Aut}(\mathbb{C}|\mathbb{R}) = \mathbb{Z}/2$ by complex conjugation. The orbits are the Archimedean places of F , with r_1 real ones and r_2 complex ones. The number field F is totally real when $d = r_1$ and $r_2 = 0$, and F is totally

imaginary when $r_1 = 0$ and $d = 2r_2$. If F is Galois over $\mathbb{Q}$, then it has to be either of those two, as the Galois group acts transitively on the set of Archimedean places of F , showing that they all have to be of the same type. However, there are totally real number fields that are not Galois over $\mathbb{Q}$.

Theorem 4.4 *For any totally real number field F , the Artin–Schreier quandle $\text{AS}(F)$ is a free profinite involutory quandle with a basis given by a Cantor space of involutions.*

Proof In the proof of Theorem 4.1, we have used the field $\mathbb{Q}^{\text{tr}}$ of totally real numbers. If the number field F is totally real, then it is contained in the field $\mathbb{Q}^{\text{tr}}$, and $\text{Gal}(F)$ sits in between $\text{Gal}(\mathbb{Q}^{\text{tr}})$ and $\text{Gal}(\mathbb{Q})$. In particular, these groups all have the same subsets of involutions, and we can deduce $\text{AS}(F) = \text{AS}(\mathbb{Q})$. $\square$

In particular, if F is Galois over $\mathbb{Q}$, then the Artin–Schreier quandle $\text{AS}(F)$ is either empty or isomorphic to $\text{AS}(\mathbb{Q})$ as described above.

One could argue that the totally real case is the most important. For instance, as Serre has remarked concerning the inverse Galois theory problem: All finite groups occur as Galois groups over $\mathbb{Q}$ if and only if all finite groups occur as Galois groups of totally real extensions of $\mathbb{Q}$ (see [32, Prop. 1]). However, there is something we can say concerning formally real number fields that are not totally real.

Proposition 4.5 *Let F_0 be a number field that is formally real, but not totally real. If F is any other formally real number field that is not totally real, then we have $\text{AS}(F) \cong \text{AS}(F_0)$. In words, the Artin–Schreier quandle is independent of the choice.*

Proof We can consider the compositum E of $\mathbb{Q}^{\text{tr}}$ with F , and this field will be a proper finite extension of $\mathbb{Q}^{\text{tr}}$. This larger field is even better than $\mathbb{Q}^{\text{tr}}$ in some sense. While the field $\mathbb{Q}^{\text{tr}}$ is pseudo real closed (PRC) by Pop (see [28]), but *not* Hilbertian, the proper finite extensions E of $\mathbb{Q}^{\text{tr}}$ are PRC by Prestel [51] and Hilbertian. In fact, every proper finite extension of $\mathbb{Q}^{\text{tr}}$ is Hilbertian (see [59, Satz 9.7] for a nonstandard proof and [20, Ch. 12] for a standard proof.) Hence, their absolute Galois groups

$$\text{Gal}(E) = \text{Gal}(F) \cap \text{Gal}(\mathbb{Q}^{\text{tr}})$$

are known by [21, Cor. 2]: an argument due to Jarden shows that, in the formally real case, the profinite group $\text{Gal}(E)$ is abstractly isomorphic to the free product of $\text{Gal}(\mathbb{Q}^{\text{tr}}) \cong F_2^\wedge(S)$ with a free profinite group of countable infinite rank (see [21, Cor. 1] and the remark following it). In particular, we see that the isomorphism type of $\text{Gal}(E)$, while different from $\text{Gal}(\mathbb{Q}^{\text{tr}})$, is independent of F . Computing the set of involutions in $\text{Gal}(F)$ is the same as computing the involutions in the intersection of $\text{Gal}(F)$ with the subgroup generated by the involutions:

$$\text{AS}(F) = \text{Inv}(\text{Gal}(F)) = \text{Inv}(\text{Gal}(F) \cap \text{Gal}(\mathbb{Q}^{\text{tr}})).$$

From the discussion above, we know that $\text{Inv}(\text{Gal}(F) \cap \text{Gal}(\mathbb{Q}^{\text{tr}})) = \text{Inv}(\text{Gal}(E))$ is independent of F . $\square$

Therefore, to determine the Artin–Schreier quandle of a field F as above, it would be sufficient to work out one particular example. However, this is difficult for reasons related to the splitting behaviour of involutions across subgroups (see the following example). In addition, it is not known whether subquandles of free involutory quandles are free.

Example 4.6 The absolute Galois group $\text{Gal}(F)$ of a number field F is a finite index subgroup of the absolute Galois group $\text{Gal}(\mathbb{Q})$ of the rational number field $\mathbb{Q}$, and the reader may wonder if there is not a more abstract description of the splitting of a conjugacy class of involutions in a group G when intersected with a finite index subgroup H and its conjugates gHg^{-1} . We have not found such, but offer the following example for contemplation. Take G to be the alternating group A_5 . It contains 15 involutions, all conjugate to $(12)(34)$. The subgroup H that is generated by (123) and $(12)(45)$ is isomorphic to the symmetric group S_3 . The group H and its conjugate gHg^{-1} with the element $g = (14)(25)$ both contain three involutions each, but they only have one of them in common, namely $(12)(45)$.

5 Laurent series and other examples

In this section, we will address two questions. First, for any given field F , we will describe the involutory quandle $\text{AS}(F((t)))$ of the field $F((t))$ of Laurent series with coefficients in F in terms of the Artin–Schreier quandle $\text{AS}(F)$. Second, we comment on the class of profinite involutory quandles that are realisable, up to isomorphism, as Artin–Schreier quandles $\text{AS}(F)$ for some field F . From what we have seen for local and global fields so far, it seems reasonable to conjecture that these are all free, but we will show by example that this is not the case (see also our Propositions 3.11 and 3.17 for other restrictions).

Theorem 5.1 *For any field F , there is an isomorphism*

$$\text{AS}(F((t))) \cong \text{AS}(F) \times \text{FQ}_2^\wedge\{\sigma, \tau\} \cong \text{AS}(F) \times \widehat{\mathbb{Z}}$$

of profinite involutory quandles, where $\text{FQ}_2^\wedge\{\sigma, \tau\}$ is the free profinite involutory quandle on a set $\{\sigma, \tau\}$ with two elements. The quandle structure is given by $a \triangleright b = 2a - b$ for $a, b \in \widehat{\mathbb{Z}}$.

Before we embark on the proof, let us recall that we can identify $\text{FQ}_2^\wedge\{\sigma, \tau\}$ with the set of involutions in the free profinite 2-group $F_2^\wedge\{\sigma, \tau\}$. This group $F_2^\wedge\{\sigma, \tau\}$ is the profinite infinite dihedral group $\widehat{D}_\infty$, and we can identify it with the semi-direct product $\widehat{\mathbb{Z}} \rtimes \mathbb{Z}/2$, where the generator of $\mathbb{Z}/2$ acts as -1 on $\widehat{\mathbb{Z}}$. An isomorphism is given by letting a pair (a, m) in the semi-direct product $\widehat{\mathbb{Z}} \rtimes \mathbb{Z}/2$ correspond to $(\sigma\tau)^a \sigma^m$ in $F_2^\wedge\{\sigma, \tau\}$. Once the groups are identified this way, we see that we can thereby also identify the subset $\text{FQ}_2^\wedge\{\sigma, \tau\}$ of involutions with the set $\widehat{\mathbb{Z}}$, where now $a \in \widehat{\mathbb{Z}}$ corresponds to the pair (a, m) with m odd in $\widehat{\mathbb{Z}} \rtimes \mathbb{Z}/2$. For m and n odd, we get

$$\begin{aligned} (a, m)(b, n)(a, m)^{-1} &= (a + (-1)^m b, m + n)((-1)^{-m}(-a), -m) \\ &= (a + (-1)^m b + (-1)^{m+n}(-1)^{-m}(-a), m + n - m) \\ &= (2a - b, n), \end{aligned}$$

and this calculation shows that the quandle structure we get on the set $\widehat{\mathbb{Z}}$ by transport of structure is given by $a \triangleright b = 2a - b$.

Proof of Theorem 5.1 The statement is void if the field F is not formally real: if the Laurent series field $F((t))$ can be ordered, so can the subfield F . In particular, we can assume that the field F has characteristic 0. For these fields, it is known that the absolute Galois group $\text{Gal}(F((t)))$ is a semidirect product (cf. [16]); in fact, there is an isomorphism $\text{Gal}(F((t))) \cong \widehat{\mathbb{Z}} \rtimes \text{Gal}(F)$ (see [23, Prop. 4.1(e)]). The multiplication takes the form

$$(a, g)(b, h) = (a + g(b), gh)$$

for some $\text{Gal}(F)$ -action on $\widehat{\mathbb{Z}}$. In particular, an element (a, g) is an involution if and only if $g = s$ is an involution and $a + s(a) = 0$.

If an involution s acted as the identity, then $a + s(a) = 0$ implies $2a = 0$, hence $a = 0$ because $\widehat{\mathbb{Z}}$ is torsionfree. In other words, the element s in $\text{AS}(F) = \text{Inv}(\text{Gal}(F))$ would have a unique pre-image in $\text{AS}(F((t)))$, and the same would hold for the conjugates of s . But for every ordering of F , there are two different orderings of $F((t))$, one where t is positive and one where t is negative (see [35, Prop. VIII.4.11], for instance). Hence, this is not possible, and s must act non-trivially. In fact, we can be more precise:

Lemma 5.2 *Every involution $s \in \text{Gal}(F)$ acts as -1 on the kernel $\widehat{\mathbb{Z}}$.*

If we had an action on the group $\mathbb{Z}$, it would be clear that an involution s can only act as ± 1 , but $\widehat{\mathbb{Z}}$ has more units than these, and we have to argue to exclude any other options. We will do this in detail once we have finished the main argument.

When the involution s acts as -1 , the equation $a + s(a) = 0$ is satisfied by *all* elements in $\widehat{\mathbb{Z}}$, and we can identify the pre-image $\{(a, s) \mid a \in \widehat{\mathbb{Z}}\}$ of any involution s canonically with $\widehat{\mathbb{Z}}$. Taken together, we thereby get a bijection between $\text{AS}(F((t)))$ and the product $\text{AS}(F) \times \widehat{\mathbb{Z}}$. The quandle operation is induced from the conjugation in the group, and the computation

$$\begin{aligned} (a, s) \triangleright (b, t) &= (a, s)(b, t)(a, s) \\ &= (a + s(b), st)(a, s) \\ &= (a + s(b) + st(a), sts) \\ &= (a - b + a, sts) \\ &= (2a - b, s \triangleright t) \end{aligned}$$

shows that this proves the statement. $\square$

Proof of Lemma 5.2 Let $\overline{F}$ be our chosen algebraic closure of F . Puiseux's theorem states that the algebraic closure of $\overline{F}((t))$ is the union $\bigcup_n \overline{F}((t^{1/n}))$, which we will denote by $\overline{F}((t^{1/\infty}))$. For the field $F((t))$, we need to be a bit more careful (see [23, Prop. 4.1] again). An algebraic closure of $F((t))$ is the compositum $\overline{F} \cdot F((t^{1/\infty}))$. It contains the subfields $F((t^{1/\infty}))$

and $\overline{F} \cdot F((t))$, with absolute Galois groups isomorphic to $\text{Gal}(F)$ and $\widehat{\mathbb{Z}}$, respectively. The latter is normal, and we find that $\text{Gal}(F((t))) \cong \widehat{\mathbb{Z}} \rtimes \text{Gal}(F)$ is a semi-direct product.

To better understand the $\text{Gal}(F)$ -action on $\widehat{\mathbb{Z}}$, we proceed as follows. A generator F_n of $\text{Gal}(\overline{F} \cdot F((t^{1/n})) \mid \overline{F} \cdot F((t))) \cong \mathbb{Z}/n$ acts by $F_n(t^{1/n}) = w_n t^{1/n}$ for a primitive n -th root of unity $w_n \in \mu_n(\overline{F})$. The elements F_n and w_n can be chosen with $(w_{mn})^m = w_n$ for all m so that the generators F_n fit together to define a topological generator of $\text{Gal}(\overline{F} \cdot F((t))) \cong \widehat{\mathbb{Z}}$. The absolute Galois group $\text{Gal}(F)$ acts on the coefficients of the Laurent series. On the normal subgroup $\text{Gal}(\overline{F} \cdot F((t)))$ of $\text{Gal}(F((t)))$, it acts by conjugation, but the computation

$$sF_n s^{-1}(t^{1/n}) = sF_n(t^{1/n}) = s(w_n t^{1/n}) = s(w_n)t^{1/n}$$

shows that this conjugation action is also just an action on the coefficients. In summary, we see that the $\text{Gal}(F)$ -action on $\widehat{\mathbb{Z}}$ is determined by the $\text{Gal}(F)$ -action on the group $\mu_\infty(\overline{F})$ of roots of unity in the algebraic closure $\overline{F}$.

It remains for us to check that all involutions in the absolute Galois group $\text{Gal}(F)$ act on the group $\mu_\infty(\overline{F})$ of roots of unity in the algebraic closure $\overline{F}$ via the inversion $w \mapsto w^{-1}$. We argue one prime at a time. If the prime p is odd, then all primitive p -th power roots of unity are totally imaginary, and they cannot be fixed by an involution s . As there is only one involution in the cyclic group $(\mathbb{Z}/p^e)^\times$, this forces $s(w) = w^{-1}$ for all $w \in \mu_{p^e}(\overline{F})$. At the even prime 2, when $w \in \mu_{2^e}(\overline{F})$, we must have $s(w) = w^{-1}$ for $e = 1$ trivially and for $e = 2$ by a similar reasoning as above: the group $(\mathbb{Z}/4)^\times$ is cyclic. However, for $e \geq 3$, there are two other options for us to consider, namely $s(w) = -w$ and $s(w) = -w^{-1}$. The first would imply that we have $s(w^2) = w^2$, which we can rule out by induction on e , as $w^2 \in \mu_{2^{e-1}}(\overline{F})$. The second would imply that $w - w^{-1}$ were fixed by s , but this element is totally imaginary. That leaves us with $s(w) = w^{-1}$ for all $w \in \mu_{2^e}(\overline{F})$ as well. $\square$

Example 5.3 As the Artin–Schreier quandle $\text{AS}(\mathbb{R})$ is a singleton, Theorem 5.1 immediately gives that the Artin–Schreier quandle $\text{AS}(\mathbb{R}((t)))$ is free, isomorphic to $\text{FQ}_2^\wedge\{\sigma, \tau\}$. By intersecting two real closed fields, Geyer [22] has constructed other formally real fields whose absolute Galois group is infinite dihedral, i.e., isomorphic to the free pro-2-group $\text{F}_2^\wedge\{\sigma, \tau\}$ on two generators. Of course, the corresponding Artin–Schreier quandle $\text{FQ}_2^\wedge\{\sigma, \tau\}$ is free on two generators as well.

We conclude with an example showing that Artin–Schreier quandles need not be free.

Example 5.4 Applying Theorem 5.1 twice, we see that

$$\text{AS}(\mathbb{R}((t_1))((t_2))) \cong \text{FQ}_2^\wedge\{\sigma_1, \tau_1\} \times \text{FQ}_2^\wedge\{\sigma_2, \tau_2\},$$

and this profinite involutory quandle is not free. In fact, it is not even isomorphic to a quandle of the form $\text{FQ}_2^\wedge(S)$ after forgetting the topologies, i.e., algebraically. To see this, we can consider the group of transvections (or displacements) of these quandles, introduced by Joyce [30, Sec. 5]: for a given quandle Q , the subgroup $\text{Tr}(Q) \leq \text{Aut}(Q)$ is the subgroup generated by the differences $\lambda_a^{-1}\lambda_b$ for all $a, b \in Q$. If S has at most one element, this group is trivial. As $\text{FQ}_2^\wedge\{\sigma, \tau\} \cong \widehat{\mathbb{Z}}$ with $a \triangleright x = 2a - x$, we can identify the

group $\text{Tr}(\text{FQ}_2^\wedge\{\sigma, \tau\})$ with the group of maps $\widehat{\mathbb{Z}} \rightarrow \widehat{\mathbb{Z}}$ of the form $x \mapsto x + 2c$, and this group is isomorphic to $\widehat{\mathbb{Z}}$ again. As $\text{Tr}(Q \times R) \cong \text{Tr}(Q) \times \text{Tr}(R)$ by [31, Lem. 5.1], we have $\text{Tr}(\text{AS}(\mathbb{R}((t_1))((t_2)))) \cong \widehat{\mathbb{Z}}^2$ for the quandle under consideration. It remains for us to argue that the groups $\text{Tr}(\text{FQ}_2^\wedge(S))$ are never of this form. From what we have computed above, this is already clear for $|S| < 3$. But if S contains three different elements s, t , and u , the group $\text{Tr}(\text{FQ}_2^\wedge(S))$ is not even abelian, as the elements $\lambda_s^{-1}\lambda_u$ and $\lambda_t^{-1}\lambda_u$ do not commute (check on u).

Acknowledgements I thank Jayanta Manoharmayum for helpful discussions on absolute Galois groups, and the anonymous referee for exceptionally detailed and constructive comments that led to improvements in several aspects of this paper.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Artin, E.: Kennzeichnung des Körpers der reellen algebraischen Zahlen. Abh. Math. Sem. Univ. Hamburg **3**, 319–323 (1924)
2. Artin, E.: Über die Zerlegung definiter Funktionen in Quadrate. Abh. Math. Sem. Univ. Hamburg **5**, 100–115 (1927)
3. Artin, E., Schreier, O.: Algebraische Konstruktion reeller Körper. Abh. Math. Sem. Univ. Hamburg **5**, 85–99 (1927)
4. Artin, E., Schreier, O.: Eine Kennzeichnung der reell abgeschlossenen Körper. Abh. Math. Sem. Univ. Hamburg **5**, 225–231 (1927)
5. Bachmann, F.: Aufbau der Geometrie aus dem Spiegelungsbegriff. Springer-Verlag, Berlin, 1959 and 1973
6. Bachmann, F.: Ebene Spiegelungsgeometrie. BI-Wissenschaftsverlag, Eine Vorlesung über Hjelmslev-Gruppen. Mannheim (1989)
7. Bergman, G.M.: Some category-theoretic ideas in algebra (a too-brief tour of algebraic structure, monads, and the adjoint tower). Proceedings of the International Congress of Mathematicians (Vancouver, B.C., 1974), vol. 1, pp. 285–296. Canad. Math. Congress, Montreal, Que (1975)
8. Bergman, G.M.: An invitation to general algebra and universal constructions, 2nd edn. Universitext. Springer, Cham (2015)
9. Binz, E., Neukirch, J., Wenzel, G.H.: A subgroup theorem for free products of profinite groups. J. Algebra **19**, 104–109 (1971)
10. Brieskorn, E.: Automorphic sets and braids and singularities. Braids (Santa Cruz, CA, 1986) 45–115. Contemp. Math. 78. Amer. Math. Soc., Providence, RI (1988)
11. Brouwer, L.E.J.: On the structure of perfect sets of points. Proc. Kon. Akad. Amsterdam **12**, 785–794 (1910)
12. Burde, G.: Knoten. Jahrbuch Überblicke Mathematik, pp. 131–147. Bibliographisches Inst, Mannheim (1978)
13. Coste, M., Roy, M.-F.: Topologies for real algebraic geometry. Topos theoretic methods in geometry, 37–100. Various Publ. Ser. 30. Aarhus Univ., Aarhus (1979)
14. Davis, A., Schlank, T.M.: Arithmetic Kei Theory. Preprint. [arXiv:2408.05489](https://arxiv.org/abs/2408.05489)
15. Dress, A.W.M.: A relation between Burnside- and Witt rings. Notes on the theory of representations of finite groups, Appendix B. Universität Bielefeld, Fakultät f (1971)
16. van den Dries, L., Ribenboim, P.: The absolute galois group of a rational function field in characteristic zero is a semidirect product. Canad. Math. Bull. **27**, 313–315 (1984)

17. Fenn, R., Rourke, C.: Racks and links in codimension two. *J. Knot Theory Ramifications* **1**, 343–406 (1992)
18. Fried, M.D., Haran, D., Völklein, H.: Absolute Galois group of the totally real numbers. *C. R. Acad. Sci. Paris Sér. I Math.* **317**, 995–999 (1993)
19. Fried, M.D., Haran, D., Völklein, H.: Real Hilbertianity and the field of totally real numbers. *Arithmetic geometry* (Tempe, AZ, 1993) 1–34. *Contemp. Math.*, 174. Amer. Math. Soc., Providence, RI (1994)
20. Fried, M.D., Jarden, M.: *Field Arithmetic*. Springer, Berlin (1986)
21. Fried, M.D., Völklein, H.: The absolute Galois group of a Hilbertian PRC field. *Isr. J. Math.* **85**, 85–101 (1994)
22. Geyer, W.-D.: Unendliche algebraische Zahlkörper, über denen jede Gleichung auflösbar von beschränkter Stufe ist. *J. Number Theory* **1**, 346–374 (1969)
23. Geyer, W.-D., Jarden, M.: On the normalizer of finitely generated subgroups of absolute Galois groups of uncountable Hilbertian fields of characteristic 0. *Israel J. Math.* **63**, 323–334 (1988)
24. Gildenhuys, D., Lim, C.-K.: Free pro- $\mathcal{C}$ -groups. *Math. Z.* **125**, 233–254 (1972)
25. Gildenhuys, D., Ribes, L.: A Kurosh subgroup theorem for free pro- $\mathcal{C}$ -products of pro- $\mathcal{C}$ -groups. *Trans. Amer. Math. Soc.* **186**, 309–329 (1973)
26. Haran, D., Jarden, M.: The absolute Galois group of a pseudo real closed field. *Ann. Sc. Norm. Super. Pisa* **12**, 449–489 (1985)
27. Haran, D., Jarden, M.: Real free groups and the absolute Galois group of $\mathbb{R}(t)$. *J. Pure Appl. Algebra* **37**, 155–165 (1985)
28. Haran, D., Jarden, M., Pop, F.: The absolute Galois group of the field of totally S -adic numbers. *Nagoya Math. J.* **194**, 91–147 (2009)
29. Jarden, M., Videla, C.: Fields on the bottom. *J. Théor. Nombres Bordeaux* **28**, 213–219 (2016)
30. Joyce, D.: A classifying invariant of knots, the knot quandle. *J. Pure Appl. Algebra* **23**, 37–65 (1982)
31. Kai, R., Tamaru, H.: On the Euler characteristics for quandles. *Internat. J. Math.* **36**, 2550034, 19 pp (2025)
32. Klüners, J., Malle, G.: A database for field extensions of the rationals. *LMS J. Comput. Math.* **4**, 182–196 (2001)
33. Knebusch, M., Scheiderer, C.: *Einführung in die reelle Algebra*. Vieweg Studium: Aufbaukurs Mathematik, 63. Friedr. Vieweg & Sohn, Braunschweig (1989)
34. Krüger, B.: *Automorphe Mengen und die artinschen Zopfgruppen*. Dissertation. Universität Bonn, Mathematisches Institut, Bonn (1990)
35. Lam, T.Y.: *Introduction to Quadratic Forms over Fields*. Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI (2005)
36. Laures, G., Szymik, M.: *A Basic Course in Topology*. Translated from the 2015 German second edition. Compact Textbooks in Mathematics. Birkhäuser/Springer, Berlin (2015)
37. Lawson, T., Szymik, M.: The homotopy types of free racks and quandles. Preprint. [arXiv:2106.01299](https://arxiv.org/abs/2106.01299)
38. Lawvere, F.W.: Functorial semantics of algebraic theories. *Proc. Nat. Acad. Sci. U.S.A.* **50**, 869–872 (1963)
39. Loos, O.: Spiegelungsräume und homogene symmetrische Räume. *Math. Z.* **99**, 141–170 (1967)
40. MacLane, S.: A proof of the subgroup theorem for free products. *Mathematika* **5**, 13–19 (1958)
41. Magnus, W., Karrass, A., Solitar, D.: *Combinatorial group theory: Presentations of groups in terms of generators and relations*. Interscience Publishers, New York (1966)
42. Matveev, S.V.: Distributive groupoids in knot theory. *Mat. Sb.* **119**, 73–83 (1982)
43. Mináč, J., Spira, M.: Formally real fields, Pythagorean fields, C -fields and W -groups. *Math. Z.* **205**, 519–530 (1990)
44. Mináč, J., Spira, M.: Witt rings and Galois groups. *Ann. Math.* **144**, 35–60 (1996)
45. Mühlherr, B.: Automorphisms of free groups and universal Coxeter groups. *Symmetries in science, IX* (Bregenz, 1996) pp. 263–268, Plenum, New York (1996)
46. Neukirch, J.: Freie Produkte pro-endlicher Gruppen und ihre Kohomologie. *Arch. Math.* **22**, 337–357 (1971)
47. Neukirch, J.: Einbettungsprobleme mit lokaler Vorgabe und freie Produkte lokaler Galoisgruppen. *J. Reine Angew. Math.* **259**, 1–47 (1973)
48. Orlov, D., Vishik, A., Voevodsky, V.: An exact sequence for $rmK_*^M/2$ with applications to quadratic forms. *Ann. Math.* **165**, 1–13 (2007)
49. Pfister, A.: On the Milnor conjectures: history, influence, applications. *Jahresber. Deutsch. Math.-Ver. ein.* **102**, 15–41 (2000)
50. Pop, F.: Embedding problems over large fields. *Ann. Math.* **144**, 1–34 (1996)
51. Prestel, A.: *Pseudo real closed fields. Set theory and model theory* (Bonn, 1979) pp. 127–156. *Lect. Notes Math.* 872. Berlin, Springer (1981)

52. Rubinsztein, R.L.: Topological quandles and invariants of links. *J. Knot Theory Ramifications* **16**, 789–808 (2007)
53. Shusterman, M.: The tamely ramified geometric quantitative minimal ramification problem. *Compos. Math.* **160**, 21–51 (2024)
54. Singh, M.: Endomorphism monoid and automorphism group of residually finite and profinite quandles. Preprint. [arXiv:2311.03708](https://arxiv.org/abs/2311.03708)
55. Szymik, M.: Permutations, power operations, and the center of the category of racks. *Comm. Algebra* **46**, 230–240 (2018)
56. Szymik, M., Vik, T.: Groups, conjugation and powers. *Involve* **18**, 387–399 (2025)
57. Takahashi, N.: Quandles associated to Galois covers of arithmetic schemes. *Kyushu J. Math.* **73**, 145–164 (2019)
58. Takasaki, M.: Abstraction of symmetric transformations. *Tôhoku Math. J.* **49**, 145–207 (1943)
59. Weissauer, R.: Der Hilbertsche Irreduzibilitätssatz. *J. Reine Angew. Math.* **334**, 203–220 (1982)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.