Artin–Schreier quandles of involutions in absolute Galois groups

Markus Szymik

October 2023

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 the rational number field, it is freely generated in its variety by a Cantor space of indeterminates.

Recall that we can identify the real spectrum of a field F with the set of conjugacy classes of involutions in the absolute Galois group $\mathrm{Gal}(F)$. Here, instead of working with equivalence classes, we define the Artin–Schreier quandle $\mathrm{AS}(F)$ directly, building on the set of all involutions inside the absolute Galois group $\mathrm{Gal}(F)$. Novel is the observation that this set not only has a topological structure as a subspace of a pro-finite group, but it also has an algebraic structure. While not a subgroup, it is still closed under conjugation. The algebraic theory of quandles is a well-established axiomatic framework to model conjugation, and $\mathrm{AS}(F)$, therefore, has the structure of an involutory quandle. Our main theorem describes the pro-finite involutory quandle $\mathrm{AS}(F)$ in the most fundamental cases:

Theorem. *The Artin–Schreier quandle* $\mathrm{AS}(\mathbb{Q})$ *of the rational number field* $\mathbb{Q}$ *is a free pro-finite involutory quandle. A basis is given by a Cantor space of involutions inside the absolute Galois group* $\mathrm{Gal}(\mathbb{Q})$.

We prove this result as Theorem 3.1 in the text. There is a similar statement for every formally real number field; see Theorem 3.6. Totally imaginary number fields have no involutions in their absolute Galois groups, and their Artin–Schreier quandles are empty.

For 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 [12]. 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, it is better to think of it as the set of orderings of F, as the set of ring morphisms $\mathrm{W}(F) \to \mathbb{Z}$, where $\mathrm{W}(F)$ 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 $\mathrm{Gal}(F)$. 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 is wider than real algebra. It extends 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 the theory of quandles. We can think of these algebraic structures as generalisations of knots: Joyce and Matveev [25, 34], 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, again, given by conjugation.

This paper contains just enough background material to be accessible to number theorists and topologists. We start with discussing involutions and involutory quandles in Section 1. The second half of that section describes the free models and covers the topological details needed for the pro-finite context. We specialise this general theory to Artin–Schreier quandles in Section 2. The rest of the paper describes the Artin–Schreier quandles of the rational number field and other global fields in Section 3.

1 Involutions and quandles

We start with some necessary recollections (and extensions to the pro-finite 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, 14, 25, 34]. The terminology and notation varies considerably among the various sources, and we shall stick to the following throughout:

Definition 1.1. A *rack* is a pair $(R,\rhd)$ consisting of a set R together with a binary operation $\rhd$ such that, for all x in R, the left-multiplication $\lambda_x\colon\ y\mapsto x\rhd y$ is an automorphism of the pair $(R,\rhd)$. Automorphisms are, of course, bijective morphisms, and the equation for it to be a morphism says

$$x\rhd(y\rhd z)=(x\rhd y)\rhd(x\rhd z) \tag{1.1}$$

for all all x, y, and z in R.

Remark 1.2. It is easy to extend the definition to allow the racks to have a topology for which the operations are continuous, and this has already been done by Rubinsztein [41], for instance. For us, it is sufficient to note that we can consider pro-finite racks as pro-objects [13] in the category of finite racks or, equivalently, as racks $(R,\rhd)$ together with a topology that makes R a totally disconnected compact Hausdorff space such that the operation $\rhd$ is continuous. (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.) In a pro-finite rack, the left-multiplications are automatically homeomorphisms because they are continuous bijections between compact Hausdorff spaces.

Remark 1.3. By definition, racks bring their own automorphisms, namely the left-multiplications, one for each element x, but there is also a *natural* automorphism, namely $x \mapsto x \rhd x$, which is compatible with all quandle morphisms and which generates all natural automorphisms [42, Thm. 5.4], and which not necessarily has the form of a left-multiplication.

Definition 1.4. If all natural automorphisms of a rack are the identity, then the rack is called a *quandle*. In symbols, this property means

$$x \rhd x = x \tag{1.2}$$

for all elements x.

Examples 1.5. The underlying set of any group forms a quandle under conjugation, i.e., if we define $g \rhd x = gxg^{-1}$. Any pro-finite group gives rise to a pro-finite quandle in this way.

Definition 1.6. A rack is called *involutory* if all left-multiplications have order at most two. It is equivalent to asking that the equation

$$x \rhd (x \rhd y) = y \tag{1.3}$$

holds for all x and y.

Remark 1.7. An involutory quandle is sometimes called a *kei*, following Takasaki [44]. The term *Takasaki quandle* is sometimes used in his honour. Our present terminology follows Joyce [25]. Fenn and Rourke [14, 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 [25, Sec. 10,11] for more information on involutory quandles.

Remark 1.8. If G is a group, the formula $g \rhd x = gx^{-1}g$ 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 [31] on the structure of symmetric spaces. As a special case, if G is the Euclidean plane, with the group structure given by addition, then we have $g \rhd x = 2g - x$, so that left-multiplication is reflection in the point g. Figure 1 illustrates the rack axiom.

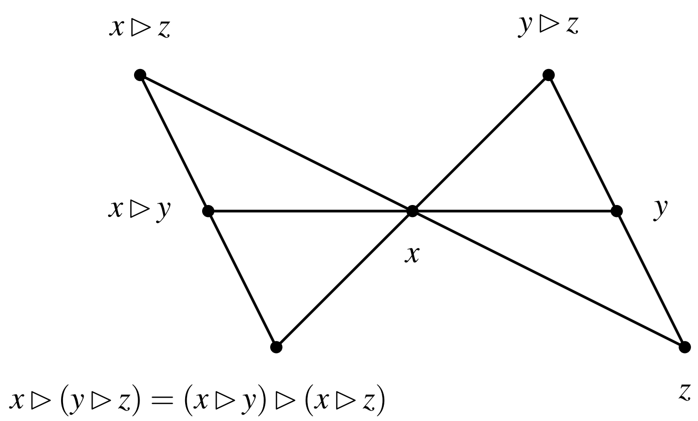

Figure 1: The rack axiom (1.1) for symmetric spaces

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 1.9. For any group G, the subset

$$\mathrm{Inv}(G) = \{\sigma \in G \,|\, \sigma^2 = \mathrm{id} \neq \sigma\} \tag{1.4}$$

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 pro-finite, and $\mathrm{Inv}(G)$ is a closed subset, then $\mathrm{Inv}(G)$ will also be pro-finite. We shall see below, in Lemma 2.8, that this is always the case in the situations we are interested in.

Any algebraic theory in the sense of Lawvere [30] is determined by its free models. For the theory of groups, for instance, we have the free groups $\mathrm{F}(S)$ generated by sets S, and if S has n elements, then the elements of $\mathrm{F}(S)$ are in bijection with the natural operations on groups of arity n. Specifically, if $S = \{x, y\}$, then the multiplication corresponds to $xy \in \mathrm{F}\{x,y\}$, whereas $xyx^{-1} \in \mathrm{F}\{x,y\}$ gives conjugation. For the theory of quandles, we can describe the free models as follows.

Proposition 1.10. *The free quandle* $\mathrm{FQ}(S)$ *on a set* S *is the union of the conjugacy classes of the basis elements* $S \subseteq \mathrm{F}(S)$ *inside the free group* $\mathrm{F}(S)$*; the operation* $\rhd$ *is given by conjugation.*

We refer to [25, Thm. 4.1] and [27, 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 $\mathrm{F}(S)$, which are the universal Artin groups, with the universal Coxeter groups: The universal Coxeter group on a set S of generators is the quotient

$$\mathrm{F}_2(S) = \langle s \in S \,|\, s^2 = e \text{ for all } s \in S\rangle$$

of the free group $\mathrm{F}(S)$ by the relations that say that the generating elements in S are involutions. When S has n elements, then $\mathrm{F}_2(S) \cong (\mathbb{Z}/2)^{\star n}$ is the coproduct of n copies of the group of order 2.

Proposition 1.11. *The free involutory quandle* $\mathrm{FQ}_2(S)$ *on a set* S *is the union of the conjugacy classes of the basis elements* $S \subseteq \mathrm{F}_2(S)$ *inside the universal Coxeter group* $\mathrm{F}_2(S)$.

We refer to [25, Cor. 10.3] and [27, Satz 2.5] once more.

Remark 1.12. We note that $\mathrm{F}_2(S)$ is not a free object in any variety of groups. The equation $s^2 = e$ is required for the generators s only, not necessarily for every group element. (The stronger condition would force the group to be abelian.) In contrast, the object $\mathrm{FQ}_2(S)$ is free in the theory of involutory quandles.

Proposition 1.13. *We have*

$$\mathrm{FQ}_2(S) = \{\, g \in \mathrm{F}_2(S) \,|\, g^2 = e \neq g \,\}. \tag{1.5}$$

Proof. Clearly, every conjugate of a generator $s \in S$ in $\mathrm{F}_2(S)$ 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 [33, Cor. 4.1.4], for instance. □

Remark 1.14. We can rephrase the observation leading to (1.5) in more conceptual terms as follows (compare [7] and [8, Sec. 10.11]). In any category with finite sums, we can take the full subcategory spanned by the finite sums of any chosen object Z, and this will be an algebraic theory in the sense of Lawvere. 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: $x \rhd u = u$ and $u \rhd y = y$ for all x,y (see [29, Def. 2.8], for example).

We now need the pro-finite versions $\mathrm{F}^\wedge(S)$ and $\mathrm{F}_2^\wedge(S)$ of the groups $\mathrm{F}(S)$ and $\mathrm{F}_2(S)$, respectively, where S can now be any pro-finite space. Suitable references come from Gildenhuys et.al. [19, 20], which build on earlier work of Neukirch et.al. [36, 37, 9] and Mac Lane [32], and the writings of Haran and Jarden [21, 22], of course.

If S is finite, we can build $\mathrm{F}^\wedge(S)$ as the pro-finite completion of $\mathrm{F}(S)$, namely the limit $\lim_N \mathrm{F}(S)/N$, where N ranges over the finite index normal subgroups of $\mathrm{F}(S)$. If S is, more generally, pro-finite, we have two choices: on the one hand, we can set $\mathrm{F}^\wedge(S) = \lim_N \mathrm{F}(S)/N$ as before, but require that $gN \cap S$ is open in S for the (finitely many) cosets gN of N in $\mathrm{F}(S)$. On the other hand, we can set $\mathrm{F}^\wedge(S) = \lim_R \mathrm{F}^\wedge(S/R)$, where R ranges over the equivalence relations on S that have a finite quotient. Both constructions give isomorphic results. For $\mathrm{F}_2^\wedge(S)$, we use $\mathrm{F}_2^\wedge(S) = \lim_N \mathrm{F}(S)/N$ with the added requirement that N contains all squares of elements in S or work with $\mathrm{F}_2^\wedge(S) = \lim_R \mathrm{F}_2^\wedge(S/R)$. Either way, a continuous homomorphism $\mathrm{F}_2(S) \to G$ into a pro-finite group G is the same thing as a continuous map $S \to G$ such that the elements in the image square to e. There are pro-finite versions of the Kurosh subgroup theorem.

Proposition 1.15. *Every involution in* $\mathrm{F}_2^\wedge(S)$ *is conjugate to an element in S.*

For a proof, see [22, Cor. 3.2], which is based on [21, Prop. 6.1].

Proposition 1.16. *For every pro-finite space S, there is a pro-finite involutory quandle* $\mathrm{FQ}_2^\wedge(S)$ *together with a continuous map* $S \to \mathrm{FQ}_2^\wedge(S)$ *that satisfies the universal property: a continuous homomorphism* $\mathrm{FQ}_2^\wedge(S) \to Q$ *into a pro-finite involutory quandle Q is, via restriction, the same thing as a continuous map* $S \to Q$.

Proof. Let us set $\mathrm{FQ}_2^\wedge(S) = \mathrm{Inv}(\mathrm{F}_2^\wedge(S))$. This is a pro-finite quandle: the involutions are closed in $\mathrm{F}_2^\wedge(S)$ as they are the image of the continuous map $\mathrm{F}_2^\wedge(S) \times S \to \mathrm{F}_2^\wedge(S)$ that sends (g,s) to gsg^{-1}. The involutory quandle $\mathrm{FQ}_2^\wedge(S)$ comes with a continuous map from S because the image of the canonical map $S \to \mathrm{F}_2^\wedge(S)$ lies inside $\mathrm{FQ}_2^\wedge(S)$.

Any continuous morphism $\mathrm{FQ}_2^\wedge(S) \to Q$ into a pro-finite involutory quandle Q restricts to a continuous map $S \to Q$. Conversely, if $\varphi\colon S \to Q$ is any such map, we can extend it functorially to a continuous morphism $\mathrm{F}_2^\wedge(\varphi)\colon \mathrm{F}_2^\wedge(S) \to \mathrm{F}_2^\wedge(Q)$ of groups. If we now have an element in $\mathrm{FQ}_2^\wedge(S) = \mathrm{Inv}(\mathrm{F}_2^\wedge(S))$, it will be conjugate to an element in S, so that we can write it as gsg^{-1} with g in $\mathrm{F}_2^\wedge(S)$ and s in S. In fact, as the centraliser of s in $\mathrm{F}_2^\wedge(S)$ is $\{e,s\}$, any other such expression $hsh^{-1} = gsg^{-1}$ will have $h \in \{g, gs\}$. Therefore, if we try to define our extension of φ to a quandle morphism $\mathrm{FQ}_2^\wedge(S) \to Q$ by sending gsg^{-1} to $\mathrm{F}_2^\wedge(\varphi)(g)\varphi(s)$, where $\mathrm{F}_2^\wedge(Q)$ acts on Q via left-multiplications, we only have to check that $\mathrm{F}_2^\wedge(\varphi)(gs)$ acts exactly the same as $\mathrm{F}_2^\wedge(\varphi)(gs)$ does on $\varphi(s)$. But that is easy: as $\mathrm{F}_2^\wedge(\varphi)$ is a morphism of groups, we have $\mathrm{F}_2^\wedge(\varphi)(gs) = \mathrm{F}_2^\wedge(\varphi)(g)\mathrm{F}_2^\wedge(\varphi)(s)$, and $\mathrm{F}_2^\wedge(\varphi)(s) = \varphi(s)$ acts trivially on itself by the quandle axioms. The preceding two constructions are inverse to each other. □

2 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 [28] and Knebusch–Scheiderer [26].

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 field is *real closed* if and only if it has a unique ordering, and in that ordering, the set P is the set of squares.

Definition 2.1. 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 pro-finite 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 $\mathrm{GW}(F) \to \mathbb{Z}$. The *Witt ring* $\mathrm{W}(F)$ 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 $\mathrm{W}(F) \to \mathbb{Z}/2$.

Proposition 2.2. *The real spectrum of a field F is in natural bijection with the set of ring morphisms $\mathrm{W}(F) \to \mathbb{Z}$ 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 '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. □

Remark 2.3. The kernel I of the parity homomorphism defines the I–adic filtration on the Witt ring $\mathrm{W}(F)$ with associated graded ring $\mathrm{gr}\,\mathrm{W}(F) = \mathrm{W}/I \oplus I/I^2 \oplus I^2/I^3 \oplus \dots$. It is a fact that $\mathrm{gr}\,\mathrm{W}(F)$ 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 the Milnor conjecture. Therefore, we can recover $\mathrm{gr}\,\mathrm{W}(F)$ from the absolute Galois group of F. Can we recover $\mathrm{W}(F)$ itself from a refinement of the absolute Galois group? This is a non-trivial question because there are examples of fields with isomorphic $\mathrm{gr}\,\mathrm{W}(F)$'s but non-isomorphic $\mathrm{W}(F)$'s (see [38] and [35]).

Remark 2.4. If $E|F$ is a Galois extension with group G, there is a map $\mathrm{A}(G) \to \mathrm{W}(F)$ from the Burnside ring 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 $(a,b) \mapsto \mathrm{tr}_{E|F}(ab)$. It is surjective if $E = F(\sqrt{a}\,|\,a \in F)$.

Proposition 2.5. *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 $P[\sigma] = \{a \in F \,|\, \sigma(\sqrt{a}) = \sqrt{a}\}$. Note that the condition $\sigma(\sqrt{a}) = \sqrt{a}$ does not depend on the choice of the square root $\sqrt{a}$ of a. □

We 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, 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 involutions. We refer to [24] 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 2.6. *Let F be a field and let $\sigma \in \mathrm{Gal}(F)$ be an involution with fixed field* $\mathrm{Fix}(\sigma)$. *Then* $\mathrm{Aut}(\mathrm{Fix}(\sigma)|F) = \{\mathrm{id}\}$. *The centraliser of the involution σ within* $\mathrm{Gal}(F)$ *is the subgroup $\langle\sigma\rangle$ generated by σ. The normaliser of* $\mathrm{Gal}(\mathrm{Fix}(\sigma))$ *within* $\mathrm{Gal}(F)$ *is* $\mathrm{Gal}(\mathrm{Fix}(\sigma))$ *itself.*

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

If τ is a field automorphism of $\mathrm{Fix}(\sigma)$ that fixes F, and $a \in \mathrm{Fix}(\sigma)$ 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 have $\tau(a) = a$ for all $a \in \mathrm{Fix}(\sigma)$, and this shows $\mathrm{Aut}(\mathrm{Fix}(\sigma)|F) = \{\mathrm{id}\}$.

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

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

Lemma 2.7. *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 group 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 $\mathrm{Gal}(F)$ cannot contain a subgroup of the form $\mathbb{Z}/2 \times \mathbb{Z}/2$: Given an involution $\sigma \neq \mathrm{id}$, Lemma 2.6 says that its centraliser within $\mathrm{Gal}(F)$ is the subgroup $\langle\sigma\rangle$ generated by σ. Therefore, there can be no other element in the group $\mathrm{Gal}(F)$ that commutes with σ. □

With these preliminaries out of our way, we can now define a new invariant of fields F. Recall that we have defined, in (1.4), the subset $\mathrm{Inv}(G)$ of involutions of a group G.

Lemma 2.8. *For any field F, the set* $\mathrm{Inv}(\mathrm{Gal}(F))$ *is a closed subspace of the absolute Galois group* $\mathrm{Gal}(F)$. *Therefore, it is pro-finite as well.*

Proof. The subset $\mathrm{Inv}(\mathrm{Gal}(F)) \cup \{\mathrm{id}\}$ is closed, as this subset is defined by the equation $\sigma^2 = \mathrm{id}$. 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 $\mathrm{Gal}(F)$ contains no involution, and we are talking about the empty set. Else, the field $F(\sqrt{-1})$ is a quadratic extension, so that $U = \mathrm{Gal}(F(\sqrt{-1}))$ is an index 2 subgroup of $\mathrm{Gal}(F)$, hence open and containing the identity. But $F(\sqrt{-1})$ is not formally real, so that U contains no involution. □

Definition 2.9. Let F be a field. The *Artin–Schreier quandle* $\mathrm{AS}(F)$ of F is the pro-finite involutory quandle

$$\mathrm{AS}(F) = \mathrm{Inv}(\mathrm{Gal}(F)). \tag{2.1}$$

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

Remark 2.10. The Artin–Schreier quandle $\mathrm{AS}(F)$ of a field F, just as its absolute Galois group $\mathrm{Gal}(F)$, depends on the choice of an algebraic closure of F. If $\omega\colon \Omega_1 \to \Omega_2$ is an F–isomorphism of algebraic closures of F, then $\sigma \mapsto \omega\sigma\omega^{-1}$ is an isomorphism $\mathrm{Aut}(\Omega_1|F) \to \mathrm{Aut}(\Omega_2|F)$ 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 2.11. It is usually a bad idea to forget everything from a group except its conjugation. In [43], 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 $\rhd$ on $\mathrm{AS}(F)$: By our definition of an involution, the unit $e = \mathrm{id}$ of $\mathrm{Gal}(F)$ is disjoint from $\mathrm{AS}(F)$, and the power operations on the disjoint union $\mathrm{AS}(F) \cup \{\mathrm{id}\}$ are determined by $\sigma^n = \mathrm{id}$ 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 $\mathrm{AS}(F)$ together with only the conjugation $\rhd$ on it as an algebraic invariant of F.

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

Proposition 2.12. *Let* $\mathrm{AS}(F)$ *be the Artin–Schreier quandle of a field* F*. For* σ *and* τ *in* $\mathrm{AS}(F)$ *we have* $\sigma \rhd \tau = \tau$ *if and only if* $\sigma = \tau$*.*

Proof. The 'if' direction is part of the quandle axioms, which are clear by now. For the 'only if' direction, note that $\sigma \rhd \tau = \tau$ 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 $\mathrm{AS}(F)$, so the result follows from Lemma 2.7. □

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

Proposition 2.13. *Let* F *be a field. Then* $\mathrm{AS}(F)$ *is non-empty if and only if* F *is formally real. This can only happen if* $\mathrm{char}(F) = 0$*.*

Proof. A field F is known to be formally real if and only if its absolute Galois group $\mathrm{Gal}(F)$ contains an involution. □

Example 2.14. The field $\mathbb{C}$ of complex numbers is not formally real, and the Artin–Schreier quandle $\mathrm{AS}(\mathbb{C})$ 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 $n \geqslant 3$.

As a consequence of Proposition 2.13, we may well restrict our attention to formally real fields.

Proposition 2.15. *Let* F *be a field. Then* $\mathrm{AS}(F)$ *is a singleton if and only if* F *is real closed.*

Proof. A field F is known to be real closed if and only if its absolute Galois group has order 2. □

Example 2.16. The field $\mathbb{R}$ of real numbers is real closed, and the unique element in the involutory quandle $\mathrm{AS}(\mathbb{R}) = \{\gamma\}$ is complex conjugation $\gamma\colon z \mapsto \bar{z}$ inside the absolute Galois group $\mathrm{Gal}(\mathbb{R}) = \mathrm{Aut}(\mathbb{C}|\mathbb{R}) = \{\mathrm{id}, \gamma\}$ of order 2. More generally, let F be a number field that is Galois over $\mathbb{Q}$ and not totally real. We can embed F into $\mathbb{C}$, and apply complex conjugation. This gives an involution in $\mathrm{Gal}(F)$, but this involution may depend on the embedding—unless F is a totally imaginary quadratic extension of a totally real number field (i.e., a CM field), such as $\mathbb{Q}(\sqrt{-1})$.

Remark 2.17. A bijection exists between the set $\mathrm{AS}(F)$ and the set of real closed subfields of the algebraic closure used to define the absolute Galois group. An involution σ corresponds to its fixed field $\mathrm{Fix}(\sigma)$.

The following result shows that the examples characterised in Propositions 2.13 and 2.15 are the only ones where the Artin–Schreier quandle is finite.

Proposition 2.18. *If* $\mathrm{AS}(F)$ *contains more than one element, it is infinite.*

Proof. If the Artin–Schreier quandle $\mathrm{AS}(F)$ contains more than one element, then the absolute Galois group $\mathrm{Gal}(F)$ contains two different involutions, say $\sigma \neq \tau$. Consider the morphism $\mathrm{F}_2\{s,t\} \to \mathrm{Gal}(F)$ of groups that sends the generator s to σ and t to τ. Suppose there were a non-trivial kernel. This kernel 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 $\mathrm{F}_2\{s,t\}$. 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 $\mathrm{Gal}(F)$, and it contains two different involutions $\sigma \neq \tau$. But the finite subgroups of $\mathrm{Gal}(F)$ have order at most 2 by Artin–Schreier—a contradiction. Hence, the morphism $\mathrm{F}_2\{s,t\} \to \mathrm{Gal}(F)$ is injective, and $\mathrm{Gal}(F)$ contains infinitely many involutions because this already holds for the infinite dihedral group $\mathrm{F}_2\{s,t\}$, and these lie in $\mathrm{AS}(F)$. □

3 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 $\mathrm{Ord}(\mathbb{Q})$ is a singleton, and all involutions in its absolute Galois group $\mathrm{Gal}(\mathbb{Q})$ form one conjugacy class. If we choose any involution $\sigma \in \mathrm{AS}(\mathbb{Q})$, then conjugation gives a homeomorphism $\mathrm{Gal}(\mathbb{Q})/\langle\sigma\rangle \cong \mathrm{AS}(\mathbb{Q})$. In particular, there are uncountably many involutions inside $\mathrm{Gal}(\mathbb{Q})$, and the topology is reasonably well understood. In contrast, the algebraic structure of the Artin–Schreier quandle $\mathrm{AS}(\mathbb{Q})$ supported on it is much more interesting:

Theorem 3.1. *The Artin–Schreier quandle* $\mathrm{AS}(\mathbb{Q})$ *of the rational number field* $\mathbb{Q}$ *is a free pro-finite involutory quandle. A basis is given by a Cantor space of involutions inside* $\mathrm{Gal}(\mathbb{Q})$.

Informally, this result says that the Artin–Schreier quandle $\mathrm{AS}(\mathbb{Q})$ 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 $\mathrm{Gal}(\mathbb{Q})$ that is a basis for it. Instead, it implicitly uses Brouwer's characterisation [11] of the Cantor space: every pro-finite 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. Our goal is to show that we can choose a subspace $S \subseteq \mathrm{Gal}(\mathbb{Q})$ homeomorphic to Cantor space and consisting of involutions so that the canonical extension

$$\mathrm{FQ}_2^{\wedge}(S) \longrightarrow \mathrm{AS}(\mathbb{Q}) \tag{3.1}$$

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

The subset $\mathrm{AS}(\mathbb{Q})$ of involutions generates a subgroup N of $\mathrm{Gal}(\mathbb{Q})$, and this subgroup is normal. Its fixed field is an infinite Galois extension $\mathbb{Q}^{\mathrm{tr}}$ of $\mathbb{Q}$, the field of totally real numbers. The normal subgroup N of $\mathrm{Gal}(\mathbb{Q})$ generated by the involutions is the absolute Galois group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}})$ of $\mathbb{Q}^{\mathrm{tr}}$. Fried–Haran–Völklein [15, 16] and (independently) Pop [39] have shown that this absolute Galois group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}})$ of the field $\mathbb{Q}^{\mathrm{tr}}$ is isomorphic to the free pro-finite Coxeter group $\mathrm{F}_2^\wedge(S)$ generated by a Cantor space S. In other words, we can choose a subspace S as above so that the canonical morphism

$$\mathrm{F}_2^\wedge(S) \longrightarrow \mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}}) \tag{3.2}$$

is an isomorphism of pro-finite groups.

We will only use that (3.2) is injective. We can precompose this injection (3.2) with the canonical morphism $\mathrm{FQ}_2^\wedge(S) \to \mathrm{F}_2^\wedge(S)$, which is also injective, to obtain an injection

$$\mathrm{FQ}_2^\wedge(S) \longrightarrow \mathrm{F}_2^\wedge(S) \longrightarrow \mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}}) \longrightarrow \mathrm{Gal}(\mathbb{Q}).$$

By the universal mapping property of $\mathrm{FQ}_2^\wedge(S)$, this composition agrees with the composition

$$\mathrm{FQ}_2^\wedge(S) \xrightarrow{(3.1)} \mathrm{AS}(\mathbb{Q}) \longrightarrow \mathrm{Gal}(\mathbb{Q}).$$

Therefore, we see that the morphism (3.1) is indeed injective.

For the proof of surjectivity of (3.1), the goal is to show that S generates $\mathrm{AS}(\mathbb{Q})$ as a quandle. An arbitrary element of $\mathrm{AS}(\mathbb{Q})$ is an involution in $N \cong \mathrm{F}_2^\wedge(S)$. By Propoition 1.15, all such involutions are conjugate to generators in S. This fact implies that $\mathrm{AS}(\mathbb{Q})$ is generated, under conjugation, and hence as a quandle, by S, and the morphism (3.1) is surjective. □

Remark 3.2. We remark that any free quandle generates a free group: the enveloping group is the value of the left-adjoint to the forgetful functor from groups to quandles, and as such, it preserves co-limits for category theoretical reasons. The proof of Theorem 3.1, however, goes the other way: it is not just categorical to deduce the freeness of a quandle from the freeness of its enveloping group, and this is why any argument given necessarily has to be non-trivial.

Remark 3.3. Our proof also used the fact that the map $\mathrm{FQ}_2(S) \to \mathrm{F}(S)$ 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 $\lambda_y = \lambda_z = \mathrm{id}$, then $y \rhd x = x$ implies that x commutes with y in the enveloping group, and $x \rhd y = z$ implies that x conjugates y into z in the enveloping group. Therefore, the elements y and z must become equal in the enveloping group, which is then easily seen as isomorphic to $\mathbb{Z}^2$.

Remark 3.4. Passage to conjugacy classes gives a surjection

$$\mathrm{AS}(F) \longrightarrow \mathrm{Ord}(F)$$

of pro-finite spaces from the Artin–Schreier quandle onto the real spectrum. This surjection should *not* suggest, however, that we can compute the real spectrum $\mathrm{Ord}(F)$ from the Artin–Schreier quandle $\mathrm{AS}(F)$ 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 set of orbits. (Recall that the orbits of a quandle are the equivalence classes of its elements under the equivalence relation generated by $x \rhd y \sim y$ for all x and y.) However, this is not the case (see the following Example 3.5). Instead, we have two surjections

$$\mathrm{AS}(F) \longrightarrow \mathrm{Orb}(\mathrm{AS}(F)) \longrightarrow \mathrm{Ord}(F), \tag{3.3}$$

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

Example 3.5. We have an equality $\mathrm{AS}(\mathbb{Q}(\sqrt{2})) = \mathrm{AS}(\mathbb{Q})$ of involutory quandles, as every involution in $\mathrm{Gal}(\mathbb{Q})$ also lies in the normal subgroup $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}))$. However, the rational number field $\mathbb{Q}$ has a unique ordering, whereas the real quadratic extension $\mathbb{Q}(\sqrt{2})$ has two. In fact, there are involutions in $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}))$ that are not conjugate in $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}))$ but become conjugate in $\mathrm{Gal}(\mathbb{Q})$. The set of orbits of $\mathrm{AS}(\mathbb{Q})$ surjects onto Cantor space, whereas the real spectrum of $\mathbb{Q}$ is trivial.

Let us finally look at other examples of small fields. The other prime fields, finite fields, and all other fields of positive characteristic are uninteresting for 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 3.1 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 $\mathrm{Mor}(F,\mathbb{R})$ of real embeddings $F \to \mathbb{R}$, which we can identify with its real spectrum, sits inside the d–element set $\mathrm{Mor}(F,\mathbb{C})$ of complex embeddings as the fixed points under the action of the Galois group $\mathrm{Aut}(\mathbb{C}|\mathbb{R}) = \mathbb{Z}/2$ 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 $d = 2r_2$, i.e., when it is not formally real ($r_1 > 0$). 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.

Theorem 3.6. *For any formally real number field F, the Artin–Schreier quandle $\mathrm{AS}(F)$ is a free pro-finite involutory quandle with a basis given by a Cantor space of involutions.*

Proof. If F is formally real and Galois over $\mathbb{Q}$, then the group $\mathrm{Gal}(F)$ contains one involution, and it is a normal subgroup of $\mathrm{Gal}(\mathbb{Q})$. As all involutions in $\mathrm{Gal}(\mathbb{Q})$ are conjugate, we see that the group $\mathrm{Gal}(F)$ contains all involutions of $\mathrm{Gal}(\mathbb{Q})$. We deduce $\mathrm{AS}(F) = \mathrm{AS}(\mathbb{Q})$, so that in the Galois case, the claim follows trivially from Theorem 3.1.

In the general case, when F is not necessarily Galois over $\mathbb{Q}$, we can proceed as in the proof of Theorem 3.1, except for one detail: we replace the field $\mathbb{Q}^{\mathrm{tr}}$ of totally real numbers and consider instead its compositum E with F. This larger field is even better than $\mathbb{Q}^{\mathrm{tr}}$ in some sense: The field $\mathbb{Q}^{\mathrm{tr}}$ is pseudo real closed (PRC) by Pop (see [23]), but not Hilbertian. In contrast, the proper finite extensions E of $\mathbb{Q}^{\mathrm{tr}}$ are PRC by Prestel [40] and Hilbertian. In fact, every proper finite extension of $\mathbb{Q}^{\mathrm{tr}}$ is Hilbertian (see [45, Satz 9.7] for a nonstandard proof and [17, Ch. 12] for a standard proof.) Hence, their absolute Galois groups

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

are known by [18, Cor. 2]: an argument due to Jarden shows that, in the formally real case, the pro-finite group $\mathrm{Gal}(E)$ is abstractly isomorphic to $\mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}})$.

The rest of the proof is nearly identical to the one for Theorem 3.1. Computing the involutions in $\mathrm{Gal}(F)$ is the same as computing the involutions in the intersection of $\mathrm{Gal}(F)$ with the subgroup generated by the involutions:

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

From the discussion above, we know

$$\mathrm{Inv}(\mathrm{Gal}(F) \cap \mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}})) = \mathrm{Inv}(\mathrm{Gal}(E)) \cong \mathrm{Inv}(\mathrm{F}_2^{\wedge}(S))$$

for some Cantor space S, and $\mathrm{Inv}(\mathrm{F}_2^{\wedge}(S)) = \mathrm{FQ}_2^{\wedge}(S)$ from Proposition 1.16. In summary, we find $\mathrm{AS}(F) \cong \mathrm{FQ}_2^{\wedge}(S)$, as claimed. □

Acknowledgements

I thank Jayanta Manoharmayum for discussions about absolute Galois groups.

References

[1] E. Artin. Kennzeichnung des Körpers der reellen algebraischen Zahlen. Abh. Math. Sem. Univ. Hamburg 3 (1924) 319–323.

[2] E. Artin. Über die Zerlegung definiter Funktionen in Quadrate. Abh. Math. Sem. Univ. Hamburg 5 (1927) 100–115.

[3] E. Artin, O. Schreier. Algebraische Konstruktion reeller Körper. Abh. Math. Sem. Univ. Hamburg 5 (1927) 85–99.

[4] E. Artin, O. Schreier. Eine Kennzeichnung der reell abgeschlossenen Körper. Abh. Math. Sem. Univ. Hamburg 5 (1927) 225–231.

[5] F. Bachmann. Aufbau der Geometrie aus dem Spiegelungsbegriff. Springer-Verlag, Berlin, 1959 and 1973.

[6] F. Bachmann. Ebene Spiegelungsgeometrie. Eine Vorlesung über Hjelmslev-Gruppen. Mannheim, BI-Wissenschaftsverlag, 1989.
[7] G.M. Bergman. 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, 285–296. Canad. Math. Congress, Montreal, Que., 1975.
[8] G.M. Bergman. An invitation to general algebra and universal constructions. Second edition. Universitext. Springer, Cham, 2015.
[9] E. Binz, J. Neukirch, G.H. Wenzel. A subgroup theorem for free products of profinite groups. J. Algebra 19 (1971) 104–109.
[10] E. Brieskorn. Automorphic sets and braids and singularities. Braids (Santa Cruz, CA, 1986) 45–115. Contemp. Math. 78. Amer. Math. Soc., Providence, RI, 1988.
[11] L.E.J. Brouwer. On the structure of perfect sets of points. Proc. Kon. Akad. Amsterdam 12 (1910) 785–794.
[12] M. Coste, M.-F. Roy. Topologies for real algebraic geometry. Topos theoretic methods in geometry, 37–100. Various Publ. Ser. 30. Aarhus Univ., Aarhus, 1979.
[13] J. Duskin. Pro-objects (after Verdier). Sém. Heidelberg–Strasbourg, 1966–67. Exp. 6. I.R.M.A. Strasbourg.
[14] R. Fenn, C. Rourke. Racks and links in codimension two. J. Knot Theory Ramifications 1 (1992) 343–406.
[15] M.D. Fried, D. Haran, H. Völklein. Absolute Galois group of the totally real numbers. C. R. Acad. Sci. Paris Sér. I Math. 317 (1993) 995–999.
[16] M.D. Fried, D. Haran, H. Völklein. 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.
[17] M.D. Fried, M. Jarden. Field arithmetic. Revised by Moshe Jarden. 3rd revised ed. Berlin, Springer, 2008.
[18] M.D. Fried, H. Völklein. The absolute Galois group of a Hilbertian PRC field. Isr. J. Math. 85 (1994) 85–101.
[19] D. Gildenhuys, C.-K. Lim. Free pro–$\mathcal{C}$–groups. Math. Z. 125 (1972) 233–254.
[20] D. Gildenhuys, L. Ribes. A Kurosh subgroup theorem for free pro–$\mathcal{C}$–products of pro–$\mathcal{C}$–groups. Trans. Amer. Math. Soc. 186 (1973) 309–329.
[21] D. Haran, M. Jarden. The absolute Galois group of a pseudo real closed field. Ann. Sc. Norm. Super. Pisa 12 (1985) 449–489.
[22] D. Haran, M. Jarden. Real free groups and the absolute Galois group of $\mathbb{R}(t)$. J. Pure Appl. Algebra 37 (1985) 155–165.
[23] D. Haran, M. Jarden, F. Pop. The absolute Galois group of the field of totally S–adic numbers. Nagoya Math. J. 194 (2009) 91–147.
[24] M. Jarden, C. Videla. Fields on the bottom. J. Théor. Nombres Bordeaux 28 (2016) 213–219.
[25] D. Joyce. A classifying invariant of knots, the knot quandle. J. Pure Appl. Algebra 23 (1982) 37–65.
[26] M. Knebusch, C. Scheiderer. Einführung in die reelle Algebra. Vieweg Studium: Aufbaukurs Mathematik, 63. Friedr. Vieweg & Sohn, Braunschweig, 1989.
[27] B. Krüger. Automorphe Mengen und die artinschen Zopfgruppen. Dissertation. Universität Bonn, Mathematisches Institut, Bonn, 1990.

[28] T.Y. Lam. Introduction to Quadratic Forms over Fields. Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI, 2005.
[29] T. Lawson, M. Szymik. The homotopy types of free racks and quandles. Preprint. arXiv:2106.01299
[30] F.W. Lawvere. Functorial semantics of algebraic theories. Proc. Nat. Acad. Sci. U.S.A. 50 (1963) 869–872.
[31] O. Loos. Spiegelungsräume und homogene symmetrische Räume. Math. Z. 99 (1967) 141–170.
[32] S. MacLane. A proof of the subgroup theorem for free products. Mathematika 5 (1958) 13–19.
[33] W. Magnus, A. Karrass, D. Solitar. Combinatorial group theory: Presentations of groups in terms of generators and relations. Interscience Publishers, New York-London-Sydney, 1966.
[34] S.V. Matveev. Distributive groupoids in knot theory. Mat. Sb. 119 (1982) 73–83.
[35] J. Mináč, M. Spira. Witt rings and Galois groups. Ann. Math. 144 (1996) 35–60.
[36] J. Neukirch. Freie Produkte pro-endlicher Gruppen und ihre Kohomologie. Arch. Math. 22 (1971) 337–357.
[37] J. Neukirch. Einbettungsprobleme mit lokaler Vorgabe und freie Produkte lokaler Galoisgruppen. J. Reine Angew. Math. 259 (1973) 1–47.
[38] A. Pfister. On the Milnor conjectures: history, influence, applications. Jahresber. Deutsch. Math.-Verein. 102 (2000) 15–41.
[39] F. Pop. Embedding problems over large fields. Ann. of Math. 144 (1996) 1–34.
[40] A. Prestel. Pseudo real closed fields. Set theory and model theory (Bonn, 1979) 127–156. Lect. Notes Math. 872. Berlin, Springer, 1981.
[41] R.L. Rubinsztein. Topological quandles and invariants of links. J. Knot Theory Ramifications 16 (2007) 789–808.
[42] M. Szymik. Permutations, power operations, and the center of the category of racks. Comm. Algebra 46 (2018) 230–240
[43] M. Szymik, T. Vik. Groups, conjugation and powers. Preprint. arXiv:2111.08998
[44] M. Takasaki. Abstraction of symmetric transformations. Tôhoku Math. J. 49 (1943) 145–207.
[45] R. Weissauer. Der Hilbertsche Irreduzibilitätssatz. J. Reine Angew. Math. 334 (1982) 203–220.

School of Mathematics and Statistics, The University of Sheffield, Hicks Building, Hounsfield Road, Sheffield S3 7RH, UK
m.szymik@sheffield.ac.uk

Department of Mathematical Sciences, NTNU Norwegian University of Science and Technology, 7491 Trondheim, NORWAY
markus.szymik@ntnu.no