PARK CITY LECTURE NOTES: AROUND THE INVERSE GALOIS PROBLEM

OLIVIER WITTENBERG

Abstract. The inverse Galois problem asks whether any finite group can be realised as the Galois group of a Galois extension of the rationals. This problem and its refinements have stimulated a large amount of research in number theory and algebraic geometry in the past century, ranging from Noether's problem (letting X denote the quotient of the affine space by a finite group acting linearly, when is X rational?) to the rigidity method (if X is not rational, does it at least contain interesting rational curves?) and to the arithmetic of unirational varieties (if all else fails, does X at least contain interesting rational points?). The goal of the present notes, which formed the basis for three lectures given at the Park City Mathematics Institute in August 2022, is to provide an introduction to these topics.

The inverse Galois problem is a simple-looking but fundamental open question of number theory on which tools coming from diverse areas of mathematics can be brought to bear. These lectures aim to explain the problem as well as a few of the many methods that have been developed to attack it, emphasising a geometric point of view whenever possible.

The first lecture introduces the problem together with a refinement of it first considered by Grunwald, and presents the strategy of Hilbert and Noether—a strategy based on Hilbert's irreducibility theorem and laid out more than a hundred years ago. This leads us to the notion of versal torsor, and to questions of rationality, stable rationality, retract rationality for quotient varieties. The second lecture is devoted to the regular inverse Galois problem, which is about the construction of Galois covers of curves. We present the rigidity method in detail, via Hurwitz moduli spaces. The third and final lecture explains how Grunwald's problem is expected to be controlled by the Brauer–Manin obstruction to weak approximation on the quotient varieties appearing in the Hilbert–Noether strategy, and discusses the descent method and its applications to the inverse Galois problem and to its variants.

Several important topics could not fit into these three lectures and had to be left aside, such as the connection between the inverse Galois problem and the construction of Galois representations (see [Shi74], [Zyw15] for some examples), the directions in which the rigidity method has been developed beyond its base case (see e.g. [DR00], [Völ01], [MM18, Chapter III] among many others), or the study of embedding problems.

Additional material on the inverse Galois problem can be found in [Ser07, MM18, Völ96, Dèb99, JLY02, Mat87, Sza09].

Date: February 14th, 2023; revised on October 3rd, 2023.

Acknowledgements. These lectures were delivered in August 2022 in Park City on the occasion of the PCMI 2022 graduate summer school, whose organisers are gratefully acknowledged. The author thanks Diego Izquierdo for leading the problem sessions, Enric Florit and Boris Kunyavskiĭ for correcting oversights in the first version of the notes, as well as Jean-Louis Colliot-Thélène, Joachim König, Jean-Pierre Serre, Tamás Szamuely and the referee for numerous useful comments that helped improve the exposition.

1. From Galois to Hilbert and Noether

1.1. **Introduction.** Galois theory turns the collection of all number fields into a profinite group, the absolute Galois group $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ of $\mathbf{Q}$. The study of this group and of its representations has been a cornerstone of number theory for more than a century. Yet, even such a basic question as the following one remains wide-open to this day: do all finite groups appear as quotients of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$? This is the so-called "inverse Galois problem".

The same question can be asked about the absolute Galois group of an arbitrary field k: given a finite group G and a field k, does there exist a Galois field extension K of k such that $\mathrm{Gal}(K/k) \simeq G$? Obviously, the answer is in the negative for some fields k that have a small absolute Galois group (e.g. the fields $\mathbf{C}$ and $\mathbf{R}$, trivially; or the field $\mathbf{Q}_p$, as its absolute Galois group is prosolvable). When k is a number field, a positive answer is known when G is solvable (Shafarevich, see [NSW08, Chapter IX, §6] and the references therein), when G is a symmetric or an alternating group (Hilbert [Hil92]), when G is a sporadic group other than M_{23} (Shih, Fried, Belyi, Matzat, Thompson, Hoyden–Siedersleben, Zeh–Marschke, Hunt, Pahlings, see [MM18]), when G belongs to various infinite families of non-abelian simple groups of Lie type (e.g. the groups $\mathrm{PSL}_2(\mathbf{F}_p)$, according to Shih, Malle, Clark, Zywina; see [Zyw15]); but the problem remains open over $\mathbf{Q}$ even for such a small group as $\mathrm{SL}_2(\mathbf{F}_{13})$, of order 2184, or as the simple group $\mathrm{PSL}_3(\mathbf{F}_8)$ (for the latter, see [Zyw13], to be complemented with [DFV22]).

Several variants or generalisations of the inverse Galois problem have been considered in the literature. Here is one of them. Given a number field k, we denote the set of its places by Ω and the completion of k at $v \in \Omega$ by k_v.

Problem 1.1.1 (Grunwald)**.** *Let k be a number field and $S \subset \Omega$ be a finite subset. Let G be a finite group. For each $v \in S$, let K_v be a Galois field extension of k_v such that the group $\mathrm{Gal}(K_v/k_v)$ can be embedded into G. Does there exist a Galois field extension K of k such that $\mathrm{Gal}(K/k) \simeq G$ and such that for all $v \in S$, the completion of K/k at any place of K lying above v is isomorphic to K_v/k_v?*

The Grunwald–Wang theorem, which was proved by Wang [Wan50] following the work of Grunwald [Gru33] and which has an interesting history (see [AT09, Chapter X, footnote on p. 73] and [Mil20, Chapter VIII, §2, p. 234, Notes]), gives a complete answer to Problem 1.1.1 when G is abelian, via class field theory. In particular, the answer to Grunwald's problem is negative for $G = \mathbf{Z}/8\mathbf{Z}$ and $k = \mathbf{Q}$ (see Proposition 1.6.2 below), but it is positive, for any number field k and any finite abelian group G, as soon as S does not contain any place dividing 2. For an arbitrary finite group G, the Grunwald problem is expected to have a positive answer whenever G does not contain any place dividing the order of G. This is the "tame" Grunwald problem, a terminology coined in [DLAN17].

Other variants include embedding problems (given a Galois field extension ℓ/k, a finite group G and a surjection $\varphi : G \twoheadrightarrow \mathrm{Gal}(\ell/k)$, can one embed ℓ/k into a Galois field extension K/k such that $G \simeq \mathrm{Gal}(K/k)$, the map φ being identified with the restriction map $\mathrm{Gal}(K/k) \twoheadrightarrow \mathrm{Gal}(\ell/k)$?) or the question of resolving the inverse Galois problem with additional constraints, such as the constraint that a given finite collection of elements of k be norms from K (a problem raised in [FLN22]).

1.2. **Torsors and Galois extensions.** Let us start by reformulating the inverse Galois problem in terms of torsors. Hereafter, a *variety* over a field k is a separated scheme of finite type over k (which may be disconnected or otherwise reducible) and $\bar{k}$ denotes an algebraic closure of k.

Definition 1.2.1. Let $\pi : Y \to X$ be a finite morphism between varieties over a field k. Let G be a finite group acting on Y, in such a way that π is G-equivariant (for the trivial action of G on X). We say that π is a *G-torsor*, or that Y is a G-torsor over X, if π is étale and G acts simply transitively on the fibres of the map $Y(\bar{k}) \to X(\bar{k})$ induced by π.

When G is a finite group acting on a variety Y, we denote by Y/G the quotient variety, characterised by the universal property of quotients, when it exists. Let us recall that the quotient Y/G exists if Y is quasi-projective; the projection $\pi : Y \to Y/G$ is then finite and surjective; it is étale if the action of G on Y is free (by which we mean that G acts freely on the set $Y(\bar{k})$); and in the affine case, if $Y = \mathrm{Spec}(A)$, then $Y/G = \mathrm{Spec}(A^G)$ (see [Mum08, Chapter II, §7 and Chapter III, §12]).

It is easy to see that a finite G-equivariant morphism $\pi : Y \to X$ is a G-torsor if and only if G acts freely on Y and π induces an isomorphism $Y/G \xrightarrow{\sim} X$. Thus, in particular, a Galois field extension K/k with Galois group G is the same thing as an irreducible G-torsor over k (that is, over $\mathrm{Spec}(k)$); and this, in turn, is the same thing as an irreducible variety of dimension 0, over k, endowed with a simply transitive action of G.

This rewording leads to a slight change in perspective, first emphasised by Hilbert and Noether: in order to solve the inverse Galois problem for G, we can now start with any irreducible quasi-projective variety Y endowed with a free action of G; setting $X = Y/G$, we obtain a G-torsor $\pi : Y \to X$; it is then enough to look for rational points $x \in X(k)$ such that the fibre $\pi^{-1}(x)$ is irreducible. Indeed, this fibre is in any case a G-torsor over k.

Remark 1.2.2. Given a subgroup $H \subseteq G$, any H-torsor $Y \to X$ gives rise to a G-torsor $Y' \to X$. Namely, if H acts on the left on Y, we let it act on the right on $G \times Y$ by $(g, y) \cdot h = (gh, h^{-1}y)$ and observe that $Y' = (G \times Y)/H$ inherits a free left action of G, turning the projection $Y' \to X$ into a G-torsor. The variety Y' is (canonically) a disjoint union indexed by G/H of varieties each of which is (non-canonically, in general) isomorphic, over X, to Y. Conversely, if $Y' \to X$ is a G-torsor and X is connected, then any connected component Y of Y' is an H-torsor over X for some subgroup H (namely, the stabiliser of Y), and Y' coincides with $(G \times Y)/H$. All in all, when X is connected, the data of a G-torsor $Y' \to X$ together with the choice of a connected component of Y' is equivalent to the data of a subgroup $H \subseteq G$ and of a connected H-torsor $Y \to X$. In particular, we see that if G is a finite group and k is a field, the data of a G-torsor over k together with the choice of a connected component is equivalent to the data of a Galois field extension K/k endowed with an embedding $\mathrm{Gal}(K/k) \hookrightarrow G$.

1.3. **Hilbert's irreducibility theorem.** When the base of the G-torsor $\pi : Y \to X$ is an open subset of $\mathbf{P}^1_k$, with k a number field, and its total space Y is irreducible, the existence of rational points $x \in X(k)$ such that the fibre $\pi^{-1}(x)$ is irreducible is guaranteed by Hilbert's irreducibility theorem, which we state next.

Theorem 1.3.1 (Hilbert)**.** *Let k be a number field. Let $X \subseteq \mathbf{P}^1_k$ be a dense open subset. Let $\pi : Y \to X$ be an irreducible étale covering (i.e. a finite étale morphism from an irreducible variety). There exists $x \in X(k)$ such that $\pi^{-1}(x)$ is irreducible.*

Theorem 1.3.1 is classically formulated in the following equivalent way: given an irreducible two-variable polynomial $f(s, t)$ with coefficients in a number field k, there exist infinitely many $t_0 \in k$ such that $f(s, t_0)$ is an irreducible one-variable polynomial with coefficients in k. In fact, the set of such t_0 is not just infinite: asymptotically, it contains 100% of the elements of k, when they are ordered by height (see [Ser97, §13.1, Theorem 3]).

A proof of Theorem 1.3.1 can be found in [Ser97, §9.2, §9.6], where the next corollary is also established.

Corollary 1.3.2. *Same statement, with X now a dense open subset of $\mathbf{P}^n_k$ for some $n \geq 1$.*

Combining Corollary 1.3.2 with the remarks of §1.2 leads to an observation, originating from Hilbert's work, which is extremely effective for the inverse Galois problem. Before stating it in Corollary 1.3.3 below, let us recall that a variety X over a field k is said to be *rational* if it is birationally equivalent to an affine space, i.e. if it contains a dense open subset isomorphic to a dense open subset of an affine space; when X is irreducible and reduced, this means that its function field $k(X)$ is a purely transcendental extension of k.

Corollary 1.3.3. *Let k be a number field. Let G be a finite group. If there exist an irreducible quasi-projective variety Y over k and a faithful action of G on Y such that the quotient Y/G is rational, then the inverse Galois problem admits a positive solution for G over k.*

Proof. As G acts faithfully on Y, it acts freely on a dense open subset of Y, say V. Indeed, for $g \in G$, the locus in Y fixed by g is a closed subset of Y of codimension ≥ 1; one can take for V the complement of the (finite) union of these fixed loci. After shrinking V, we may assume that V/G is isomorphic to an open subset of $\mathbf{P}^n_k$. Corollary 1.3.2 can now be applied to the projection $V \to V/G$. $\square$

Example 1.3.4. The order 3 automorphism of $\mathbf{P}^1_k$ given, in homogeneous coordinates, by $[x : y] \mapsto [y : y - x]$ induces a faithful action of $G = \mathbf{Z}/3\mathbf{Z}$ on $\mathbf{P}^1_k$. The quotient $\mathbf{P}^1_k/G$ is rational since it is a unirational curve (Lüroth's theorem). Thus, any number field admits a cyclic extension of degree 3.

Ekedahl proved the following useful generalisation of Hilbert's irreducibility theorem. We recall that Ω denotes the set of places of a number field k.

Theorem 1.3.5 ([Eke90])**.** *Let $\pi : Y \to X$ be a finite étale morphism between geometrically irreducible varieties over a number field k. Let $S \subset \Omega$ be a finite subset. If $X(k) \neq \varnothing$, then there exists a nonempty open subset $\mathscr{U} \subset \prod_{v \in \Omega \setminus S} X(k_v)$ such that for all $x \in X(k) \cap \mathscr{U}$, the fibre $\pi^{-1}(x)$ is irreducible.*

In the above statement, we view $X(k)$ as diagonally embedded into $\prod_{v \in \Omega \setminus S} X(k_v)$, which we endow with the product of the v-adic topologies. When X is rational, the set $X(k) \cap \mathscr{U}$ is automatically nonempty, by the weak approximation property for affine spaces. In general, though, this set can be empty. A proof of Theorem 1.3.5, at least in the Galois case[1], which is the only one that we shall use (we use it in the proof of Proposition 1.5.5 below), can be found in [Eke90, Theorem 1.3].

1.4. **Noether's problem: statement.** The following problem, raised by Emmy Noether, takes on particular importance in view of Corollary 1.3.3.

Problem 1.4.1 (Noether)**.** *Let G be a finite group and k be a field. Choose an embedding $G \hookrightarrow S_n$ for some $n \geq 1$. Let G act on $\mathbf{A}^n_k$ through this embedding by permuting the coordinates. Is the quotient $\mathbf{A}^n_k/G$ rational over k?*

By Corollary 1.3.3, when k is a number field, a positive answer to Noether's problem for G over k implies a positive answer to the inverse Galois problem for G over k. Beyond this implication, Noether's problem has become a central problem in the study of rationality, and has been the focus of much research for its own sake.

Example 1.4.2. Noether's problem has a positive answer, over any field, for the symmetric group $G = S_n$. Indeed, for $G = S_n$, the quotient $\mathbf{A}^n_k/G$ is in fact isomorphic to $\mathbf{A}^n_k$, as the ring $k[x_1, \ldots, x_n]^{S_n}$ of symmetric polynomials coincides with the polynomial ring in the elementary symmetric polynomials. Thus, in particular, every number field admits a Galois field extension with group S_n, for every $n \geq 1$.

Example 1.4.3. Noether's problem has a positive answer, for any $n \geq 1$ and any embedding $G \hookrightarrow S_n$, when G is an abelian group of exponent e and k is a field that contains the eth roots of unity and whose characteristic does not divide e. In particular, it has a positive answer for all abelian groups over $\mathbf{C}$. This is a theorem of Fischer [Fis15].

Example 1.4.4. Noether's problem has a positive answer, over any field, for the alternating group $G = A_5$. This is a theorem of Maeda [Mae89]. On the other hand, as soon as $n \geq 6$, Noether's problem for $G = A_n$ is still open, over any field.

[1] It can be checked that Theorem 1.3.5, in the Galois case, still holds when Y is only assumed to be irreducible, instead of geometrically irreducible. Under this weaker assumption on Y, the Galois case does imply the general case; hence the validity of Theorem 1.3.5 as stated (and even slightly more generally than stated, since this weaker assumption on Y also suffices in the non-Galois case).

Noether knew that her problem has a positive answer for small groups (namely, for all subgroups of S_4). In general, however, its answer is often negative, as we discuss in some detail in §1.6 below.

1.5. **Versal torsors.** For some G-torsors $\pi : Y \to X$, the existence of rational points $x \in X(k)$ such that $\pi^{-1}(x)$ is irreducible is not only a sufficient condition for a positive answer to the inverse Galois problem for G over k, but it is also necessary. These are the *versal* torsors.

Definition 1.5.1. Let G be a finite group, let k be a field and let X be a variety over k. A G-torsor $\pi : Y \to X$ is *weakly versal* if for any field extension k'/k with k' infinite, every G-torsor over k' can be realised as the fibre of π above a k'-point of X. It is *versal* if for any dense open subset $U \subseteq X$, the induced G-torsor $\pi^{-1}(U) \to U$ is weakly versal.

Example 1.5.2. Choose an embedding $G \hookrightarrow S_n$ for some $n \geq 1$ and let G act on $\mathbf{A}^n_k$ through this embedding by permuting the coordinates. Let Y be the open subset of $\mathbf{A}^n_k$ consisting of the points whose coordinates are all pairwise distinct. Then G acts freely on Y and it can be checked, as a consequence of Hilbert's[2] Theorem 90, according to which the Galois cohomology set $H^1(k', \mathrm{GL}_n)$ is a singleton for any field k', that the resulting torsor $\pi : Y \to X = Y/G$ is versal (see [GMS03, Example 5.5]).

Example 1.5.3. Choose an embedding $G \hookrightarrow \mathrm{SL}_n(k)$ for some $n \geq 1$ and let G act on the algebraic group SL_n over k through this embedding by right multiplication. This action is free and it can again be checked, as a consequence of Hilbert's Theorem 90, that the resulting torsor $\pi : \mathrm{SL}_n \to \mathrm{SL}_n/G$ is versal. The argument for this is the same as in [GMS03, Example 5.5] once one knows that the Galois cohomology set $H^1(k', \mathrm{SL}_n)$ is a singleton for any field k'; the latter fact easily follows from Hilbert's Theorem 90.

Remark 1.5.4. Two varieties V and W over k are called *stably birationally equivalent* if $V \times \mathbf{A}^r_k$ and $W \times \mathbf{A}^s_k$ are birationally equivalent for some r, s. It can be shown that for any finite group G, the varieties $\mathbf{A}^m_k/G$ and SL_n/G appearing in Examples 1.5.2 and 1.5.3, for all values of m, n and all possible choices of embeddings $G \hookrightarrow S_m$ and $G \hookrightarrow \mathrm{SL}_n(k)$, all fall into the same stable birational equivalence class of varieties over k. This is the so-called "no-name lemma", see [CTS07, Corollary 3.9].

The notion of versality, in the context of these notes[3], is motivated by the following observation, which is an improved version of Corollary 1.3.3:

Proposition 1.5.5. *Let k be a number field. Let $S_0 \subset \Omega$ be a finite subset. Let G be a finite group. Suppose that there exist an irreducible smooth quasi-projective variety Y over k and a free action of G on Y satisfying the following two conditions:*

[2]Despite its name Hilbert's Theorem 90, this theorem, for arbitrary n, is due to Speiser [Spe19].

[3]Outside of the context discussed here, the notion of versality notably also gives rise to the definition of the "essential dimension" of a finite group G over a field k—this is the minimal dimension of a versal G-torsor defined over k—which is interesting in its own right and has been the focus of many works (see [BR97, BF03, Rei11, Mer13, Mer17, Rei21]). Even determining the essential dimension of $\mathbf{Z}/8\mathbf{Z}$ over $\mathbf{Q}$ is a highly nontrivial task (see [Flo08]).

(i) the variety $X = Y/G$ satisfies weak approximation off S_0, i.e. the diagonal embedding $X(k) \hookrightarrow \prod_{v\in\Omega\setminus S_0} X(k_v)$ has dense image;
(ii) the G-torsor $\pi : Y \to X$ is weakly versal.

Then Grunwald's problem admits a positive answer for G over k, for any finite subset $S \subset \Omega$ disjoint from S_0.

Proof. We shall need the following classical lemma, proved in [Poo17, Proposition 3.5.74] and whose statement holds for any finite étale morphism π.

Lemma 1.5.6 (Krasner)**.** *For $v \in \Omega$, the isomorphism class of the variety $\pi^{-1}(x_v)$ over k_v is a locally constant function of $x_v \in X(k_v)$ with respect to the v-adic topology.*

Fix Galois field extensions K_v/k_v for $v \in S$ as in Problem 1.1.1 and choose embeddings $\mathrm{Gal}(K_v/k_v) \hookrightarrow G$ for $v \in S$. By Remark 1.2.2, these choices give rise to G-torsors over k_v for $v \in S$. By weak versality, the latter come from k_v-points $x_v \in X(k_v)$.

Lemma 1.5.6 provides, for every $v \in S$, a neighbourhood $\mathscr{U}_v \subset X(k_v)$ of x_v such that $\pi^{-1}(x'_v)$ and $\pi^{-1}(x_v)$ are isomorphic, as varieties over k_v, for all $x'_v \in \mathscr{U}_v$. In particular, by Remark 1.2.2 again, for all $v \in S$ and all $x'_v \in \mathscr{U}_v$, the fibre $\pi^{-1}(x'_v)$ is isomorphic, over k_v, to a disjoint union of copies of $\mathrm{Spec}(K_v)$.

The weak versality of π also implies that $X(k) \neq \varnothing$. Theorem 1.3.5 therefore provides a nonempty open subset $\mathscr{U}^0 \subset \prod_{v\in\Omega\setminus(S\cup S_0)} X(k_v)$ such that $\pi^{-1}(x)$ is irreducible for all $x \in X(k) \cap \mathscr{U}^0$. Let $\mathscr{U} = \left(\prod_{v\in S} \mathscr{U}_v\right) \times \mathscr{U}^0$. As the variety X satisfies weak approximation off S_0, the set $X(k) \cap \mathscr{U}$ is nonempty. We fix $x \in X(k) \cap \mathscr{U}$.

The fibre $\pi^{-1}(x)$ is now an irreducible G-torsor (i.e. $\mathrm{Spec}(K)$ for some Galois field extension K/k with Galois group G) whose scalar extension from k to k_v, for each $v \in S$, is a disjoint union of copies of $\mathrm{Spec}(K_v)$. This proves the proposition. □

As smooth rational varieties satisfy weak approximation, one can apply Proposition 1.5.5 with $S_0 = \varnothing$ whenever the variety Y/G is rational and the torsor $Y \to Y/G$ is weakly versal. In view of Example 1.5.2, we deduce:

Corollary 1.5.7. *Given a finite group G and a number field k, a positive answer to Noether's problem for G and k implies a positive answer to Grunwald's problem for G and k, for any $S \subset \Omega$.*

Corollary 1.5.7 was first established by Saltman (see [Sal82, Theorem 5.1, Theorem 5.9]). As an example of an application, Corollary 1.5.7 implies that over any number field k, Grunwald's problem has a positive answer for S_n and for A_5 over k, without the need to exclude any place from $S \subset \Omega$ (see Example 1.4.2 and Example 1.4.4).

1.6. **Noether's problem: some counterexamples.** The hope that a positive solution to the inverse Galois problem might in general come from a positive solution to Noether's problem turned out, however, to be too optimistic. Indeed, Noether's problem seems to have a negative solution more often than not, as we briefly discuss below.

1.6.1. *Counterexamples among abelian groups.* Noether's problem has a negative answer even for cyclic groups over $\mathbf{Q}$. Swan and Voskresenskiĭ discovered, at the end of the 1960's, the counterexample $\mathbf{Z}/47\mathbf{Z}$ over $\mathbf{Q}$ (see [Swa69], [Vos70]). An even smaller counterexample, the group $\mathbf{Z}/8\mathbf{Z}$ over $\mathbf{Q}$, was then exhibited in [EM73], [Len74], [Vos73]. As Saltman [Sal82] later observed, Corollary 1.5.7 provides a direct proof that Noether's problem admits a negative answer for $\mathbf{Z}/8\mathbf{Z}$ over $\mathbf{Q}$. Indeed, by this corollary, it suffices to show that Grunwald's problem has a negative answer for $G = \mathbf{Z}/8\mathbf{Z}$, $k = \mathbf{Q}$ and $S = \varnothing$, and this is exactly what Wang had done in the 1940's:

Proposition 1.6.2 (Wang)**.** *In a cyclic field extension $K/\mathbf{Q}$ of degree 8, the prime 2 cannot be inert. In other words, the completion of a cyclic field extension $K/\mathbf{Q}$ of degree 8 at a place dividing 2 cannot be the unramified extension of $\mathbf{Q}_2$ of degree 8.*

An elementary proof can be found in [Swa83, p. 29, end of §5].

Further work on Noether's problem for abelian groups, by Endo, Miyata, Voskresenskiĭ and Lenstra, led to a complete characterisation, by Lenstra [Len74], of the stable rationality of the quotient $\mathbf{A}^n_k/G$ appearing in Problem 1.4.1 (and even of its rationality, in the case where G acts through its regular representation), when G is a finite abelian group and k is an arbitrary field. This characterisation is in terms of the arithmetic of cyclotomic number fields. For cyclic groups over $\mathbf{Q}$, it reads as follows (see [Len80, §3]):

Theorem 1.6.3 (Lenstra)**.** *Let $n \geq 1$ be an integer. Let $G = \mathbf{Z}/n\mathbf{Z}$ faithfully act on $\mathbf{A}^n_{\mathbf{Q}}$ by cyclically permuting the coordinates. The following conditions are equivalent:*

(1) The variety $\mathbf{A}^n_{\mathbf{Q}}/G$ is rational.
(2) The variety $\mathbf{A}^n_{\mathbf{Q}}/G$ is stably rational.
(3) The integer n is not divisible by 8, and for every prime factor p of n, if s denotes the p-adic valuation of n, the cyclotomic ring $\mathbf{Z}[\zeta_{(p-1)p^{s-1}}]$ contains an element whose norm is equal to p or to $-p$.

We recall that a variety is said to be *stably rational* if its product with an affine space of large enough dimension is rational. Stable rationality is known to be strictly weaker than rationality in general, even over $\mathbf{C}$, see [BCTSSD85].

Theorem 1.6.3 when n is a prime number is due to Voskresenskiĭ [Vos71]. Even when n is prime, determining whether condition (3) of Theorem 1.6.3 does or does not hold for a given n is in general a hard problem; for instance, it is only recently that this condition was shown to fail for $n = 59$ (see [Hos15, Added remark 3.2]). Even more recently, based on Theorem 1.6.3, on a height estimate due to Amoroso and Dvornicich [AD00] and on extensive computer calculations run by Hoshi [Hos15], among other tools, Plans [Pla17] was able to give a complete answer to Noether's problem for cyclic groups over $\mathbf{Q}$:

Theorem 1.6.4 (Plans)**.** *The conditions of Theorem 1.6.3 are equivalent to the following:*

(4) The integer n divides $2^2 \cdot 3^m \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 67 \cdot 71$ for some integer $m \geq 0$.

In particular, Noether's problem has a negative answer over $\mathbf{Q}$ for $G = \mathbf{Z}/p\mathbf{Z}$ for all but finitely many prime numbers p.

1.6.5. *Counterexamples over* $\mathbf{C}$. For non-abelian groups, Noether's problem has a negative answer even over $\mathbf{C}$. Saltman [Sal84] gave the first counterexamples over $\mathbf{C}$. His results were then generalised by Bogomolov [Bog88], who established the following theorem (see [CTS07, §7] and [GS17, §6.6] for accounts of its proof):

Theorem 1.6.6 (Bogomolov's formula). *Let $n \geq 1$ and $G \subset \mathrm{SL}_n(\mathbf{C})$ be a finite subgroup. The unramified Brauer group of the complex variety SL_n/G is isomorphic to*

$$\mathrm{Ker}\Big(H^2(G, \mathbf{Q}/\mathbf{Z}) \to \prod H^2(H, \mathbf{Q}/\mathbf{Z})\Big), \tag{1.6.7}$$

where the product ranges over all bicyclic *subgroups $H \subseteq G$ (i.e. abelian subgroups of G that are generated by at most two elements).*

We recall that the Brauer group, defined by Grothendieck as $H^2_{\text{ét}}(-, \mathbf{G}_\mathrm{m})$, is a stable birational invariant among smooth proper varieties over a field of characteristic 0, and that the *unramified Brauer group* of a variety over a field of characteristic 0 is by definition the Brauer group of any smooth proper variety birationally equivalent to it; for instance, the unramified Brauer group of $\mathbf{A}^n_\mathbf{C}$ is trivial. Thus, if the unramified Brauer group of a variety over $\mathbf{C}$ does not vanish, then this variety is not stably rational, a fortiori it is not rational. The unramified Brauer group was first considered and used as a tool for rationality questions by Saltman [Sal85, Sal84]. For smooth proper unirational varieties over $\mathbf{C}$, it coincides with the invariant that had earlier been employed by Artin and Mumford [AM72] to give "elementary" examples of complex unirational threefolds failing to be rational. For a thorough treatment of the Brauer group, we refer the reader to [CTS21].

In view of Remark 1.5.4, Bogomolov's formula gives an easy recipe for computing the unramified Brauer group of the variety $\mathbf{A}^n_\mathbf{C}/G$ that appears in Noether's problem over $\mathbf{C}$. The kernel (1.6.7) can be computed to be nonzero for some p-groups G, thus yielding counterexamples to Noether's problem over $\mathbf{C}$ (see [CTS07, Example 7.5], [GS17, §6.7]).

Other counterexamples over $\mathbf{C}$ were later produced by Peyre [Pey08] based on a further stable birational invariant introduced by Colliot-Thélène and Ojanguren [CTO89], called *unramified cohomology of degree* 3. The unramified Brauer group coincides with unramified cohomology of degree 2.

Many more results about Noether's problem can be found in the survey [Hos20].

1.7. **Retract rationality.** Saltman introduced a useful weakening of the notion of stable rationality: a variety X over a field k is said to be *retract rational* if there exist an integer $n \geq 1$, a dense open subset $U \subseteq \mathbf{A}^n_k$ and a morphism $U \to X$ that admits a rational section. Retract rationality is a stable birational invariant.

In the situation of Noether's problem, it can happen that the variety $\mathbf{A}^n_k/G$ fails to be rational and even to be stably rational, but is nevertheless retract rational. For instance this is so when $G = \mathbf{Z}/47\mathbf{Z}$ and $k = \mathbf{Q}$:

Theorem 1.7.1 (Saltman [Sal82]). *Taking up the notation of Problem 1.4.1, assume that G is abelian, that k has characteristic 0, and, letting 2^r denote the highest power of 2 that divides the exponent of G, that the cyclotomic field extension $k(\zeta_{2^r})/k$ is cyclic. Then the quotient $\mathbf{A}^n_k/G$ is retract rational over k.*

Theorem 1.7.1 can in particular be applied to all finite abelian groups of odd order. Thus, retract rationality is weaker than rationality (compare with Theorem 1.6.4). Nevertheless, as far as the applications to the inverse Galois problem are concerned, it is just as good: indeed, as Saltman observed, smooth retract rational varieties over number fields are easily seen to satisfy weak approximation, so that Proposition 1.5.5 can be applied with $S_0 = \varnothing$ whenever the variety Y/G is retract rational and the torsor $Y \to Y/G$ is weakly versal.

Combining this observation with Theorem 1.7.1 and with Proposition 1.5.5, we deduce, in view of Example 1.5.2, that Grunwald's problem has a positive answer over any number field k, without excluding any place, for all abelian groups G satisfying the assumption of Theorem 1.7.1—a conclusion that already resulted from the Grunwald–Wang theorem, but whose proof now fits into the framework of Hilbert's and Noether's general strategy, even though, according to Theorem 1.6.4, Noether's problem itself has a negative answer for many of these groups G (perhaps even for "almost all" of them?).

Conversely, by the same token, Wang's negative answer to Grunwald's problem (see Proposition 1.6.2) implies that when $G = \mathbf{Z}/8\mathbf{Z}$ and $k = \mathbf{Q}$, the quotient $\mathbf{A}^n_k/G$ fails not only to be stably rational but also to be retract rational. Similarly, the negative answers to Noether's problem over $\mathbf{C}$ discussed in §1.6.5 are in fact counterexamples to the retract rationality of the quotients $\mathbf{A}^n_{\mathbf{C}}/G$ in question. Thus, despite the wider scope of applicability of the Hilbert–Noether method when rationality is replaced with the weaker notion of retract rationality, further ideas are necessary to address arbitrary finite groups.

2. Regular inverse Galois problem

2.1. **Statement.** We saw, in §1, that Noether's problem does not always admit a positive answer, i.e. the quotient variety $\mathbf{A}^n_k/G$ can fail to be rational, or stably rational, or even retract rational. A simple way out, if one still wants to apply Hilbert's irreducibility theorem, is to look for rational *subvarieties* of $\mathbf{A}^n_k/G$, in particular rational curves. To take advantage of the geometry of the situation, it is natural to focus on those rational curves whose inverse image in $\mathbf{A}^n_k$ is geometrically irreducible and meets the locus $Y \subset \mathbf{A}^n_k$ on which G acts freely. By the versality of the torsor $Y \to Y/G$ (Example 1.5.2), finding such curves is the same as solving the *regular inverse Galois problem* (when k is perfect):

Problem 2.1.1 (regular inverse Galois)**.** *Let k be a field. Let G be a finite group. Do there exist a smooth, projective, geometrically irreducible curve C over k and a finite morphism $\pi : C \to \mathbf{P}^1_k$ such that the corresponding extension of function fields $k(C)/k(t)$ is Galois with* $\mathrm{Gal}(k(C)/k(t)) \simeq G$*?*

When k is a perfect field, this is equivalent to asking for the existence of a field extension of $k(t)$ with Galois group G in which k is algebraically closed, i.e. a field extension that is regular over k. Following standard practice, we shall refer to such a field extension as a *regular Galois extension of $k(t)$ with group G*.

When k is a number field, a positive answer to Problem 2.1.1 for k and G implies a positive answer to the inverse Galois problem for k and G, by Hilbert's irreducibility theorem. Over an arbitrary field and for an arbitrary finite group, the inverse Galois problem and Noether's problem both have negative answers in general, as we have seen; in contrast, Problem 2.1.1 might well always have a positive answer.

Remark 2.1.2. It follows from the Bertini theorem that if k is infinite and perfect, a positive answer to Noether's problem for k and G implies a positive answer to the regular inverse Galois problem for k and G (see [Jou83, Théorème 6.3]). In fact, for such k, one can check that the retract rationality of $\mathbf{A}^n_k/G$ already implies a positive answer to the regular inverse Galois problem for k and G.

2.2. **Riemann's existence theorem.** A solution to the regular inverse Galois problem over k gives rise, by scalar extension, to a solution over any field extension of k. Thus, in order to find a solution over $\mathbf{Q}$, it is necessary to first solve the problem over $\mathbf{C}$ and over $\bar{\mathbf{Q}}$. The key tool for this is Riemann's existence theorem, which allows one to transform this algebraic question into a purely topological one.

Theorem 2.2.1 (Riemann's existence theorem). *Let k be an algebraically closed subfield of $\mathbf{C}$. Let X be a variety over k. The natural functor*

$$\Big(\textit{étale coverings of } X\Big) \to \Big(\textit{finite topological coverings of } X(\mathbf{C})\Big)$$

that maps $Y \to X$ to $Y(\mathbf{C}) \to X(\mathbf{C})$ is an equivalence of categories.

An *étale covering* of X is a variety over k endowed with a finite étale morphism to X. A topological covering is *finite* if its fibres are finite. Theorem 2.2.1 in the above formulation is proved in [Gro03]. To be precise, the case where $k = \mathbf{C}$ is [Gro03, Exp. XII, Théorème 5.1] and builds on Grothendieck's reworking of Serre's GAGA theorems; the case of an arbitrary algebraically closed subfield of $\mathbf{C}$ then results from it by [Gro03, Exp. XIII, Corollaire 3.5].

Corollary 2.2.2. *Let k be an algebraically closed subfield of $\mathbf{C}$. Let X be a connected variety over k. Let $x \in X(k)$. For any finite group G, isomorphism classes of G-torsors (resp. of connected G-torsors) $Y \to X$ endowed with a lift $y \in Y(k)$ of x are canonically in one-to-one correspondence with homomorphisms $\pi_1(X(\mathbf{C}), x) \to G$ (resp. with surjective homomorphisms $\pi_1(X(\mathbf{C}), x) \twoheadrightarrow G$). Changing the choice of y amounts to conjugating the homomorphism by an element of G.*

Proof. Indeed, this follows from Theorem 2.2.1 combined with the well-known equivalence of categories between the category of topological coverings of $X(\mathbf{C})$ and the category of sets endowed with an action of $\pi_1(X(\mathbf{C}), x)$ (see [Sza09, Theorem 2.3.4]). The homomorphism $\pi_1(X(\mathbf{C}), x) \to G$ corresponding to $Y \to X$ sends $\gamma \in \pi_1(X(\mathbf{C}), x)$ to the unique $g \in G$ such that $\gamma y = yg$, where we are taking the convention that the action of G on Y is a right action and that the monodromy action of $\pi_1(X(\mathbf{C}), x)$ on the fibre of $Y(\mathbf{C}) \to X(\mathbf{C})$ above x is a left action. □

Remark 2.2.3 (reminder on monodromy groups and Galois groups). Let k and X be as in Corollary 2.2.2. Let $x \in X(\mathbf{C})$. The *monodromy group* M of an étale covering $Y \to X$ is, by definition, the largest quotient of $\pi_1(X(\mathbf{C}), x)$ through which the monodromy action of this group on the fibre of $Y(\mathbf{C}) \to X(\mathbf{C})$ above x factors. Assume that X is normal and irreducible and let $Y' \to Y \to X$ be a tower of irreducible étale coverings such that the field extension $k(Y')/k(X)$ is a Galois closure of $k(Y)/k(X)$. Let $G = \mathrm{Gal}(k(Y')/k(X))$. Then $Y' \to X$ is the normalisation of X in $k(Y')$; as such, it receives an action of G, with respect to which it is a G-torsor; in addition, the surjective homomorphism $\pi_1(X(\mathbf{C}), x) \twoheadrightarrow G$ that Corollary 2.2.2 associates with $Y' \to X$ and with the choice of a lift $y' \in Y'(k)$ of x induces an isomorphism $M \xrightarrow{\sim} G$. (Changing the choice of the lift y' amounts to composing this isomorphism with an inner automorphism.) Thus, computing the Galois group of the Galois closure of the field extension $k(Y)/k(X)$ is tantamount to computing a monodromy group in the topological setting.

2.3. **Classifying Galois covers of the projective line over $\mathbf{C}$ or over $\bar{\mathbf{Q}}$.** Let us apply Theorem 2.2.1 to the open subsets of the projective line. The fundamental group of the complement of finitely many points in $\mathbf{P}^1(\mathbf{C})$ is easy to describe:

Proposition 2.3.1. *Let $X \subseteq \mathbf{P}^1_{\mathbf{C}}$ be a dense open subset. Write $\mathbf{P}^1_{\mathbf{C}} \setminus X = \{b_1, \dots, b_r\}$. Let $x \in X(\mathbf{C})$. The group $\pi_1(X(\mathbf{C}), x)$ admits a presentation with r generators $\gamma_1, \dots, \gamma_r$ and a unique relation $\gamma_1 \cdots \gamma_r = 1$, such that γ_i belongs, for every $i \in \{1, \dots, r\}$, to the conjugacy class in $\pi_1(X(\mathbf{C}), x)$ of a local counterclockwise loop around b_i.*

What the last sentence of Proposition 2.3.1 means is this: if N_i denotes a small enough open neighbourhood of b_i in $\mathbf{P}^1(\mathbf{C})$ that is biholomorphic to the unit disc, then a loop contained in $N_i \setminus \{b_i\}$ and going once around b_i in the counterclockwise direction gives rise, after choosing a path from x to a point of this loop, to an element of $\pi_1(X(\mathbf{C}), x)$ whose conjugacy class does not depend on the chosen path. The content of Proposition 2.3.1 is that these paths can be chosen in such a way that the γ_i generate $\pi_1(X(\mathbf{C}), x)$ and satisfy the relation $\gamma_1 \cdots \gamma_r = 1$. This is elementary and well-known.

Using Proposition 2.3.1, we can draw the following corollary from Riemann's existence theorem. Corollary 2.3.2 completely describes G-torsors over dense open subsets of the projective line over algebraically closed subfields of $\mathbf{C}$, and implies a positive solution to the regular inverse Galois problem over such fields. (The notation $\mathrm{ni}_r^*(G)$ appearing in its statement refers to the name Nielsen, see [Völ96, §9.2], [RW06, §3.1].)

Corollary 2.3.2. *Let k be an algebraically closed subfield of $\mathbf{C}$. Let $X \subseteq \mathbf{P}^1_k$ be a dense open subset. Write $\mathbf{P}^1_{\mathbf{C}} \setminus X = \{b_1, \dots, b_r\}$. Let G be a finite group. Consider the set of r-tuples $(g_1, \dots, g_r) \in G^r$ such that $g_1 \cdots g_r = 1$ and that $g_1, \dots, g_r$ generate G. Let $\mathrm{ni}_r^*(G)$ denote the quotient of this set by the action of G by simultaneous conjugation. The set of isomorphism classes of irreducible G-torsors over X is in bijection with $\mathrm{ni}_r^*(G)$ (through a bijection that is canonically determined once a presentation of $\pi_1(X(\mathbf{C}), x)$ as in Proposition 2.3.1 is fixed).*

Proof. By Corollary 2.2.2, isomorphism classes of irreducible G-torsors over X are canonically in one-to-one correspondence with conjugacy classes of surjections $\pi_1(X(\mathbf{C}), x) \twoheadrightarrow G$. Apply Proposition 2.3.1 to conclude. □

Corollary 2.3.3. *For any finite group G, the regular inverse Galois problem admits a positive answer over $\bar{\mathbf{Q}}$.*

Proof. Let r be an integer, large enough that G can be generated by $r-1$ elements. Pick r points of $\mathbf{P}^1(\bar{\mathbf{Q}})$ and let $X \subset \mathbf{P}^1_{\bar{\mathbf{Q}}}$ denote their complement. As $\mathrm{ni}^*_r(G) \neq \varnothing$, Corollary 2.3.2 ensures the existence of an irreducible G-torsor $p : Y \to X$. As Y is normal and p is finite, the normalisation of $\mathbf{P}^1_{\bar{\mathbf{Q}}}$ in the function field of Y is a smooth curve C over $\bar{\mathbf{Q}}$ containing Y as a dense open subset, equipped with a finite morphism $\pi : C \to \mathbf{P}^1_{\bar{\mathbf{Q}}}$ that extends p. As p is a G-torsor, the function field extension $\bar{\mathbf{Q}}(C)/\bar{\mathbf{Q}}(t)$ is Galois with group G (see §1.2). □

2.4. **Monodromy of some non-Galois covers of the projective line.** Proposition 2.3.1 is also useful for computing the monodromy of ramified covers of the complex projective line that are not necessarily Galois, via the following result.

Proposition 2.4.1. *Let C be a smooth, projective, irreducible curve over $\mathbf{C}$, endowed with a finite morphism $\pi : C \to \mathbf{P}^1_{\mathbf{C}}$. Let $X \subseteq \mathbf{P}^1_{\mathbf{C}}$ be a dense open subset over which π is étale. Fix $x \in X(\mathbf{C})$ and write $\mathbf{P}^1_{\mathbf{C}} \setminus X = \{b_1, \dots, b_r\}$. Let M denote the monodromy group of π, i.e. the largest quotient of $\pi_1(X(\mathbf{C}), x)$ that still acts on $\pi^{-1}(x)$. After choosing a bijection $\pi^{-1}(x) \simeq \{1, \dots, n\}$, we view M as a transitive subgroup of the symmetric group S_n. There exist $\mu_1, \dots, \mu_r \in M$ satisfying the following three properties:*

1. *the elements $\mu_1, \dots, \mu_r$ generate the group M;*
2. *their product $\mu_1 \cdots \mu_r$ is the identity of M;*
3. *for each $i \in \{1, \dots, r\}$, the element $\mu_i \in S_n$ is a product of cycles whose lengths are the ramification indices of π at the points of $\pi^{-1}(b_i)$.*

Proof. Applying Proposition 2.3.1 and letting μ_i denote the image of γ_i in M, we obtain (1) and (2). Property (3) only depends on the conjugacy class of γ_i and is a standard calculation of the monodromy of the étale coverings of the punctured unit disc. □

Example 2.4.2. Let C be a smooth, projective, irreducible curve over an algebraically closed subfield k of $\mathbf{C}$, endowed with a morphism $\pi : C \to \mathbf{P}^1_k$ of degree $n \geq 1$. Assume that all ramification points have ramification index 2 and that no two of them lie in the same fibre of π. Then the Galois group of a Galois closure of the function field extension $k(C)/k(t)$ is the full symmetric group S_n. Indeed, Remark 2.2.3 and Proposition 2.4.1 show that this Galois group is a transitive subgroup of S_n generated by transpositions; the only such subgroup is S_n itself.

Remark 2.4.3. Let k be a field of characteristic 0. Let $k(t) \subseteq K \subseteq K' \subset \overline{k(t)}$ be a tower of fields, where $\overline{k(t)}$ denotes an algebraic closure of $k(t)$, where $K/k(t)$ is a finite extension and where $K'/k(t)$ is its Galois closure inside $\overline{k(t)}$. Let us assume that k is algebraically closed in K. The field k need not, in general, be algebraically closed in K'. (For example, if $k = \mathbf{Q}$ and $K = \mathbf{Q}(t^{1/n})$, then $K' = \mathbf{Q}(\zeta_n)(t^{1/n})$, where ζ_n denotes a primitive nth root of unity.) This pathology, however, cannot occur if the underlying topological monodromy group is the full symmetric group, or, more generally, if it is a self-normalising subgroup of the ambient symmetric group. Indeed, let k' denote the algebraic closure of k in K', set $G = \mathrm{Gal}(K'/k(t))$ and $G_{\mathrm{geom}} = \mathrm{Gal}(K'/k'(t))$. Letting $\bar{k}$ denote the algebraic closure of k in $\overline{k(t)}$, we remark that $K' \otimes_{k'} \bar{k}$ and $K \otimes_k \bar{k}$ are fields and that the field extension

$K' \otimes_{k'} \bar{k}/\bar{k}(t)$ is a Galois closure of $K \otimes_k \bar{k}/\bar{k}(t)$, so that its Galois group G_{geom} can be viewed as the topological monodromy group associated with $K/k(t)$ (see Remark 2.2.3). Fix a primitive element $\alpha_1 \in K$ over $k(t)$. Denote by $\alpha_1, \dots, \alpha_n \in K'$ the collection of its Galois conjugates. As G acts faithfully on the α_i's, there is a sequence of inclusions $G_{\mathrm{geom}} \subseteq G \subseteq S_n$. As k'/k is a Galois field extension, the group G_{geom} is normal in G; hence, if G_{geom} is self-normalising in S_n, then $G = G_{\mathrm{geom}}$ and k is algebraically closed in K'. Thus, for instance, if the curve C and the morphism π of Example 2.4.2 come by scalar extension from a curve and a morphism defined over $\mathbf{Q}$, and if $K/\mathbf{Q}(t)$ denotes the function field extension given by the latter morphism, then a Galois closure of $K/\mathbf{Q}(t)$ has Galois group S_n.

In conjunction with Remark 2.4.3, Example 2.4.2 leads to many concrete examples of regular Galois extensions of $\mathbf{Q}(t)$ with group S_n. Let us recall, however, that the mere existence of regular Galois extensions of $\mathbf{Q}(t)$ with group S_n already followed from the positive answer to Noether's problem for S_n over $\mathbf{Q}$ (see Example 1.4.2 and Remark 2.1.2). As Noether's problem is open for the alternating group A_n over $\mathbf{Q}$ as soon as $n \geq 6$, it is of interest to note that Proposition 2.4.1 also leads to concrete examples of regular Galois extensions of $\mathbf{Q}(t)$ with group A_n for all values of n, as we now illustrate.

Example 2.4.4. Let C be a smooth, projective, geometrically irreducible curve over a subfield k of $\mathbf{C}$, endowed with a morphism $\pi : C \to \mathbf{P}^1_k$ of degree $n \geq 3$. Assume that π has exactly three ramification points, that these ramification points are rational points of C lying above $0, 1, \infty \in \mathbf{P}^1(k)$, with ramification indices e_0, e_1, e_∞, respectively, and that $(e_0, e_1, e_\infty) = (n, n-1, 2)$ if n is even and $(e_0, e_1, e_\infty) = (n-1, n, 2)$ if n is odd. Let $K'/k(t)$ denote a Galois closure of the function field extension $k(C)/k(t)$. We first note that K' is a regular Galois extension of $k(t)$ with group S_n. Indeed, when k is algebraically closed, Remark 2.2.3 and Proposition 2.4.1 imply that $\mathrm{Gal}(K'/k(t))$ is a transitive subgroup of S_n that contains a cycle of order $n-1$ and a transposition, but the only such subgroup is S_n itself (see [Ser07, Lemma 4.4.3]); by Remark 2.4.3, the case of arbitrary k follows. Secondly, we claim that there exists $\alpha \in k^*$ such that αt is a square in K'. Setting $u = \sqrt{\alpha t}$, this will imply that K' is a regular Galois extension of $k(u)$ with group A_n (where u can now be viewed as a free variable), as desired. To verify this claim, we note that the topological monodromy of the double cover of $\mathbf{P}^1_k$ corresponding to the (unique) quadratic subextension $L/k(t)$ of $K'/k(t)$ is obtained by composing the topological monodromy of π with the signature morphism $S_n \to \mathbf{Z}/2\mathbf{Z}$. As the local monodromy of π at 1 is given by a cycle of odd length, it follows that $L/k(t)$ is unramified outside of 0 and ∞, and, hence, that $L = k(\sqrt{\alpha t})$ for some $\alpha \in k^*$ (as k is algebraically closed in L).

For explicit equations to which Example 2.4.4 can be applied, see [Ser07, §4.5].

2.5. **Looking for covers over non-algebraically closed ground fields.** Now that we know that the regular inverse Galois problem has a positive answer over $\bar{\mathbf{Q}}$, we can try to find solutions over $\mathbf{Q}$ or at least over overfields of $\mathbf{Q}$ as small as possible. This has been achieved over the completions of $\mathbf{Q}$, thus yielding, for all finite groups, a positive answer to the regular inverse Galois problem over $\mathbf{R}$ (Krull and Neukirch [KN71]) and over the field $\mathbf{Q}_p$ of p-adic numbers for every prime p (Harbater [Har87]). Pop [Pop96] generalised these results as follows[4,5]:

Theorem 2.5.1 (Harbater and Pop)**.** *The regular inverse Galois problem has a positive answer over any large field, for any finite group.*

By definition, a field k is *large* when every smooth curve over k that has a rational point has infinitely many of them. Examples include all fields that are complete with respect to an absolute value, such as $\mathbf{R}$ and $\mathbf{Q}_p$, as well as infinite algebraic extensions of finite fields or more generally all so-called pseudo-algebraically closed fields (fields over which every smooth geometrically connected curve has infinitely many rational points).

The proofs of Theorem 2.5.1 given by Harbater and by Pop rely, in the formal or in the rigid analytic context over a complete discretely valued ground field, on the construction, by patching, of appropriate "topological coverings", and on a variant, in the corresponding context, of Riemann's existence theorem. Over $\mathbf{C}$, the underlying patching construction is presented in [Sza09, §3.5].

Theorem 2.5.1 had previously been established by Fried and Völklein [FV91] in the case of pseudo-algebraically closed fields of characteristic 0. From this special case they deduced the following result in positive characteristic:

Theorem 2.5.2 (Fried and Völklein)**.** *Let G be a finite group. The regular inverse Galois problem has a positive answer for G over $\mathbf{F}_p(t)$ for all but finitely many primes p.*

Colliot-Thélène later shed new light on Theorem 2.5.1 by recasting it as a theorem about the existence of suitable rational curves on the varieties $\mathbf{A}^n_k/G$ appearing in Noether's problem, and by noting that even though these varieties can fail to be rational, they are in any case *rationally connected*, which opens the door to applications of the theory of deformation of rational curves on rationally connected varieties over large fields—a theory developed, in great generality, by Kollár [Kol99]. Over large fields of characteristic 0, a geometric proof of Theorem 2.5.1 that proceeds by constructing rational curves on $\mathbf{A}^n_k/G$ was thus given in [CT00]. See also [Kol00], [Kol03], [MB01] for generalisations.

Unfortunately, no method for the systematic construction of rational curves on rationally connected varieties over $\mathbf{Q}$ is known; more generally, the various methods on which all known proofs of Theorem 2.5.1 rely fall short of solving any case of the regular inverse Galois problem over a given number field. As of today, all known constructions of realisations of finite groups as regular Galois groups over $\mathbf{Q}$ exploit more or less ad hoc ideas. One of the most successful approaches is the rigidity method, initiated by Shih, Fried, Belyi, Matzat and Thompson in the 1970's and the 1980's, which we discuss next, in §§2.6–2.7.

[4] It is not immediately clear that the article [Pop96] establishes Theorem 2.5.1 as we have stated it, without assuming the field to be perfect: in our definition of the regular inverse Galois problem, the sought-for field extension of $k(t)$ was required to admit a *smooth* projective model, which could fail over imperfect fields. However, in any case, Theorem 2.5.1 as we have stated it is proved in [MB01, Théorème 1.1].

[5] Theorem 2.5.1 (at least for perfect large fields, see the previous footnote) also follows from the results of Harbater [Har87], see [Har95, §4.5].

Remark 2.5.3. In practice, the rigidity method is particularly useful for realising finite simple groups. Considering the regular inverse Galois problem for various classes of non-simple groups, especially central extensions, also leads to interesting challenges, better dealt with by other methods. We refer the reader to the work of Mestre [Mes90, Mes94, Mes98], who solved it for the central extensions of A_n for all n, as well as for $\mathrm{SL}_2(\mathbf{F}_7)$ and for the unique nontrivial central extension of the Mathieu group M_{12} by $\mathbf{Z}/2\mathbf{Z}$ (starting from known regular realisations of $\mathrm{PSL}_2(\mathbf{F}_7)$ and of M_{12}). To put these results into perspective, let us note that Noether's problem has negative answers, over $\mathbf{Q}$, for the unique nontrivial central extensions of A_6 and of A_7 by $\mathbf{Z}/2\mathbf{Z}$ (Serre [GMS03, Theorem 33.25]).

2.6. **Hurwitz spaces.** Even though Hurwitz spaces are not necessary for the description and the implementation of the rigidity method, their introduction makes the theory rather transparent; in addition, they are indeed indispensable for some of its refinements. Hurwitz spaces are moduli spaces of smooth projective irreducible covers of the projective line. We shall consider them only in characteristic 0. In addition, we shall restrict attention to the moduli space of G-covers; the term "G-cover" is another name for the regular Galois extensions of $k(t)$ with group G that we have been considering since the beginning of §2:

Definition 2.6.1. Let G be a finite group. Let k be a field. A *G-cover* over k is a smooth, proper, geometrically irreducible curve C over k endowed, on the one hand, with a finite morphism $\pi : C \to \mathbf{P}^1_k$ such that the corresponding extension of function fields $k(C)/k(t)$ is Galois, and, on the other hand, with an isomorphism $G \xrightarrow{\sim} \mathrm{Gal}(k(C)/k(t))$. (In particular G acts faithfully on C and the morphism $\pi^{-1}(U) \to U$ induced by π is a G-torsor for any dense open subset $U \subset \mathbf{P}^1_k$ above which π is étale.)

The group of automorphisms of any G-cover, i.e. the group of automorphisms of C that respect not only the morphism π but also the given isomorphism $G \xrightarrow{\sim} \mathrm{Gal}(k(C)/k(t))$, is the centre of G. We shall assume, until the end of §2, that G has trivial centre. This is not too serious a restriction (as any finite group is a quotient of a finite group with trivial centre, see [FV91, Lemma 2]) and it will ensure that our moduli space is a variety rather than a stack (as the objects that we want to classify have no nontrivial automorphism).

To prepare for the statement of the next theorem, we need to introduce some notation. When k has characteristic 0, the *branch locus* of $\pi : C \to \mathbf{P}^1_k$ is by definition the smallest reduced 0-dimensional subvariety B of $\mathbf{P}^1_k$ such that π is étale over $\mathbf{P}^1_k \setminus B$. Its *degree* is the cardinality of $B(\bar{k})$, where $\bar{k}$ denotes an algebraic closure of k. For any integer $r \geq 1$, we denote by $\mathscr{U}^r \subset (\mathbf{P}^1_{\mathbf{Q}})^r$ the locus of r-tuples with pairwise distinct components, and by $\mathscr{U}_r$ the quotient of $\mathscr{U}^r$ by the natural action of the symmetric group S_r. Thus $\mathscr{U}_r$ is a smooth variety over $\mathbf{Q}$, and for any field k of characteristic 0, the set $\mathscr{U}_r(k)$ can be identified with the set of reduced 0-dimensional subvarieties of $\mathbf{P}^1_k$ of degree r, i.e. with the set of subsets of $\mathbf{P}^1(\bar{k})$ of cardinality r that are stable under $\mathrm{Gal}(\bar{k}/k)$.

Theorem 2.6.2 (Fried and Völklein [FV91])**.** *Let G be a finite group with trivial centre and $r \geq 1$ be an integer. With G and r, one can canonically associate a smooth variety $\mathscr{H}_{G,r}$ over $\mathbf{Q}$ such that for any field k of characteristic 0, the set $\mathscr{H}_{G,r}(k)$ is the set of isomorphism* *classes of G-covers over k whose branch locus has degree r. It is equipped with a finite étale morphism $\rho : \mathscr{H}_{G,r} \to \mathscr{U}_r$ that maps the isomorphism class of a G-cover to its branch locus.*

The variety $\mathscr{H}_{G,r}$ is called a *Hurwitz space*.

A modern approach to Theorem 2.6.2 consists in defining G-covers not just over fields, as in Definition 2.6.1, but more generally over schemes; one then proves that the resulting moduli functor on the category of schemes of characteristic 0 is representable, by $\mathscr{H}_{G,r}$. This is the approach adopted by Wewers [Wew98], who works more generally over $\mathbf{Z}$ (with tame covers) and without assuming that the centre of G is trivial (thus obtaining a moduli stack $\mathscr{H}_{G,r}$). See [RW06].

We note that Hurwitz spaces were first contemplated by Hurwitz [Hur91], and, with a functorial point of view, by Fulton [Ful69]. However, these authors only considered (non-Galois) covers with "simple" ramification, i.e. such that all ramification points have ramification index 2 and no two of them lie over the same branch point. This is insufficient for the purposes of the regular inverse Galois problem (see Example 2.4.2).

Let us come back to our motivation. It is tautological that for any finite group G with trivial centre, the regular inverse Galois problem admits a positive answer for G over $\mathbf{Q}$ if and only if there exists an integer $r \geq 1$ such that $\mathscr{H}_{G,r}(\mathbf{Q}) \neq \varnothing$. For the question of the existence of a rational point on one of the varieties $\mathscr{H}_{G,r}$ to be tractable, one needs, in turn, some understanding of their geometry.

The varieties $\mathscr{H}_{G,r}$ can be described in a very explicit combinatorial fashion, at least geometrically, thanks to the finite étale morphism $\rho : \mathscr{H}_{G,r} \to \mathscr{U}_r$ given by Theorem 2.6.2. Let us pick up the notation $\mathrm{ni}^*_r(G)$ introduced in Corollary 2.3.2 and write $\mathrm{ni}_r(G) \subseteq \mathrm{ni}^*_r(G)$ for the subset formed by the conjugacy classes of those r-tuples $(g_1, \dots, g_r)$ such that none of the g_i's is equal to 1. It then follows from (the proof of) Corollary 2.3.2 that the fibre of ρ above any complex point of $\mathscr{U}_r$ can be identified with $\mathrm{ni}_r(G)$. In addition, the fundamental group of $\mathscr{U}_r(\mathbf{C})$ admits a down-to-earth presentation (as a quotient of the Artin braid group by one relation) and its action on $\mathrm{ni}_r(G)$ can also be made explicit (see [FV91, §1.3]). Thus, for instance, the task of describing the irreducible components of the variety $(\mathscr{H}_{G,r})_{\bar{\mathbf{Q}}}$ becomes equivalent to that of computing the orbits of a certain action of the braid group on $\mathrm{ni}_r(G)$. Unfortunately, as r increases, even this "simple" task quickly becomes computationally infeasible for modern computers (see e.g. [Hä22]).

2.7. **The rigidity method.** This method consists in cleverly identifying irreducible components of $\mathscr{H}_{G,r}$ that contain rational points for somehow "trivial" reasons. To explain it, we need to refine the étale covering ρ that appears in Theorem 2.6.2.

2.7.1. *Algebraic local monodromy.* Let k be a field of characteristic 0. Let $\pi : C \to \mathbf{P}^1_k$ be a G-cover over k. Let $b_i \in \mathbf{P}^1(k)$ be a rational branch point. Let $X \subset \mathbf{P}^1_k$ be a dense open subset over which π is étale.

Under the assumption that k is a subfield of $\mathbf{C}$, we have associated with π and b_i, in §2.3, a canonical conjugacy class of G, namely the conjugacy class of the element g_i appearing in Corollary 2.3.2. This is the "local monodromy" of π at b_i. We recall that it is the image, by a surjection $\pi_1(X(\mathbf{C}), x) \twoheadrightarrow G$ that is well-defined up to conjugation, of the conjugacy class of a local counterclockwise loop around b_i. To make this topological definition fit in with the moduli picture of Theorem 2.6.2 and in particular to understand how it behaves with respect to the action of the group of automorphisms of k, we need to make it algebraic.

We do this as follows. Let $\bar{k}$ be an algebraic closure of k. The completion $\bar{k}(t)_{b_i}$ of $\bar{k}(t)$ at the discrete valuation defined by b_i is isomorphic to the field of formal power series $\bar{k}((u))$, whose algebraic closure is the field of Puiseux series $\bigcup_{n\geq 1} \bar{k}((u^{1/n}))$. By Kummer theory, the absolute Galois group of $\bar{k}(t)_{b_i}$ is canonically isomorphic to $\hat{\mathbf{Z}}(1)_{\bar{k}} = \varprojlim_{n\geq 1} \boldsymbol{\mu}_n(\bar{k})$. The inclusion of fields $\bar{k}(t) \hookrightarrow \bar{k}(t)_{b_i}$ induces a continuous homomorphism in the reverse direction, well-defined up to conjugation, between their absolute Galois groups; hence it induces a continuous homomorphism $\hat{\mathbf{Z}}(1)_{\bar{k}} \to G$, well-defined up to conjugation by an element of G. This conjugacy class of homomorphisms $\hat{\mathbf{Z}}(1)_{\bar{k}} \to G$ is the analogue of the g_i from Corollary 2.3.2. We call it the *algebraic local monodromy* of π at b_i.

Remarks 2.7.2. (i) When k is a subfield of $\mathbf{C}$, one can use the generator $\zeta_n = e^{2i\pi/n}$ of $\boldsymbol{\mu}_n(\bar{k})$ to identify $\hat{\mathbf{Z}}(1)_{\bar{k}}$ with $\hat{\mathbf{Z}}$ as topological groups (i.e. disregarding Galois actions). The algebraic local monodromy of π at b_i then becomes identified with a conjugacy class of G. One verifies that through this identification, the algebraic local monodromy of π at b_i coincides with the conjugacy class of g_i from Corollary 2.3.2.

(ii) The natural action of $\mathrm{Gal}(\bar{k}/k)$ on $\hat{\mathbf{Z}}(1)_{\bar{k}}$ induces an action of $\mathrm{Gal}(\bar{k}/k)$ on the set of conjugacy classes of homomorphisms $\hat{\mathbf{Z}}(1)_{\bar{k}} \to G$. It therefore makes sense to consider the conjugates, under this action of $\mathrm{Gal}(\bar{k}/k)$, of the algebraic local monodromy of π at b_i. (We recall that $b_i \in \mathbf{P}^1(k)$.) This feature of the algebraic point of view plays a crucial rôle in the rigidity method. It is not visible on the topological side of the identification of Remark 2.7.2 (i), except when $k = \mathbf{R}$. Indeed, in this case, complex conjugation acts by multiplication by -1 on $\hat{\mathbf{Z}}(1)_{\bar{k}}$, hence maps the algebraic local monodromy of π at b_i to its "inverse"; while on the topological side, it sends a local counterclockwise loop around b_i to a local clockwise loop around b_i, and hence again it maps the conjugacy class of g_i to the conjugacy class of g_i^{-1}.

(iii) For an arbitrary field k of characteristic 0, the choice of a topological generator of the procyclic group $\hat{\mathbf{Z}}(1)_{\bar{k}}$ should be thought of as an algebraic analogue of the choice of an orientation of the punctured unit disc (an insight of Grothendieck, see [Del73, (2.1)]), as is illustrated by Remark 2.7.2 (ii).

2.7.3. *Factoring ρ.* The natural action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on the finite set $\mathrm{Hom}_{\mathrm{cont}}\Big(\hat{\mathbf{Z}}(1)_{\bar{\mathbf{Q}}}, G\Big)$ of continuous homomorphisms $\hat{\mathbf{Z}}(1)_{\bar{\mathbf{Q}}} \to G$ induces a continuous action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on the quotient of this finite set by the conjugation action of G. As the functor

$$\Big(\text{reduced 0-dimensional varieties over } \mathbf{Q}\Big) \to \left(\begin{array}{c}\text{finite sets endowed with a}\\ \text{continuous action of } \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})\end{array}\right)$$

that sends a variety Z to the set $Z(\bar{\mathbf{Q}})$ is an equivalence of categories, we can canonically associate with G a reduced 0-dimensional variety $\mathscr{C}_G$ over $\mathbf{Q}$ such that

$$\mathscr{C}_G(\bar{\mathbf{Q}}) = \mathrm{Hom}_{\mathrm{cont}}\Big(\hat{\mathbf{Z}}(1)_{\bar{\mathbf{Q}}}, G\Big)/(\text{conjugation by } G),$$

compatibly with the natural continuous actions of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on both sides. One then has a canonical $\mathrm{Gal}(\bar{k}/k)$-equivariant identification

$$\mathscr{C}_G(\bar{k}) = \mathrm{Hom}_{\mathrm{cont}}\Big(\hat{\mathbf{Z}}(1)_{\bar{k}}, G\Big)/(\text{conjugation by } G)$$

for any field k of characteristic 0, with algebraic closure $\bar{k}$.

Given a G-cover $\pi : C \to \mathbf{P}^1_k$ over a field k of characteristic 0 and a rational branch point $b \in \mathbf{P}^1(k)$, the algebraic local monodromy of π at b defined in §2.7.1 is thus an element of $\mathscr{C}_G(k)$. More generally, if $b \in \mathbf{P}^1_k$ is an arbitrary branch point of π (i.e. a closed point, not necessarily rational), applying the definition of §2.7.1 to the G-cover over $k(b)$ obtained from π by scalar extension from k to $k(b)$ and to the rational branch point of this G-cover induced by b, we obtain an element of $\mathscr{C}_G(k(b))$, which we still call the *algebraic local monodromy of* π *at* b. Viewing this element as a morphism $\mathrm{Spec}(k(b)) \to \mathscr{C}_G$ and writing the branch locus $B \subset \mathbf{P}^1_k$ of π as the disjoint union, over the points $b \in B$, of the schemes $\mathrm{Spec}(k(b))$, we thus obtain a morphism of varieties $B \to \mathscr{C}_G$. We call it the *algebraic local monodromy morphism of* π.

For any $r \geq 1$, we denote by $\mathscr{V}^r \subset (\mathbf{P}^1_{\mathbf{Q}} \times \mathscr{C}_G)^r$ the inverse image of $\mathscr{U}^r$ by the projection $(\mathbf{P}^1_{\mathbf{Q}} \times \mathscr{C}_G)^r \to (\mathbf{P}^1_{\mathbf{Q}})^r$, and by $\mathscr{V}_r$ the quotient of $\mathscr{V}^r$ by the natural action of the symmetric group S_r. We have thus produced an étale covering $\nu : \mathscr{V}_r \to \mathscr{U}_r$ of smooth varieties over $\mathbf{Q}$. For any field k of characteristic 0, the set $\mathscr{V}_r(k)$ can be identified with the set of reduced 0-dimensional subvarieties of $\mathbf{P}^1_k \times \mathscr{C}_G$ of degree r that map isomorphically to their image in $\mathbf{P}^1_k$, or, what is the same, to the set of reduced 0-dimensional subvarieties B of $\mathbf{P}^1_k$ of degree r endowed with a morphism $B \to \mathscr{C}_G$.

For any field k of characteristic 0, associating with each G-cover its branch locus together with its algebraic local monodromy morphism provides us with a map $\mathscr{H}_{G,r}(k) \to \mathscr{V}_r(k)$. When $k = \mathbf{Q}(I)$ is the function field of a connected component I of $\mathscr{H}_{G,r}$, the image of the generic point of I by this map gives rise to a rational map $I \dashrightarrow \mathscr{V}_r$. Being a rational map between étale coverings of the normal variety $\mathscr{U}_r$, it is in fact a morphism. By letting I vary over all connected components of $\mathscr{H}_{G,r}$, we obtain, in this way, a morphism $\rho' : \mathscr{H}_{G,r} \to \mathscr{V}_r$ such that $\rho = \nu \circ \rho'$.

Let $\mathrm{Cl}(G)$ denote the set of conjugacy classes of G. Remark 2.7.2 (i) and (the proof of) Corollary 2.3.2 together imply the following explicit description of the complex fibres of ρ':

Proposition 2.7.4. *Let $B \subset \mathbf{P}^1_{\mathbf{C}}$ be a reduced 0-dimensional subvariety of degree r. Write $B = \{b_1, \ldots, b_r\}$. Let $C = (C_1, \ldots, C_r)$ be an r-tuple of nontrivial conjugacy classes of G, viewed as a map $B(\mathbf{C}) \to \mathscr{C}_G(\mathbf{C})$ via the identification $\mathscr{C}_G(\mathbf{C}) = \mathrm{Cl}(G)$ of Remark 2.7.2 (i). Then the fibre of ρ' above the point of $\mathscr{V}_r(\mathbf{C})$ defined by B and C can be identified with the quotient $\mathrm{ni}^C_r(G)$ of the set of r-tuples $(g_1, \ldots, g_r) \in G^r$ satisfying the following three conditions by the action of G on this set by simultaneous conjugation:*

(1) $g_1 \cdots g_r = 1$*;*
(2) $g_1, \ldots, g_r$ *generate* G*;*
(3) $g_i \in C_i$ *for all* $i \in \{1, \ldots, r\}$*.*

Proof. This would be a direct consequence of the quoted references if we knew that for a field k of characteristic 0 (here $k = \mathbf{C}$), the map $\mathscr{H}_{G,r}(k) \to \mathscr{V}_r(k)$ induced by ρ' sends the isomorphism class of any G-cover over k to its algebraic local monodromy morphism. By the definition of ρ', this is true for those G-covers whose branch locus is "generic", in the sense that it is a point of $\mathscr{U}_r(k)$ lying over the generic point of the variety $\mathscr{U}_r$ over $\mathbf{Q}$ (i.e. when viewed as a morphism $\mathrm{Spec}(k) \to \mathscr{U}_r$, its image is the generic point). Thus, Proposition 2.7.4 holds when B is "generic". As ρ' is a morphism between étale coverings of $\mathscr{U}_r$, the validity of Proposition 2.7.4 for arbitrary B follows. □

2.7.5. *Rational points of* $\mathscr{C}_G$*.* Viewing $\bar{\mathbf{Q}}$ as a subfield of $\mathbf{C}$, Remark 2.7.2 (i) also induces an identification $\mathscr{C}_G(\bar{\mathbf{Q}}) = \mathrm{Cl}(G)$. Via this identification, the natural action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on $\mathscr{C}_G(\bar{\mathbf{Q}})$ gives rise to the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on $\mathrm{Cl}(G)$ given by the formula $\sigma(g) = g^{-\chi(\sigma)}$ for $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ and $g \in G$, where $\chi : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \twoheadrightarrow \hat{\mathbf{Z}}^*$ denotes the cyclotomic character. As a consequence, the set $\mathscr{C}_G(\mathbf{Q})$ of rational points of $\mathscr{C}_G$ gets identified with the set of *rational* conjugacy classes of G in the following sense:

Definition 2.7.6. A conjugacy class C of a finite group G is *rational* if for every $g \in C$ and every integer $n \geq 1$ prime to the order of g, the element g^n belongs to C.

2.7.7. *Rational points of* $\mathscr{V}_r$*.* Here is a simple way to exhibit rational points of $\mathscr{V}_r$. Let $b_1, \ldots, b_r \in \mathbf{P}^1(\mathbf{Q})$ be pairwise distinct. Let $B = \{b_1, \ldots, b_r\}$. The rational points of $\mathscr{V}_r$ lying above the rational point of $\mathscr{U}_r$ defined by B are exactly the r-tuples of rational points of $\mathscr{C}_G$, i.e. they are the r-tuples of rational conjugacy classes of G.

2.7.8. *Rational points of* $\mathscr{H}_{G,r}$*.* The morphism $\rho' : \mathscr{H}_{G,r} \to \mathscr{V}_r$ is an étale covering. As such, it has a degree, which is a locally constant function on $\mathscr{V}_r$. This function is not constant on $\mathscr{V}_r$ in general—unlike the degree of ρ, which is constant, equal to the cardinality of $\mathrm{ni}_r(G)$, as we have seen in §2.6. A connected component of $\mathscr{V}_r$ over which ρ' has degree 1, i.e. over which ρ' restricts to an isomorphism, is said to be *rigid*.

It is a trivial but fruitful observation, which forms the basis of the rigidity method, that the existence of a rational point of a rigid connected component of $\mathscr{V}_r$ implies the existence of a rational point of $\mathscr{H}_{G,r}$.

By Proposition 2.7.4, the rigidity of a connected component can be verified by computing the set $\mathrm{ni}_r^C(G)$ associated with its complex points. This motivates the following definition:

Definition 2.7.9. An r-tuple $C = (C_1, \ldots, C_r)$ of nontrivial conjugacy classes of G is *rigid* if the set $\mathrm{ni}_r^C(G)$ defined in Proposition 2.7.4 has cardinality 1.

2.7.10. *Summing up.* We thus arrive at a down-to-earth condition that implies that the rational points of $\mathscr{V}_r$ constructed in §2.7.7 can be lifted to rational points of $\mathscr{H}_{G,r}$.

Theorem 2.7.11. *Let* G *be a finite group with trivial centre. Let* $r \geq 1$ *be an integer. If there exists a rigid* r*-tuple* $C = (C_1, \ldots, C_r)$ *of nontrivial rational conjugacy classes of* G*,* *then for any pairwise distinct $b_1, \dots, b_r \in \mathbf{P}^1(\mathbf{Q})$, the $\mathbf{Q}$-point of $\mathscr{U}_r$ defined by $\{b_1, \dots, b_r\}$ can be lifted to a $\mathbf{Q}$-point of $\mathscr{H}_{G,r}$. In particular, the regular inverse Galois problem admits a positive solution for G over $\mathbf{Q}$.*

Theorem 2.7.11 represents the base case of the rigidity method. It admits many variants; for instance, one can allow non-rational branch points. (Pro: this weakens the condition that the prescribed conjugacy classes be rational; con: these conjugacy classes cannot be chosen independently of one another any longer.) One could also work over a number field other than $\mathbf{Q}$, which would simultaneously weaken the conclusion of the theorem and the rationality assumption on the conjugacy classes C_i.

Even just the above base case is already unreasonably effective: the hypothesis of Theorem 2.7.11 has been shown to be satisfied, with $r = 3$, for at least 10 of the 26 sporadic simple groups, including the monster (by Thompson) and the baby monster (by Malle and Matzat); see [MM18, Chapter II, §9]. As another example, the variant of Theorem 2.7.11 in which $r = 3$ and b_1 is rational while b_2 and b_3 are conjugate quadratic points of the projective line can be applied to $\mathrm{PSL}_2(\mathbf{F}_p)$ for all primes p such that 2 or 3 is not a square modulo p (see [Ser07, §8.3.3]), thus recovering the positive answer to the regular inverse Galois problem over $\mathbf{Q}$ for this infinite family of groups that had been obtained by Shih using modular curves rather than the rigidity method.

When the rigidity method is applicable, it is in principle possible to deduce from it an explicit polynomial that realises the desired regular Galois extension of $\mathbf{Q}(t)$ (see [MM18, Chapter II, §9]). This has some limits in practice (e.g. for the monster group, the degree of the polynomial cannot have less than 20 digits) but it leads to interesting computational challenges (see e.g. [BW21]).

3. Grunwald's problem and the Brauer–Manin obstruction

3.1. **Looking for rational points.** Despite its successes, the rigidity method, discussed in §2.7, often fails to be applicable. For instance, it fails, in general, for p-groups; indeed, the regular inverse Galois problem is still open for most p-groups over $\mathbf{Q}$, even though the inverse Galois problem itself is known to have a positive answer, over any number field, for all p-groups—and more generally, for all solvable groups, by a celebrated theorem of Shafarevich (see [NSW08, Chapter IX, §6]). In other words, after learning, in §1, that the quotient variety $\mathbf{A}^n_k/G$ can fail to be rational or even retract rational, we now find ourselves unable, at least in practice, to salvage the Hilbert–Noether method by constructing rational curves in $\mathbf{A}^n_k/G$ over which to apply Hilbert's irreducibility theorem, as envisaged at the beginning of §2.1. This leads us to our next question: letting $Y \subseteq \mathbf{A}^n_k$ denote the locus where G acts freely, can we directly construct rational points of Y/G above which the fibre of the quotient map $Y \to Y/G$ is irreducible? An approach put forward by Colliot-Thélène consists in noting that Ekedahl's Theorem 1.3.5 reduces this question, in full generality, to the problem of finding rational points on Y/G subject to certain weak approximation conditions. In particular, if the variety Y/G satisfies weak approximation off a finite set of places of k, then the inverse Galois problem has a positive answer for G over k. Such a weak approximation property can be proved unconditionally in some cases; for instance, under the assumptions of the following remarkable theorem from [Neu79], in which no place of k is excluded:

Theorem 3.1.1 (Neukirch). *Let k be a number field. Let G be a finite solvable group, acting linearly on $\mathbf{A}^n_k$ for some $n \geq 1$. Let $Y \subseteq \mathbf{A}^n_k$ be the locus where G acts freely. Let $X = Y/G$. Assume that the order of G and the number of roots of unity contained in k are coprime. Then X satisfies weak approximation, i.e. the set $X(k)$ is dense in $X(k_\Omega)$. In particular, Grunwald's problem admits a positive answer for G over k, for any finite subset $S \subset \Omega$.*

We recall that Grunwald's problem is Problem 1.1.1. Without the assumption on the order of G, the conclusion of this theorem can fail, as we have seen in Proposition 1.6.2.

The validity of the weak approximation property is a problem of general interest that makes sense, and has been studied, for arbitrary smooth varieties. As we shall now explain, the tools that have been developed for its study on arbitrary smooth varieties turn out to be useful also in the special case of the quotient Y/G.

3.2. **Brauer–Manin obstruction.** A general mechanism, introduced by Manin [Man71] and now called the *Brauer–Manin obstruction*, explains, in some cases, why the weak approximation property fails for certain varieties over number fields. Let us recall it briefly. (For details, see [CTS21, §13.3].) Let X be a smooth variety over a number field k. Let $\mathrm{Br}_{\mathrm{nr}}(X)$ denote its unramified Brauer group (see §1.6.5). We let $X(k_\Omega) = \prod_{v\in\Omega} X(k_v)$ and endow this set with the product of the v-adic topologies.

The *Brauer–Manin set* $X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}(X)}$ is the set of all families $(x_v)_{v\in\Omega} \in X(k_\Omega)$ such that $\sum_{v\in\Omega} \mathrm{inv}_v\, \beta(x_v) = 0$ for all $\beta \in \mathrm{Br}_{\mathrm{nr}}(X)$. Here $\beta(x_v) \in \mathrm{Br}(k_v)$ denotes the evaluation of β at x_v, and $\mathrm{inv}_v : \mathrm{Br}(k_v) \hookrightarrow \mathbf{Q}/\mathbf{Z}$ is the invariant map from local class field theory. (To make sense of the sum, one checks that only finitely many of its terms are nonzero.) Manin's fundamental observation is that the image of the diagonal embedding $X(k) \hookrightarrow X(k_\Omega)$ is contained in the Brauer–Manin set, as a consequence of the reciprocity law of global class field theory. Thus, we have a sequence of inclusions

$$X(k) \subseteq X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}(X)} \subseteq X(k_\Omega). \tag{3.2.1}$$

As $X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}(X)}$ is a closed subset of $X(k_\Omega)$, the weak approximation property, i.e. the density of $X(k)$ in $X(k_\Omega)$, can hold only if $X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}(X)} = X(k_\Omega)$. When this last equality fails, one says that there is a Brauer–Manin obstruction to weak approximation on X.

3.3. **Reinterpreting the Grunwald–Wang theorem.** Let us come back to the variety $X = Y/G$ considered in §3.1: G is a subgroup of S_n, which acts on $\mathbf{A}^n_k$ by permuting the coordinates, and $Y \subseteq \mathbf{A}^n_k$ is the locus where G acts freely. As Grunwald's problem has a negative answer for $G = \mathbf{Z}/8\mathbf{Z}$ and $k = \mathbf{Q}$ (see Proposition 1.6.2) and as $Y \to X$ is a versal G-torsor (see Example 1.5.2), the variety X cannot satisfy the weak approximation property in this case, according to Proposition 1.5.5. Hence a natural question: is there a Brauer–Manin obstruction to weak approximation on X when $G = \mathbf{Z}/8\mathbf{Z}$ and $k = \mathbf{Q}$? The answer is yes by the following theorem, which states, more precisely, that the weak approximation property on X is fully controlled by the Brauer–Manin obstruction as soon as G is abelian.

Theorem 3.3.1 (Voskresenskiĭ, Sansuc)**.** *Let k be a number field. Let G be a finite abelian group, acting linearly on $\mathbf{A}^n_k$ for some $n \geq 1$. Let $Y \subseteq \mathbf{A}^n_k$ be the locus where G acts freely. Let $X = Y/G$. The set $X(k)$ is dense in $X(k_\Omega)^{\mathrm{Br_{nr}}(X)}$.*

Theorem 3.3.1 can be found in the literature by combining [Vos98, §7.2, Theorem] with [San81, Corollaire 8.13]. We shall explain a proof of it in §3.8 below.

Returning to an arbitrary finite group G and keeping k, Y and X as above, it is a general fact that the density of $X(k)$ in $X(k_\Omega)^{\mathrm{Br_{nr}}(X)}$ implies the existence of a finite subset $S_0 \subset \Omega$ such that X satisfies weak approximation off S_0. When such an S_0 exists, a refinement of the arguments underlying the proof of Proposition 1.5.5 leads to the following conclusion (a point of view advocated in [Che95] and in [Har07, §1.2]): fully solving Grunwald's problem for G over k is in fact equivalent to describing the closure of $X(k)$ inside $X(k_\Omega)$. Thus, the Grunwald–Wang theorem, which indeed fully solves Grunwald's problem when G is abelian, can now be viewed, in retrospect, as the combination of Theorem 3.3.1 with an explicit computation of the Brauer–Manin set $X(k_\Omega)^{\mathrm{Br_{nr}}(X)}$ when G is abelian.

3.4. **Rationally connected varieties.** Whether or not the abelianness hypothesis on G can be removed from Theorem 3.3.1 is a fundamental open question. When X is an arbitrary smooth variety possessing a rational point, the set $X(k)$ cannot be expected to be dense in $X(k_\Omega)^{\mathrm{Br_{nr}}(X)}$ without strong assumptions on the geometry of X; for instance, Lang's conjectures predict that for d and N such that $d-2 \geq N \geq 4$, this density should fail for all smooth hypersurfaces of degree d in $\mathbf{P}^N$ that have a rational point (see [PV04, Appendix A]). The variety $X = Y/G$ that we have been considering in §3.1 and in §3.3, despite not being geometrically rational for an arbitrary finite group G (see §1.6.5), still has a reasonably tame geometry: it is unirational and therefore belongs to the class of *rationally connected varieties* according to the following definition[6].

Definition 3.4.1 (Campana, Kollár, Miyaoka, Mori)**.** A smooth variety X over a field k is said to be *rationally connected* if for any algebraically closed field extension K/k and any two general K-points $x_0, x_1 \in X(K)$, there exists a rational map $f : \mathbf{A}^1_K \dashrightarrow X_K$ over K, defined in a neighbourhood of 0 and 1, such that $f(0) = x_0$ and $f(1) = x_1$. ("General" means that the set of pairs (x_0, x_1) satisfying the stated condition contains a dense Zariski open subset of $X(K) \times X(K)$.)

Theorem 3.3.1 conjecturally extends to all smooth rationally connected varieties:

Conjecture 3.4.2 (Colliot-Thélène)**.** *Let X be a smooth, rationally connected variety, over a number field k. The set $X(k)$ is dense in $X(k_\Omega)^{\mathrm{Br_{nr}}(X)}$.*

A number of known results towards this conjecture are listed in [Wit18]. Conjecture 3.4.2 would imply that all smooth rationally connected varieties satisfy weak approximation off

[6] To be precise, Definition 3.4.1 coincides with the standard definition (found, e.g., in [Kol96, Chapter IV]) only when X is proper.

a finite set of places (see e.g. [Wit18, Remarks 2.4 (i)–(ii)]). In particular, it would imply a positive answer to the inverse Galois problem in general, by Theorem 1.3.5 applied to the torsor of Example 1.5.2.

A list of groups G of small order for which Conjecture 3.4.2 is still open for the variety $X = Y/G$ appearing in Example 1.5.2 can be found in [BN23].

3.5. **Determining the Brauer–Manin set.** As discussed in §3.3, Conjecture 3.4.2 in the case $X = Y/G$ would, more precisely, reduce Grunwald's problem for G over k to the computation of the Brauer–Manin set of X. Even partial knowledge of the Brauer–Manin set can lead to concrete results, as the following theorem illustrates:

Theorem 3.5.1 (Lucchini Arteche [LA19])**.** *Let k be a number field and G be a finite group acting linearly on $\mathbf{A}^n_k$. Let $Y \subseteq \mathbf{A}^n_k$ be the locus where G acts freely. Let $X = Y/G$. Let S_0 be the set of finite places of k that divide the order of G. If X satisfies Conjecture 3.4.2, then Grunwald's problem admits a positive answer for G over k, for any finite subset $S \subset \Omega$ disjoint from S_0.*

The proof of Theorem 3.5.1 consists in studying the evaluation of unramified Brauer classes at the local points of X, so as to deduce, from the density of $X(k)$ in $X(k_\Omega)^{\mathrm{Br_{nr}}(X)}$, that X satisfies weak approximation off S_0; Proposition 1.5.5 then yields the desired statement.

The complete determination of $X(k_\Omega)^{\mathrm{Br_{nr}}(X)}$, for X as in the statement of Theorem 3.5.1, is in general a difficult task. The case of a metabelian group G is investigated in [Dem21]. In general, even the computation of $\mathrm{Br_{nr}}(X)$ itself is a delicate problem. Over an algebraic closure $\bar{k}$ of k, one can apply Bogomolov's formula (Theorem 1.6.6). If the unramified Brauer group of $X_{\bar{k}}$ turns out to be nontrivial, one has to find out which classes of the finite group $\mathrm{Br_{nr}}(X_{\bar{k}})$ are invariant under $\mathrm{Gal}(\bar{k}/k)$, and to determine the image of the natural map $\mathrm{Br_{nr}}(X) \to \mathrm{Br_{nr}}(X_{\bar{k}})^{\mathrm{Gal}(\bar{k}/k)}$; there is no general recipe for carrying this out. The kernel of the latter map, on the other hand, is now well understood: its quotient by the image of the natural map $\mathrm{Br}(k) \to \mathrm{Br_{nr}}(X)$ is finite and is described by a formula due to Harari [Har07, Proposition 4]. In the most favourable cases, the combination of these formulae can lead to the conclusion that the natural map $\mathrm{Br}(k) \to \mathrm{Br_{nr}}(X)$ is onto, so that $X(k_\Omega)^{\mathrm{Br_{nr}}(X)} = X(k_\Omega)$ and Grunwald's problem is then expected to have a positive solution for G over k with no restriction on the finite subset $S \subset \Omega$. See [Dem10, Remarque 7] for a concrete example. In a different direction, by adapting the proof of Bogomolov's formula to non-algebraically closed ground fields, Colliot-Thélène [CT14, Corollaire 5.7] showed that the natural map $\mathrm{Br}(k) \to \mathrm{Br_{nr}}(X)$ is onto, and hence that $X(k_\Omega)^{\mathrm{Br_{nr}}(X)} = X(k_\Omega)$, whenever the order of G and the number of roots of unity contained in k are coprime, which explains, a posteriori, why the Brauer–Manin obstruction plays no rôle in Neukirch's Theorem 3.1.1.

3.6. **Supersolvable groups.** A finite group G is said to be *supersolvable* if there exists a filtration $1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$ such that each G_i is a normal subgroup of G and each successive quotient G_{i+1}/G_i is cyclic. All nilpotent groups (in particular, all p-groups) are supersolvable. We proved, in [HW20], that Theorem 3.3.1 generalises to such groups:

Theorem 3.6.1 (Harpaz, W.). *Let k be a number field. Let G be a finite supersolvable group, acting linearly on $\mathbf{A}^n_k$ for some $n \geq 1$. Let $Y \subseteq \mathbf{A}^n_k$ be the locus where G acts freely. Let $X = Y/G$. The set $X(k)$ is dense in $X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}(X)}$.*

A positive answer to the inverse Galois problem for supersolvable groups results from this (via Theorem 1.3.5) but had already been established—more generally, for solvable groups—by Shafarevich, as mentioned in §3.1. As discussed in §§3.3–3.5, Theorem 3.6.1 refines this positive answer by bringing information about Grunwald's problem.

It may be that the strategy underlying the proof of Theorem 3.6.1 can be extended to all solvable groups. It will not, however, be of any help with non-abelian simple groups; in fact, to this day, no approach is known towards Grunwald's problem for non-abelian simple groups (with the exception of A_5 and $\mathrm{PSL}_2(\mathbf{F}_7)$, for which Noether's problem itself has a positive answer; see Example 1.4.4, [Mes05] and Corollary 1.5.7).

3.7. **Descent in a nutshell.** Theorem 3.6.1 can be seen as a direct application of a general tool that is useful for proving cases of Conjecture 3.4.2, the so-called "descent" method. We now briefly discuss it. We shall illustrate it by proving Theorem 3.3.1 in §3.8, before indicating its applicability to other variants of the inverse Galois problem in §3.10.

To get started, we need to extend the notion of G-torsor from the case where G is a finite abstract group (Definition 1.2.1) to the case where G is an algebraic group (i.e. a group scheme over a field, possibly disconnected or of positive dimension).

Definition 3.7.1. Let $\pi : Y \to X$ be a surjective morphism between smooth varieties over a field k of characteristic 0, with algebraic closure $\bar{k}$. Let G be an algebraic group over k, acting on Y in such a way that π is G-equivariant (for the trivial action of G on X). We say that π is a *G-torsor*, or that Y is a G-torsor over X, if π is smooth and $G(\bar{k})$ acts simply transitively on the fibres of the map $Y(\bar{k}) \to X(\bar{k})$ induced by π.

Unless otherwise specified, we now let k denote an arbitrary field of characteristic 0. (For the correct definition of a torsor without this assumption, see [Sko01, Definition 2.2.1].) As usual, by a *G-torsor over k* we shall mean a G-torsor over $\mathrm{Spec}(k)$. When $\pi : Y \to X$ is a G-torsor, the morphism π identifies X with the categorical quotient Y/G (see [MFK94, Proposition 0.2, Proposition 0.1]).

Example 3.7.2. Hilbert's Theorem 90, which we encountered in Example 1.5.2, is equivalent to the following statement: for any integer $n \geq 1$, any GL_n-torsor over k is isomorphic to GL_n. As an easy consequence, any SL_n-torsor over k is isomorphic to SL_n.

Definition 3.7.3. Let X be a smooth variety over k. Let G be an algebraic group over k. Let $\pi : Y \to X$ be a G-torsor. The *twist* of Y by a G-torsor P over k is the quotient

$$_PY = (P \times Y)/G$$

of $P \times Y$ by the diagonal action of G, endowed with the natural morphism $_P\pi : {_PY} \to X$ induced by the second projection $P \times Y \to Y$ and the identification $Y/G = X$. (We are not claiming that $_P\pi$ is a G-torsor. This is true when G is commutative, not in general. This point, which will be irrelevant for us, is discussed in [Sko01, p. 21].)

The gist of the descent method is summarised in the following conjecture.

Conjecture 3.7.4. *Let X be a smooth variety over a number field k. Let G be a linear algebraic group over k. Let $\pi : Y \to X$ be a G-torsor, with Y rationally connected. Assume that for every twist Y' of Y by a G-torsor over k, the set $Y'(k)$ is dense in $Y'(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}(Y')}$. Then the set $X(k)$ is dense in $X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}(X)}$.*

Conjecture 3.7.4, and the first significant cases in which it was established, appeared in a series of works by Colliot-Thélène and Sansuc. See [Sko01] for an account. We content ourselves with mentioning the following positive result[7], which in this form can be found in [HW20, Corollaire 2.2].

Theorem 3.7.5 (Colliot-Thélène, Sansuc, Harpaz, W.)**.** *Conjecture 3.7.4 holds true if G is a torus (i.e. an algebraic group such that $G_{\bar{k}} \simeq \mathbf{G}_{\mathrm{m},\bar{k}} \times \cdots \times \mathbf{G}_{\mathrm{m},\bar{k}}$).*

3.8. **Sketch of proof of Theorem 3.3.1.** We shall deduce Theorem 3.3.1 from Theorem 3.7.5. (More precisely, descent will be applied to a geometrically rational variety; Theorem 3.7.5 in the case of such varieties is due to Colliot-Thélène and Sansuc alone, see [CTS87].)

Before starting the proof of Theorem 3.3.1, let us slightly change notation. We now fix an embedding $G \hookrightarrow \mathrm{SL}_n(k)$ for some $n \geq 1$, let Y be the algebraic group SL_n over k, and let G act on Y by right multiplication. As the resulting variety $X = Y/G$ is stably birationally equivalent to the variety X of Theorem 3.3.1 (see Remark 1.5.4), and as the density of $X(k)$ in $X(k_\Omega)^{\mathrm{Br}_{\mathrm{nr}}(X)}$ is a stable birational invariant among smooth, rationally connected varieties (see [CTPS16, Proposition 6.1 (iii)] and [Wit18, Remark 2.4 (ii)]), this change of notation is harmless.

Recall that G, by assumption, is a finite abelian group. Let us view it as a constant algebraic group over k. It is easy to see that G fits into a short exact sequence

$$1 \to G \to T \to Q \to 1 \tag{3.8.1}$$

of algebraic groups over k, where T and Q are tori and Q is quasi-trivial, i.e. the character group $\mathrm{Hom}(Q_{\bar{k}}, \mathbf{G}_{\mathrm{m},\bar{k}})$ of Q admits a basis over $\mathbf{Z}$ that is stable under the action of $\mathrm{Gal}(\bar{k}/k)$ (see [Ser07, Proposition 4.2.1]). Letting G act on T by translation, we now consider the quotient $W = (\mathrm{SL}_n \times T)/G$ of $\mathrm{SL}_n \times T$ by the diagonal action, together with the morphism $\pi : W \to X = \mathrm{SL}_n/G$ induced by the first projection.

The action of T on $\mathrm{SL}_n \times T$ by multiplication on the second factor induces an action of T on W, with respect to which π is a T-torsor. According to Theorem 3.7.5 applied to π, it will suffice, in order to complete the proof of Theorem 3.3.1, to show that for every T-torsor P over k, the variety ${}_PW$ satisfies Conjecture 3.4.2.

We observe that ${}_PW = (\mathrm{SL}_n \times P)/G$, that the morphism $p : {}_PW \to P/G$ induced by the second projection is an SL_n-torsor (with respect to the action of SL_n on ${}_PW$ coming from its action on $\mathrm{SL}_n \times P$ by left multiplication on the first factor), and that P/G is a Q-torsor over k. By Hilbert's Theorem 90 (see Example 3.7.2), the generic fibre of p is isomorphic

[7] More generally, after the writing of these notes, Conjecture 3.7.4 was proved by Nguyễn to be true as soon as G is connected; see [Ngu23], which builds on [HW20, §2] and on Borovoi's abelianisation technique.

to SL_n, in particular it is rational. It also follows from Hilbert's Theorem 90 (case $n=1$ of Example 3.7.2), combined with Shapiro's lemma, that any torsor under a quasi-trivial torus over k is rational; in particlar, the variety P/G is rational. These two remarks imply that ${}_PW$ is itself rational over k. Thus, it satisfies Conjecture 3.4.2 for trivial reasons, and Theorem 3.3.1 is proved.

3.9. **Supersolvable descent.** The ideas sketched in §3.8 are a starting point for the proof of the following theorem, established in [HW22, Corollary 3.3].

Theorem 3.9.1 (Harpaz, W.)**.** *Conjecture 3.7.4 holds true if G is finite and supersolvable.*

Here "supersolvable" means that $G(\bar{k})$ is supersolvable in the sense recalled at the beginning of §3.6, except that the filtration is now required, in addition, to be stable under the action of $\mathrm{Gal}(\bar{k}/k)$ on $G(\bar{k})$, in case this action is not trivial.

Theorem 3.9.1 implies Theorem 3.6.1: in the notation introduced at the beginning of §3.8, it suffices to apply Theorem 3.9.1 to the G-torsor $\mathrm{SL}_n \to \mathrm{SL}_n/G$ and to note that any twist of SL_n by a G-torsor over k is an SL_n-torsor (through left multiplication), hence is isomorphic to SL_n, by Hilbert's Theorem 90, hence is rational and satisfies Conjecture 3.4.2.

Remark 3.9.2. Theorem 3.9.1 implies in particular that Conjecture 3.7.4 holds true for $G=\mathbf{Z}/2\mathbf{Z}$. We recall that Conjecture 3.7.4 assumes that the variety Y appearing in its statement is rationally connected. As was pointed out to the author by Mạnh Linh Nguyễn, this assumption cannot be dropped, even when $G=\mathbf{Z}/2\mathbf{Z}$. Indeed, there exist examples of double covers $Y \to X$, where Y is a $K3$ surface and X is an Enriques surface over $k=\mathbf{Q}$, such that $X(k)$ and the sets $Y'(k_\Omega)^{\mathrm{Br_{nr}}(Y')}$ are all empty, while $X(k_\Omega)^{\mathrm{Br_{nr}}(X)}$ is not (see [BBM+16, Theorem 1.2]).

3.10. **Prescribed norms.** Our last theorem is an application of supersolvable descent to a variant of the inverse Galois problem of a slightly different flavour, meant to demonstrate the flexibility of descent as a tool.

Theorem 3.10.1 ([HW22, Theorem 4.16])**.** *Let G be a finite group. Let k be a number field. Let $\alpha_1,\dots,\alpha_m \in k^*$. If G is supersolvable, there exists a Galois field extension K of k such that* $\mathrm{Gal}(K/k) \simeq G$ *and $\alpha_1,\dots,\alpha_m \in N_{K/k}(K)$.*

The idea of the proof is to construct, in a formal and explicit way, a G-torsor $\pi : Y \to X$ together with invertible functions $\beta_1,\dots,\beta_m$ on Y whose norms along π are equal to the constant invertible functions $\alpha_1,\dots,\alpha_m$ on X. Namely, say $m=1$ for simplicity, embed G into $\mathrm{SL}_n(k)$ and consider the subvariety Y of $\mathrm{SL}_n \times \prod_{g\in G} \mathbf{G}_\mathrm{m}$ consisting of all $(s,(t_g)_{g\in G})$ such that $\prod_{g\in G} t_g = \alpha_1$; the invertible function β_1 on Y given by projection onto the $\mathbf{G}_\mathrm{m}$ factor corresponding to $1 \in G$ has the required norm. One then checks that the twists of Y satisfy Conjecture 3.4.2 (despite not being rational in general, even when they have a rational point and G is assumed abelian), so that Theorem 3.9.1 implies the validity of Conjecture 3.4.2, and hence of weak approximation off a finite set of places, for X. As $X(k) \neq \varnothing$ (indeed even $Y(k) \neq \varnothing$), it follows, by Theorem 1.3.5, that there exists $x \in X(k)$ such that $\pi^{-1}(x)$ is irreducible, i.e. gives rise to a Galois field extension K/k with group G. Restricting $\beta_1,\dots,\beta_m$ to $\pi^{-1}(x)$ yields elements of K^* with norms $\alpha_1,\dots,\alpha_m$.

In the case where G is abelian, Theorem 3.10.1 was first shown to hold by Frei, Loughran and Newton [FLN22], who established an asymptotic estimate for the number of such K.

References

[AD00] F. Amoroso and R. Dvornicich, *A lower bound for the height in abelian extensions*, J. Number Theory **80** (2000), no. 2, 260–272.

[AM72] M. Artin and D. Mumford, *Some elementary examples of unirational varieties which are not rational*, Proc. Lond. Math. Soc. (3) **25** (1972), 75–95.

[AT09] E. Artin and J. Tate, *Class field theory*, AMS Chelsea Publishing, Providence, RI, 2009, reprinted with corrections from the 1967 original.

[BBM$^+$16] F. Balestrieri, J. Berg, M. Manes, J. Park, and B. Viray, *Insufficiency of the Brauer-Manin obstruction for rational points on Enriques surfaces*, Directions in number theory. Proceedings of the 2014 Women in Numbers, WIN3 workshop. Banff, Alberta, Canada, April 21–25, 2014, Cham: Springer, 2016, pp. 1–31.

[BCTSSD85] A. Beauville, J.-L. Colliot-Thélène, J.-J. Sansuc, and P. Swinnerton-Dyer, *Variétés stablement rationnelles non rationnelles*, Ann. Math. (2) **121** (1985), 283–318.

[BF03] G. Berhuy and G. Favi, *Essential dimension: A functorial point of view (after A. Merkurjev)*, Doc. Math. **8** (2003), 279–330.

[BN23] E. Boughattas and D. Neftin, *The sufficiency of the Brauer–Manin obstruction to Grunwald problems*, preprint, 2023.

[Bog88] F. A. Bogomolov, *The Brauer group of quotient spaces by linear group actions*, Math. USSR, Izv. **30** (1988), no. 3, 455–485.

[BR97] J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compos. Math. **106** (1997), no. 2, 159–179.

[BW21] D. Barth and A. Wenz, *Computation of Belyi maps with prescribed ramification and applications in Galois theory*, J. Algebra **569** (2021), 616–642.

[Che95] V. I. Chernousov, *Galois cohomologies and the weak approximation for quotient varieties A^n/G*, Number theory, algebra and algebraic geometry. Collected papers. In honor of the seventieth birthday of Academician Igor Rostislavovich Shafarevich, Moscow: Maik Nauka/Interperiodica Publishing, 1995, pp. 296–308.

[CT00] J.-L. Colliot-Thélène, *Rational connectedness and Galois covers of the projective line*, Ann. Math. (2) **151** (2000), no. 1, 359–373.

[CT14] ———, *Groupe de Brauer non ramifié de quotients par un groupe fini*, Proc. Am. Math. Soc. **142** (2014), no. 5, 1457–1469.

[CTO89] J.-L. Colliot-Thélène and M. Ojanguren, *Variétés unirationelles non rationelles : au-delà de l'exemple d'Artin et Mumford*, Invent. math. **97** (1989), no. 1, 141–158.

[CTPS16] J.-L. Colliot-Thélène, A. Pál, and A. N. Skorobogatov, *Pathologies of the Brauer-Manin obstruction*, Math. Z. **282** (2016), no. 3-4, 799–817.

[CTS87] J.-L. Colliot-Thélène and J.-J. Sansuc, *La descente sur les variétés rationnelles. II*, Duke Math. J. **54** (1987), no. 2, 375–492.

[CTS07] J.-L. Colliot-Thélène and J.-J. Sansuc, *The rationality problem for fields of invariants under linear algebraic groups (with special regards to the Brauer group)*, Algebraic groups and homogeneous spaces, Tata Inst. Fund. Res. Stud. Math., vol. 19, Tata Inst. Fund. Res., Mumbai, 2007, pp. 113–186.

[CTS21] J.-L. Colliot-Thélène and A. N. Skorobogatov, *The Brauer-Grothendieck group*, Ergeb. Math. Grenzgeb., 3. Folge, vol. 71, Springer, Cham, 2021.

[Dèb99] P. Dèbes, *Arithmétique et espaces de modules de revêtements*, Number theory in progress. Proceedings of the international conference organized by the Stefan Banach International Mathematical Center in honor of the 60th birthday of Andrzej Schinzel, Zakopane, Poland, June 30–July 9, 1997. Volume 1: Diophantine problems and polynomials, Berlin: de Gruyter, 1999, pp. 75–102.

[Del73] P. Deligne, *La conjecture de Weil. I*, Publ. Math. de l'I.H.É.S. **43** (1973), 273–307.

[Dem10] C. Demarche, *Groupe de Brauer non ramifié d'espaces homogènes à stabilisateurs finis*, Math. Ann. **346** (2010), no. 4, 949–968.

[Dem21] J. L. Demeio, *Ramified descent*, arXiv:2112.00843, 2021.

[DFV22] L. Dieulefait, E. Florit, and N. Vila, *Seven small simple groups not previously known to be Galois over* $\mathbf{Q}$, Mathematics **10** (2022), no. 12, 2048, 10 pages.

[DLAN17] C. Demarche, G. Lucchini Arteche, and D. Neftin, *The Grunwald problem and approximation properties for homogeneous spaces*, Ann. Inst. Fourier (Grenoble) **67** (2017), no. 3, 1009–1033.

[DR00] M. Dettweiler and S. Reiter, *An algorithm of Katz and its application to the inverse Galois problem*, J. Symb. Comput. **30** (2000), no. 6, 761–798.

[Eke90] T. Ekedahl, *An effective version of Hilbert's irreducibility theorem*, Séminaire de Théorie des Nombres, Paris 1988–1989, Progr. Math., vol. 91, Birkhäuser Boston, Boston, MA, 1990, pp. 241–249.

[EM73] S. Endo and T. Miyata, *Invariants of finite Abelian groups*, J. Math. Soc. Japan **25** (1973), 7–26.

[Fis15] E. Fischer, *Die Isomorphie der Invariantenkörper der endlichen Abelschen Gruppen linearer Transformationen*, Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl. **1915** (1915), 77–80.

[FLN22] C. Frei, D. Loughran, and R. Newton, *Number fields with prescribed norms (with an appendix by Y. Harpaz and O. Wittenberg)*, Comment. Math. Helv. **97** (2022), no. 1, 133–181.

[Flo08] M. Florence, *On the essential dimension of cyclic p-groups*, Invent. math. **171** (2008), no. 1, 175–189.

[Ful69] W. Fulton, *Hurwitz schemes and irreducibility of moduli of algebraic curves*, Ann. Math. (2) **90** (1969), 542–575.

[FV91] M. D. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli spaces*, Math. Ann. **290** (1991), no. 4, 771–800.

[GMS03] S. Garibaldi, A. Merkurjev, and J.-P. Serre, *Cohomological invariants in Galois cohomology*, Univ. Lect. Ser., vol. 28, Providence, RI: American Mathematical Society (AMS), 2003.

[Gro03] A. Grothendieck (ed.), *Séminaire de géométrie algébrique du Bois Marie 1960-61 : revêtements étales et groupe fondamental (SGA 1)*, Documents Mathématiques, vol. 3, Société Mathématique de France, 2003.

[Gru33] W. Grunwald, *A general existence theorem for algebraic number fields*, J. reine angew. Math. **169** (1933), 103–107.

[GS17] P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*, 2nd ed., Camb. Stud. Adv. Math., vol. 165, Cambridge: Cambridge University Press, 2017.

[Har87] D. Harbater, *Galois coverings of the arithmetic line*, Number theory. A Seminar held at the Graduate School and University Center of the City University of New York 1984-85, Lect. Notes Math., vol. 1240, Springer, Cham, 1987.

[Har95] ———, *Fundamental groups of curves in characteristic p*, Proceedings of the international congress of mathematicians, ICM '94, August 3-11, 1994, Zürich, Switzerland. Vol. I, Birkhäuser, Basel, 1995, pp. 656–666.

[Har07] D. Harari, *Quelques propriétés d'approximation reliées à la cohomologie galoisienne d'un groupe algébrique fini*, Bull. Soc. Math. France **135** (2007), no. 4, 549–564.

[Hil92] D. Hilbert, *Über die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten*, J. reine angew. Math. **110** (1892), 104–129.

[Hos15] A. Hoshi, *On Noether's problem for cyclic groups of prime order*, Proc. Japan Acad., Ser. A **91** (2015), no. 3, 39–44.

[Hos20] ———, *Noether's problem and rationality problem for multiplicative invariant fields: a survey*, RIMS Kôkyûroku Bessatsu **B77** (2020), 29–53.

[Hur91] A. Hurwitz, *Ueber Riemann'sche Flächen mit gegebenen Verzweigungspunkten*, Math. Ann. **39** (1891), 1–61.

[HW20] Y. Harpaz and O. Wittenberg, *Zéro-cycles sur les espaces homogènes et problème de Galois inverse*, J. Amer. Math. Soc. **33** (2020), no. 3, 775–805.

[HW22] ———, *Supersolvable descent for rational points*, arXiv:2206.13832, 2022.

[Hä22] F. Häfner, *Braid orbits and the Mathieu group M_{23} as Galois group*, arXiv:2202.08222, 2022.

[JLY02] C. U. Jensen, A. Ledet, and N. Yui, *Generic polynomials. Constructive aspects of the inverse Galois problem*, Math. Sci. Res. Inst. Publ., vol. 45, Cambridge: Cambridge University Press, 2002.

[Jou83] J.-P. Jouanolou, *Théorèmes de Bertini et applications*, Prog. Math., vol. 42, Birkhäuser, Cham, 1983.

[KN71] W. Krull and J. Neukirch, *Die Struktur der absoluten Galoisgruppe über dem Körper $\mathbf{R}(t)$*, Math. Ann. **193** (1971), 197–209.

[Kol96] J. Kollár, *Rational curves on algebraic varieties*, Ergeb. Math. Grenzgeb. (3), vol. 32, Springer-Verlag, Berlin, 1996.

[Kol99] ———, *Rationally connected varieties over local fields*, Ann. Math. (2) **150** (1999), no. 1, 357–367.

[Kol00] ———, *Fundamental groups of rationally connected varieties*, Mich. Math. J. **48** (2000), 359–368.

[Kol03] ———, *Rationally connected varieties and fundamental groups*, Higher dimensional varieties and rational points. Lectures of the summer school and conference, Budapest, Hungary, September 3–21, 2001, Berlin: Springer; Budapest: János Bolyai Mathematical Society, 2003, pp. 69–92.

[LA19] G. Lucchini Arteche, *The unramified Brauer group of homogeneous spaces with finite stabilizer*, Trans. Amer. Math. Soc. **372** (2019), no. 8, 5393–5408.

[Len74] H. W. Jr. Lenstra, *Rational functions invariant under a finite Abelian group*, Invent. math. **25** (1974), 299–325.

[Len80] ———, *Rational functions invariant under a cyclic group*, Proc. Queen's Number Theory Conf. 1979, Queen's Pap. Pure Appl. Math. 54, 91-99 (1980), 1980.

[Mae89] T. Maeda, *Noether's problem for A_5*, J. Algebra **125** (1989), no. 2, 418–430.

[Man71] Yu. I. Manin, *Le groupe de Brauer-Grothendieck en géométrie diophantienne*, Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1, Gauthier-Villars, Paris, 1971, pp. 401–411.

[Mat87] B. H. Matzat, *Konstruktive Galoistheorie*, Lect. Notes Math., vol. 1284, Springer, Cham, 1987.

[MB01] L. Moret-Bailly, *Construction de revêtements de courbes pointées*, J. Algebra **240** (2001), no. 2, 505–534.

[Mer13] A. S. Merkurjev, *Essential dimension: a survey*, Transform. Groups **18** (2013), no. 2, 415–481.

[Mer17] ———, *Essential dimension*, Bull. Am. Math. Soc., New Ser. **54** (2017), no. 4, 635–661.

[Mes90] J.-F. Mestre, *Extensions régulières de $\mathbb{Q}(T)$ de groupe de galois $\tilde{A}_n$*, J. Algebra **131** (1990), no. 2, 483–495.

[Mes94] ———, *Construction of regular extensions of $\mathbb{Q}(t)$ with galois groups $SL_2(\mathbb{F}_7)$ and $\widetilde{M}_{12}$*, C. R. Acad. Sci., Paris, Sér. I **319** (1994), no. 8, 781–782.

[Mes98] ———, *$\mathbb{Q}$-regular extensions of $\mathbb{Q}(t)$ with galois groups $6.A_6$ and $6.A_7$*, Isr. J. Math. **107** (1998), 333–341.

[Mes05] ———, *Correspondances compatibles avec une relation binaire, relèvement d'extensions de groupe de Galois* $\mathrm{L}_3(2)$ *et problème de Noether pour* $\mathrm{L}_3(2)$, arXiv:math/0402187, 2005.

[MFK94] D. Mumford, J. Fogarty, and F. Kirwan, *Geometric invariant theory*, 3rd enl. ed., Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, vol. 34, Berlin: Springer-Verlag, 1994.

[Mil20] J. S. Milne, *Class field theory*, 2020, course notes, version 4.03, available from the author's webpage at https://www.jmilne.org/math/CourseNotes/CFT.pdf, pp. 287+viii.

[MM18] G. Malle and B. H. Matzat, *Inverse Galois theory*, 2nd ed., Springer Monogr. Math., Berlin: Springer, 2018.

[Mum08] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Hindustan Book Agency, New Delhi, 2008, with appendices by C. P. Ramanujam and Yu. Manin; corrected reprint of the second (1974) edition.

[Neu79] J. Neukirch, *On solvable number fields*, Invent. math. **53** (1979), no. 2, 135–164.

[Ngu23] M. L. Nguyễn, *Around the descent conjecture*, preprint, 42 pages, 2023.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer-Verlag, Berlin, 2008.

[Pey08] E. Peyre, *Unramified cohomology of degree 3 and Noether's problem*, Invent. math. **171** (2008), no. 1, 191–225.

[Pla17] B. Plans, *On Noether's rationality problem for cyclic groups over* $\mathbb{Q}$, Proc. Am. Math. Soc. **145** (2017), no. 6, 2407–2409.

[Poo17] B. Poonen, *Rational points on varieties*, Grad. Stud. Math., vol. 186, Providence, RI: American Mathematical Society (AMS), 2017.

[Pop96] F. Pop, *Embedding problems over large fields*, Ann. Math. (2) **144** (1996), no. 1, 1–34.

[PV04] B. Poonen and J. F. Voloch, *Random Diophantine equations*, Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002), Progr. Math., vol. 226, Birkhäuser Boston, Boston, MA, 2004, with appendices by J.-L. Colliot-Thélène and N. M. Katz, pp. 175–184.

[Rei11] Z. Reichstein, *Essential dimension*, Proceedings of the international congress of mathematicians (ICM 2010), Hyderabad, India, August 19–27, 2010. Vol. II: Invited lectures, Hackensack, NJ: World Scientific; New Delhi: Hindustan Book Agency, 2011, pp. 162–188.

[Rei21] ———, *From Hilbert's 13th problem to essential dimension and back*, Eur. Math. Soc. Mag. **122** (2021), 4–15.

[RW06] M. Romagny and S. Wewers, *Hurwitz spaces*, Groupes de Galois arithmétique et différentiels, Société Mathématique de France, 2006, pp. 313–341.

[Sal82] D. J. Saltman, *Generic Galois extensions and problems in field theory*, Adv. Math. **43** (1982), 250–283.

[Sal84] ———, *Noether's problem over an algebraically closed field*, Invent. math. **77** (1984), 71–84.

[Sal85] ———, *The Brauer group and the center of generic matrices*, J. Algebra **97** (1985), 53–67.

[San81] J.-J. Sansuc, *Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres*, J. reine angew. Math. **327** (1981), 12–80.

[Ser97] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, 3rd ed., Aspects Math., vol. E15, Wiesbaden: Vieweg, 1997.

[Ser07] ———, *Topics in Galois theory*, 2nd ed., Res. Notes Math., vol. 1, Wellesley, MA: A K Peters, 2007.

[Shi74] K.-y. Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Ann. **207** (1974), 99–120.

[Sko01] A. N. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, Cambridge, 2001.

[Spe19] A. Speiser, *Zahlentheoretische Sätze aus der Gruppentheorie*, Math. Z. **5** (1919), 1–6.

[Swa69] R. G. Swan, *Invariant rational functions and a problem of Steenrod*, Invent. math. **7** (1969), 148–158.

[Swa83] ———, *Noether's problem in Galois theory*, Emmy Noether in Bryn Mawr, Proc. Symp., Bryn Mawr/USA 1982, 21–40 (1983), 1983.

[Sza09] T. Szamuely, *Galois groups and fundamental groups*, Camb. Stud. Adv. Math., vol. 117, Cambridge: Cambridge University Press, 2009.

[Völ96] H. Völklein, *Groups as Galois groups: an introduction*, Camb. Stud. Adv. Math., vol. 53, Cambridge: Cambridge Univ. Press, 1996.

[Völ01] ———, *The braid group and linear rigidity*, Geom. Dedicata **84** (2001), no. 1-3, 135–150.

[Vos70] V. E. Voskresenskiĭ, *Birational properties of linear algebraic groups*, Izv. Akad. Nauk SSSR, Ser. Mat. **34** (1970), 3–19.

[Vos71] ———, *Rationality of certain algebraic tori*, Izv. Akad. Nauk SSSR, Ser. Mat. **35** (1971), 1037–1046.

[Vos73] V. E. Voskresenskii, *Fields of invariants for Abelian groups*, Usp. Mat. Nauk **28** (1973), no. 4 (172), 77–102.

[Vos98] V. E. Voskresenskiĭ, *Algebraic groups and their birational invariants*, Translations of Mathematical Monographs, vol. 179, American Mathematical Society, Providence, RI, 1998.

[Wan50] S. Wang, *On Grunwald's theorem*, Ann. Math. (2) **51** (1950), 471–484.

[Wew98] S. Wewers, *Construction of Hurwitz spaces*, Ph.D. thesis, Essen, 1998.

[Wit18] O. Wittenberg, *Rational points and zero-cycles on rationally connected varieties over number fields*, Algebraic geometry: Salt Lake City 2015, Proc. Sympos. Pure Math., vol. 97, Amer. Math. Soc., Providence, RI, 2018, pp. 597–635.

[Zyw13] D. Zywina, *Inverse Galois problem for small simple groups*, unpublished note, available from the author's webpage at http://pi.math.cornell.edu/~zywina/papers/smallGalois.pdf, 2013.

[Zyw15] ———, *The inverse Galois problem for* $\mathrm{PSL}_2(\mathbb{F}_p)$, Duke Math. J. **164** (2015), no. 12, 2253–2292.

Institut Galilée, Université Sorbonne Paris Nord, 99 avenue Jean-Baptiste Clément, 93430 Villetaneuse, France

Email address: `wittenberg@math.univ-paris13.fr`