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 lecture series will be 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.

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

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. In other words, given a finite group G and a field k, does there exist a Galois field extension K of k with $\mathrm{Gal}(K/k) \simeq G$? 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 $\mathbf{Q}_p$, 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), when G is a sporadic group other than M_{23} (Shih, Fried, Belyi, Matzat, Thompson, Hoyden-Siedersleben, Zeh-Marschke, Hunt, Pahlings), 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,

Date: July 28th, 2022.

Zywina; see [Zyw15]); but the problem remains open over $\mathbf{Q}$ even for such a small group as $\mathrm{PSL}_2(\mathbf{F}_{27})$ (see [Zyw13]).

Several variants or generalisations of the inverse Galois problem have been considered. 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 (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 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 the completion of K/k at any place of K lying above a place $v \in S$ 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 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 1.20 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 and a surjection $\varphi : G \twoheadrightarrow \mathrm{Gal}(\ell/k)$ from a finite group G, can one embed ℓ/k into a Galois field extension K/k such that $G \simeq \mathrm{Gal}(K/k)$, with φ being identified with the restriction map between Galois groups?) 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 (see [FLN18]).

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. 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, in more fancy language, as an irreducible G-torsor over k (that is, over $\mathrm{Spec}(k)$); which is the same 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 1.3. Given a subgroup $H \subseteq G$, any H-torsor $Y \to X$ gives rise to a G-torsor $Y' \to X$. Namely, say G acts on the right on Y, we let H act on the left on $Y \times G$ by $h \cdot (y, g) = (yh^{-1}, hg)$ and observe that $Y' = (Y \times G)/H$ receives a free right action of G. The variety Y' is the disjoint union of $(G : H)$ copies of 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, and Y' coincides with $(Y \times G)/H$.

1.3. **Hilbert's irreducibility theorem.** When the base is an open subset of $\mathbf{P}^1_k$, the existence of irreducible fibres above rational points of the base is guaranteed by Hilbert's irreducibility theorem, classically formulated in the following way, equivalent to the statement of Theorem 1.4 below: given an irreducible two-variable polynomial $f(x, t)$ with coefficients in a number field k, there exist infinitely many $t_0 \in k$ such that $f(x, t_0)$ is an irreducible one-variable polynomial with coefficients in k.

Theorem 1.4. *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.*

Corollary 1.5. *Same statement, with X now a dense open subset of $\mathbf{P}^n_k$ for some $n \geq 1$.*

Combining Corollary 1.5 with the remarks of §1.2 leads to the following extremely useful observation, due to Hilbert. We recall that a variety X over a field k is said to be *rational* if it is birationally equivalent to 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 1.6. *Let k be a number field. Let G be a finite group. If there exist a 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.*

Note that if G acts faithfully on Y, then it acts freely on a dense open subset of Y.

Example 1.7. 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).

Ekedahl proved a useful generalisation of Hilbert's irreducibility theorem:

Theorem 1.8 ([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. There exists* *a nonempty open subset $\mathscr{U} \subset \prod_{v\in\Omega\setminus S} X(k_v)$ such that for any $x \in X(k) \cap \mathscr{U}$, 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 is endowed with the product of the v-adic topologies.

1.4. **Noether's problem: statement.** Corollary 1.6 led Emmy Noether to ask:

Problem 1.9 (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 1.6, 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. Noether's problem, however, is a central problem in the study of rationality and has been the focus of much research for its own sake.

Example 1.10. 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 even isomophic 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.

Example 1.11. Noether's problem has a positive answer for abelian groups of exponent n over fields whose characteristic does not divide n and which contain the nth roots of unity; in particular, for all abelian groups over $\mathbf{C}$. This is a theorem of Fischer [Fis15].

Example 1.12. 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, for any $n \geq 6$ and any field k, Noether's problem is open for $G = A_n$ over k.

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 §1.6.

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 1.13. 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 *versal*[1] if for any field extension k'/k, any G-torsor over k' can be realised as the fibre of π above a k'-point of X.

Example 1.14. 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

[1] Usually one requires that the set of k'-points of X satisfying this condition be not only nonempty but even Zariski dense. We shall refer to torsors satisfying this stronger property as being "strongly versal".

and it can be checked, as a consequence of Hilbert's Theorem 90, according to which the Galois cohomology set $H^1(k', \mathrm{GL}_n)$ is trivial, that the resulting torsor $\pi : Y \to X = Y/G$ is versal.

Example 1.15. 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 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.

Remark 1.16. 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 $\mathbf{A}^n_k/G$ and SL_n/G appearing in Examples 1.14 and 1.15 all fall into the same stable birational equivalence class of varieties over k (regardless of the choices of embeddings $G \hookrightarrow S_n$ or $G \hookrightarrow \mathrm{SL}_n(k)$). This is the so-called "no-name lemma", see [CTS07, Corollary 3.9].

The notion of versality, in the context of these notes[2], is motivated by the following observation, which is an improved version of Corollary 1.6:

Proposition 1.17. *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 a smooth quasi-projective variety Y over k and a free action of G on Y such that the G-torsor $Y \to Y/G$ is versal and the variety Y/G satisfies weak approximation off S_0 (that is, the diagonal embedding $X(k) \hookrightarrow \prod_{v\in\Omega\setminus S_0} X(k_v)$ has dense image). Then Grunwald's problem admits a positive answer for G over k, for any finite subset $S \subset \Omega$ disjoint from S_0.*

Proof. Set $X = Y/G$ and let $\pi : Y \to X$ be the quotient map. 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 1.18 (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, choose embeddings $\mathrm{Gal}(K_v/k_v) \hookrightarrow G$ for $v \in S$. The resulting G-torsors over k_v for $v \in S$ given by Remark 1.3 come, by versality, from k_v-points $x_v \in X(k_v)$. Lemma 1.18 provides, for every $v \in S$, a neighbourhood $\mathscr{U}_v \subset X(k_v)$ of x_v such that $\pi^{-1}(x'_v)$ is isomorphic to $\pi^{-1}(x_v)$ for all $x'_v \in \mathscr{U}_v$. In particular, by Remark 1.3 again, for all $x'_v \in \mathscr{U}_v$, the connected components of $\pi^{-1}(x'_v)$ are isomorphic to $\mathrm{Spec}(K_v)$. On the other hand, applying Theorem 1.8 to π and S produces 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. For $x \in X(k) \cap \mathscr{U}$, the fibre

[2] 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 strongly versal G-torsor defined over k—which is interesting in its own right and has been the focus of many works. Even determining the essential dimension of $\mathbf{Z}/8\mathbf{Z}$ over $\mathbf{Q}$ is a highly nontrivial task (see [Flo08]).

$\pi^{-1}(x)$ is now an irreducible G-torsor (i.e. $\mathrm{Spec}(K)$ for some Galois 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 1.17 with $S_0 = \varnothing$ whenever Y/G is rational. In view of Example 1.14, we deduce:

Corollary 1.19. *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 $S \subset \Omega$.*

In particular, 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 1.10 and Example 1.12).

1.6. Noether's problem: some counterexamples.

Unfortunately, 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 counterexamples $\mathbf{Z}/8\mathbf{Z}$ and $\mathbf{Z}/47\mathbf{Z}$ over $\mathbf{Q}$. As Saltman later observed, Corollary 1.19 provides a direct proof that Noether's problem admits a negative answer for $\mathbf{Z}/8\mathbf{Z}$ over $\mathbf{Q}$. Namely, 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 what Wang had done in the 1940's:

Proposition 1.20 (Wang)**.** *In a cyclic field extension $K/\mathbf{Q}$ of degree 8, the prime 2 cannot be inert. In other words, the completion of K 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] or in the exercises.

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 1.9 (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, in terms of the arithmetic of cyclotomic number fields. For cyclic groups over $\mathbf{Q}$, this characterisation reads as follows (see [Len80, §3]):

Theorem 1.21 (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 1.21 when n is a prime number is due to Voskresenskiĭ [Vos71]. Even when n is prime, determining whether condition (3) of Theorem 1.21 does or does not hold for a given n is in general a hard problem; for instance this condition was only recently shown to fail when $n = 59$ (see [Hos15, Added remark 3.2]). Even more recently, based on Theorem 1.21, 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 1.22 (Plans)**.** *Condition (3) of Theorem 1.21 is also 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.

1.6.2. *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 work was then generalised by Bogomolov [Bog88], who proved the following theorem:

Theorem 1.23 (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*

$$\mathrm{Ker}\Big(H^2(G, \mathbf{Q}/\mathbf{Z}) \to \prod H^2(H, \mathbf{Q}/\mathbf{Z})\Big), \tag{1.1}$$

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. 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 used as a tool for rationality questions by Artin and Mumford [AM72], who applied it 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 1.16, 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 (1.1) 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]).

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 1.24 (Saltman [Sal82])**.** *In the situation of Problem 1.9, 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 1.24 can in particular be applied to all finite abelian groups of odd order.

Retract rationality is weaker than rationality, but as far as the applications to the inverse Galois problem are concerned, it is just as good: indeed, smooth retract rational varieties over number fields are easily seen to satisfy weak approximation.

Combining this observation with Theorem 1.24 and with Proposition 1.17, we deduce, in view of Example 1.14, 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 1.24—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.

Conversely, by the same token, Wang's negative answer to Grunwald's problem (see Proposition 1.20) 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 §1.6.2 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 gets weakened to 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 even 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 on which G acts freely. This is the regular inverse Galois problem:

Problem 2.1 (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. 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.*

By Hilbert's irreducibility theorem, when k is a number field, a positive answer to Problem 2.1 for k and G implies a positive answer to the inverse Galois problem for k and G. Unlike the latter, though, and also unlike Noether's problem, Problem 2.1 might have a positive answer for every finite group G and every field k, as far as one knows.

Remark 2.2. 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]).

2.2. **Riemann's existence theorem.** A solution to the regular inverse Galois problem over k is in particular also 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 $\bar{\mathbf{Q}}$; the key tool for this is Riemann's existence theorem, which allows one to transform this algebraic question into a purely topological one.

Theorem 2.3 (Riemann's existence theorem)**.** *Let k be an algebraically closed subfield of $\mathbf{C}$. Let V be a variety over k. The natural functor*

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

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

An *étale covering* of V is a variety over k endowed with a finite étale morphism to V and a topological covering is *finite* if its fibres are finite. Theorem 2.3 in the above formulation is proved in [Gro03] (see Exp. XII, Théorème 5.1 and Exp. XIII, Corollaire 3.5) and builds on Grothendieck's reworking of Serre's GAGA theorems.

Corollary 2.4. *Fix $v \in V(k)$ and assume that V is connected. For any finite group G, isomorphism classes of G-torsors (resp. of connected G-torsors) $W \to V$ endowed with a lift $w \in W(k)$ of v are canonically in one-to-one correspondence with homomorphisms $\pi_1(V(\mathbf{C}), v) \to G$ (resp. with surjective homomorphisms $\pi_1(V(\mathbf{C}), v) \twoheadrightarrow G$). Changing the choice of w amounts to conjugating the homomorphism by an element of G.*

Proof. Indeed, this follows from Theorem 2.3 combined with the well-known equivalence of categories between the category of topological coverings of $V(\mathbf{C})$ and the category of sets endowed with an action of $\pi_1(V(\mathbf{C}), v)$ (see [Sza09, Theorem 2.3.4]). The homomorphism $\pi_1(V(\mathbf{C}), v) \to G$ corresponding to $W \to V$ sends $\gamma \in \pi_1(V(\mathbf{C}), v)$ to the unique $g \in G$ such that $\gamma w = wg$, where we are taking the convention that the action of G on W is a right action and that the monodromy action of $\pi_1(V(\mathbf{C}), v)$ on the fibre of $W(\mathbf{C}) \to V(\mathbf{C})$ above v is a left action. □

Remark 2.5 (reminder on monodromy groups and Galois groups)**.** Let k and V be as in Theorem 2.3. Let $v \in V(\mathbf{C})$. The *monodromy group M* of an étale covering $W \to V$ is, by definition, the largest quotient of $\pi_1(V(\mathbf{C}),v)$ through which the monodromy action of this group on the fibre of $W(\mathbf{C}) \to V(\mathbf{C})$ above v factors. Assume that V is normal and irreducible and let $W' \to W \to V$ be a tower of irreducible étale coverings such that the field extension $k(W')/k(V)$ is a Galois closure of $k(W)/k(V)$. Let $G = \mathrm{Gal}(k(W')/k(V))$. Then $W' \to V$ is the normalisation of V in $k(W')$; as such, it receives an action of G, with respect to which it is a G-torsor; in addition, the surjective homomorphism $\pi_1(V(\mathbf{C}),v) \twoheadrightarrow G$ corresponding, by Corollary 2.4, to $W' \to V$ and to the choice of a lift $w' \in W'(k)$ of v induces an isomorphism $M \xrightarrow{\sim} G$. (Changing the choice of the lift w' amounts to composing this isomorphism with an inner automorphism.) Thus, computing the Galois group of the Galois closure of the field extension $k(W)/k(V)$ 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 2.3 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 2.6. *Let $V \subseteq \mathbf{P}^1_{\mathbf{C}}$ be a dense open subset. Write $\mathbf{P}^1_{\mathbf{C}} \setminus V = \{b_1,\dots,b_r\}$. Let $v \in V(\mathbf{C})$. The group $\pi_1(V(\mathbf{C}),v)$ admits a canonical 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 $\pi_1(V(\mathbf{C}),v)$ of a local counterclockwise loop around b_i.*

What the last sentence of Proposition 2.6 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 v to a point of this loop, to an element of $\pi_1(V(\mathbf{C}),v)$ whose conjugacy class does not depend on the chosen path. The content of Proposition 2.6 is that these paths can be chosen in such a way that the γ_i generate $\pi_1(V(\mathbf{C}),v)$ and satisfy the relation $\gamma_1 \cdots \gamma_r = 1$. This is elementary and well-known.

Using Proposition 2.6, we can draw the following corollary from Riemann's existence theorem. It 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 Corollary 2.7 refers to the name Nielsen, see [Völ96, §9.2], [RW06, §3.1].)

Corollary 2.7. *Let k be an algebraically closed subfield of $\mathbf{C}$. Let $V \subseteq \mathbf{P}^1_k$ be a dense open subset. Write $\mathbf{P}^1_{\mathbf{C}} \setminus V = \{b_1,\dots,b_r\}$. 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 V is canonically in bijection with $\mathrm{ni}^*_r(G)$.*

Proof. By Corollary 2.4, isomorphism classes of irreducible G-torsors over V are canonically in one-to-one correspondence with conjugacy classes of surjections $\pi_1(V(\mathbf{C}),v) \twoheadrightarrow G$. Apply Proposition 2.6 to conclude. □

Corollary 2.8. *For any finite group G, the regular inverse Galois problem admits a positive answer over $\bar{\mathbf{Q}}$.*

Proof. Let r be a large enough integer that G can be generated by $r-1$ elements. Choose r points of $\mathbf{P}^1(\bar{\mathbf{Q}})$. Let $V \subset \mathbf{P}^1_{\bar{\mathbf{Q}}}$ denote their complement. As $\mathrm{ni}_r^*(G) \neq \varnothing$, Corollary 2.7 ensures the existence of an irreducible G-torsor $p : W \to V$. As W is normal and p is finite, the normalisation of $\mathbf{P}^1_{\bar{\mathbf{Q}}}$ in the function field of W is a smooth curve C over $\bar{\mathbf{Q}}$ containing W 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), as desired. □

2.4. Monodromy of some non-Galois covers of the projective line.

Proposition 2.6 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 2.9. *Let C be a smooth, projective, irreducible curve over $\mathbf{C}$. Let $\pi : C \to \mathbf{P}^1_{\mathbf{C}}$ be a finite morphism, étale over a dense open subset $V \subseteq \mathbf{P}^1_{\mathbf{C}}$. Fix $v \in V(\mathbf{C})$ and write $\mathbf{P}^1_{\mathbf{C}} \setminus V = \{b_1, \dots, b_r\}$. Let M denote the monodromy group of π, i.e. the largest quotient of $\pi_1(V(\mathbf{C}), v)$ that still acts on $\pi^{-1}(v)$. After choosing a bijection $\pi^{-1}(v) \simeq \{1, \dots, n\}$, 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 2.6 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 2.10. 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 2.5 and Proposition 2.9 show that this Galois group is a transitive subgroup of S_n generated by transpositions; the only such subgroup is S_n itself (exercise).

In conjunction with Remark 2.11 below, Example 2.10 leads to many concrete examples of regular Galois extensions of $\mathbf{Q}(t)$ with group S_n. Recall, though, that we already knew that the regular inverse Galois problem admits a positive answer for S_n over $\mathbf{Q}$, thanks to the positive answer to Noether's problem for S_n over $\mathbf{Q}$ (Example 1.10), see Remark 2.2. 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 2.9 also leads to concrete examples of regular Galois extensions of $\mathbf{Q}(t)$ with group A_n, as we shall see in the exercises.

Remark 2.11. Let $\mathbf{Q}(t) \subseteq K \subseteq K' \subset \overline{\mathbf{Q}(t)}$ be a tower of fields, where $\overline{\mathbf{Q}(t)}$ denotes an algebraic closure of $\mathbf{Q}(t)$ and where $K/\mathbf{Q}(t)$ is a finite extension and $K'/\mathbf{Q}(t)$ is its

Galois closure inside $\overline{\mathbf{Q}(t)}$. Even if $\mathbf{Q}$ is algebraically closed in K, it need not, in general, be algebraically closed in K'. (Example: if $K = \mathbf{Q}(t^{1/n})$, then $K' = \mathbf{Q}(\zeta_n)(t^{1/n})$.) This pathology, however, cannot occur if the geometric Galois group is the full symmetric group. Indeed, set $G = \mathrm{Gal}(K'/\mathbf{Q}(t))$ and $G_{\mathrm{geom}} = \mathrm{Gal}(\bar{\mathbf{Q}}K'/\bar{\mathbf{Q}}(t))$, where $\bar{\mathbf{Q}}K'$ denotes the subfield of $\bar{\mathbf{Q}}(t)$ generated by $\bar{\mathbf{Q}}$ and K'. We remark that $\bar{\mathbf{Q}}K'/\bar{\mathbf{Q}}(t)$ is a Galois closure of $\bar{\mathbf{Q}}K/\bar{\mathbf{Q}}(t)$, so that its Galois group G_{geom} can be viewed as the topological monodromy group associated with $K/\mathbf{Q}(t)$ (see Remark 2.5). Fix a primitive element $\alpha_1 \in K$ over $\mathbf{Q}(t)$. 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 $G_{\mathrm{geom}} \subseteq G \subseteq S_n$. Obviously, if $G_{\mathrm{geom}} = S_n$, then $G = G_{\mathrm{geom}}$ and hence $\mathbf{Q}$ is algebraically closed in K'. Thus, for instance, if the curve C and the morphism π of Example 2.10 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.

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 take advantage of the solutions constructed over $\bar{\mathbf{Q}}$ 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[3,4]:

Theorem 2.12 (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 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).

Theorem 2.12 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 had deduced the following result in positive characteristic:

Theorem 2.13 (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 shed new light on Theorem 2.12 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

[3] It is not clear on a first reading whether or not the article [Pop96] proves Theorem 2.12 as we have stated it, without assuming the field to be perfect; indeed, we have required, in our definition of the regular inverse Galois problem, that the sought-for field extension of $k(t)$ admit a *smooth* projective model, which could fail over imperfect fields. In any case, Theorem 2.12 as we have stated it is also shown in [MB01, Théorème 1.1].

[4] Theorem 2.12 (at least for perfect large fields, see the previous footnote) also follows from the results of Harbater [Har87], see [Har95, §4.5].

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 2.12 that proceeds by constructing rational curves of $\mathbf{A}^n_k/G$ was thus given in [CT00] (see also [Kol00], [Kol03], [MB01] for generalisations).

Unfortunately, no method is known for the systematic construction of rational curves on rationally connected varieties over $\mathbf{Q}$; and more generally, the various methods on which all known proofs of Theorem 2.12 rely fall short of solving any case of the regular inverse Galois problem over any given number field.

As of today, all 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 Fried, Belyi, Matzat and Thompson in the 1970's and the 1980's, which we discuss next.

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; this 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 2.14. 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. 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 (any finite group is a quotient of a finite group with trivial centre) and it will ensure that the objects that we want to classify have no nontrivial automorphism, and hence that the moduli space we are after is a variety rather than a stack.

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 $\mathscr{U}_r$ its quotient 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 2.15 (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.*

A modern approach to Theorem 2.15 consists in defining G-covers not just over fields, as in Definition 2.14, 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. 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 covers with "simple" ramification, i.e. all ramification points have ramification index 2 and no two of them lie over the same branch point, which is insufficient for the purposes of the regular inverse Galois problem (see Example 2.10).

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 such a question to be tractable, one needs some understanding of the geometry of $\mathscr{H}_{G,r}$.

The varieties $\mathscr{H}_{G,r}$ can be described in a very explicit combinatorial fashion, at least geometrically. Let us pick up the notation $\mathrm{ni}^*_r(G)$ introduced in Corollary 2.7 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 Corollary 2.7 that the fibre of ρ above any complex point of $\mathscr{U}_r$ can be canonically 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 2.15.

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 branch point. Let $V \subset \mathbf{P}^1_k$ 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 2.7. We recall that it is the image, by a surjection $\pi_1(V(\mathbf{C}), v) \twoheadrightarrow G$ 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 2.15 and in particular understand how it behaves with respect to the action of the group of automorphisms of k, we need to make it algebraic. This is done as follows. 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 $\bar{k}((u))$ and its absolute Galois group is canonically isomorphic to $\hat{\mathbf{Z}}(1)_{\bar{k}} = \varprojlim_{n\geq 1} \boldsymbol{\mu}_n(\bar{k})$. The inclusion $\bar{k}(t) \hookrightarrow \bar{k}(t)_{b_i}$ induces a homomorphism in the reverse direction, well-defined up to conjugation, between the absolute Galois groups of these fields, and hence 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 2.7. We call it the *algebraic local monodromy* of π at b_i.

Remark 2.16. When k is a subfield of $\mathbf{C}$, setting $\zeta_n = e^{2i\pi/n}$ allows one to identify $\hat{\mathbf{Z}}(1)_{\bar{k}}$ with $\hat{\mathbf{Z}}$ as topological groups (i.e. disregarding Galois actions), so that we do canonically recover, in this case, a conjugacy class of G from the algebraic local monodromy of π at b_i. One verifies that it coincides with the conjugacy class of g_i from Corollary 2.7.

2.7.2. *Factoring ρ.* For any field k of characteristic 0, there is a natural continuous action of $\mathrm{Gal}(\bar{k}/k)$ on the finite set of continuous homomorphisms $\hat{\mathbf{Z}}(1)_{\bar{k}} \to G$ and hence also on its quotient by the conjugation action of G. We can therefore view the latter quotient set as the group of $\bar{k}$-points of a reduced 0-dimensional variety over $\mathbf{Q}$ that is canonically associated with G. Let us denote it by $\mathscr{C}_G$. Let us endow $(\mathscr{C}_G)^r = \mathscr{C}_G \times \cdots \times \mathscr{C}_G$ with the natural action of the symmetric group S_r and denote by $\mathscr{V}_r$ the quotient of $\mathscr{U}^r \times (\mathscr{C}_G)^r$ by the diagonal action of S_r. We have thus produced an étale covering $\nu : \mathscr{V}_r \to \mathscr{U}_r$. 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 $\mathbf{P}^1_k$ of degree r endowed with a morphism to $\mathscr{C}_G$. Associating with each G-cover and each branch point the corresponding algebraic local monodromy (in the sense of §2.7.1) finally provides us with a morphism $\rho' : \mathscr{H}_{G,r} \to \mathscr{V}_r$ such that $\rho = \nu \circ \rho'$.

Noting that Remark 2.16 identifies $\mathscr{C}_G(\mathbf{C})$ with the set $\mathrm{Cl}(G)$ of conjugacy classes of G, Corollary 2.7 and Remark 2.16 imply the following description of the complex fibres of ρ':

Proposition 2.17. *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 2.16. 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 $i \in \{1, \ldots, r\}$.

2.7.3. *Rational points on $\mathscr{C}_G$.* Viewing $\bar{\mathbf{Q}}$ as a subfield of $\mathbf{C}$, Remark 2.16 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 $\mathscr{C}_G(\mathbf{Q})$ gets identified with the set of *rational* conjugacy classes of G in the following sense:

Definition 2.18. A conjugacy class of a finite group G is *rational* if its elements g are such that g^n and g are conjugate in G for any integer $n \geq 1$ prime to the order of g.

2.7.4. *Rational points on $\mathscr{V}_r$.* Here is a simple way to exhibit rational points on $\mathscr{V}_r$. Let $b_1, \dots, b_r \in \mathbf{P}^1(\mathbf{Q})$ be pairwise distinct. Let $B = \{b_1, \dots, b_r\}$. 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.

2.7.5. *Rational points on $\mathscr{H}_{G,r}$.* The morphism $\rho' : \mathscr{H}_{G,r} \to \mathscr{V}_r$ is an étale covering and 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 equal to the cardinality of $\mathrm{ni}_r(G)$ as we have seen in §2.6. A trivial but nevertheless favourable situation for producing rational points of $\mathscr{H}_{G,r}$ is when ρ' has degree 1 (i.e. induces an isomorphism) over a connected component of $\mathscr{V}_r$. Such connected components of $\mathscr{V}_r$ are said to be *rigid*. By Proposition 2.17, the rigidity of a connected component can be verified by computing the set $\mathrm{ni}_r^C(G)$ corresponding to its complex points. This motivates the following definition:

Definition 2.19. An r-tuple $C = (C_1, \dots, C_r)$ of nontrivial conjugacy classes of G is *rigid* if the set $\mathrm{ni}_r^C(G)$ defined in Proposition 2.17 has cardinality 1.

2.7.6. *Summing up.* We thus arrive at a down-to-earth condition that implies that the rational points of $\mathscr{V}_r$ constructed in §2.7.4 can be lifted to rational points of $\mathscr{H}_{G,r}$.

Theorem 2.20. *Let G be a finite group with trivial centre. Let $r \geq 1$ be an integer. If there exists a rigid collection $C = (C_1, \dots, C_r)$ 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 2.20 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 rationality condition; con: the conjugacy classes cannot be chosen independently of one another any longer.) Even just the above base case is already unreasonably effective: the hypothesis of Theorem 2.20 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].

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. The Grunwald problem and the Brauer–Manin obstruction

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.

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

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

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

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

[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.

[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.

[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.

[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.

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

[FLN18] C. Frei, D. Loughran, and R. Newton, *Number fields with prescribed norms*, arXiv:1810.06024, to appear, Commentarii Mathematici Helvetici, 2018.

[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.

[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.

[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.

[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.

[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, *Théoremes 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.

[Kol99] J. Kollár, *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.

[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.

[Mat87] B. H. Matzat, *Konstruktive Galoistheorie. (Constructive Galois theory)*, 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.

[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.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, seconde 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.

[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.

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

[Swa83] R. G. Swan, *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.

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

[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.

[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`