The scheme of monogenic generators II: local monogenicity and twists

Arpin, S.A.; Bozlee, S.; Herr, L.S.; Smith, H.

RESEARCH

The scheme of monogenic generators II: local monogenicity and twists

Sarah Arpin[1], Sebastian Bozlee[2*] [iD], Leo Herr[1] and Hanson Smith[3]

*Correspondence:
sebastian.bozlee@tufts.edu
[2]Tufts University, Medford, USA
Full list of author information is
available at the end of the article

Abstract

This is the second paper in a series of two studying monogenicity of number rings from a moduli-theoretic perspective. By the results of the first paper in this series, a choice of a generator θ for an A-algebra B is a point of the scheme $\mathcal{M}_{B/A}$. In this paper, we study and relate several notions of local monogenicity that emerge from this perspective. We first consider the conditions under which the extension B/A admits monogenerators locally in the Zariski and finer topologies, recovering a theorem of Pleasants as a special case. We next consider the case in which B/A is étale, where the local structure of étale maps allows us to construct a universal monogenicity space and relate it to an unordered configuration space. Finally, we consider when B/A admits local monogenerators that differ only by the action of some group (usually $\mathbb{G}_m$ or Aff^1), giving rise to a notion of twisted monogenerators. In particular, we show a number ring A has class number one if and only if each twisted monogenerator is in fact a global monogenerator θ.

Mathematics Subject Classification: Primary 14D20, Secondary 11R04, 13E15

Contents

1 Introduction

We begin by recalling the essential points of the previous paper of this series [4]. Given an extension of commutative rings with identity (henceforth, rings) B/A, we say that that B is *monogenic over A* if there is an element $\theta \in B$ so that $B = A[\theta]$. Such an element is called a *monogenerator*. Similarly, B is said to be *k-genic over A* if there exists a tuple $(\theta_1, \ldots, \theta_k) \in B^k$ so that $B = A[\theta_1, \ldots, \theta_k]$. Such a tuple is a *generating k-tuple*. We are motivated by the case of an extension of number rings $\mathbb{Z}_L/\mathbb{Z}_K$.

Such extensions of number rings are finite locally free over a Noetherian base. In fact all we need for our results are maps of schemes that are Zariski locally of this form. We gather these hypotheses into a common "Situation" for convenience.

Situation 1.1 *Let $\pi : S' \to S$ be a finite locally free morphism of schemes of constant degree $n \geq 1$ with S locally noetherian, and let $X \to S$ be a quasiprojective morphism (almost always $\mathbb{A}_S^1$ or $\mathbb{A}_S^k$).*

In the preceding paper we prove the following representability result, which implies in particular that if B is finite locally free over a Noetherian ring A, then there is a scheme that represents the monogenerators for B over A.

Theorem 1.2 *([4, Proposition 2.3, Corollary 3.8]) Let $\pi : S' \to S$ be as in Situation 1.1. Then*

(1) *There exists a smooth, quasiaffine S-scheme $\mathcal{M}_{X,S'/S}$ representing the contravariant functor on S-schemes*

$$(T \to S) \mapsto \left\{ \begin{array}{c} S' \times_S T \xrightarrow{\quad s \quad} X \times_S T \\ \searrow \quad \swarrow \\ T \end{array} \;\middle|\; s \text{ is a closed immersion.} \right\}.$$

(2) *If $X = \mathbb{A}_S^1$, then $\mathcal{M}_{X,S'/S}$ is an affine S-scheme.*

We write $\mathcal{M}_{k,S'/S}$ for the case in which $X = \mathbb{A}_S^k$. We call the scheme $\mathcal{M}_{k,S'/S}$ the *scheme of k-generators*. If $k = 1$, we write $\mathcal{M}_{S'/S}$ instead of $\mathcal{M}_{1,S'/S}$ and call it the *scheme of monogenerators* or *monogenicity space*. If $S' = \operatorname{Spec} B$ and $S = \operatorname{Spec} A$ are affine, we may write $\mathcal{M}_{k,B/A}$ or $\mathcal{M}_{B/A}$ instead.

In the case that $S = \operatorname{Spec} A, S' = \operatorname{Spec} B$, and $T = \operatorname{Spec} C$, standard universal properties imply that the T-points of $\mathcal{M}_{k,S'/S}$ are in natural bijection with the generating k-tuples of $B \otimes_A C$ over C. If we assume further that $T \simeq S$, we find that the S-points of $\mathcal{M}_{k,B/A}$ are in bijection with generating k-tuples for B over A.

By analogy with the affine case, we therefore say that the S-points of $\mathcal{M}_{k,S'/S}$ are *generating k-tuples* and the S-points of $\mathcal{M}_{S'/S}$ are *monogenerators* for $S' \to S$. Such a morphism is *monogenic* if a monogenerator exists.

1.1 Equations in local coordinates

The scheme $\mathcal{M}_{1,S'/S}$ has a simple description in local coordinates on S which we recall so that we may use it in computations. We start by noticing that $\mathcal{M}_{1,S'/S}$ is naturally a subscheme of another moduli scheme, the Weil Restriction.

Definition 1.3 Let $\pi : S' \to S$ be as in Situation 1.1. The *Weil Restriction* of $X \times_S S'$ to S, denoted $\mathcal{R}_{X,S'/S}$, is the scheme (unique up to isomorphism) which represents the contravariant functor

$$(T \to S) \mapsto \left\{ \begin{array}{c} S' \times_S T \xrightarrow{\quad s \quad} X \times_S T \\ \searrow \quad \swarrow \\ T \end{array} \right\}$$

on S-schemes.

We abbreviate $\mathcal{R}_{X,S'/S}$ in a parallel fashion to $\mathcal{M}_{X,S'/S}$. It is proven in [23, Theorem 1.3, Proposition 2.10] that the Weil Restriction exists and is a quasiprojective S-scheme. We prove in [4, Proposition 2.3] that the natural map $\mathcal{M}_{X,S'/S} \to \mathcal{R}_{X,S'/S}$ is a quasi-compact open immersion.

In the case that B is a finite free Noetherian A-algebra with A-basis $e_1, \ldots, e_n$, things are simpler. It is easy to check that

$$\mathbb{A}_S^n \cong \mathcal{R}_{1,S'/S}$$

via the isomorphism sending $(x_1, \ldots, x_n)$ to the unique map $S' \times_S T \to \mathbb{A}_T^1 = \operatorname{Spec} \mathscr{O}_T[t]$ over T sending t to $x_1 e_1 + \cdots + x_n e_n$.

Definition 1.4 Suppose B is a finite free Noetherian A-algebra with A-basis $e_1, \ldots, e_n$. Let a_{ij} for $1 \le i,j \le n$ be the unique elements of $A[x_1, \ldots, x_n]$ so that we have

$$(x_1 e_1 + \cdots + x_n e_n)^{i-1} = a_{i,1} e_1 + \cdots + a_{i,n} e_n$$

in the ring $B[x_1, \ldots, x_n]$. We call the matrix $M(e_1, \ldots, e_n) = [a_{ij}]_{1 \le i,j \le n}$ the *matrix of coefficients* with respect to the basis $e_1, \ldots, e_n$. Its determinant $i(e_1, \ldots, e_n) \in A[x_1, \ldots, x_n]$ is the *local index form* with respect to the basis $e_1, \ldots, e_n$.

Theorem 1.5 ([4, Theorem 3.1]) *With notation as above, $\mathcal{M}_{1,B/A}$ is the distinguished open subscheme of $\mathcal{R}_{1,S'/S}$ cut out by the non-vanishing of the local index form. In particular,*

$$\mathcal{M}_{1,B/A} \cong \operatorname{Spec} A[x_1, \ldots, x_n, i(e_1, \ldots, e_n)^{-1}].$$

Additionally, we recall from [4] that the local index forms give the complement of $\mathcal{M}_{S'/S}$ in $\mathcal{R}_{S'/S}$ a closed subscheme structure:

Definition 1.6 (Non-monogenerators $\mathcal{N}_{S'/S}$) Let $\mathcal{I}_{S'/S}$ be the ideal sheaf on $\mathcal{R}_{S'/S}$ generated locally by local index forms. We call this the *index form ideal*. Let $\mathcal{N}_{S'/S}$ be the closed subscheme of $\mathcal{R}$ cut out by the vanishing of $\mathcal{I}_{S'/S}$. We call this the *scheme of non-monogenerators*, since its support is the complement of $\mathcal{M}_{S'/S}$ inside of $\mathcal{R}_{S'/S}$.

Since $\mathcal{M}_{k,S'/S}$ is a scheme, it is a sheaf in the fpqc topology on (Sch/S). This invites a local study of monogenicity[1] of $S' \to S$, the subject of this paper.

---

[1] 'Monogeneity' is also common in the literature.

Fig. 1 A guide to notions of monogenicity and their relationships. The vertical dashed implication holds under additional hypotheses, see Cor. 2.11
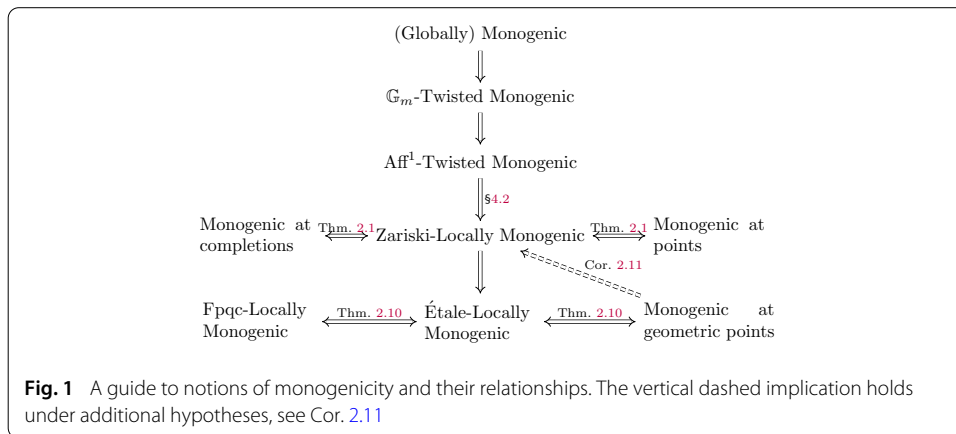
1.2 Results

We identify and relate several "local" notions of monogenicity. To guide the reader, their relationships are indicated in Figure 1.

A sheaf theoretic notion of local monogenicity immediately presents itself.[2]

Definition 1.7 Let τ be a subcanonical Grothendieck topology on schemes, for example the Zariski, Nisnevich, étale, fppf, or fpqc topologies. We say that S'/S is τ-*locally k-genic* if the sheaf $\mathcal{M}_{k,S'/S}$ is locally non-empty in the topology τ. I.e., there is a τ-cover $\{U_i \to S\}_{i \in I}$ of S such that $\mathcal{M}_{k,S'/S}(U_i)$ is non-empty for all $i \in I$.

The notions of τ-local monogenicity are considered in Sect. 2, and we find that these reduce to just two notions of "local monogenicity."

Theorem 1.8 *Let $\pi : S' \to S$ be as in Situation* 1.1.

(1) (Theorem 2.1) *The following are equivalent:*

    (a) *π is locally monogenic in the Zariski topology;*

    (b) *π is "monogenic at completions," i.e. for all points x of S, we have that $S' \times_S$ Spec $\hat{\mathcal{O}}_{S,x}$ is monogenic;*

    (c) *π is "monogenic at points," i.e. for each point x of S with residue field $k(x)$, we have that $S' \times_S$ Spec $k(x) \to$ Spec $k(x)$ is monogenic.*

(2) (Theorem 2.10) *The following are equivalent:*

    (a) *π is locally monogenic in the étale topology;*

    (b) *π is locally monogenic in the fpqc topology;*

    (c) *π is "monogenic at geometric points," i.e. for all algebraically closed fields k and maps Spec $k \to S$, we have that $S' \times_S$ Spec $k \to$ Spec k is monogenic.*

We then use the structure of finite algebras over fields to classify monogenicity at points. In particular, we recover Pleasants's characterization [32, Theorems 1 and 2] of monogenicity at completions as a corollary.

---

[2]We remark that Zariski local monogenicity is equivalent to the condition of "local monogenicity" considered by Bhargava et al. in [2] but strictly weaker than their condition of "no local obstruction to monogenicity."

Theorem 1.9 *Let $S' \to S$ be induced by $k \to B$ where k is a field and B is a local Artinian k-algebra with residue field ℓ and maximal ideal $\mathfrak{m}$. Then $S' \to S$ is monogenic if and only if*

(1) $\operatorname{Spec} \ell \to \operatorname{Spec} k$ *is monogenic;*
(2) $\dim_\ell \mathfrak{m}/\mathfrak{m}^2 \leq 1$*; and*
(3) *If $\dim_\ell \mathfrak{m}/\mathfrak{m}^2 = 1$ and ℓ/k is inseparable, then*

$$0 \to \mathfrak{m}/\mathfrak{m}^2 \to B/\mathfrak{m}^2 \to \ell \to 0$$

    is a non-split extension.

Theorem 1.10 *Suppose $S' \to S$ is induced by $k \to A$ where k is a field and B is an Artinian k-algebra. Write $B = \prod_i B_i$ where the B_i are local artinian k-algebras with respective residue fields ℓ_i. Then $S' \to S$ is monogenic if and only if*

(1) $\operatorname{Spec} B_i \to S$ *is monogenic for each i;*
(2) *for each finite extension ℓ of k, S' has fewer points with residue field isomorphic to ℓ than $\mathbb{A}^1_S$.*

In Sect. 3, we consider monogenicity spaces of étale $S' \to S$, a salient case since extensions of number rings are generically étale and such étale maps share a common local structure: Finite étale maps are étale-locally isomorphic to the trivial n-sheeted cover $S \sqcup \cdots \sqcup S \to S$. The latter has $\mathcal{M}_{S'/S}$ equal to the configuration space of n distinct points in $\mathbb{A}^1$. Therefore we may interpret monogenicity spaces as twisted generalizations of configuration spaces, at least when $S' \to S$ is étale.

Using the fact [38, 04HN] that every finite étale map of degree n is pulled back from the morphism of stacks $B\Sigma_{n-1} \to B\Sigma_n$, we then construct a monogenicity space $\mathcal{M}_{B\Sigma_{n-1}/B\Sigma_n}$.

Theorem 1.11 *There are isomorphisms*

$$\mathcal{R}_{B\Sigma_{n-1}/B\Sigma_n} \cong [\mathbb{A}^n/\Sigma_n],$$
$$\mathcal{N}_{B\Sigma_{n-1}/B\Sigma_n} \cong [\hat{\Delta}/\Sigma_n],$$
$$\text{and } \mathcal{M}_{B\Sigma_{n-1}/B\Sigma_n} \cong [(\mathbb{A}^n - \hat{\Delta})/\Sigma_n]$$

in which the action by Σ_n is in each case the appropriate restriction of the permutation action on coordinates of $\mathbb{A}^n$, and $\hat{\Delta}$ denotes the "fat diagonal" of $\mathbb{A}^n$, the locus where some pair of coordinates coincide.

In particular, the $\mathbb{C}$-points of $\mathcal{M}_{B\Sigma_{n-1}/B\Sigma_n}$ coincide with the points of the unordered configuration space of n points in $\mathbb{C}$. This monogenicity space is universal for étale maps in the sense that the monogenicity space $\mathcal{M}_{S'/S}$ of each étale $S' \to S$ is pulled back from $\mathcal{M}_{B\Sigma_{n-1}/B\Sigma_n}$.

We then consider several examples enabled by the structure of $\mathcal{M}_{S'/S}$ in the étale case, among them a connection to braid groups, a construction of the moduli space of genus zero pointed curves from monogenicity spaces, the monogenicity space of a G-torsor, and the monogenicity space of an isogeny of elliptic curves.

We remark that the monogenicity space $\mathcal{M}_{B\Sigma_{n-1}/B\Sigma_n}$ appears to be a scheme theoretic enhancement of the universal spaces of [18, Sect. 3] and [16, Sect. 1] in the category of

topological spaces. Meanwhile, the universal monogenicity space $\mathcal{M}_{*/BG}$ for G-torsors appears to be a scheme theoretic enhancement of the space $B_1 G$ considered in [11, Theorem 1.3].

A local-to-global sequence is missing for τ-local monogenicity. Yet there are natural group actions on $\mathcal{M}_{S'/S}$, in particular by $\mathbb{G}_m$ and Aff^1. In Sect. 4 we study "twisted" versions of monogenicity in which $S' \to S$ has local monogenerators that differ from each other by the action of such groups. More precisely:

Definition 1.12 (*Twisted monogenerators*)

A $(\mathbb{G}_m)$-twisted monogenerator for B/A is:

(1) a Zariski open cover $\operatorname{Spec} A = \bigcup_i D(f_i)$ for elements $f_i \in A$,
(2) a system of "local" monogenerators $\theta_i \in B\left[f_i^{-1}\right]$ for $B[f_i^{-1}]$ over $A[f_i^{-1}]$, and
(3) units $a_{ij} \in A\left[f_i^{-1}, f_j^{-1}\right]^*$

such that

- for all i, j, we have $a_{ij}.\theta_j = \theta_i$,
- for all i, j, k, the "cocycle condition" holds:

$$a_{ij}.a_{jk} = a_{ik}.$$

Two such systems $\{(a_{ij}), (\theta_i)\}$, $\{(a'_{ij}), (\theta'_i)\}$ are *equivalent* if, after passing to a common refinement of their respective covers, there is a global unit $u \in A^*$ such that $u \cdot a_{ij} = a'_{ij}$ and $u \cdot \theta_i = \theta'_i$. Likewise B/A is Aff^1-*twisted monogenic* if there is a cover with θ_i's as above, but with the units in item (3) replaced by pairs $a_{ij}, b_{ij} \in A\left[f_i^{-1}, f_j^{-1}\right]$ such that each a_{ij} is a unit and $a_{ij}\theta_j + b_{ij} = \theta_i$.

Under certain hypotheses, we show:

Proposition 4.14: B/A is $\mathbb{G}_m$-twisted monogenic if and only if it is Aff^1-twisted monogenic.
Theorem 4.19: The class number of a number ring $\mathbb{Z}_K$ is one if and only if all twisted monogenic extensions of number rings $\mathbb{Z}_L/\mathbb{Z}_K$ are in fact monogenic.
Remark 4.12: There is a local-to-global sequence relating affine equivalence classes of monogenerators with global monogenerators as above.
Theorem 4.2: There are moduli spaces of $\mathbb{G}_m$ and Aff^1-twisted monogenerators analogous to $\mathcal{M}_{S'/S}$.
Theorem 4.17: There are finitely many twisted monogenerators up to equivalence.

We remark that a $\mathbb{G}_m$-twisted monogenerator is equivalent to an embedding S' over S into a line bundle L on S. Such embeddings into line bundles were considered for topological spaces in [25].

Section 5 concludes with ample examples of the scheme of monogenerators and the various interactions between the forms of local monogenicity.

To avoid repetition, we invite the reader to consult the first paper in this series for a more detailed survey of the relevant literature.

2 Local monogenicity

2.1 Zariski-local monogenicity

This section shows Zariski-local monogenicity can be detected over points and completions as spelled out in Remark 2.3. We will make frequent use of the vocabulary and notation of [4, Sect. 3].

Theorem 2.1 *The following are equivalent:*

(1) $\pi : S' \to S$ *is Zariski-locally monogenic.*

(2) *There exists a family of maps $\{f_i : U_i \to S\}$ such that*

     (a) *the f_i are jointly surjective;*

     (b) *for each point $p \in S$, there is an index i and point $q_p \in f_i^{-1}(p)$ so that f_i induces an isomorphism $k(p) \to k(q_i)$;*

     (c) $S' \times_S U_i \to U_i$ *is monogenic for all i.*

(3) $\pi : S' \to S$ *is monogenic over points, i.e., $S' \times_S \operatorname{Spec} k(p) \to \operatorname{Spec} k(p)$ is monogenic for each point $p \in S$.*

Proof (1) $\implies$ (2): Choose the U_i to be a Zariski cover on which $S' \to S$ is monogenic.

(2) $\implies$ (3): Suppose such a cover $\{f_i : U_i \to S\}$ is given. For each i, let $\sigma_p : \operatorname{Spec} k(p) \to U_i$ be the section through q_p. monogenicity is preserved by pullback on the base, so pulling back $S' \times_S U_i \to U_i$ along σ_p implies (3).

(3) $\implies$ (1): Let $p \in S$ be a point with residue field $k(p)$ and let θ be a monogenerator for $S' \times_S \operatorname{Spec} k(p) \to \operatorname{Spec} k(p)$. We claim that θ extends to a monogenerator over an open subset $U \subseteq S$ containing p, from which (1) follows. The claim is Zariski local, so assume $S = \operatorname{Spec} A$ and $\pi_* \mathcal{O}_{S'} \simeq \bigoplus_{i=1}^n \mathcal{O}_S e_i$ is globally free. The Weil Restriction $\mathcal{R}_{S'/S} := \underline{\operatorname{Hom}}_S(S', X')$ is then isomorphic to affine space $\mathbb{A}_S^n$.

We first extend θ to a section of $\mathcal{R}_{S'/S}$. The monogenerator entails a point $\theta : \operatorname{Spec} k(p) \to \mathcal{M}_{S'/S} \subseteq \mathcal{R}_{S'/S} \simeq \mathbb{A}_S^n$, i.e. n elements $\overline{x}_1, \ldots, \overline{x}_n \in k(p)$. Choose arbitrary lifts $x_i \in A_{(p)}$ of $\overline{x}_i$. The n elements x_i must have a common denominator, so we have $x_1, \ldots, x_n \in A[f^{-1}]$ for some f. Thus our point $\theta : \operatorname{Spec} k(p) \to \mathbb{A}_S^n$ extends to $\widetilde{\theta} : D(f) \to \mathcal{R}_{S'/S}$ for some distinguished open neighborhood $D(f) \subseteq S$ containing p.

Finally, we restrict $\widetilde{\theta}$ to a section of $\mathcal{M}_{S'/S}$. The monogenicity space $\mathcal{M}_{S'/S}$ is an open subscheme of the Weil Restriction $\mathcal{R}_{S'/S}$, so $\widetilde{\theta} : D(f) \to \mathcal{R}_{S'/S}$ restricts to a monogenerator $\widetilde{\theta}|_U : U \to \mathcal{M}_{S'/S}$ where $U = \widetilde{\theta}^{-1}(\mathcal{M}_{S'/S}) \subset D(f)$. By hypothesis, $p \in U$, so $\widetilde{\theta}|_U$ is the desired extension of θ. $\qquad \square$

Remark 2.2 The same proof shows that $S' \to S$ is Zariski-locally k-genic if and only if its fibers $S' \times_S \operatorname{Spec} k(p) \to \operatorname{Spec} k(p)$ are k-genic.

Remark 2.3 Item (2) of Theorem 2.1 implies the following are also equivalent to Zariski-local monogenicity:

(1) $S' \to S$ is "monogenic at local rings," i.e, for each point p of S, $S' \times_S \operatorname{Spec} \mathcal{O}_{S,p} \to \operatorname{Spec} \mathcal{O}_{S,p}$ is monogenic.

(2) $S' \to S$ is "monogenic at completions," i.e., for each point p of S, $S' \times_S \operatorname{Spec} \hat{\mathcal{O}}_{S,p} \to \operatorname{Spec} \hat{\mathcal{O}}_{S,p}$ is monogenic, where $\hat{\mathcal{O}}_{S,p}$ denotes the completion of $\mathcal{O}_{S,p}$ with respect to its maximal ideal.

(3) $S' \to S$ is locally monogenic in the Nisnevich topology as in Definition 1.7.

Corollary 2.4 ([36, Proposition III.6.12]) *Let $S' \to S$ be an extension of local rings inducing a separable extension of residue fields. Then S' is monogenic over S.*

Proof Use the equivalence of item (1) in Remark 2.3 and (3) in Theorem 2.1. □

We now recall some ideas in order to compare with related results in the number ring case.

Definition 2.5 Let $\mathbb{Z}_L/\mathbb{Z}_K$ be an extension of number rings. Given $\theta \in \mathbb{Z}_L$ generating L/K, we write $\mathrm{Index}_{\mathbb{Z}_L/\mathbb{Z}_K}(\theta)$ for the index $[\mathbb{Z}_L : \mathbb{Z}_K[\theta]]$. A non-zero prime of $\mathfrak{p} \subset \mathbb{Z}_K$ is a *common index divisor*[3] for the extension $\mathbb{Z}_L/\mathbb{Z}_K$ if $\mathrm{Index}_{\mathbb{Z}_L/\mathbb{Z}_K}(\theta) \in \mathfrak{p}$ for every $\theta \in \mathbb{Z}_L$ generating L/K.

Common index divisors are exactly the primes $\mathfrak{p}$ whose splitting in $\mathbb{Z}_L$ cannot be mirrored by irreducible polynomials in $k(\mathfrak{p})[x]$; see [19,32].

We recall [4, Remark 3.11] that if U is an open affine subscheme of S on which S' is free with basis $e_1, \ldots, e_n$ then $\mathrm{Index}_{\mathbb{Z}_L/\mathbb{Z}_K}(x_1 e_1 + \cdots + x_n e_n)$ is a local index form on U.

Restating the property of being monogenic at points in terms of the index form, we obtain a generalization of the notion of having no common index divisors:

Proposition 2.6 *$S' \to S$ is monogenic over points if and only if for each point p of S and local index form i around p, there is a tuple $(x_1, \ldots, x_n) \in k(p)^n$ such that $i(x_1, \ldots, x_n)$ is nonzero in $k(p)$.*

Proof $S' \times \mathrm{Spec}\, k(p) \to \mathrm{Spec}\, k(p)$ is monogenic precisely when $\mathrm{Spec}\, k(p)[x_1, \ldots, x_n, i(x_1, \ldots, x_n)^{-1}]$ has a $k(p)$ point. □

Immediately we recover an explicit corollary validating the generalization:

Corollary 2.7 *Suppose $S' \to S$ is induced by an extension of number rings $\mathbb{Z}_L/\mathbb{Z}_K$. Then $S' \to S$ is Zariski-locally monogenic if and only if there are no common index divisors for $\mathbb{Z}_L/\mathbb{Z}_K$.*

Example 2.8 There are extensions of number rings that are locally monogenic but not monogenic.

In [2], Alpöge, Bhargava, and Shnidman say that an extension $\mathbb{Z}_K/\mathbb{Z}$ has *no local obstruction to monogenicity* if a local index form represents 1 over $\mathbb{Z}_p$ for all primes p or -1 over $\mathbb{Z}_p$ for all primes p. This is a stronger condition than Zariski-local monogenicity, and they show in [2,3] that a positive proportion of quartic and cubic fields are not monogenic despite having no local obstruction to monogenicity.

Narkiewicz [29, p. 65] gives the following concrete example of a locally monogenic but not monogenic extension. Let $L = \mathbb{Q}(\sqrt[3]{m})$ with $m = ab^2$, ab square-free, $3 \nmid m$, and $m \not\equiv \pm 1 \bmod 9$. The number ring $\mathbb{Z}_L$ is not monogenic over $\mathbb{Z}$ despite having no common index divisors. We consider the case $ab^2 = 7 \cdot 5^2$ in Example 5.3. This also gives an example

---

[3]Common index divisors are also called *essential discriminant divisors* and *inessential or nonessential discriminant divisors*. The shortcomings of the English nomenclature likely come from what Neukirch [30, page 207] calls "the untranslatable German catch phrase [...] 'außerwesentliche Diskriminantenteile.'" Our nomenclature is closer to Fricke's 'ständiger Indexteiler.'

of an extension which is Zariski locally monogenic but which has a local obstruction to monogenicity.

2.2 Monogenicity over geometric points

Definition 2.9 Say that S' over S is *monogenic over geometric points* if, for each morphism $\operatorname{Spec} k \to S$ where k is an algebraically closed field, $S' \times_S \operatorname{Spec} k \to \operatorname{Spec} k$ is monogenic.

While it is a weaker condition than monogenicity over points in general, it is equivalent to some conditions that might seem more natural.

Theorem 2.10 *The following are equivalent:*

(1) *the local index forms for S'/S are nonzero on each fiber of $\mathcal{R}_{S'/S} \to S$;*
(2) *for each point $p \in S$ with residue field $k(p)$, there is a finite Galois extension $L/k(p)$ such that $S' \times_S \operatorname{Spec} L \to \operatorname{Spec} L$ is monogenic, and this extension may be chosen to be trivial if $k(p)$ is an infinite field;*
(3) *$S' \to S$ is monogenic over geometric points;*
(4) *there is a jointly surjective collection of maps $\{U_i \to S\}$ so that $S' \times_S U_i \to U_i$ is monogenic for each i;*
(5) *$\mathcal{M}_{S'/S} \to S$ is surjective;*
(6) *$S' \to S$ is étale-, smooth-, fppf-, or fpqc-locally monogenic.*

If, in addition, $\mathfrak{n}_{S'/S}$ is a Cartier divisor in $\mathcal{R}$ (i.e., the local index forms are non-zero divisors), the above are also equivalent to:

(7) *$\mathfrak{n}_{S'/S} \to S$ (Definition 1.6) is flat.*

To see some of the subtleties one can compare item (1) above with Lemma 2.6 and item (4) above with item (2) of Theorem 2.1.

Proof The assertions are Zariski-local, so we may choose local coordinates as usual ($S = \operatorname{Spec} A$, $S' = \operatorname{Spec} B$, coordinates x_I).

(1) $\implies$ (2): Suppose first that $p \in S$ is a point with $k(p)$ an infinite field. Let $\mathfrak{p}$ be the corresponding prime of A and write $\bar{\imath}$ for the restriction of the local index form modulo $\mathfrak{p}$. Recall that since $k(p)$ is infinite, polynomials in $k(p)[x_1, \ldots, x_n]$ are determined by their values on $(x_i) \in k(p)^n$. Since $\bar{\imath}$ is nonzero, $\bar{\imath}(a_1, \ldots, a_n)$ must be nonzero for some $(a_1, \ldots, a_n) \in k(p)^n$. This shows that $S' \times_S \operatorname{Spec} k(p) \to \operatorname{Spec} k(p)$ is monogenic, so we have (2).

Next suppose $k(p)$ is a finite field. Then, since $\bar{\imath}$ is nonzero, there is a finite field extension L (necessarily Galois) of $k(p)$ such that there exists $(a_1, \ldots, a_n) \in L^n$ with $\bar{\imath}(a_1, \ldots, a_n) \neq 0$. This shows that $S' \times_S \operatorname{Spec} L \to \operatorname{Spec} L$ is monogenic, so we have (2) again.

(2) $\implies$ (3): Let k be an algebraically closed field and $\operatorname{Spec} k \to S$ a map. Let p be the image of $\operatorname{Spec} k$, and let L be the field extension given by (2). Then pullback along $\operatorname{Spec} k \to \operatorname{Spec} L$ implies that $S' \times_S \operatorname{Spec} k \to \operatorname{Spec} k$ is monogenic.

(3) $\implies$ (4): Take $\{U_i \to S\}$ to be $\{\operatorname{Spec} \overline{k(p)} \to S\}_{p \in S}$.

(4) $\implies$ (1): For each point $p \in S$, choose an index i and a point $q_p \in U_i$ mapping to p. Let i be an index form around p. By pullback, $S' \times_S q_p \to q_p$ is monogenic, so i pulls back to a nonzero function over $k(q_p)$. Therefore i is nonzero over $k(p)$ as well.

(2) $\implies$ (5): For each point $p \in S$, the $\operatorname{Spec} L$ point of $\mathcal{M}_{S'/S}$ witnessing monogenicity of $S' \times_S \operatorname{Spec} L \to \operatorname{Spec} L$ is a preimage of p.

(5) $\implies$ (6): Note that $\mathcal{M}_{S'/S} \to S$ is smooth, since $\mathcal{M}_{S'/S} \to \mathcal{R}_{S'/S} \to S$ is the composite of an open immersion and an affine bundle. Moreover, the identity function on $\mathcal{M}_{S'/S}$ by definition yields a monogenerator for $S' \times_S \mathcal{M}_{S'/S} \to \mathcal{M}_{S'/S}$. Therefore, S'/S is smooth-locally monogenic. Since the smooth topology is equivalent to the étale topology, there is an étale cover $U \to S$ factoring through $\mathcal{M}_{S'/S} \to S$. Since $S' \times_S \mathcal{M}_{S'/S} \to \mathcal{M}_{S'/S}$ is already monogenic, $S' \times_S U \to U$ is also monogenic. This étale cover is also a cover in the fppf and fpqc topologies.

(6) $\implies$ (4): Trivial.

(1) $\iff$ (7): The sequence

$$0 \to \mathcal{I}_{S'/S} \to \mathcal{O}_{\mathcal{R}_{1,S'/S}} \to \mathcal{O}n_{S'/S} \to 0$$

may be written as

$$0 \to A[x_I] \xrightarrow{i} A[x_I] \to A[x_I]/i \to 0$$

where i is a local index form for S'/S.

Recall that an $A[x_I]$-module M is flat if and only if for each prime $\mathfrak{p}$ of A and ideal $\mathfrak{q}$ of $A[x_I]$ lying over $\mathfrak{p}$, $M_{\mathfrak{q}}$ is flat over $A_{\mathfrak{p}}$. Therefore, by the local criterion for flatness [38, 00MK], $n_{S'/S}$ is flat over S if and only if

$$\operatorname{Tor}_1^{A_{\mathfrak{p}}}(A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}, (A[x_I]/i)_{\mathfrak{q}}) = 0$$

for all such ideals $\mathfrak{p}$ and $\mathfrak{q}$. Therefore, $n_{S'/S}$ is flat if and only if

$$A[x_I]_{\mathfrak{q}}/\mathfrak{p}A[x_I]_{\mathfrak{q}} \xrightarrow{i \,(\mathrm{mod}\,\mathfrak{p})} A[x_I]_{\mathfrak{q}}/\mathfrak{p}A[x_I]_{\mathfrak{q}}$$

is injective for all $\mathfrak{p}$ and $\mathfrak{q}$ as above. All of these maps are injective if and only if the maps of $A[x_I]$-modules

$$A_{\mathfrak{p}}[x_I]/\mathfrak{p}A_{\mathfrak{p}}[x_I] \xrightarrow{i \,(\mathrm{mod}\,\mathfrak{p})} A_{\mathfrak{p}}[x_I]/\mathfrak{p}A_{\mathfrak{p}}[x_I]$$

are all injective as $\mathfrak{p}$ varies over the prime ideals of A. Since $A_{\mathfrak{p}}[x_I]/\mathfrak{p}A_{\mathfrak{p}}[x_I] \cong (A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}})[x_I]$ is an integral domain for each $\mathfrak{p}$, injectivity fails if and only if i reduces to 0 in the fiber over some $\mathfrak{p}$. We conclude that (1) holds if and only if (7) holds. □

Corollary 2.11 *If all of the points of S have infinite residue fields, then the following are equivalent:*

(1) *$S' \to S$ is monogenic over geometric points;*
(2) *S'/S is Zariski-locally monogenic.*

Remark 2.12 The conclusion of Corollary 2.11 fails dramatically if S has finite residue fields. For $S' \to S$ coming from an extension of number rings condition (1) *always* holds (see Corollary 2.16 below), yet there are extensions that are not locally monogenic. In this sense, monogenicity is more subtle in the arithmetic context than the geometric one. For an example of an extension that is monogenic over geometric points but is not monogenic over points see Example 5.1.

2.3 Monogenicity over points

In light of Theorems 2.1 and 2.10, it is particularly interesting to characterize monogenicity of $S' \to S$ in the case that S is the spectrum of a field k. In this case S' is the spectrum of an n-dimensional k-algebra B. Such algebras are Artinian rings, and a well-known structure theorem implies that B is a direct product of local Artinian rings B_i. We will exploit this to give a complete characterization of Zariski-local monogenicity.

The result in the case that both S' and S are spectra of fields is well-known.

Theorem 2.13 (Theorem of the primitive element) *Let ℓ/k be a finite field extension. Then $\operatorname{Spec} \ell \to \operatorname{Spec} k$ is monogenic if and only if there are finitely many intermediate subfields $\ell/\ell'/k$.*

In particular, a finite separable extension of fields is monogenic.

We next consider the monogenicity of $S' \to S$ when S' is a nilpotent thickening of $\operatorname{Spec} \ell$, leaving $S = \operatorname{Spec} k$ fixed. A key ingredient is a study of the square zero extensions of $\operatorname{Spec} \ell$.

We remark for comparison that the proof below does not consider a nilpotent thickening of the base $S \to \tilde{S}$. In fact, if $S \to \tilde{S}$ is a nilpotent closed immersion with $S' = S \times_{\tilde{S}} \tilde{S}'$, any monogenerator $\theta : S \to \mathcal{M}_{S'/S}$ extends to $\tilde{S}$ locally in the étale topology. This results from the smoothness of $\mathcal{M}_{\tilde{S}'/\tilde{S}} \to \tilde{S}$.

Theorem 1.9. Let $S' \to S$ be induced by $k \to B$ where k is a field and B is a local Artinian k-algebra with residue field ℓ and maximal ideal $\mathfrak{m}$. Then $S' \to S$ is monogenic if and only if

(1) $\operatorname{Spec} \ell \to \operatorname{Spec} k$ is monogenic;
(2) $\dim_\ell \mathfrak{m}/\mathfrak{m}^2 \leq 1$; and
(3) If $\dim_\ell \mathfrak{m}/\mathfrak{m}^2 = 1$ and ℓ/k is inseparable, then

$$0 \to \mathfrak{m}/\mathfrak{m}^2 \to B/\mathfrak{m}^2 \to \ell \to 0$$

is a non-split extension.

Proof If the tangent space $(\mathfrak{m}/\mathfrak{m}^2)^\vee$ has dimension greater than 1, then no map $S' \to \mathbb{A}^1_S$ can be injective on tangent vectors as is required for a closed immersion.

On the other hand, if the tangent space of S' has dimension 0, we have $B = \ell$, and the result is true by hypothesis.

Now suppose the tangent space of S' has dimension 1. A morphism $S' \to \mathbb{A}^1_S$ is a closed immersion if and only if it is universally closed, universally injective, and unramified [38, Tag 04XV].

Choose a closed immersion $\operatorname{Spec} \ell \to \mathbb{A}^1_k$. Equivalently, write $\ell = k[t]/(f(t))$ where $f(t)$ is the monic minimal polynomial of some element $\theta \in \ell$. Since $\operatorname{Spec} \ell \to S'$ is a universal homeomorphism [38, Tag 054M], any extension of $\operatorname{Spec} \ell \to \mathbb{A}^1_k$ to $S' \to \mathbb{A}^1_k$ inherits the properties of being universally injective and universally closed from $\operatorname{Spec} \ell \to \mathbb{A}^1_k$.

Whether such an extension $S' \to \mathbb{A}^1_k$ is ramified can be checked on the level of tangent vectors [38, Tag 0B2G]. It follows that a morphism $S' \to \mathbb{A}^1_k$ is a closed immersion if and only if its restriction to the vanishing of $\mathfrak{m}^2$ is. On the other hand, any map $V(\mathfrak{m}^2) \to \mathbb{A}^1_k$ extends to $S' \to \mathbb{A}^1_k$ (choose a lift of the image of t arbitrarily). Therefore, it suffices to consider the case that S' is a square zero extension of $\operatorname{Spec} \ell$.

By hypothesis, we have a presentation of ℓ as $k[t]/(f(t))$. We conclude with some elementary deformation theory, see for example [35, §1.1]. We have a square zero extension of ℓ

$$0 \to (f(t))/(f(t)^2) \to k[t]/(f(t))^2 \to \ell \to 0.$$

By assumption, B is also a square zero extension of ℓ:

$$0 \to \mathfrak{m} \to B \to \ell \to 0.$$

By [35, Proposition 1.1.7], there is a morphism of k-algebras $\phi : k[t]/(f(t))^2 \to B$ inducing the identity on ℓ. Since $(f(t))/(f(t)^2) \cong \ell$ as a $k[t]/(f(t)^2)$ module, ϕ either restricts to an isomorphism $f(t)/(f(t))^2 \to \mathfrak{m}$ or else the zero map. In the former case, the composite $k[t] \to k[t]/(f(t))^2 \to B$ is a surjection, and we are done. In the latter case, B is the pushout of the extension $k[t]/(f(t))^2$ along $(f(t))/(f(t)^2) \xrightarrow{0} \mathfrak{m}$, so B is the split extension $\ell[\epsilon]/\epsilon^2$.

If ℓ/k is separable, then the extension $k[t]/(f(t))^2$ is itself split [35, Proposition B.1, Theorem 1.1.10], i.e. there an isomorphism $k[t]/(f(t))^2 \cong \ell[\epsilon]/\epsilon^2$. Composing with $k[t] \to k[t]/(f(t)^2)$ gives the required monogenerator.

If ℓ/k is inseparable and $B \cong \ell[\epsilon]/\epsilon^2$, we will show that $S' \to S$ is not monogenic. Any generator for $\ell[\epsilon]/\epsilon^2$ over k must also be a generator for $\ell[\epsilon]/\epsilon^2$ over the maximal separable subextension k' of ℓ/k, so we may assume that ℓ/k is purely inseparable. Moreover, any generator θ for $\ell[\epsilon]/\epsilon^2$ over k must reduce modulo ϵ to a generator $\overline{\theta}$ of ℓ/k. Since ℓ/k is purely inseparable, the minimal polynomial $f(t)$ of $\overline{\theta}$ satisfies $f'(t) = 0$. Note $\theta = \overline{\theta} + c\epsilon$ for some $c \in \ell$. Since θ is assumed to be a monogenerator, there is a polynomial $g(t) \in k[t]$ such that $\epsilon = g(\theta)$. Reducing, $\overline{g(\theta)} = g(\overline{\theta}) = 0$, so $g(t) = q(t)f(t)$ for some $q(t) \in k[t]$. Then

$$\begin{aligned} g(\theta) &= g(\overline{\theta}) + g'(\overline{\theta})c\epsilon \\ &= 0 + q'(\overline{\theta})f(\overline{\theta})c\epsilon + q(\overline{\theta})f'(\overline{\theta})c\epsilon \\ &= 0, \end{aligned}$$

a contradiction. We conclude that in this case $S' \to S$ is not monogenic.   □

Remark 2.14 In the case that k is perfect, the first and third conditions hold automatically. If S' is regular of dimension 1 the second condition is trivial.

Theorem 1.10. Suppose $S' \to S$ is induced by $k \to A$ where k is a field and B is an Artinian k-algebra. Write $B = \prod_i B_i$ where the B_i are local artinian k-algebras with respective residue fields ℓ_i. Then $S' \to S$ is monogenic if and only if

(1) $\operatorname{Spec} B_i \to S$ is monogenic for each i;
(2) for each finite extension ℓ of k, S' has fewer points with residue field isomorphic to ℓ than $\mathbb{A}^1_S$.

Proof Note that a map $\bigsqcup_i \operatorname{Spec} B_i \to \mathbb{A}^1_S$ is a closed immersion if and only if each map $\operatorname{Spec} B_i \to \mathbb{A}^1_S$ is a closed immersion and the closed immersions are disjoint: $\operatorname{Spec} B_i \times_{\mathbb{A}^1_S} \operatorname{Spec} B_j = \varnothing$ for all $i \neq j$. This is equivalent to the statement that $A[t] \to \prod_i B_i$ is surjective if and only if $A[t] \to B_i$ is surjective for each i and $B_i \otimes_{A[t]} B_j = 0$ whenever $i \neq j$, which follows quickly in turn from the Chinese remainder theorem.

The proof of Theorem 1.9 shows that a closed immersion $\operatorname{Spec} B_i \to \mathbb{A}^1$ can be chosen with image any of the points of $\mathbb{A}_S^1$ with residue field ℓ_i. Then the condition on numbers of points is exactly what we need for the images of the $\operatorname{Spec} B_i$s not to overlap without running out of points. (Since topologically, the components are single points.)   □

Remark 2.15 Condition (2) is trivial in the case that the residue fields of S are infinite, highlighting the relative simplicity of monogenicity in the geometric context.

If $S' \to S$ is instead induced by an extension of number rings, then Remark 2.14 implies condition (1) is trivial. In particular, an extension of $\mathbb{Z}$ has common index divisors if and only if there is "too much prime splitting" in the sense of condition (2). This recovers the theorem of [19] (also see [32, Cor. to Thm. 3]) that $\mathfrak{p}$ is a common index divisor if and only if there are more primes in $\mathbb{Z}_L$ above $\mathfrak{p}$ of residue class degree f than there are irreducible polynomials of degree f in $k(\mathfrak{p})[x]$ for some positive integer f.

Corollary 2.16 *If $S' \to S$ is induced by an extension of number rings $\mathbb{Z}_L/\mathbb{Z}_K$, then $S' \to S$ is monogenic over geometric points.*

Proof Let p be a point of S. Let $A = \mathbb{Z}_L \otimes_{\mathbb{Z}_K} k(p)$ be the ring for the fiber of S' over $\operatorname{Spec} k(p)$. Note that $k(p)$ is either of characteristic 0 or finite, so $k(p)$ is perfect. Decompose A into a direct product of local Artinian $k(p)$ algebras A_i. Since $k(p)$ is perfect, conditions (1) and (3) of Theorem 1.9 hold for $\operatorname{Spec} A_i \to \operatorname{Spec} k(p)$. Condition (2) holds as well since S' is regular of dimension 1. Therefore $\operatorname{Spec} A_i \to \operatorname{Spec} k(p)$ is monogenic for each i.

Now consider the base change of S' to the algebraic closure $\overline{k(p)}$ of $k(p)$. Write B for the ring of functions $\mathbb{Z}_L \otimes_{\mathbb{Z}_K} \overline{k(p)}$ of this base change, and write B as a product of local Artinian algebras B_j. For each i we have that $\operatorname{Spec} A_i \otimes_{k(p)} \overline{k(p)} \to \operatorname{Spec} \overline{k(p)}$ is monogenic. Each $\operatorname{Spec} B_j$ is a closed subscheme of exactly one of the $\operatorname{Spec} A_i \otimes_{k(p)} \overline{k(p)}$s, so by composition, $\operatorname{Spec} B_j \to \operatorname{Spec} \overline{k(p)}$ is monogenic for each j. This gives us condition (1) of Theorem 1.10 for $S' \times_S \operatorname{Spec} \overline{k(p)} \to \operatorname{Spec} \overline{k(p)}$. Since $\overline{k(p)}$ is infinite, condition (2) holds triviallly. We conclude that $S' \times_S \operatorname{Spec} \overline{k(p)} \to \operatorname{Spec} \overline{k(p)}$ is monogenic, as required.   □

3 Étale maps, configuration spaces, and monogenicity

This section concerns maps $\pi : S' \to S$ that are *étale*, or unramified. Locally, the monogenicity space becomes a configuration space, classifying arrangements of n distinct points on a given topological space. Philosophically, $\mathcal{M}_{S'/S}$ therefore regards $S' \to S$ as a twisted family of points to be configured in $\mathbb{A}^1$. We are led to interpret $\mathcal{M}_{S'/S}$ as an arithmetic refinement of the configuration space of $\mathbb{A}^1$. In Remark 3.5, we see that an action of the absolute Galois group $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the étale fundamental group of $\mathcal{M}_{S'/S}$ has been observed in anabelian geometry. We end Subsection 3.2 with a handful of exotic applications in other areas.

All extensions $S' \to S$ sit somewhere between the étale case and jet spaces $\operatorname{Spec} A[\epsilon]/\epsilon^n \to \operatorname{Spec} A$ (see [4, Example 2.7, 4.3, 4.16]), between being totally unramified and totally ramified. In Sect. 3.4, we recall a general construction of the discriminant which cuts out the locus of ramification. Specifically, [33, Sect. 6] says that our description in the étale case holds precisely away from the vanishing of the discriminant. The discriminant plays a similar role in the classical case when investigating the monogenicity of an extension defined by a polynomial. We end with some remarks on using stacks to promote a ramified cover of curves to an étale cover of stacky curves as in [9].

3.1 The trivial cover

We start with the simplest case of an étale cover: the trivial cover of S by several copies of itself. We work rather concretely and revisit the general situation with more sophistication in the next subsection. Write $\langle n \rangle = \{1, 2, \ldots, n\}$ and $\langle n \rangle_S = \bigsqcup_{1 \leq i \leq n} S \to S$ for the trivial degree n finite étale cover.

Example 3.1 (Monogenicity of a trivial cover) Let $S' = \langle n \rangle_S$ and let $\pi : \langle n \rangle_S \to S$ be the map induced by the identity on each copy of S. Given a commutative diagram

$$
\begin{array}{ccc}
 & & \mathbb{A}^1_S \\
 & \overset{\sqcup_i f_i}{\nearrow} & \downarrow \\
\langle n \rangle_S & \xrightarrow{\ \pi\ } & S,
\end{array}
$$

one expects that the map $\sqcup_i f_i$ will be a closed immersion if and only if $f_i(s) \neq f_j(s)$ for all $1 \leq i < j \leq n$ and $s \in S$. A computation in coordinates will confirm this.

We will use the notation of Definition 1.4 and Theorem 1.5 to compute $\mathcal{M}_{S'/S}$ in local coordinates. Working Zariski locally on S, we may assume that $S' = \operatorname{Spec} A^n$, $S = \operatorname{Spec} A$, and that $e_1, \ldots, e_n$ are the standard basis vectors for A^n. Let $x_1, \ldots, x_n$ be the corresponding coordinates for $\mathcal{R}_{S'/S}$, so that

$$
\mathcal{R}_{S'/S} \cong \mathbb{A}^n_S.
$$

This isomorphism identifies the T-point $(x_1, \ldots, x_n)$ of $\mathbb{A}^n_S$ with the map $\sqcup_i x_i : \langle n \rangle_T \to \mathbb{A}^1_T$ whose restriction to the ith copy of T in $\langle n \rangle_T$ is x_i.

Next, observe that in $\mathscr{O}_{\mathcal{R}_{S'/S}}(S)$

$$
(x_1 e_1 + \cdots + x_n e_n)^j = x_1^j e_1 + \cdots + x_n^j e_n
$$

for all $0 \leq j \leq n-1$. Therefore, the matrix of coefficients $M(e_1, \ldots, e_n)$ is the Vandermonde matrix with ith column given by $\begin{bmatrix} 1 & x_i & x_i^2 & \cdots & x_i^{n-1} \end{bmatrix}^T$. The index form is then the well-known Vandermonde determinant:

$$
i(e_1, \ldots, e_n)(x_1, \ldots, x_n) = \det M(e_1, \ldots, e_n) = \pm \prod_{i<j} (x_i - x_j).
$$

The index form vanishes therefore on the so-called *fat diagonal* $\hat{\Delta} \subseteq \mathbb{A}^n$, given by the union of all loci $V(x_i - x_j)$ where two coordinates are equal.

It follows that

$$
\mathcal{M}_{S'/S} \cong \underline{\operatorname{Spec}}_S \mathscr{O}_S \left[x_1, \ldots, x_n, \prod_{i<j}(x_i - x_j)^{-1} \right],
$$

the complement in $\mathbb{A}^n_S$ of $\hat{\Delta}$. This space is otherwise known as the space of *ordered configurations* of n points, $\operatorname{Conf}_n(\mathbb{A}^1_S) \to S$.

Slightly more abstract reasoning yields a similar result if X is any quasi-projective S scheme.

Example 3.2 ($\mathcal{M}_{X,S'/S}$ for a trivial cover) Let $X \to S$ be a quasiprojective map, $S' = \langle n \rangle_S$ and let $\pi : \langle n \rangle_S \to S$ be the map induced by the identity on each copy of S. Observe that

if $T \to S$ is an S-scheme, we have natural identifications

$$
\begin{aligned}
\mathcal{R}_{X,S'/S}(T) &\cong \big\{ \text{ maps of } T\text{-schemes } f : \langle n \rangle_T \to X \times_S T \big\} \\
&\cong \big\{ n\text{-tuples of maps of } T\text{-schemes } f_i : T \to X \times_S T, \text{ where } i = 1, \ldots, n \big\} \\
&\cong \big\{ n\text{-tuples of maps of } S\text{-schemes } f_i : T \to X, \text{ where } i = 1, \ldots, n \big\} \\
&\cong \underbrace{X \times_S X \times_S \cdots \times_S X}_{n\text{-times}}(T) = X^{\times_S^n}(T),
\end{aligned}
$$

so we may identify $\mathcal{R}_{X,S'/S}$ with the n-fold fiber product of X over S.

For each $1 \le i < j \le n$, we can construct a subscheme $\Delta_{i,j}$ of $X^{\times_S^n}$ consisting of the points whose ith and j coordinates are equal. We let the fat diagonal $\hat{\Delta}$ be the scheme theoretic union of the subschemes $\Delta_{i,j}$. Since $X \to S$ is separated, this fat diagonal is a closed subscheme of $X^{\times_S^n}$.

Observe that any morphism of T-schemes $f = \bigsqcup_{i=1}^n f_i : \langle n \rangle_T \to X \times_S T$ in $\mathcal{R}_{X,S'/S}(T)$ will be proper and unramified as $\pi : \langle n \rangle_T \to T$ is proper and unramified and $X \times_S T \to T$ is separated. In addition, for each point $x \in \langle n \rangle_T$, the induced field extension $\kappa(x) \supseteq \kappa(f(x))$ is an isomorphism, since the same is true of the map $\pi : \langle n \rangle_T \to T$.

Now, by [38, Tag 01S4, (2) $\iff$ (3)] and [38, Tag 04XV, (1) $\iff$ (3)], f is a closed immersion if and only if it is injective. This happens if and only if the corresponding function $\prod_{i=1}^n f_i : T \to X^{\times_S^n}$ factors through the complement of the fat diagonal. Therefore $\mathcal{M}_{X,S'/S} \cong X^{\times_S^n} - \hat{\Delta}$.

3.2 The case of étale $S' \to S$

Consider the category $(Sch/*)$ of schemes over a final scheme $*$ equipped with the étale topology. For example, take $* = \operatorname{Spec} \mathbb{Z}$ or $\operatorname{Spec} \mathbb{C}$. Write Σ_n for the symmetric group on n letters and $B\Sigma_n$ for the stack on $(Sch/*)$ of étale Σ_n-torsors.

Regard Σ_{n-1} as the subgroup of Σ_n of permutations fixing the nth letter, and let $B\Sigma_{n-1} \to B\Sigma_n$ be the map induced by the inclusion. The isomorphism class of the resulting map of classifying spaces is unchanged if Σ_{n-1} is taken as the subgroup fixing some other letter, since resulting inclusion map only differs from this one by conjugation. The morphism $B\Sigma_{n-1} \to B\Sigma_n$ is the universal n-sheeted cover in the following sense.

Lemma 3.3 ([9, Lemma 2.2.1], [22, Lemma 3.2]) *Let n be a positive integer. Let $\mathcal{C}$ be the fibered category over $(Sch/*)$ with:*

(1) *objects the finite étale morphisms $\pi : S' \to S$ of degree n;*
(2) *arrows the cartesion diagrams*

$$
\begin{array}{ccc}
T' & \longrightarrow & S' \\
\downarrow & & \downarrow \\
T & \longrightarrow & S;
\end{array}
$$

(3) *projection to $(Sch/*)$ given by $S' \to S \mapsto S$.*

Then there is an equivalence of fibered categories $B\Sigma_n \to \mathcal{C}$ given by taking a map $f : S \to B\Sigma_n$ to the pullback of $B\Sigma_{n-1} \to B\Sigma_n$ along f.

Recall that pullback squares of schemes

$$
\begin{array}{ccc}
T' & \longrightarrow & S' \\
\downarrow & \ulcorner & \downarrow \\
T & \longrightarrow & S
\end{array}
$$

induce identifications

$$
\mathcal{R}_{T'/T} \simeq \mathcal{R}_{S'/S} \times_S T \qquad \text{and} \qquad \mathcal{M}_{1,T'/T} \simeq \mathcal{M}_{1,S'/S} \times_S T.
$$

Reduce thereby to the universal n-sheeted finite étale cover $S' = B\Sigma_{n-1}$, $S = B\Sigma_n$. Each has an affine line $\mathbb{A}^1_{B\Sigma_n} = [\mathbb{A}^1/\Sigma_n]$ obtained via quotienting by the trivial action.

Theorem 1.11. There are isomorphisms

$$
\mathcal{R}_{B\Sigma_{n-1}/B\Sigma_n} \cong [\mathbb{A}^n/\Sigma_n],
$$
$$
\mathcal{N}_{B\Sigma_{n-1}/B\Sigma_n} \cong [\hat{\Delta}/\Sigma_n],
$$
$$
\text{and } \mathcal{M}_{B\Sigma_{n-1}/B\Sigma_n} \cong [(\mathbb{A}^n - \hat{\Delta})/\Sigma_n]
$$

in which the action by Σ_n is in each case the appropriate restriction of the permutation action on coordinates of $\mathbb{A}^n$.

Proof We observe that the n-sheeted cover associated to the trivial torsor $* \to B\Sigma_n$ is the trivial cover $\langle n \rangle \to *$. Therefore, by our work in the case of a trivial cover

$$
\mathcal{R}_{B\Sigma_{n-1}/B\Sigma_n} \times_{B\Sigma_n} * \cong \mathcal{R}_{\langle n \rangle/*} \cong \mathbb{A}^n
$$
$$
\mathcal{N}_{B\Sigma_{n-1}/B\Sigma_n} \times_{B\Sigma_n} * \cong \mathcal{N}_{\langle n \rangle/*} \cong \hat{\Delta}
$$
$$
\mathcal{M}_{B\Sigma_{n-1}/B\Sigma_n} \times_{B\Sigma_n} * \cong \mathcal{M}_{\langle n \rangle/*} \cong \mathbb{A}^n - \hat{\Delta} \cong \mathrm{Conf}_n(\mathbb{A}^1).
$$

There is a Σ_n action on $\mathcal{R}_{\langle n \rangle/*}$ so that $\mathcal{R}_{B\Sigma_{n-1}/B\Sigma_n}$ is the stack quotient of $\mathcal{R}_{\langle n \rangle/*}$ by Σ_n. Pulling back $\mathcal{R}_{\langle n \rangle/*} \to *$ to $* \times_{B\Sigma_n} *$ in both ways shows that the action is given by permuting the sheets of $\langle n \rangle$. Under the isomorphism of $\mathcal{R}_{\langle n \rangle/*}$ with $\mathbb{A}^n$ of Example 3.1, the action is given by permuting the coordinates.

We conclude

$$
\mathcal{R}_{B\Sigma_{n-1}/B\Sigma_n} \cong [\mathbb{A}^n/\Sigma_n]
$$
$$
\mathcal{N}_{B\Sigma_{n-1}/B\Sigma_n} \cong [\hat{\Delta}/\Sigma_n]
$$
$$
\mathcal{M}_{B\Sigma_{n-1}/B\Sigma_n} \cong [(\mathbb{A}^n - \hat{\Delta})/\Sigma_n]
$$

in which the action by Σ_n is in each case the appropriate restriction of the permutation action on coordinates of $\mathbb{A}^n$.   □

The space $\mathcal{M}_{B\Sigma_{n-1}/B\Sigma_n}$ is also interpretable as the space of *unordered configurations of points*:

$$
\mathcal{M}_{B\Sigma_{n-1}/B\Sigma_n} \cong \mathrm{UConf}_n(\mathbb{A}^1) = \{(x_1, \ldots, x_n) \mid x_i \neq x_j\}/\Sigma_n.
$$

Observe that the fat diagonal $\hat{\Delta}$ is exactly the locus of $\mathbb{A}^n$ where Σ_n has stabilizers. The coarse moduli space of $[\mathbb{A}^n/\Sigma_n]$ is $\mathbb{A}^n$ by the fundamental theorem of symmetric functions, with the composite

$$\mathbb{A}^n \to \left[\mathbb{A}^n/\Sigma_n\right] \to \mathbb{A}^n; \qquad \overline{x} = (x_1, \ldots, x_n) \mapsto (s_1(\overline{x}), s_2(\overline{x}), \ldots, s_n(\overline{x}))$$

given by the elementary symmetric polynomials $s_i(x_1, \ldots, x_n)$ [5, Sect. 16.1-2]. The composite sends a list of n roots to the coefficients of the monic polynomial of degree n vanishing at those roots, up to sign:

$$(t - x_1) \cdots (t - x_n) = t^n - s_1(\overline{x})t^{n-1} + s_2(\overline{x})t^{n-2} - \cdots \pm s_n(\overline{x}).$$

The assignment is plainly invariant under relabeling the x_i by Σ_n.

The map to the coarse moduli space $[\mathbb{A}^n/\Sigma_n] \to \mathbb{A}^n$ is an isomorphism precisely over $\mathcal{M}_{1,B\Sigma_{n-1}/B\Sigma_n}$. The image of $\mathcal{N}_{B\Sigma_{n-1}/B\Sigma_n}$ in $\mathbb{A}^n$ is the closed subscheme cut out by the discriminant of the above polynomial

$$\mathrm{Disc}\left(\prod_{i=1}^{n}(t - x_i)\right) = D(s_1(\overline{x}), s_2(\overline{x}), \ldots, s_n(\overline{x}))$$
$$= \prod_{i<j}(x_i - x_j)^2,$$

the square of the Vandermonde determinant. The resulting divisor is the pushforward of $\mathcal{N}_{B\Sigma_{n-1}/B\Sigma_n}$ to the coarse moduli space $\mathbb{A}^n$.

We summarize the above discussion for general targets X in the place of $\mathbb{A}^1$:

Theorem 3.4 *Let X be a quasiprojective scheme, and let $X_{B\Sigma_n} := [X/\Sigma_n] = X \times B\Sigma_n$ be the stack quotient by the trivial Σ_n action.*

- *The Weil Restriction is the stacky symmetric product:*

$$\mathcal{R}_{[X/\Sigma_n],B\Sigma_{n-1}/B\Sigma_n} := \left[Sym^n X\right] = \left[X^n/\Sigma_n\right].$$

- *The space of monogenerators for $S' = B\Sigma_{n-1}$, $S = B\Sigma_n$ is the nth unordered configuration space:*

$$\mathcal{M}_{[X/\Sigma_n],B\Sigma_{n-1}/B\Sigma_n} = UConf_n X := \{(x_1, \ldots, x_n) \mid x_i \neq x_j \text{ for } i \neq j\}/\Sigma_n.$$

- *The complementary space of non-monogenerators is the stack quotient by Σ_n of the "fat diagonal" of n points in X which are not pairwise distinct:*

$$\mathcal{N}_{[X/\Sigma_n],B\Sigma_{n-1}/B\Sigma_n} = \left[\hat{\Delta}_X/\Sigma_n\right] = \{(x_1, \ldots, x_n) \mid \text{some } x_i = x_j, i \neq j\}/\Sigma_n.$$

3.3 Implications

The rest of the section gives sample applications, exotic examples, and directions based on the correspondence with configuration spaces.

Remark 3.5 Classical work on the analogues of monogenicity in complex geometry, such as [17], has recognized that embeddings into $\mathbb{A}^1$-bundles are closely related to the braid group, essentially because the fundamental group of the configuration space of n points in $\mathbb{C}$ is the braid group on n strands. In the scheme theoretic setting, our best analogue of the fundamental group is the étale fundamental group.

The computations above imply that

$$\mathcal{M}_{1,B\Sigma_{n-1}/B\Sigma_n} \times_{\mathbb{Z}} \mathbb{Q} \cong \mathrm{UConf}(\mathbb{A}^1_{\mathbb{Q}}).$$

In [15], it is computed that this space has étale fundamental group a semi-direct product

$$\hat{B}_n \rtimes G_{\mathbb{Q}},$$

where $\hat{B}_n$ is the profinite completion of the braid group on n strands and $G_{\mathbb{Q}}$ is the absolute Galois group of $\mathbb{Q}$. As discussed in [15], the conjugation action of $G_{\mathbb{Q}}$ on $\hat{B}_n$ extends to an action by the Grothendieck-Teichmüller group $\hat{GT}$. Conjecturally, $G_{\mathbb{Q}} = \hat{GT}$. Though all varieties over $\mathbb{Q}$ yield actions of the Galois group $G_{\mathbb{Q}}$, we were surprised to rediscover one of its central representations used in number theory.

The following result is well-known, as the square of the Steinitz class is the discriminant, and the discriminant is a unit when $S' \to S$ is étale. However, we have a pleasant alternative proof in terms of our universal étale cover.

Theorem 3.6 *If $S' \to S$ is étale, the Steinitz class is 2-torsion in $\mathrm{Pic}(S)$. If S has characteristic 2, the Steinitz class vanishes.*

Proof It is enough to show that the Steinitz class $\det \pi_* \mathcal{O}_{S'}$ is 2-torsion for the universal case $\pi : B\Sigma_{n-1} \to B\Sigma_n$. Consider the pullback square

$$
\begin{array}{ccc}
\langle n \rangle & \xrightarrow{\ j\ } & B\Sigma_{n-1} \\
\downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \pi} \\
* & \xrightarrow{\ i\ } & B\Sigma_n.
\end{array}
$$

The pushforward $\pi_* \mathcal{O}_{B\Sigma_{n-1}}$ is trivialized on the étale cover $i : * \to B\Sigma_n$, as

$$i^*(\pi_* \mathcal{O}_{B\Sigma_{n-1}}) \cong \tau_* \mathcal{O}_{\langle n \rangle} = \mathcal{O}_*^n.$$

We find that the descent datum for $\pi_* \mathcal{O}_{B\Sigma_{n-1}}$ with respect to this cover has gluing $\mathcal{O}_{*\times\Sigma_n}^n \to \mathcal{O}_{*\times\Sigma_n}^n$ on $* \times_{B\Sigma_n} * \cong * \times \Sigma_n$ given by permuting the coordinates by σ over $* \times \sigma$ for each $\sigma \in \Sigma_n$. This is represented by a permutation matrix, which has determinant ± 1. Therefore the gluing data for $\det \pi_* \mathcal{O}_{B\Sigma_{n-1}}$ is given locally by multiplying by ± 1. Since ± 1 is 2-torsion in $\mathcal{O}^*$ and trivial if S has characteristic 2, the result follows. $\square$

Example 3.7 (Torsors for finite groups)

Let G be a finite group. A G-torsor $S' \to S$ is, in particular, a finite étale map of degree $n = \#G$ admitting the above description. Notice that the action of G on S' induces an action of G on $\mathcal{M}_{S'/S}$.

The map $S' \to S$ is classified by a map $S \to BG$, the stack of G-torsors, and we may regard $\mathcal{M}_{S'/S}$ as pulled back from either the monogenicity space of the universal G-torsor, $\mathcal{M}_{*/BG}$, or the monogenicity space of the universal n-fold cover $\mathcal{M}_{B\Sigma_{n-1}/B\Sigma_n}$. To compare the two, observe that the left regular representation $G \circlearrowright G$ gives an inclusion $G \subseteq \Sigma_n$ upon ordering the set G. The induced representable map $BG \to B\Sigma_n$ is essentially independent of the ordering since different orderings induce conjugate maps. The classifying map $S \to B\Sigma_n$ is the composite $S \to BG \to B\Sigma_n$ with the left regular representation. The monogenicity space $\mathcal{M}_{*/BG}$ is $[\mathbb{A}^{|G|} - \hat{\Delta}/G]$ where G acts on $\mathbb{A}^{|G|}$ by permuting the basis vectors by the left regular representation.

A similar description locally holds for other finite étale group schemes. For merely finite flat group schemes G such as α_p, μ_p in characteristic p, the group action on the monogenicity space of G-torsors $S' \to S$ still holds but the local decomposition $S' = \bigsqcup_n S$ and Σ_n action do not.

Corollary 3.8 *If $S' \to S$ is a G-torsor for G a finite group, and either*

(1) *$|G|$ is odd*
(2) *$|G|$ is even and G has non-cyclic Sylow 2-subgroup*

then the Steinitz class of $S' \to S$ is trivial in $Pic(S)$

Proof Repeating the construction of Theorem 3.6, we see that if the left regular representation of G factors through A_n, the Steinitz class is trivial. The conditions given identify precisely when this happens. $\square$

The stacks $\mathcal{R}_{1,B\Sigma_{n-1}/B\Sigma_n}$ we study arise naturally in log geometry as "Artin fans" [1].

Example 3.9 (Moduli spaces of curves in genus 0)

Let $M_{0,n}$ be the moduli stack of *smooth* curves of genus 0 (i.e. $\mathbb{P}^1$) with n marked points. The evident [41] isomorphism with a quotient of configuration space gives:

$$\left[\mathcal{M}_{\mathbb{P}^1,\mathbb{C}^n/\mathbb{C}}/\mathrm{PGL}_2\right] \simeq \left[\mathrm{Conf}_n(\mathbb{P}^1)/\mathrm{PGL}_2\right] \simeq M_{0,n}.$$

One can always put the first point at ∞ and get equivalent descriptions:

$$M_{0,n} \simeq \left[\mathcal{M}_{\mathbb{A}^1,\mathbb{C}^n/\mathbb{C}}/\mathrm{Aff}^1\right] \simeq \left[\mathrm{Conf}_n(\mathbb{C})/\mathrm{Aff}^1\right],$$

where Aff^1 is the group of affine transformations $\mathbb{G}_m \ltimes \mathbb{A}^1$. The stack quotient classifies local affine equivalence classes of monogenerators, as detailed in Sect. 4.

One can likewise obtain the other moduli spaces of curves by an ad hoc construction. Consider $\mathfrak{U} \to \mathfrak{M}$ the universal connected, proper, genus-g nodal curve, its relative smooth locus $\mathfrak{U}^{sm} \subseteq \mathfrak{U}$, and the monogenicity space

$$\mathcal{M}_{\mathfrak{U}^{sm},\langle n\rangle_{\mathfrak{M}}/\mathfrak{M}}$$

of the trivial cover $\langle n\rangle$ over the moduli space $\mathfrak{M}$. The monogenicity stack is naturally isomorphic to the space of nodal, n-marked curves $\mathfrak{M}_{g,n}$. One can also obtain the open substack of *stable* curves as the universal Deligne-Mumford locus $\overline{\mathcal{M}}_{g,n} \subseteq \mathfrak{M}_{g,n}$.

3.4 When is a map étale?

We recall from [33, Sect. 6] that a map $S' \to S$ is étale precisely when the discriminant of the algebra does not vanish. We recall from [33] that there is an algebraic moduli stack $\mathfrak{A}_n$ of finite locally free algebras and the affine scheme of finite type $\mathfrak{B}_n$ parametrizing such algebras together with a choice of global basis $\mathcal{Q} \simeq \bigoplus \mathcal{O}_S \cdot e_i$.

Suppose $\pi : S' \to S$ comes from a finite flat algebra $\mathcal{Q}$ with a global basis $\varphi : \mathcal{Q} \simeq \bigoplus_{i=1}^n \mathcal{O}_S \cdot e_i$, corresponding to a map $S \to \mathfrak{B}_n$. There is a trace pairing $\mathrm{Tr} : \mathcal{Q} \to \mathcal{O}_S$ [38, 0BSY] which we can use to define the discriminant:

$$\mathrm{Disc}(\mathcal{Q},\varphi) := \det\left[\mathrm{Tr}(e_i e_j)\right] \in \Gamma(\mathcal{O}_S)$$

Changing φ changes the function Disc by a unit. The function Disc does not descend to $\mathfrak{A}_n$, but the vanishing locus $V(\mathrm{Disc}) \subseteq \mathfrak{B}_n$ does. Writing $\mathfrak{B}_n^{et}, \mathfrak{A}_n^{et}$ for the open com-

plements of the vanishing locus $V(\mathrm{Disc})$, a map $\pi : S' \to S$ is étale if and only if $S \to \mathfrak{A}_n$ factors through the open substack $\mathfrak{A}_n^{et} \subseteq \mathfrak{A}_n$ [33, Proposition 6.1].

Remark 3.10 Most finite flat algebras are *not* étale, nor are they degenerations of étale algebras. B. Poonen shows the moduli of étale algebras inside of all finite flat algebras $\mathfrak{A}_n^{et} \subseteq \mathfrak{A}_n$ cannot be dense by computing dimensions [33, Remark 6.11]. The closure $\overline{\mathfrak{A}}_n^{et}$ is nevertheless an irreducible component.

What if $S' \to S$ is not étale? Readers familiar with [9] know one can sometimes endow a ramified map $S' \to S$ with stack structure $\tilde{S}$ and $\tilde{S}'$ at the ramification to make $\tilde{S}' \to \tilde{S}$ étale. Then all $\tilde{S}' \to \tilde{S}$ are Σ_n-torsors, and not just ramified covers $S' \to S$. The ideas in Sect. 3.2, in particular an analogue of Theorem 3.4, apply in this level of generality. We sketch these ideas over $\mathbb{C}$.

Consider

$$y^2 = x(x-1)(x-\lambda),$$

for some $\lambda \in \mathbb{C}$. If $C := \mathbb{P}_{\mathbb{C}}^1$ and C' is the projective closure of the above affine equation, the projection $(x, y) \mapsto x$ extends to a finite locally free map $\pi : C' \to C$. This is in Situation 1.1 so our definitions make sense for it. However π is ramified at four points, preventing us from interpreting its monogenicity space using the perspective of this section. Nevertheless, we may observe that the function y gives a section of $\mathcal{M}_{1,C'/C}$ over $C \setminus \infty$. The section naturally extends to a section of $\mathcal{R}_{\mathbb{P}^1,C'/C}$ over all of C.

Let $X := \mathbb{P}_C^1$. If we work over $\mathbb{C}$ and endow C' and C with stack structure to obtain a finite *étale* cover of stacky curves $\tilde{C}' \to \tilde{C}$ as in [9], the stacky finite étale cover together with the map $\tilde{C}' \to X$ is parameterized by a representable map $\tilde{C} \to [\mathrm{Sym}^n X]$ to the stack quotient

$$[\mathrm{Sym}^n X] := [X^n / \Sigma_n].$$

We can similarly allow C' and C to be nodal families of curves over some base S. Maps from nodal curves $\tilde{C}$ over S entail an S-point of the moduli stack $\mathfrak{M}([\mathrm{Sym}^n X])$ of prestable maps to the symmetric product. As in [4, Proposition 2.3], there is an open substack for which the map from the coarse space C' to X is a closed immersion. The stack $\mathfrak{M}([\mathrm{Sym}^n X])$ splits into components indexed by the ramification profiles of the cover of coarse spaces $C' \to C$.

There are some subtleties in characteristic p—one cannot treat all ramification as a μ_n torsor because some ramification is a $\mathbb{Z}/p\mathbb{Z}$-torsor in characteristic p. The formalism of tuning stacks [13] is a substitute in arbitrary characteristic.

4 Twisted monogenicity

The *Hasse local-to-global principle* is the idea that "local" solutions to a polynomial equation over all the p-adic fields $\mathbb{Q}_p$ and the real field $\mathbb{R}$ can piece together to a single "global" solution over $\mathbb{Q}$. We ask the same for monogenicity: given local monogenerators, say over completions or local in the Zariski or étale topologies, do they piece together to a single global monogenerator?

The Hasse principle fails for elliptic curves. Let E be an elliptic curve over a number field K and consider all its places ν. The Shafarevich-Tate group $\mathrm{III}(E/K)$ of an elliptic curve sits in an exact sequence

$$0 \to \text{III}(E/K) \to H^1_{et}(K, E) \to \prod_\nu H^1_{et}(K_\nu, E).$$

Elements of III are genus-one curves with rational points over each completion K_ν that do *not* have a point over K. Similarly, we want sequences of cohomology groups to control when local monogenerators do or do not come from a global monogenerator.

For such a sequence, one needs to know how a pair of local monogenerators can differ. One would like a group G or sheaf of groups transitively acting on the set of local monogenerators so that cohomology groups can record the struggle to patch local monogenerators together into a global monogenerator.

Suppose B/A is an algebra extension inducing $S' \to S$ and $\theta_1, \theta_2 \in B$ are both monogenerators. Then

$$\theta_1 \in B = A[\theta_2], \qquad \theta_2 \in B = A[\theta_1],$$

so each monogenerator is a polynomial in the other:

$$\theta_1 = p_1(\theta_2) \quad \text{and} \quad \theta_2 = p_2(\theta_1), \quad \text{with} \quad p_1(x), p_2(x) \in A[x].$$

We can think of the $p_i(x)$ as transition functions or endomorphisms of the affine line $\mathbb{A}^1$. Even though $p_1(p_2(\theta_1)) = \theta_1$, it is doubtful that $p_1 \circ p_2 = \text{id}_{\mathbb{A}^1}$ or even that $p_i(x)$ are automorphisms of $\mathbb{A}^1$.

One might attempt to find a group G containing all possible polynomials $p_1(x), p_2(x)$. We would then have a homomorphism (of non-commutative monoids) $E \to G$ where E is some sub-monoid of $\text{End}(\mathbb{A}^1)$, the monoid of endomorphisms of $\mathbb{A}^1$ (equivalently, the monoid of one-variable polynomials under composition). Even if we only insist that E contains x, $-x$, and x^2, we find that the images of x and $-x$ coincide in G since both compose with x^2 to the same polynomial. This is not acceptable as x and $-x$ act in distinct ways on monogenerators.

Instead of working with the group of all possible polynomial transition functions as above, we *require* our transition functions $p_i(x)$ to lie in a group $G \circlearrowleft \mathbb{A}^1$ acting on $\mathbb{A}^1$. Two particularly natural options for G present themeselves, namely the group sheaves:

$$\mathbb{G}_m(A) = A^*, \qquad u \cdot u' := uu'$$

$$\text{Aff}^1(A) = A^* \ltimes A, \qquad (u, v) \cdot (u', v') := (uu', uv' + v).$$

Affine transformations Aff^1 are essentially polynomials $ux + v$ of degree one under composition. These act on monogenerators:

$$\mathbb{G}_m \circlearrowleft \mathbb{A}^1 : \qquad\qquad a \in A^*, \theta \in \mathcal{M}(A), \qquad a.\theta := a \cdot \theta,$$

$$\text{Aff}^1 \circlearrowleft \mathbb{A}^1 : \qquad a \in A^*, b \in A, \theta \in \mathcal{M}(A), \qquad (a, b).\theta := a\theta + b.$$

Definition 4.1 (*Twisted monogenerators*)

A ($\mathbb{G}_m$)-twisted monogenerator for B/A is:

(1) a Zariski open cover $\text{Spec } A = \bigcup_i D(f_i)$ for elements $f_i \in A$,
(2) a system of "local" monogenerators $\theta_i \in B\left[f_i^{-1}\right]$ for $B[f_i^{-1}]$ over $A[f_i^{-1}]$, and
(3) units $a_{ij} \in A\left[f_i^{-1}, f_j^{-1}\right]^*$

such that

- for all i, j, we have $a_{ij}.\theta_j = \theta_i$,
- for all i, j, k, the "cocycle condition" holds:

$$a_{ij}.a_{jk} = a_{ik}.$$

Two such systems $\{(a_{ij}), (\theta_i)\}$, $\{(a'_{ij}), (\theta'_i)\}$ are *equivalent* if they differ by further refining the cover $\mathrm{Spec}\, A = \bigcup D(f_i)$ or global units $u \in A^*$: $u \cdot a_{ij} = a'_{ij}$, $u \cdot \theta_i = \theta'_i$.

Likewise B/A is Aff^1-*twisted monogenic* if there is a cover with θ_i's as above, but with units (3) replaced by pairs $a_{ij}, b_{ij} \in A\left[\frac{1}{f_i}, \frac{1}{f_j}\right]$ such that each a_{ij} is a unit and $a_{ij}\theta_j + b_{ij} = \theta_i$.

The elements θ_i may or may not come from a single global monogenerator $\theta \in A$. Nevertheless, the transition functions (a_{ij}) or (a_{ij}, b_{ij}) define an affine bundle L on $\mathrm{Spec}\, A$ with global section θ induced by the θ_i's. We say S'/S is "twisted monogenic" to mean there exists a $\mathbb{G}_m$-twisted monogenerator and similarly say "Aff^1-twisted" monogenic. Both are clearly Zariski-locally monogenic.

Compare with Cartier divisors:

twisted monogenerator	Cartier divisor
global monogenerator	rational function
$\mathbb{G}_m/\mathrm{Aff}^1$ action	differing by units.

We recall the notions of "multiply monogenic orders" and "affine equivalence" in the literature. Two monogenerators $\theta_1, \theta_2 \in \Gamma(\mathrm{Spec}\, A, \mathcal{M}_{B/A})$ are said to be "affine equivalent" if there are $u \in A^*$, $v \in A$ such that $u\theta_1 + v = \theta_2$. In other words, affine equivalence classes are elements of the quotient $\Gamma(\mathrm{Spec}\, A, \mathcal{M}_{B/A})/\mathrm{Aff}^1(A)$. Under certain hypotheses in Remark 4.12, Aff^1-twisted monogenicity is parameterized by the sheaf quotient $\mathcal{M}_{B/A}/\mathrm{Aff}^1$. There is almost an "exact sequence"

$$\mathrm{Aff}^1(A) \to \Gamma(\mathcal{M}_{B/A}) \to \Gamma(\mathcal{M}_{B/A}/\mathrm{Aff}^1) \to H^1(\mathrm{Aff}^1)$$

that dictates whether a twisted monogenerator comes from an affine equivalence class of global monogenerators.

We warm up with a classical approach to $\mathbb{G}_m$-quotients, namely taking Proj. Then we study Aff^1-twisted monogenerators before finally introducing G-twisted monogenerators for arbitrary groups G.

There is a moduli space for each notion of twisted monogenicity. We use these moduli spaces now and defer the proof until Theorem 4.26:

Theorem 4.2 (=Theorem 4.26) *Let $\mathbb{G}_m, \mathrm{Aff}^1$ act on $\mathbb{A}^1$ on the left in the natural way, inducing a left action on $\mathcal{M}_{S'/S}$. The stack quotients $[\mathcal{M}/\mathbb{G}_m]$ and $\left[\mathcal{M}/\mathrm{Aff}^1\right]$ represent $\mathbb{G}_m$- and Aff^1-twisted monogenerators up to equivalence, respectively.*

4.1 $\mathbb{G}_m$-twisted monogenerators and proj of the weil restriction

Writing $S' = \mathrm{Spec}\, B$ and $S = \mathrm{Spec}\, A$, a twisted monogenerator amounts to a Zariski cover $S = \mathrm{Spec}\, A = \bigcup U_i$, a system of closed embeddings $\theta_i : S'_{U_i} \subseteq \mathbb{A}^1_{U_i}$ over U_i, and elements $a_{ij} \in \mathbb{G}_m(U_i)$ such that

$$a_{ij}.\theta_j = \theta_i : S'_{U_{ij}} \to \mathbb{A}^1_{U_{ij}}.$$

Equivalently, a twisted monogenerator is a line bundle L on S defined by the above cocycle a_{ij} and a global embedding $\theta : S' \subseteq L$ over S. Twisted monogenerators $(\theta_i)_{i \in I}, (\theta'_j)_{j \in J}$ with

respect to covers covers $\{U_i\}_{i \in I}$, $U'_{j\,j \in J}$ are identified if they differ by global units $u \in \mathbb{G}_m(S)$ on a common refinement of the covers $\{U_i\}_{i \in I}$, $U'_{j\,j \in J}$, i.e., if the corresponding line bundles L, L' are isomorphic in a way that identifies the closed embeddings θ, θ'.

For number fields L/K with $\theta \in \mathbb{Z}_L$ and $a \in \mathbb{Z}_K$, one has $a\theta \in \mathbb{Z}_L$. If $a \in \mathbb{Z}_K^*$, then θ is a monogenerator if and only if $a\theta$ is. The multiplication action $\mathbb{G}_m(\mathbb{Z}_K) \circlearrowright \mathcal{R}(\mathbb{Z}_K)$ corresponds to the global $\mathbb{G}_m$ action on the vector bundle $\mathcal{R}$ over S.

An action of $\mathbb{G}_m$ corresponds to a $\mathbb{Z}$-grading on the sheaf of algebras [38, 0EKJ]. Locally in S, $\pi_* \mathcal{O}_{S'} \simeq \bigoplus_{i=1}^n \mathcal{O}_S \cdot e_i$ and $\mathcal{R} \simeq \mathbb{A}_S^n$. The $\mathbb{G}_m$ action is the diagonal action and corresponds to the total degree of polynomials in $\mathcal{O}_{\mathbb{A}_S^n} = \mathcal{O}_S[x_1, \ldots, x_n]$.

The associated projective bundle to the vector bundle $\mathcal{R}$ is given by the relative Proj [38, 01NS]

$$\mathbb{P}\mathcal{R}_{S'/S} := \underline{\text{Proj}}_S \mathcal{O}_{\mathcal{R}},$$

with the total-degree grading. The ideal $\mathcal{I}_{S'/S}$ cutting out the complement $\mathcal{N}_{S'/S}$ of $\mathcal{M}_{1,S'/S} \subseteq \mathcal{R}$ is graded by [4, Remark 3.10], defining a closed subscheme $\mathbb{P}\mathcal{N}_{S'/S} \subseteq \mathbb{P}\mathcal{R}$.

Definition 4.3 Define the *scheme of projective monogenerators*

$$\mathbb{P}\mathcal{M}_{S'/S} \subseteq \mathbb{P}\mathcal{R}_{S'/S} := \underline{\text{Proj}}_S \mathcal{O}_{\mathcal{R}_{S'/S}}$$

to be the open complement of the closed subscheme $\mathbb{P}\mathcal{N}_{S'/S}$ cut out by the graded homogeneous ideal $\mathcal{I}_{S'/S}$.

The reader may define projective polygenerators in the same fashion.

Lemma 4.4 *The vanishing of the irrelevant ideal $V(\mathcal{O}_{\mathcal{R},+})$ of $\mathcal{R}_{S'/S}$ is contained inside of the non-monogenicity locus $\mathcal{N}_{S'/S}$ for $S' \neq S$.*

Proof Locally, the lemma states that $\theta = 0$ is not a monogenerator. $\qquad\square$

Remark 4.5 We relate the Proj construction to stack quotients by $\mathbb{G}_m$ according to [31, Example 10.2.8]. The ring $\mathcal{O}_{\mathcal{R}_{S'/S}}$ is generated by elements of degree one. Locally, $\mathcal{R}_{S'/S} \simeq \mathbb{A}_S^n$ and $\mathcal{O}_{\mathcal{R}_{S'/S}} \simeq \mathcal{O}_S[x_1, \ldots, x_n]$ is generated by the degree one elements x_i. Write $\underline{\text{Spec}}_S \mathcal{O}_{\mathcal{R}}$ for the relative spectrum [38, 01LQ]. The map

$$\underline{\text{Spec}}_S \mathcal{O}_{\mathcal{R}} \setminus V(\mathcal{O}_{\mathcal{R},+}) \xrightarrow{-/\mathbb{G}_m} \underline{\text{Proj}}_S \mathcal{O}_{\mathcal{R}}$$

is therefore a stack quotient or $\mathbb{G}_m$-torsor.

We have a pullback square

$$\begin{array}{ccc} \mathcal{M}_{S'/S} & \longrightarrow & \underline{\text{Spec}}_S \mathcal{O}_{\mathcal{R}} \setminus V(\mathcal{O}_{\mathcal{R},+}) \\ \downarrow & \ulcorner & \downarrow \\ \mathbb{P}\mathcal{M}_{S'/S} & \longrightarrow & \underline{\text{Proj}}_S \mathcal{O}_{\mathcal{R}} \end{array}$$

of $\mathbb{G}_m$-torsors and a stack quotient $\mathbb{P}\mathcal{M}_{S'/S} = [\mathcal{M}_{S'/S}/\mathbb{G}_m]$.

Theorem 4.2 states that $[\mathcal{M}/\mathbb{G}_m]$ represents twisted monogenerators, and now we know the quotient stack is wondrously a *scheme*:

Corollary 4.6 *The scheme* $\mathbb{P}\mathcal{M}_{S'/S} = [\mathcal{M}/\mathbb{G}_m]$ *represents the* $\mathbb{G}_m$*-twisted monogenerators of Definition* 4.1*. That is,* $\mathbb{P}\mathcal{M}_{S'/S}$ *is a moduli space for twisted monogenerators. The action* $\mathbb{G}_m \circlearrowleft \mathcal{M}_{S'/S}$ *is free.*

Warning 4.7 Given a monogenerator $\theta \in \mathbb{Z}_L$ and a pair $a \in \mathbb{Z}_K^*$, $\beta \in \mathbb{Z}_L$, write

$$\beta = b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1}.$$

One may try to define a second action

$$a.\beta \overset{?}{:=} b_0 + b_1 a\theta + b_2 a^2 \theta^2 + \cdots + b_{n-1} a^{n-1} \theta^{n-1}$$

encoding the degree with respect to θ, but this action does not define a grading as it is almost never multiplicative. For example, take $\mathbb{Z}_L = \mathbb{Z}[\sqrt{2}]$ with monogenerator $\sqrt{2}$ over $\mathbb{Z}_K = \mathbb{Z}$. Then

$$a.2 = 2 \neq a.\sqrt{2} \cdot a.\sqrt{2}.$$

In the case that $S' = \operatorname{Spec} A[\epsilon]/\epsilon^{m+1}$ and $S = \operatorname{Spec} A$, we recall that $\mathcal{R}_{S'/S} = J_{\mathbb{A}_A^1, m}$ is the jet space of $\mathbb{A}_A^1$. Here, the action $a.x$ *is* multiplicative and induces a second action $\mathbb{G}_m \circlearrowleft \mathcal{R}_{S'/S} = J_{\mathbb{A}^1, m}$. The two actions of $\lambda \in \mathbb{G}_m$ on a jet

$$f(\epsilon) = a_0 + a_1\epsilon + \cdots + a_m\epsilon^m$$

on $\mathbb{A}^1$ are $\lambda.f(\epsilon) = \lambda \cdot f(\epsilon)$ and $\lambda.f(\epsilon) = f(\lambda\epsilon)$. The Proj of $J_{X,m}$ with respect to this second $\mathbb{G}_m$ action is known as a "Demailly-Semple jet" or a "Green-Griffiths jet" in the literature [40, Definition 6.1]. For certain $S' \to S$, there may be a distinguished one-parameter subgroup, i.e., the image of $\mathbb{G}_m \to \operatorname{Aut}_S(S')$, that results in a second action $\mathbb{G}_m \circlearrowleft \mathcal{R}_{S'/S}$ and allows an analogous construction.

4.2 Aff¹-twisted monogenerators and affine equivalence

We enlarge our study to representing spaces of Aff¹-twisted monogenerators and the related study of affine equivalence classes of ordinary monogenerators. We delay twisting by general sheaves of groups other than $\mathbb{G}_m$ and Aff¹ until the next section. For an S-scheme X, the *automorphism sheaf* $\operatorname{Aut}(X)$ is the subsheaf of automorphisms in $\underline{\operatorname{Hom}}_S(X, X)$.

Remark 4.8 The automorphism sheaf $\operatorname{Aut}_S(\mathbb{A}^1)$ has a subgroup of affine transformations Aff¹ under composition. These are identified in turn with $\mathbb{A}^1 \rtimes \mathbb{G}_m$ via

$$(a, b) \mapsto (x \mapsto bx + a).$$

The automorphism sheaf can be much larger for other $\mathbb{A}_S^k$. For example,

$$(x, y) \mapsto (x + y^3, y)$$

is an automorphism of $\mathbb{A}^2$.

The automorphism sheaf $\operatorname{Aut}(\mathbb{A}^1)$ is *not* the same as Aff¹, though they have the same points over reduced rings. See [12] for some discussion over nonreduced rings.

Recall that two monogenerators θ_1, θ_2 of an A-algebra B are said to be *equivalent* if

$$\theta_1 = u\theta_2 + v,$$

where $u \in A^*$ and $v \in A$. Likewise, say that two embeddings $\theta_1, \theta_2 : S' \to \mathcal{L}$ of S' into an Aff^1 bundle $\mathcal{L}$ over S are *equivalent* if there is in $f \in \mathrm{Aff}^1(S)$ such that $\theta_1 = f.\theta_2$. The set of monogenerators up to equivalence is then

$$\Gamma(S, \mathcal{M})/\Gamma(S, \mathrm{Aff}^1).$$

If $S' \overset{\sim}{\to} S$ is an isomorphism and $n = 1$, the action of Aff^1 is trivial. Otherwise, the Aff^1-action is often free:

Lemma 4.9 *The action* $\mathrm{Aut}(S') \circlearrowright \mathcal{M}_X$ *has trivial stabilizers, for any quasiprojective X. If S is normal and $S' \to S$ is not an isomorphism, the action* $\mathrm{Aff}^1 \circlearrowright \mathcal{M}_{S'/S}$ *has trivial stabilizers as well.*

Proof A stabilizer of the action $\mathrm{Aut}_S(S') \circlearrowright \mathcal{M}_X$ entails a diagram

$$
\begin{array}{ccc}
X & == & X \\
\uparrow & & \uparrow \\
S' & \overset{\sim}{\rule{1.5em}{0pt}} & S'.
\end{array}
$$

The fact that $S' \subseteq X$ is a monomorphism forces $S' \simeq S'$ to be the identity.

Normality of S means S is a finite disjoint union of integral schemes [38, 033N]; we assume S is integral without loss of generality.

Computing stabilizers of $\mathrm{Aff}^1 \circlearrowright \mathcal{M}_{S'/S}$ is local, so we may assume $S' \to S$ is induced by a non-identity finite map $A \to B$ of rings where A is an integrally closed domain with field of fractions K. A stabilizer

$$a + b\theta = \theta; \qquad a \in A, b \in A^*$$

implies $(1 - b)\theta = a$. If $b = 1$, then $a = 0$ and the stabilizing affine transformation is trivial. Otherwise, $1 - b \in K^*$ and $\theta = \dfrac{a}{1 - b} \in K$. Elements $\theta \in B$ are all integral over A. Since A is integrally closed, $\theta \in A$. Hence $B = A[\theta] = A$, a contradiction. $\qquad \square$

Remark 4.10 Suppose given transition functions (a_{ij}, b_{ij}) and local monogenerators (θ_i) as in an Aff^1-twisted monogenerator that *may not* satisfy the cocycle condition *a priori*. For normal S with $n > 1$ as in the lemma, the cocycle condition holds automatically, since Aff^1 acts without stabilizers.

Corollary 4.11 *If S is normal, the stack quotient* $\left[\mathcal{M}_{1,S'/S}/\mathrm{Aff}^1 \right]$ *is represented by the ordinary sheaf quotient* $\mathcal{M}/\mathrm{Aff}^1$.

Proof If $G \circlearrowright X$ is a free action, the stack quotient $[X/G]$ coincides with the sheaf quotient X/G. $\qquad \square$

Remark 4.12 If S is normal, Corollary 4.11 tells us that an Aff^1-twisted monogenerator is the same as a global section $\Gamma(S, \mathcal{M}/\mathrm{Aff}^1)$. Equivalence classes of monogenerators are given by the presheaf quotient $\Gamma(S, \mathcal{M})/\Gamma(S, \mathrm{Aff}^1)$.

Affine equivalence classes of monogenerators thereby relate to twisted monogenerators in an exact sequence of pointed sets:

$$\Gamma(S, \mathcal{M})/\Gamma(S, \mathrm{Aff}^1) \to \Gamma(S, \mathcal{M}/\mathrm{Aff}^1) \to H^1(S, \mathrm{Aff}^1).$$

As in sheaf cohomology, the second map takes $\overline{\theta}$ to its torsor of lifts $\delta(\overline{\theta})$ in $\mathcal{M}_{S'/S}$:

$$\delta(\overline{\theta})(U) = \{f \in \mathcal{M}(U) : f + \mathrm{Aff}^1(U) = \overline{\theta}|_U\}.$$

A section of the sheaf quotient

$$\overline{\theta} \in \Gamma(S, \mathcal{M}/\mathrm{Aff}^1)$$

lifts to an affine equivalence class in the presheaf quotient $\theta \in \Gamma(S, \mathcal{M})/\Gamma(S, \mathrm{Aff}^1)$ if and only if the induced Aff^1-torsor is trivial.

The exact sequence is analogous to Cartier divisors. If X is an integral scheme with rational function field $K(X)$, the long exact sequence associated to

$$1 \to \mathcal{O}_X^* \to K(X)^* \to K(X)^*/\mathcal{O}_X^* \to 1$$

is analogous to the above.

Remark 4.13 One can do the same with $\mathbb{G}_m$, or any other group that acts freely. Compare twisted monogenerators $\mathbb{P}\mathcal{M} = [\mathcal{M}/\mathbb{G}_m]$ with ordinary monogenerators $\mathcal{M}_{S'/S}$ up to $\mathbb{G}_m$-equivalence to obtain a sequence

$$\Gamma(S, \mathcal{M})/\Gamma(S, \mathbb{G}_m) \to \Gamma(S, \mathcal{M}/\mathbb{G}_m) \to H^1(S, \mathbb{G}_m).$$

Freeness of the action is necessary to identify the stack quotient with the ordinary sheaf quotient.

Sometimes, being $\mathbb{G}_m$-twisted monogenic is the same as being Aff^1-twisted monogenic:

Proposition 4.14 *If $S = \mathrm{Spec}\, A$ is affine, all Aff^1-torsors on S are induced by $\mathbb{G}_m$-torsors:*

$$H^1(\mathrm{Spec}\, A, \mathbb{G}_m) \simeq H^1(\mathrm{Spec}\, A, \mathit{Aff}^1).$$

The corresponding twisted forms of $\mathbb{A}^1$ are the same, so we can furthermore identify $\mathbb{G}_m$-twisted monogenerators with Aff^1-twisted monogenerators.

Proof The maps

$$\begin{array}{cc} \mathbb{A}^1 \to \mathrm{Aff}^1 & \mathrm{Aff}^1 \to \mathbb{G}_m \\ a \mapsto (x \mapsto x + a) & (x \mapsto bx + a) \mapsto b \end{array} \quad \text{and}$$

fit into a short exact sequence

$$0 \to \mathbb{A}^1 \to \mathrm{Aff}^1 \to \mathbb{G}_m \to 1.$$

The sheaf Aff^1 is *not* commutative. Cohomology *sets* $H^i(S, \mathrm{Aff}^1)$ are nevertheless defined for $i = 0, 1, 2$. By Serre Vanishing [38, 01XB] we have $H^i(\mathrm{Spec}\, A, \mathbb{A}^1) = 0$ for $i \neq 0$, and therefore $\Gamma(\mathrm{Aff}^1) \to \Gamma(\mathbb{G}_m)$ is surjective, yielding an identification in all nonzero degrees:

$$H^i(\mathrm{Spec}\, A, \mathrm{Aff}^1) \simeq H^i(\mathrm{Spec}\, A, \mathbb{G}_m), \qquad i = 1, 2.$$

The action $\mathbb{G}_m \circlearrowright \mathbb{A}^1$ is the restriction of that of Aff^1, factoring

$$\mathbb{G}_m \subseteq \mathrm{Aff}^1 \to \mathrm{Aut}(\mathbb{A}^1).$$

The corresponding twisted forms of $\mathbb{A}^1$ are the same. $\qquad\square$

4.3 Consequences of Aff^1-twisted monogenicity

We conclude with several consequences of twisted monogenicity and our Theorem 4.19 that shows twisted monogenerators detect class number-one number rings.

The following theorem constrains the line bundles that may be used for twisted monogenicity. This result constrains the possible Steinitz classes of a twisted monogenic extension. This is an effective constraint in geometric situations: see Lemma 5.4. The structure of the set of ideals corresponding to Steinitz classes of number rings is the subject of a variety of open questions. This has traditionally been the domain of class field theory; two notable papers are [8,28]. For $n > 0$, write $d(n) = \gcd\left(\{\frac{\ell-1}{2} : \ell \text{ prime}, \ell \mid n\}\right)$. Theorems 1 and 2 of [28] imply that if K contains a primitive nth root of unity, then the Steinitz classes of Galois extensions L/K of degree n are precisely the $d(n)^{\text{th}}$ powers in the class group of K. Compare this to the following:

Theorem 4.15 *Suppose $S' \to S$ is $\mathbb{G}_m$-twisted monogenic, with an embedding into a line bundle E. Let $\mathcal{E}$ be the sheaf of sections of E. Then*

$$\det(\pi_*\mathcal{O}_{S'}):= \wedge^{top} \pi_*\mathcal{O}_{S'} \simeq \mathcal{E}^{-\frac{n(n-1)}{2}}$$

in Pic(S).

In particular, if an extension of number rings $\mathbb{Z}_L/\mathbb{Z}_K$ is twisted monogenic, then its Steinitz class is an $\frac{n(n-1)}{2}$th power in the class group.

Proof Write $\text{Sym}^*\mathcal{E}:=\bigoplus_d \text{Sym}^d\mathcal{E}$ for the symmetric algebra. Recall that $E \simeq \mathbb{V}(\mathcal{E}^\vee):= \underline{\text{Spec}}_S \text{Sym}^*(\mathcal{E}^\vee)$. We have a surjection of $\mathcal{O}_S$-modules

$$\text{Sym}^*\mathcal{E}^\vee \twoheadrightarrow \pi_*\mathcal{O}_{S'},$$

which we claim factors through the projection of $\mathcal{O}_S$-modules $\text{Sym}^*\mathcal{E}^\vee \to \bigoplus_{i=0}^{n-1} \text{Sym}^i\mathcal{E}^\vee$. Such a factorization is a local question and local factorizations automatically glue because there is at most one. Locally, we may assume $S' \to S$ is induced by a ring homomorphism $A \to B$ and $\mathcal{E}^\vee$ is trivialized. We have a factorization of A-modules

$$\text{Sym}^*\mathcal{E}^\vee \cong A[t] \relbar\joinrel\twoheadrightarrow B$$
$$\searrow \qquad \nearrow$$
$$\bigoplus_{i=0}^{n-1} \text{Sym}^i\mathcal{E}^\vee \simeq \bigoplus_{i=0}^{n-1} A \cdot t^i$$

due to the existence of a monic polynomial $m_\theta(t)$ of degree n for the image θ of t in $\mathcal{O}_{S'}$ [4, Lemma 2.11]. The A-modules $\bigoplus_{i=0}^{n-1} A \cdot t^i$ and B are abstractly isomorphic, and any surjective endomorphism of a finitely generated module is an isomorphism [27, Theorem 2.4].

We conclude that globally

$$\pi_*\mathcal{O}_{S'} \simeq \bigoplus_{i=0}^{n-1} \text{Sym}^i\mathcal{E}^\vee.$$

Since $\mathcal{E}$ is invertible, $\text{Sym}^i\mathcal{E}^\vee = (\mathcal{E}^\vee)^i$. Taking the determinant,

$$\det(\pi_*\mathcal{O}_{S'}) = \det\left(\bigoplus_{i=0}^{n-1}(\mathcal{E}^\vee)^i\right) = \mathcal{E}^{-\sum_{i=0}^{n-1} i} = \mathcal{E}^{-\frac{n(n-1)}{2}}.$$

$\square$

The literature abounds with finiteness results on equivalence classes of monogenerators, for example:

Theorem 4.16 ([14, Theorem 5.4.4]) *Let A be an integrally closed integral domain of characteristic zero and finitely generated over $\mathbb{Z}$. Let K be the quotient field of A, Ω a finite étale K-algebra with $\Omega \neq K$, and B the integral closure of A in Ω. Then there are finitely many equivalence classes of monogenic generators of B over A.*

We have an analogous finiteness result for equivalence classes of Aff^1-twisted monogenerators:

Corollary 4.17 *Let A, K, Ω, B be as in Theorem 4.16, with $S' \to S$ induced from $A \to B$. Assume Pic(A) is finitely generated. Then there are finitely many equivalence classes of Aff^1-twisted monogenerators for $S' \to S$.*

Proof We essentially use the sequence

$$\Gamma(S, \mathcal{M})/\Gamma(S, \mathrm{Aff}^1) \to \Gamma(S, \mathcal{M}/\mathrm{Aff}^1) \to H^1(S, \mathrm{Aff}^1)$$

of Remark 4.12. If this *were* a short exact sequence of groups, the outer terms being finite would force the middle term to be; our proof is similar in spirit.

Since S is quasicompact and there are finitely many elements of the Picard group which are $\frac{n(n-1)}{2}$th-roots of the Steinitz class

$$\mathrm{Pic}(S) := H^1(S, \mathbb{G}_m) = H^1(S, \mathrm{Aff}^1),$$

we can find an affine open cover $S = \bigcup_i U_i$ by finitely many open sets of S that simultaneously trivializes all $\frac{n(n-1)}{2}$th-roots of the Steinitz class on S.

The above sequence of presheaves restricts to the U_i's in a commutative diagram

$$\begin{array}{ccccc}
\Gamma(S, \mathcal{M})/\Gamma(S, \mathrm{Aff}^1) & \longrightarrow & \Gamma(S, \mathcal{M}/\mathrm{Aff}^1) & \longrightarrow & H^1(S, \mathrm{Aff}^1) \\
\downarrow & & \downarrow{\scriptstyle\rho} & & \downarrow \\
\prod \Gamma(U_i, \mathcal{M})/\Gamma(U_i, \mathrm{Aff}^1) & \longrightarrow & \prod \Gamma(U_i, \mathcal{M}/\mathrm{Aff}^1) & \longrightarrow & \prod H^1(U_i, \mathrm{Aff}^1).
\end{array}$$

The restriction $H^1(S, \mathrm{Aff}^1) \to \prod H^1(U_i, \mathrm{Aff}^1)$ is zero on the $\frac{n(n-1)}{2}$th-roots of the Steinitz class by construction of the U_i's. The restriction $\rho : \Gamma(S, \mathcal{M}/\mathrm{Aff}^1) \hookrightarrow \prod \Gamma(U_i, \mathcal{M}/\mathrm{Aff}^1)$ is injective by the sheaf condition. A diagram chase reveals that the restriction $\rho(\overline{\theta})$ of any section $\overline{\theta} \in \Gamma(S, \mathcal{M}/\mathrm{Aff}^1)$ is in the image of $\prod \Gamma(U_i, \mathcal{M})/\Gamma(U_i, \mathrm{Aff}^1)$. Theorem 4.16 asserts that each set $\Gamma(U_i, \mathcal{M})/\Gamma(U_i, \mathrm{Aff}^1)$ is finite. $\qquad\square$

Lemma 4.18 *Degree-two extensions are all Aff^1-twisted monogenic. If S is affine, they are also $\mathbb{G}_m$-twisted monogenic.*

Proof Localize and choose a basis containing 1 to write $\pi_* \mathcal{O}_{S'} \simeq \mathcal{O}_S \oplus \mathcal{O}_S \theta_1$ for some $\theta_1 \in \Gamma(\mathcal{O}_{S'})$. Given an element θ_2 so that $\{1, \theta_2\}$ is also a basis, we may write

$$\theta_1 = a + b\theta_2, \qquad \theta_2 = c + d\theta_1, \qquad a, b, c, d \in \mathcal{O}_S.$$

Hence $bd = 1$ are units, and the transition functions come from $\mathrm{Aff}^1 = \mathbb{A}^1 \rtimes \mathbb{G}_m$. By choosing such generators on a cover of S, one obtains a twisted monogenerator. Proposition 4.14 further refines our affine bundle to a line bundle. $\qquad\square$

Theorem 4.19 *A number ring $\mathbb{Z}_K$ has class number one if and only if all twisted monogenic extensions of $\mathbb{Z}_K$ are in fact monogenic.*

Proof If the class number of K is one, then all line bundles on $\mathrm{Spec}\,\mathbb{Z}_K$ are trivial and the equivalence is clear. Mann [26] has shown that K has quadratic extensions without an integral basis if and only if the class number of K is not one: adjoin the square root of α, where $(\alpha) = \mathfrak{b}^2\mathfrak{c}$ with $\mathfrak{b}$ non-principal and $\mathfrak{c}$ square-free. By Lemma 4.18, such an extension is necessarily $\mathbb{G}_m$-twisted monogenic. As the monogenicity of quadratic extensions is equivalent to the existence of an integral basis, the result follows.   □

Remark 4.20 Theorem 4.19 implies that the ring of integers of a number field is twisted monogenic over $\mathbb{Z}$ if and only if it is monogenic over $\mathbb{Z}$. Example 5.3 thus provides an example of a number field which is not twisted monogenic.

Given that twisted monogenic extensions and monogenic extensions coincide over $\mathbb{Z}$, we should ask for an example where we have twisted monogenicity but not monogenicity. All degree 2 extensions of number rings are twisted monogenic as Lemma 4.18 shows. Thus every quadratic extension without an integral basis is twisted monogenic but not monogenic, and [26] provides a construction of such extensions. The aim of the following is the very explicit construction of a higher degree example of such an extension. Though we are ultimately unable to prove non-monogenicity in the following example, we hope it gives the reader a concrete sense of the concepts and methods employed in this section.

Example 4.21 (Properly twisted monogenic, not quadratic) Let $K = \mathbb{Q}(\sqrt[3]{5\cdot 23})$ and let $\mathfrak{p}_3$, $\mathfrak{p}_5$, and $\mathfrak{p}_{23}$ be the unique primes of K above 3, 5, and 23, respectively. One can compute $\mathfrak{p}_3 = (\rho_3 := 1970(\sqrt[3]{5\cdot 23})^2 + 9580(\sqrt[3]{5\cdot 23}) + 46587)$. Consider $\mathbb{Z}_L/\mathbb{Z}_K$, where $L = K(\sqrt[3]{23\rho_3})$. On $D(\mathfrak{p}_{23})$, the local index form with respect to the local basis $\{1, \sqrt[3]{23\rho_3}, (\sqrt[3]{23\rho_3})^2\}$ is $b^3 - 23\rho_3 c^3$. On $D(\mathfrak{p}_5)$, we have the local index form $B^3 - 5^2\rho_3 C^3$ with respect to the local basis $\{1, \sqrt[3]{5^2\rho_3}, (\sqrt[3]{5^2\rho_3})^2\}$. We transition via $\sqrt[3]{23^2\cdot 5^2}/23$, which is not a global unit, so the extension $\mathbb{Z}_L/\mathbb{Z}_K$ is twisted monogenic.

To see what is going on more explicitly, we investigate how the transitions affect the local index forms. We have

$$b^3 - 23\rho_3 c^3 = \frac{5^2}{23}B^3 - \frac{5^4}{23^2}\cdot 23\rho_3 C^3 = \frac{5^2}{23}B^3 - \frac{5^4}{23}\rho_3 C^3 = \text{ a unit in } \mathcal{O}_{D(\mathfrak{p}_{23})}.$$

If B and C could be chosen to be $\mathbb{Z}_K$-integral so that local index form represented a unit of $\mathbb{Z}_K$, then $\sqrt[3]{5^2\rho_3}$ would be a global monogenerator. However, $\mathfrak{p}_5$-adic valuations tell us $\sqrt[3]{5^2\rho_3}$ is not a monogenerator. One can also apply Dedekind's index criterion to $x^3 - 5^2\rho_3$. Similarly, we have

$$B^3 - 5^2\rho_3 C^3 = \frac{23}{5^2}b^3 - \frac{23^2}{5^4}\cdot 5^2\rho_3 c^3 = \frac{23}{5^2}b^3 - \frac{23^2}{5^2}\rho_3 c^3 = \text{ a unit in } \mathcal{O}_{D(\mathfrak{p}_5)}.$$

If b and c could be chosen to be $\mathbb{Z}_K$-integral so that local index form represented a unit of $\mathbb{Z}_K$, then $\sqrt[3]{23\rho_3}$ would be a global monogenerator. As above, the $\mathfrak{p}_{23}$-adic valuations tell us this cannot be the case. Again, we could also use polynomial-specific methods.

We have shown that $\mathbb{Z}_L/\mathbb{Z}_K$ is twisted monogenic, but it remains to show that the twisting is non-trivial. We need to show the ideal $\mathfrak{p}_5 = (5, \sqrt[3]{5\cdot 23})$ is not principal. On $D(\mathfrak{p}_{23})$ it can be generated by $\sqrt[3]{5\cdot 23}$ and on $D(\mathfrak{p}_5)$ it can be generated by 5. We

transition between these two generators via $\sqrt[3]{5^2 \cdot 23^2}/23$, exactly as above. Thus our twisted monogenerators correspond to a non-trivial ideal class.

A computer algebra system can compute a K-integral basis for $\mathbb{Z}_L$:

$$\left\{ 1, \left(-2\sqrt[3]{23 \cdot 5} + \frac{5}{25}\left(\sqrt[3]{23 \cdot 5}\right)^2 \right) \sqrt[3]{23\rho_3} + \left(-3 + \frac{3}{23}\sqrt[3]{23 \cdot 5} \right)\left(\sqrt[3]{23\rho_3}\right)^2, \right.$$

$$\left(120589 + 5243\sqrt[3]{23 \cdot 5} + \frac{5243}{23}\left(\sqrt[3]{23 \cdot 5}\right)^2 \right)\sqrt[3]{23\rho_3}$$

$$\left. + \left(22850 + \frac{57125}{23}\sqrt[3]{23 \cdot 5} + 1828\left(\sqrt[3]{23 \cdot 5}\right)^2 \right)\left(\sqrt[3]{23\rho_3}\right)^2 \right\},$$

with index form:

$$\begin{aligned}
i_{\mathbb{Z}_L/\mathbb{Z}_K} = \ & 13796817(\sqrt[3]{5 \cdot 23})^2 b^3 - 1367479703949(\sqrt[3]{5 \cdot 23})^2 b^2 c \\
& + 45179341009193328(\sqrt[3]{5 \cdot 23})^2 bc^2 + 67103709\sqrt[3]{5 \cdot 23}\, b^3 \\
& - 497537273719431009077(\sqrt[3]{5 \cdot 23})^2 c^3 - 6650125342740\sqrt[3]{5 \cdot 23}\, b^2 c \\
& + 219702478196413227\sqrt[3]{5 \cdot 23}\, bc^2 - 2419492830176044167763\sqrt[3]{5 \cdot 23}\, c^3 \\
& + 326269891 b^3 - 32339923090800 b^2 c + 1068411032584717260 bc^2 \\
& - 11765841517121285321908 c^3.
\end{aligned}$$

Because $\mathbb{Z}_L/\mathbb{Z}_K$ is twisted monogenic, there are no common index divisors. Thus we will always find solutions to $i_{\mathbb{Z}_L/\mathbb{Z}_K}$ when we reduce modulo a prime of $\mathbb{Z}_K$. We do not expect $\mathbb{Z}_L$ to be monogenic over $\mathbb{Z}_K$; however, showing that there are no values of $b, c \in \mathbb{Z}_K$ such that $i_{\mathbb{Z}_L/\mathbb{Z}_K}(b, c) \in \mathbb{Z}_K^*$ appears to be rather difficult.

A clever way to get around this issue would be to show that the different of L/K was non-principal. This would preclude monogenicity by prohibiting an integral basis all together. Unfortunately, one can compute that the different is principal, so the extension does have a relative integral basis.

Remark 4.22 One can perform the same construction of Example 4.21 with radical cubic number rings other than $\mathbb{Q}(\sqrt[3]{5 \cdot 23})$. Specifically, take any radical cubic where $(3) = \mathfrak{p}_3^3 = (\alpha)^3$, ℓ, and q are distinct primes with $(\ell) = \mathfrak{l}^3$, $(q) = \mathfrak{q}^3$, and neither $\mathfrak{l}$ nor $\mathfrak{q}$ principal. The ideas behind this construction can be taken further by making appropriate modifications.

4.4 Twisting in general

Throughout this section, fix notation as in Situation 1.1 and work in the category (Sch/S) of schemes over S equipped with the étale topology. In particular, we allow X to be any quasiprojective S-scheme.

Definition 4.1 readily generalizes. Replace $\mathbb{G}_m$ by any étale sheaf of groups G with a left action $G \circlearrowright X$. A G-twisted monogenerator for $S' \to S$ (into X) is an étale cover $U_i \to S$, closed embeddings $\theta_i : S'_{U_i} \subseteq X_{U_i}$, and elements $g_{ij} \in G(U_{ij})$ such that

$$g_{ij}.\theta_j = \theta_i : S'_{U_{ij}} \to X_{U_{ij}}.$$

Say two G-twisted monogenerators (θ_i), (η_i) are *equivalent* if, after passing to a common refinement of the associated covers, there is a global section $g \in G(S)$ so that $\theta_i = g|_{U_i} \cdot \eta_i$ for all i. Equivalently, the θ_i's glue to a global closed embedding $S' \subseteq \hat{X}$ into a twisted form $\hat{X}$ of X the same way the $\mathbb{G}_m$-twisted monogenerators give embeddings into a line bundle.

The twisted form $\hat{X}$ arises from transition functions in G, meaning there is a G-torsor P such that $\hat{X}$ is the contracted product:

$$\hat{X} = X \wedge^G P := X \times P/(G, \Delta)$$

We have already seen the variant $G = \mathrm{Aff}^1$, $X = \mathbb{A}^1$. Other interesting cases include $G = \mathrm{PGL}_2 \circlearrowright \mathbb{P}^1$, $\mathrm{GL}_n \circlearrowright \mathbb{A}^n$, an ellliptic curve E acting on itself $E \circlearrowright E$, etc.

Remark 4.23 Usually, contracted products are defined for a left action $G \circlearrowright P$ and a *right* action $G \circlearrowleft X$ by quotienting by the antidiagonal action

$$X \wedge^G P := X \times P/(-\Delta, G)$$

defined by

$$G \circlearrowright X \times P; \qquad g.(x, p) := (x.g^{-1}, g.p).$$

We instead take two left actions and quotient by the diagonal action of G. The literature often turns left actions $\mathbb{G}_m \circlearrowright \mathbb{A}^1$ into right actions anyway, as in [7, Remark 1.7].

Group sheaves G beget stacks $BG = BG_S$ classifying G-torsors on S-schemes with universal G-torsor $S \to BG$.

Twisted forms $\hat{X}$ of X are equivalent to torsors for $\mathrm{Aut}(X)$ ([34, Theorem 4.5.2]), as follows: Given a twisted form $\hat{X} \to S$, we obtain the torsor $\underline{\mathrm{Isom}}(\hat{X}, X)$ of local isomorphisms. Given a $\mathrm{Aut}(X)$-torsor P, we define a twisted form via contracted product:

$$\hat{X}_P := X \wedge^{\mathrm{Aut}(X)} P$$

The stack $B\mathrm{Aut}(X)$ is thereby a moduli space for twisted forms of X with universal family $X \wedge^{\mathrm{Aut}(X)}_{B\mathrm{Aut}(X)} S = [X/\mathrm{Aut}(X)]$. An action $G \to \mathrm{Aut}(X)$ lets one turn a G-torsor P into a twisted form

$$\hat{X}_P := X \wedge^G P$$

classified by the map $BG \to B\mathrm{Aut}(X)$.

The automorphism sheaf $\mathrm{Aut}(X)$ acts on the scheme $\mathcal{M}_X$ via postcomposition with the embeddings $S' \to X$, yielding a map of sheaves

$$\gamma : \mathrm{Aut}(X) \to \mathrm{Aut}(\mathcal{M}_X)^4.$$

Similarly, the automorphism sheaf $\mathrm{Aut}(S')$ acts on $\mathcal{M}_X$ on the right via precomposition:

$$\xi : \mathrm{Aut}(S')^{op} \to \mathrm{Aut}(\mathcal{M}_X).$$

The induced map $H^1(S, \mathrm{Aut}(X)) \to H^1(S, \mathrm{Aut}(\mathcal{M}_X))$ sends a twisted form $\widehat{X}$ of X to the twisted form $\mathcal{M}_{\widehat{X}}$ of $\mathcal{M}_X$ given by looking at closed embeddings into $\widehat{X}$. We package these twisted forms $\mathcal{M}_{\hat{X}}$ into a universal version: $\mathrm{Twist}\mathcal{M}$.

Definition 4.24 ($\mathrm{Twist}\mathcal{M}$) Let $\mathrm{Twist}\mathcal{M} \to B\mathrm{Aut}(X)$ be the $B\mathrm{Aut}(X)$-stack whose T-points are given by

$$\left\{ \begin{array}{c} \mathrm{Twist}\mathcal{M} \\ \nearrow \quad \downarrow \\ T \xrightarrow[\widehat{X}]{} B\mathrm{Aut}(X) \end{array} \right\} := \left\{ \begin{array}{c} S' \times_S T \dashrightarrow^{s} \widehat{X} \\ \searrow \quad \swarrow \\ T \end{array} \;\middle|\; s \text{ is a closed immersion} \right\}.$$

---

[4] The map γ need not be injective. Consider $S = \mathrm{Spec}\, k$ a geometric point, $S' = \bigsqcup^3 S$ the trivial 3-sheeted cover, and $X = \bigsqcup^2 S$ only 2-sheeted. There are no closed immersions $S' \subseteq X$, so $\mathcal{M}_X = \varnothing$ has global automorphisms $\mathrm{Aut}(\varnothing) \simeq \{id\}$, but $\mathrm{Aut}(X) \simeq \mathbb{Z}/2\mathbb{Z}$ is nontrivial. Similar examples abound for non-monogenic $S' \to S$.

The map $\text{Twist}\mathcal{M} \to B\text{Aut}(X)$ is representable by schemes, since pullbacks are twisted forms $\mathcal{M}_{\hat{X}}$ of $\mathcal{M}_X$ itself:

$$
\begin{array}{ccc}
\mathcal{M}_{\hat{X}} & \longrightarrow & S \\
\downarrow & \ulcorner & \downarrow{\scriptstyle\hat{X}} \\
\text{Twist}\mathcal{M} & \longrightarrow & B\text{Aut}(X).
\end{array}
$$

The universal torsor over $B\text{Aut}(X)$ is S, but the universal twisted form is obtained by the contracted product with X over $B\text{Aut}(X)$:

$$
X \wedge^{\text{Aut}(X)}_{B\text{Aut}(X)} S \simeq [X/\text{Aut}(X)].
$$

One can exhibit $\text{Twist}\mathcal{M}$ as an open substack of the Weil Restriction of $[X/\text{Aut}(X)] \to B\text{Aut}(X)$ as in [4, Proposition 2.3]. There is a universal closed embedding over $\text{Twist}\mathcal{M}$ into the universal twisted form of X as in the definition of $\mathcal{M}_{S'/S}$:

$$
\begin{array}{ccc}
\text{Twist}\mathcal{M} \times_S S' & \xhookrightarrow{\quad u \quad} & [X/\text{Aut}(X)]. \\
& \searrow \qquad \swarrow & \\
& \text{Twist}\mathcal{M} &
\end{array}
$$

The universal case is concise to describe but unwieldy because $\text{Aut}(X)$ need not be finite, smooth, or well-behaved in any sense. We simplify by specifying our twisted form $\hat{X} \to T$ to get a scheme $\text{Twist}\mathcal{M}_{\hat{X}} = T \times_{\hat{X},B\text{Aut}(X)} \text{Twist}\mathcal{M}$ or by specifying the structure group G.

Fixing the structure group G requires $\hat{X} = X \wedge^G P$ for the specified sheaf of groups G and some G-torsor P. These G-twisted forms are parameterized by the pullback

$$
\begin{array}{ccc}
\text{Twist}\mathcal{M}^G & \longrightarrow & \text{Twist}\mathcal{M} \\
\downarrow & \ulcorner & \downarrow \\
BG & \longrightarrow & B\text{Aut}(X).
\end{array}
$$

The fibers of $\text{Twist}\mathcal{M}^G \to BG$ over maps $T \to BG$ are again twisted forms of $\mathcal{M}_X$. If $X = \mathbb{A}^k$ and $\hat{X}$ is a G-twisted form, we may refer to the existence of sections of $\text{Twist}\mathcal{M}_{\hat{X}}$ by saying S'/S is G-twisted k-genic, etc.

Remark 4.25 Trivializing $\hat{X}$ is not the same as trivializing the torsor P that induces $\hat{X}$ unless the group G is $\text{Aut}(X)$ itself. For example, take the trivial action $G \circlearrowright X$.

Theorem 4.26 *The stack of twisted monogenerators $\text{Twist}\mathcal{M}$ is isomorphic to $[\mathcal{M}_X/\text{Aut}(X)]$ over $B\text{Aut}(X)$. More generally, for any sheaf of groups $G \circlearrowright X$, we have an isomorphism $\text{Twist}\mathcal{M}^G \simeq [\mathcal{M}_X/G]$ over BG.*

Proof Address the second, more general assertion and let T be an S-scheme. Write $X_T := X \times_S T$, $T' := T \times_S S'$, etc. A T-point of $\text{Twist}\mathcal{M}^G$ is a G-torsor $P \to T$ and a solid

diagram
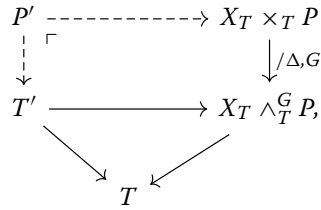
with $T' \to X_T \wedge_T^G P$ a closed immersion. Form P' by pullback: P' is a left G-torsor with an equivariant map to $X_T \times_T P$ with the diagonal action. The map $P' \to X_T \times_T P$ entails a pair of equivariant maps $P' \to P$ and $P' \to X_T$. The map $P' \to P$ over T forces $P' \simeq P \times_T T'$. These data form an equivariant map $P \to \mathcal{M}_X$ over T, or $T \to [\mathcal{M}_X/G]$. Reverse the process to finish the proof. $\qquad\square$

To see this theorem in practice, we have the following example.

Definition 4.27 The group sheaf $\mathrm{Aff}^k \subseteq \mathrm{Aut}(\mathbb{A}^k)$ of *affine transformations* is the set of functions

$$\mathbf{x} \mapsto M\mathbf{x} + \mathbf{b}$$

where $M \in \mathrm{GL}_k$ and $\mathbf{b} \in \mathbb{A}^k$, under composition. Note $\mathrm{Aff}^k \cong \mathbb{A}^k \rtimes \mathrm{GL}_k$.

Example 4.28 Let S' be the spectrum of a quadratic order such as $\mathbb{Z}[i]$, and take $S = \mathrm{Spec}\,\mathbb{Z}$. The space of k-generators is $\mathcal{M}_{k,S'/S} = \mathbb{A}^k \times (\mathbb{A}^k \setminus 0)$ according to [4, Proposition 4.5]. Take the quotient by the groups of affine transformations:

$$[\mathcal{M}_{k,S'/S}/\mathbb{A}^k \rtimes \mathbb{G}_m] = \mathbb{P}^{k-1}, \qquad [\mathcal{M}_{k,S'/S}/\mathrm{Aff}^k] = [\mathbb{A}^k/\mathrm{GL}_k] = [\mathbb{P}^{k-1}/\mathrm{PGL}_k].$$

These quotients represent twisted monogenerators according to Theorem 4.26. The corresponding PGL_k-torsors were classically identified with Azumaya algebras and Severi-Brauer varieties (see the exposition in [24]) or twisted forms of $\mathbb{P}^{k-1}$. These yield classes in the Brauer group $H^2(\mathbb{G}_m)$ via the connecting homomorphism from

$$1 \to \mathbb{G}_m \to \mathrm{GL}_k \to \mathrm{PGL}_k \to 1.$$

The same holds locally for any degree-two extension $S' \to S$ with S integral using [4, Proposition 4.5].

If G is an abelian variety over a number field $S = \mathrm{Spec}\,K$, let $P \to S$ be a G-torsor inducing a twisted form $\hat{X}$ of X. Given a twisted monogenerator $\theta : S' \subseteq \hat{X}$, one can try to promote θ to a global monogenerator by trivializing P and thus X.

Suppose one is given trivializations of P over the completions K_v at each place. Whether these glue to a global trivialization of P over K and thus a monogenerator $S' \subseteq X$ is governed by the Shafarevich-Tate group $\mathрш(G/K)$.

Given a G-twisted monogenerator with local trivializations, the Shafarevich-Tate group obstructs lifts of θ to a global monogenerator the same way classes of line bundles in Pic obstruct $\mathbb{G}_m$-twisted monogenerators from being global monogenerators. Theorem 4.19 showed a converse—nontrivial elements of Pic imply twisted monogenerators that are not global monogenerators.

Question 4.29 *Is the same true for* Ш*? Does every element of the Shafarevich-Tate group arise this way?*

The Shafarevich-Tate group approach is useless for $G = \mathbb{G}_m$ or GL_n because of Hilbert's Theorem 90 [38, 03P8]:

$$H^1_{et}(\operatorname{Spec} K, G) = H^1_{Zar}(\operatorname{Spec} K, G) = 0.$$

The same goes for any "special" group with étale and Zariski cohomology identified. The strategy may work better for PGL_n or elliptic curves E.

Remark 4.30 This section defined G-twisted monogenerators using covers in the étale topology, whereas Definition 4.1 used the Zariski topology. For $G = \mathbb{G}_m$ or Aff^1, either topology gives the same notion of twisted monogenerators. Observe that $\mathbb{G}_m$ has the same Zariski and étale cohomology by Hilbert's Theorem 90. The same is true for $\mathbb{A}^1$ by [38, 03P2] and so also $\mathrm{Aff}^1 = \mathbb{G}_m \ltimes \mathbb{A}^1$.

5 Examples of the scheme of monogenerators

We conclude with several examples to further illustrate the interaction of the various forms of monogenicity considered in this paper. We will make frequent reference to computation of the index form using the techniques of the previous paper in this series. Some of these examples were already considered in the previous paper, but are revisited in order to add some commentary on their relationship to notions of local monogenicity.

5.1 Orders in number rings

Example 5.1 (Dedekind's non-monogenic cubic field) Let η denote a root of the polynomial $X^3 - X^2 - 2X - 8$ and consider the field extension $L:=\mathbb{Q}(\eta)$ over $K:=\mathbb{Q}$. When Dedekind constructed this example [10] it was the first example of a non-monogenic extension of number rings. Indeed two generators are necessary to generate $\mathbb{Z}_L/\mathbb{Z}_K$: take η^2 and $\frac{\eta+\eta^2}{2}$, for example. In fact, $\{1, \frac{\eta+\eta^2}{2}, \eta^2\}$ is a $\mathbb{Z}$-basis for $\mathbb{Z}_K$. The matrix of coefficients with respect to the basis $\{1, \frac{\eta+\eta^2}{2}, \eta^2\}$ is

$$\begin{bmatrix} 1 & a & a^2 + 6b^2 + 16bc + 8c^2 \\ 0 & b & 2ab + 7b^2 + 24bc + 20c^2 \\ 0 & c & -2b^2 + 2ac - 8bc - 7c^2 \end{bmatrix}.$$

Taking its determinant, the index form associated to this basis is

$$-2b^3 - 15b^2c - 31bc^2 - 20c^3.$$

Were the extension monogenic, we would be able to find $a, b, c \in \mathbb{Z}$ so that the index form above is equal to ± 1.

In fact, $\mathbb{Z}_{\mathbb{Q}(\eta)}/\mathbb{Z}$ is not even locally monogenic. By Lemma 2.6, we may check by reducing at primes. Over the prime 2 the index form reduces to

$$b^2c + bc^2,$$

and iterating through the four possible values of $(b, c) \in (\mathbb{Z}/2\mathbb{Z})^2$ shows that the index form always to reduces to 0. That is, 2 is a common index divisor.

Dedekind showed that $\mathbb{Z}_{\mathbb{Q}(\eta)}/\mathbb{Z}$ is non-monogenic, not by using an index form, but by deriving a contradiction from the $\mathbb{Z}_L$-factorization of the ideal 2, which splits into three primes. In our terms, $\operatorname{Spec}\mathbb{Z}_{\mathbb{Q}(\eta)} \to \operatorname{Spec}\mathbb{Z}$ has three points over $\operatorname{Spec}\mathbb{F}_2$, all with residue field $\mathbb{F}_2$. Therefore, condition (2) of Theorem 1.10 for monogenicity at the prime (2) fails, so $S' \to S$ is not monogenic.

With base extension, one can eventually resolve the obstructions presented by common index divisors. The following example illustrates a non-maximal order where we have a slightly different obstruction to monogenicity.

Example 5.2 (An order that fails to be monogenic over geometric points)
Consider the extension $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$ of $\mathbb{Z}$. (This is not the maximal order of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.) We recall from [4, Example 4.13] that the index form with respect to the basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is

$$= -4(2b^2 - 3c^2)(b^2 - 3d^2)(c^2 - 2d^2).$$

By Proposition 2.10, $S' \to S$ fails to be monogenic, even over geometric points, since the index form reduces to 0 in the fiber over 2. In terms of Theorem 1.9, $S' \to S$ fails to be monogenic since the fiber over 2 consists of a single point with a two dimensional tangent space.

We can contrast the above examples with the following example where the obstruction to monogenicity is global as opposed to local.

Example 5.3 (A Zariski-locally monogenic, but not twisted-monogenic extension) Here we take a closer look at one member of the family in Example 2.8. Let $K = \mathbb{Q}$, $L = K(\sqrt[3]{5^2 \cdot 7})$. The ring of integers $\mathbb{Z}_L = \mathbb{Z}[\sqrt[3]{5^2 \cdot 7}, \sqrt[3]{5 \cdot 7^2}]$ is not monogenic over $\mathbb{Z}$. Let $\alpha = \sqrt[3]{5^2 \cdot 7}$, $\beta = \sqrt[3]{5 \cdot 7^2}$. We recall from [4, Example 4.14] that $\{1, \alpha, \beta\}$ is a $\mathbb{Z}$-basis for $\mathbb{Z}_L$ and the associated index form is $5b^3 - 7c^3$. Thus, for a given choice of $a, b, c \in \mathbb{Z}$, the primes which divide the value $5b^3 - 7c^3$ are precisely the primes at which $a + b\alpha + c\beta$ will fail to generate the extension.

The values obtained by this index form are $\{0, \pm 5\}$ modulo 7. Since 5 is a unit in $\mathbb{Z}/7\mathbb{Z}$, we do have local monogenerators over $D(7)$. Similarly, we have local monogenerators over $D(5)$. Together, $D(5)$ and $D(7)$ form an open cover, and we see that this extension is Zariski-locally monogenic. However, as we can see by reducing modulo 7, the index form cannot be equal to ± 1. Therefore there are no global monogenerators and $\mathbb{Z}_L/\mathbb{Z}$ is not monogenic: in the language of [2], $\mathbb{Z}_L/\mathbb{Z}$ has a local obstruction to monogenicity, despite being locally monogenic.

This is not a $\mathbb{G}_m$-twisted monogenic extension by Theorem 4.19, because $h(\mathbb{Z}) = 1$ and this extension is not globally monogenic. See Example 4.21 for a properly $\mathbb{G}_m$-twisted monogenic extension and a comparison to the example presented here.

5.2 Maps of curves
One benefit of our more geometric notion of monogenicity is it allows us readily ask questions about monogenicity in classical geometric situations with the same language that we use in the arithmetic context. Our next examples concern the case that $S' \to S$ is a finite map of algebraic curves, which is essentially never monogenic. On the other hand,

we find explicit examples of $\mathbb{G}_m$-twisted monogenic $S' \to S$. Theorem 4.15 constrains the possible line bundles that we may use to show $\mathbb{G}_m$-twisted monogenicity. We make this precise in the lemma below.

Lemma 5.4 *Let $\pi : C \to D$ be a finite map of smooth projective curves of degree n and let g denote the genus.*

(1) *π is only monogenic if it is the identity map;*
(2) *If π is $\mathbb{G}_m$-twisted monogenic, then $1 - g(C) - n(1 - g(D))$ is divisible by $\frac{1}{2}n(n-1)$ in $\mathbb{Z}$. Moreover, if π factors through a closed embedding into a line bundle E with sheaf of sections $\mathcal{E}$, then*

$$\deg(\mathcal{E}) = -\frac{1 - g(C) - n(1 - g(D))}{\frac{1}{2}n(n-1)}.$$

Proof To see (1), note that a map $f : C \to \mathbb{A}_D^1$ is determined by a global section of $\mathcal{O}_C$. Since C is a proper variety, the global sections of $\mathcal{O}_C$ are constant functions. It follows that a map $f : C \to \mathbb{A}_D^1$ is constant on fibers of π. Therefore f cannot be an immersion unless π has degree 1, i.e., is the identity.

Suppose $\pi : C \to D$ is $\mathbb{G}_m$-twisted monogenic with an embedding into a line bundle E. By [38, 0AYQ] and Riemann-Roch,

$$\deg(\det(\pi_* \mathcal{O}_C)) = 1 - g(C) - n(1 - g(D)).$$

By Theorem 4.15,

$$\det(\pi_* \mathcal{O}_{S'}) \simeq \mathcal{E}^{-\frac{n(n-1)}{2}}$$

where $\mathcal{E}$ is the sheaf of sections of E. Taking degrees of both sides,

$$1 - g(C) - n(1 - g(D)) = -\deg(\mathcal{E}) \cdot \frac{n(n-1)}{2}.$$

This shows (2). $\square$

First, we will investigate one of the most basic families of maps of curves.

Example 5.5 (Maps $\mathbb{P}^1 \to \mathbb{P}^1$) Let k be an algebraically closed field and let $\pi : \mathbb{P}_k^1 \to \mathbb{P}_k^1$ be a finite map of degree n. If $n = 1$, then π is trivially monogenic. When $n = 2$, Lemma 5.4 tells us that π cannot be monogenic, while Lemma 4.18 tells us that π is Aff^1-twisted monogenic. Lemma 5.4 tells us that for degrees $n > 2$ the map π is neither monogenic nor $\mathbb{G}_m$-twisted monogenic, although Theorems 2.1 and 1.10 tell us that π is Zariski-locally monogenic.

Working with $\mathbb{Z}$ instead of an algebraically closed field, consider the map $\pi : S' = \mathbb{P}_{\mathbb{Z}}^1 \to S = \mathbb{P}_{\mathbb{Z}}^1$ given by $[a : b] \mapsto [a^2 : b^2]$. We will show by direct computation that this map is $\mathbb{G}_m$-twisted monogenic. Write $U = \text{Spec}\,\mathbb{Z}[x]$ and $V = \text{Spec}\,\mathbb{Z}[y]$ for the standard affine charts of the target $\mathbb{P}^1$. The map π is then given on charts by

$$\mathbb{Z}[x] \to \mathbb{Z}[a]$$
$$x \mapsto a^2$$

and

$$\mathbb{Z}[y] \rightarrow \mathbb{Z}[b]$$
$$y \mapsto b^2.$$

Let us compute $m_{1,S'/S}$. Over U, $\pi_* \mathcal{O}_{\mathbb{P}^1}$ has $\mathbb{Z}[x]$-basis $\{1, a\}$. Let c_1, c_2 be the coordinates of $\mathcal{R}|_U = \mathbb{A}^2$, with universal map

$$\mathbb{Z}[c_1, c_2, t] \rightarrow \mathbb{Z}[c_1, c_2, a], \qquad t \mapsto c_1 + c_2 a.$$

The index form associated to this basis is

$$i(c_1, c_2) = c_2.$$

Similarly, $\pi_* \mathcal{O}_{\mathbb{P}^1}$ has $\mathbb{Z}[y]$-basis $\{1, b\}$, $\mathcal{R}|_V$ analogous coordinates d_1, d_2, and the index form associated to this basis is

$$i(d_1, d_2) = d_2.$$

An element of $\mathbb{Z}[x]$ (resp. $\mathbb{Z}[y]$) is a unit if and only if it is ± 1, so

$$m_{S'/S}(U) = \{c_1 \pm a \mid c_1 \in \mathbb{Z}[x]\}$$
$$m_{S'/S}(V) = \{d_1 \pm b \mid d_1 \in \mathbb{Z}[y]\}.$$

We can see directly that π is not monogenic: the condition that a monogenerator $c_1 \pm a$ on U glue with a monogenerator $d_1 \pm b$ on V is that

$$(c_1 \pm a)|_{U \cap V} = (d_1 \pm b)|_{U \cap V}.$$

But this is impossible to satisfy since $a|_{U \cap V} = b|_{U \cap V}^{-1}$.

Lemma 5.4 tells us that if $S' \rightarrow S$ is twisted monogenic, the line bundle into which S' embeds must have degree 1. Let us therefore attempt to embed S' into the line bundle with sheaf of sections $\mathcal{O}_{\mathbb{P}^1}(1)$. The sheaf $\mathcal{O}_{\mathbb{P}^1}(1)$ restricts to the trivial line bundle on both U and V, and a section $f \in \mathcal{O}_U$ glues to a section $g \in \mathcal{O}_V$ if

$$y \cdot f|_{U \cap V} = g|_{U \cap V}.$$

Embedding S' into this line bundle is therefore equivalent to finding a monogenerator $c_1 \pm a$ on U, and a monogenerator $d_1 \pm b$ on V such that

$$y\big((c_1 \pm a)|_{U \cap V}\big) = (d_1 \pm b)|_{U \cap V}.$$

Bearing in mind that $y = b^2 = a^{-2}$ on $U \cap V$, we find a solution by taking positive signs, $c_1 = 0$, and $d_1 = 0$. Therefore $\pi : \mathbb{P}^1_{\mathbb{Z}} \rightarrow \mathbb{P}^1_{\mathbb{Z}}$ is twisted monogenic.

Lemma 5.4 tells us that we must pass to higher genus to find a $\mathbb{G}_m$-twisted monogenic cover of $\mathbb{P}^1$ of degree greater than 2. Here is an example where the source is an elliptic curve.

Example 5.6 (Twisted monogenic cover of degree 3) Let E be the Fermat elliptic curve $V(x^3 + y^3 - z^3) \subset \mathbb{P}^2_{\mathbb{Z}}$. Consider the projection from $[0 : 0 : 1]$, i.e., the map $\pi : E \rightarrow \mathbb{P}^1$ defined by $[x : y : z] \mapsto [x : y]$. Write $U = \operatorname{Spec} \mathbb{Z}[x]$ and $V = \operatorname{Spec} \mathbb{Z}[y]$ for the standard affine charts of $\mathbb{P}^1$. The map is given on charts by $\mathbb{Z}[x] \rightarrow \mathbb{Z}[x, z]/(x^3 + 1 - z^3)$ and

$\mathbb{Z}[y] \to \mathbb{Z}[y, yz]/(1 + y^3 - (yz)^3)$. The gluing on overlaps is given by $x \mapsto y^{-1}$ on $\mathbb{P}^1$ and by $x \mapsto y^{-1}, z \mapsto z$ on E.

We now compute $\mathcal{M}_{E/\mathbb{P}^1}$. Note that over U, $\mathcal{O}_E$ has the $\mathbb{Z}[x]$-basis $1, z, z^2$. The index form associated to $1, z, z^2$ is

$$i(c_1, c_2, c_3) = c_2^3 - c_3^3(x^3 + 1).$$

Over V, $\mathcal{O}_E$ has the $\mathbb{Z}[x]$-basis $1, yz, y^2z^2$. The index form associated to this basis is

$$i(d_1, d_2, d_3) = d_2^3 - d_3^3(y^3 + 1).$$

An element of $\mathbb{Z}[x]$ or $\mathbb{Z}[y]$ is a unit if and only if it is ± 1. This implies that

$$\mathcal{M}_{S'/S}(U) = \{c_1 \pm z \mid c_1 \in \mathbb{Z}[x]\}$$
$$\mathcal{M}_{S'/S}(V) = \{d_1 \pm yz \mid d_1 \in \mathbb{Z}[y]\}.$$

We see that there are no global sections of $\mathcal{M}_{S'/S}$, since coefficients of z cannot match on overlaps.

However, if we twist so that we are considering embeddings of E into $\mathcal{O}_{\mathbb{P}^1}(1)$, then the condition for a monogenerator $c_1 \pm z$ on U to glue with a monogenerator $d_1 \pm yz$ on V is that

$$y\big((c_1 \pm z)|_{U \cap V}\big) = (d_1 \pm yz)|_{U \cap V}.$$

This is satisfied, for example by taking the positive sign for both generators and $c_1 = d_1 = 0$. Therefore $E \to \mathbb{P}^1$ is twisted monogenic with class $1 \in \mathrm{Pic}(\mathbb{P}^1_{\mathbb{Z}})$.

Data availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Author details
[1]Universiteit Leiden, Leiden, The Netherlands, [2]Tufts University, Medford, USA, [3]California State University San Marcos, San Marcos, USA.

Declarations

Conflict of interest
All authors declare no conflicts of interest.

References
1. Abramovich, D., Chen, Q., Marcus, S., Wise, J.: Boundedness of the space of stable logarithmic maps. J. Eur. Math. Soc. **19**, 2783 (2014)

2. Alpöge, L., Bhargava, M., Shnidman, A.: A positive proportion of cubic fields are not monogenic yet have no local obstruction to being so. (2020)
3. Alpöge, L., Bhargava, M., Shnidman, A.: A positive proportion of quartic fields are not monogenic yet have no local obstruction to being so. (2021)
4. Arpin, S., Bozlee, S., Herr, L., Smith, H.: The scheme of monogenic generators I: representability. Res. Number Theory **9**(1), 14 (2023)
5. Artin, M.: Algebra. Pearson Prentice Hall, Hoboken (2011)
6. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**, 235–265 (1997)
7. Breen, L.: Notes on 1- and 2-gerbes. arXiv Mathematics e-prints. (2006). arXiv:math/0611317
8. Cobbe, A.: Steinitz classes of tamely ramified Galois extensions of algebraic number fields. J. Numb. Theory **130**, 1129–1154 (2010)
9. Costello, K.: Higher genus Gromov–Witten invariants as genus zero invariants of symmetric products. Ann. Math. (2) **164**, 561–601 (2006)
10. Dedekind, R.: Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. Gött. Abhandlungen, pp. 1–23 (1878)
11. Duchamp, T., Hain, R.: Primitive elements in rings of holomorphic functions. Journal für die reine und angewandte Mathematik **346**, 199–220 (1984)
12. Dupuy, T.: Automorphisms of the affine line over nonreduced rings. (2013). arXiv:1311.0973
13. Ellenberg, J.S., Satriano, M., Zureick-Brown, D.: Heights on stacks and a generalized Batyrev–Manin–Malle conjecture. (2021). arXiv:2106.11340
14. Evertse, J.-H., Győry, K.: Discriminant Equations in Diophantine Number Theory. New Mathematical Monographs, vol. 32. Cambridge University Press, Cambridge (2017)
15. Furusho, H.: Galois action on knots I: action of the absolute Galois group. Quantum Topol. **8**, 295 (2012)
16. Gorin, E.A., Lin, V.J.: Algebraic equations with continuous coefficients and some problems of the algebraic theory of braids. Math. USSR-Sbornik **7**, 569–596 (1969)
17. Hansen, V.L.: Polynomial covering spaces and homomorphisms into the braid groups. Pac. J. Math. **81**, 399–410 (1979)
18. Hansen, V.L.: Coverings defined by weierstrass polynomials. J. Reine Angew. Math. **314**, 29–39 (1980)
19. Hensel, K.: Arithmetische Untersuchungen über die gemeinsamen ausserwesentlichen Discriminantentheiler einer Gattung. J. Reine Angew. Math. **113**, 128–160 (1894)
20. Herr, L.: If the normalization is affine, is it affine? (If quasiaffine). MathOverflow. version. (2020)
21. Herr, L.: When is a twisted form coming from a Torsor trivial? MathOverflow. version. (2020)
22. Herr, L., Wise, J.: Costello's pushforward formula: errata and generalization. (2021). arXiv:2103.10348
23. Ji, L., Li, S., McFaddin, P., Moore, D.D., Stevenson, M.: Weil restriction for schemes and beyond. (2017)
24. Kollár, J.: Severi–Brauer varieties; a geometric treatment. (2016). arXiv:1606.04368
25. Lønsted, K.: On the embedding of coverings into 1-dimensional bundles. J. Reine Angew. Math. **317**, 88–101 (1980)
26. Mann, H.B.: On integral bases. Proc. Am. Math. Soc. **9**, 167–172 (1958)
27. Matsumura, H., Reid, M., Bollobas, B.: Commutative Ring Theory, Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge (1989)
28. McCulloh, L.R.: Cyclic extensions without relative integral bases. Proc. Am. Math. Soc. **17**, 1191–1194 (1966)
29. Narkiewicz, W.: Elementary and Analytic Theory of Algebraic Numbers, Springer Monographs in Mathematics. Springer, Berlin (2004)
30. Neukirch, J.: Algebraic number theory, vol. 322 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin: Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G, Harder (1999)
31. Olsson, M.: Algebraic Spaces and Stacks. American Mathematical Society Colloquium Publications, vol. 62. American Mathematical Society, Providence (2016)
32. Pleasants, P.A.B.: The number of generators of the integers of a number field. Mathematika **21**, 160–167 (1974)
33. Poonen, B.: The moduli space of commutative algebras of finite rank. J. Eur. Math. Soc. **10**, 817 (2006)
34. Poonen, B.: Rational Points on Varieties. American Mathematical Society, Providence (2017)
35. Sernesi, E.: Deformations of Algebraic Schemes. Grundlehren der mathematischen Wissenschaften. Springer, Berlin (2006)
36. Serre, J.-P.: Local Fields, vol. 67 of Graduate Texts in Mathematics. Springer, New York (1979). Translated from the French by Marvin Jay Greenberg
37. T. LMFDB Collaboration: The L-functions and modular forms database. (2021). http://www.lmfdb.org
38. T. Stacks Project Authors: *Stacks Project*. (2020). http://stacks.math.columbia.edu
39. The Sage Developers: *SageMath, the Sage Mathematics Software System (Version 8.7)*. (2019). https://www.sagemath.org
40. Vojta, P.: Jets via Hasse–Schmidt Derivations. (2004). arXiv:math/0407113
41. Westerland, C.: Configuration spaces in topology and geometry. Austral. Math. Soc. Gaz. **38**, 279–283 (2011)

Publisher's Note