Algebra & Number Theory

Volume 19
2025
No. 5

msp

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2025 is US $565/year for the electronic version, and $820/year (+$70, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

ALGEBRA AND NUMBER THEORY 19:5 (2025)
https://doi.org/10.2140/ant.2025.19.835

Presentations of Galois groups of maximal extensions with restricted ramification

Yuan Liu

Motivated by the work of Lubotzky, we use Galois cohomology to study the difference between the number of generators and the minimal number of relations in a presentation of $G_S(k)$, the Galois group of the maximal extension of a global field k that is unramified outside a finite set S of places, as k varies among a certain family of extensions of a fixed global field Q. We define a group $\text{Б}_S(k, A)$, for each finite simple $G_S(k)$-module A, to generalize the work of Koch and Shafarevich on the pro-ℓ completion of $G_S(k)$. We prove that $G_S(k)$ always admits a balanced presentation when it is finitely generated. In the setting of the nonabelian Cohen–Lenstra heuristics, we prove that the unramified Galois groups studied by the Liu–Wood–Zureick-Brown conjecture always admit a balanced presentation in the form of the random group in the conjecture.

1. Introduction

For a global field k and a set S of primes of k, we denote by $G_S(k)$ the Galois group of the maximal extension of k that is unramified outside S. Determining whether $G_\varnothing(k)$ is finitely generated and finitely presented is a long-existing open question. It is well known by class field theory that the abelianization of $G_\varnothing(k)$ is finitely presented and, in particular, is finite when k is a number field. Golod and Shafarevich [1964] constructed the first infinite ℓ-class tower group of a number field, where the ℓ-class tower group of k is the pro-ℓ completion of $G_\varnothing(k)$ for a prime number ℓ. The minimal numbers of generators and relations, which are called the generator rank and relator rank, in presentations of a pro-ℓ group is determined by its group cohomology with coefficient $\mathbb{F}_\ell$. Using this idea, Koch [2002] employed Galois cohomology to give an exact formula for the generator rank and estimate the relator rank of the pro-ℓ completion of $G_S(k)$ when S is finite and $\ell \neq \operatorname{char}(k)$; and in particular, in such cases, the pro-ℓ completion of $G_S(k)$ is always finitely presented.

Recently the development on the nonabelian Cohen–Lenstra program pushes us to study canonical quotients of $G_\varnothing(k)$ beyond the pro-ℓ completion. Let Γ be a finite group, Q the global field $\mathbb{Q}$ or $\mathbb{F}_q(t)$, and $\mu(Q)$ the group of roots of unity of Q. For a Galois extension k/Q with $\operatorname{Gal}(k/Q) \simeq \Gamma$, define $k^\#$ to be the maximal unramified extension of k, that is split completely at places of k over ∞ and of order relatively prime to $|\mu(Q)||\Gamma|$ and $\operatorname{char}(Q)$ (if nonzero). Wood, Zureick-Brown and the author [Liu et al. 2024] constructed random group models to make conjectures on the distributions for some

MSC2020: 11R29, 11R32, 11R34.
Keywords: presentation of Galois groups, class groups, nonabelian Cohen–Lenstra heuristics.

families of canonical quotients $\mathrm{Gal}(k^{\#}/k)$ of $G_{\varnothing}(k)$ as k varies among all Γ-extensions of Q split completely at ∞. Because $\mathrm{Gal}(k^{\#}/k)$ has (supernatural) order prime to $|\Gamma|$, a homomorphic split of $\mathrm{Gal}(k^{\#}/Q) \twoheadrightarrow \mathrm{Gal}(k/Q)$ defines by conjugation a continuous Γ action on $\mathrm{Gal}(k^{\#}/k)$; and this action is *admissible* (see Definition 4.1). The set of all isomorphism classes of all admissible profinite Γ-groups is closed under taking Γ-equivariant quotients, and we can construct *the free admissible profinite* Γ*-group* $\mathcal{F}_n(\Gamma)$ *on n generators* (see Section 4 for its definition). For a profinite Γ-group G and a finite set $\mathcal{C}$ of isomorphism classes of finite Γ-groups, let $G^{\mathcal{C}}$ denote the *pro-$\mathcal{C}$ completion* of G with respect to $\mathcal{C}$ (the definition of pro-$\mathcal{C}$ completions is given in Section 5 and it is different from the one that is commonly used). The work [Liu et al. 2024] uses quotients of $\mathcal{F}_n(\Gamma)$ as $n \to \infty$ to construct a random group model; this model together with the conjectures implies a surprising phenomenon of the structure of $\mathrm{Gal}(k^{\#}/k)$ that was not known before: for any finite set $\mathcal{C}$ of finite Γ-groups, the following occur with probability 1.

(1) The pro-$\mathcal{C}$ completion $\mathrm{Gal}(k^{\#}/k)^{\mathcal{C}}$ is a finite group.

(2) There exists a finite integer n_0 depending on $\mathcal{C}$, Γ and k, such that for every $n \geq n_0$, $\mathrm{Gal}(k^{\#}/k)^{\mathcal{C}}$ can be presented as the quotient of $\mathcal{F}_n(\Gamma)^{\mathcal{C}}$ by $[r^{-1}\gamma(r)]_{r\in X,\,\gamma\in\Gamma}$ for some subset X of $\mathcal{F}_n(\Gamma)^{\mathcal{C}}$ of cardinality $n+1$. Here, the symbol $[r^{-1}\gamma(r)]_{r\in X,\,\gamma\in\Gamma}$ denotes the Γ-closed normal subgroup of $\mathcal{F}_n(\Gamma)^{\mathcal{C}}$ generated by $r^{-1}\gamma(r)$ for all $r \in X$ and $\gamma \in \Gamma$.

The statement in (2) implies that the deficiency (i.e., the difference between the minimal number of generators and the minimal number of relations) of $\mathrm{Gal}(k^{\#}/k)^{\mathcal{C}}$ has an upper bound depending only on the order of Γ. In this paper, we prove that both (1) and (2) hold for all Γ-extensions k/Q split completely above ∞, which strongly supports that the random group model in [Liu et al. 2024] is the right object to study.

Theorem 1.1. *Let Γ be a nontrivial finite group and Q be either $\mathbb{Q}$ or $\mathbb{F}_q(t)$ with q relatively prime to $|\Gamma|$. Let $\mathcal{C}$ be a finite set of isomorphism classes of finite Γ-groups all of whose orders are prime to $|\mu(Q)||\Gamma|$ and* $\mathrm{char}(Q)$ *(if nonzero). Then for a Galois extension k/Q with Galois group Γ that is split completely over ∞, we have the following isomorphism of Γ-groups* (Γ *acts on the left-hand side via* $\Gamma \simeq \mathrm{Gal}(k/Q)$):

$$\mathrm{Gal}(k^{\#}/k)^{\mathcal{C}} \simeq \mathcal{F}_n(\Gamma)^{\mathcal{C}}/[r^{-1}\gamma(r)]_{r\in X,\gamma\in\Gamma} \tag{1-1}$$

for some positive integer n and some set X consisting of $n+1$ elements of $\mathcal{F}_n(\Gamma)^{\mathcal{C}}$.

Let $G_{\varnothing,\infty}(k)$ denote the Galois group of the maximal unramified extension of k that is completely split at every place above ∞, and note that with the assumptions in Theorem 1.1 one has $\mathrm{Gal}(k^{\#}/k)^{\mathcal{C}} = G_{\varnothing,\infty}(k)^{\mathcal{C}}$. The method we develop in this paper in fact works for $G_S(k)^{\mathcal{C}}$ for any finite set S of primes of k and any global base field Q, so it can be used to study the presentation of Galois groups with restricted ramification. In the case that k is a function field and $\Gamma = 1$ (so $k = Q$), building on the theorem of Lubotzky [2001], Shusterman [2022] showed that $G_{\varnothing}(k)$ admits a finite presentation in which the number of relations is exactly the same as the number of generators (such a presentation is called a balanced presentation). Note that, in [Shusterman 2022], the fact that $G_{\varnothing}(k)$ is finitely generated follows by Grothendieck's result on the geometric fundamental group of a smooth projective curve defined over a finite field, but when k is a number field, whether $G_{\varnothing}(k)$ is finitely generated or not is unknown. We prove an analogous result regarding the number field case.

Theorem 1.2. *Let k be a number field and S a finite set of places of k. If $G_S(k)$ is topologically generated by n elements, then it admits a finite presentation on n generators and $[k:\mathbb{Q}]+n$ relations.*

We also apply our methods to the situations that are not considered in Theorem 1.1. We study the presentation of the pro-ℓ completion of $G_{\varnothing,\infty}(k)$ for a Galois Γ-extension k/Q in two exceptional cases:

(i) Q is a number field not containing the ℓ-th roots of unity and we do not make any assumptions on the ramification of ∞ in k (Section 11.1).

(ii) Q is a global field containing the ℓ-th roots of unity (Section 11.2).

When considering the ℓ-parts of class groups, it has been known for a long time that the Cohen–Lenstra heuristics need to be corrected in these two cases (see [Cohen and Martinet 1987; Malle 2010]). In each of these two cases, we use our method to compute an upper bound for the deficiency of $G_{\varnothing,\infty}(k)$ at the pro-ℓ level, and then show why the Liu–Wood–Zureick-Brown conjecture doesn't work in these two exceptional cases. This computation of deficiencies also provides insights of how the random group model should be modified in these two cases.

1.1. ***Method of the proof.*** The bulk of this paper is devoted to establishing the techniques for proving Theorem 1.1. Motivated by [Lubotzky 2001], we first translate the question to understanding the Galois cohomology groups. In Section 3, we construct the *free profinite Γ-group $F_n(\Gamma)$ on n generators*, and, for a finitely generated profinite Γ-group G, we study the minimal number of relations of a presentation defined by a Γ-equivariant surjection $\pi : F_n(\Gamma) \twoheadrightarrow G$. The minimal number of relations is closely related to the multiplicities of the finite irreducible $G \rtimes \Gamma$-modules appearing as quotients of $\ker(\pi)$ (Definition 3.1). In Lemma 3.2, we show that for a finite simple $\mathbb{F}_\ell[G \rtimes \Gamma]$-module A with $\ell \nmid |\Gamma|$, the multiplicity of A can be computed by a formula involving $\dim_{\mathbb{F}_\ell} H^2(G \rtimes \Gamma, A) - \dim_{\mathbb{F}_\ell} H^1(G \rtimes \Gamma, A)$. So when restricted to the category of profinite Γ-groups whose order is prime to $|\Gamma|$, by using these multiplicities, we obtain formulas for the minimal number of relations of the presentation $F'_n(\Gamma) \twoheadrightarrow G'$, where $F'_n(\Gamma)$ and G' are the maximal pro-prime-to-$|\Gamma|$ quotients of $F_n(\Gamma)$ and G respectively (Propositions 3.4 and 3.7). In particular, the formulas provide an upper bound for the minimal number of relations of this presentation using $\dim_{\mathbb{F}_\ell} H^2(G, A)^\Gamma - \dim_{\mathbb{F}_\ell} H^1(G, A)^\Gamma$, where Γ acts on the cohomology groups by conjugation. These upper bound formulas set up the strategy of the proof of Theorem 1.1. Building upon it, we explore the multiplicities of *admissible presentations* $\mathcal{F}_n(\Gamma) \twoheadrightarrow G$ in Section 4 and the multiplicities of *pro-$\mathcal{C}$ presentations* in Section 5, where we obtain formulas that will be directly applied to the proof of Theorem 1.1. Then in Section 6, we define *the height of a group* and show in Proposition 6.3 that there is an upper bound for the heights of pro-$\mathcal{C}$ groups (not necessarily finitely generated) when $\mathcal{C}$ is a finite set. Then Theorem 6.4 proves the finiteness of $G_S(k)^{\mathcal{C}}$ when S is a finite set of primes of k and $\mathcal{C}$ is a finite set of finite groups, which confirms the phenomenon (1).

Therefore, in order to prove Theorem 1.1, we need to deal with the Galois cohomology groups. In a more general setting, assuming that Q is an arbitrary global field, that k/Q is a Galois extension with $\mathrm{Gal}(k/Q) \simeq \Gamma$, and that S is a finite set of primes of k, we want to understand

$$\delta_{k/Q,S}(A) := \dim_{\mathbb{F}_\ell} H^2(G_S(k), A)^\Gamma - \dim_{\mathbb{F}_\ell} H^1(G_S(k), A)^\Gamma \tag{1-2}$$

for all prime integers ℓ relatively prime to $|\Gamma|$ and $\mathrm{char}(Q)$, and all finite simple $\mathbb{F}_\ell[\mathrm{Gal}(k_S/Q)]$-modules A. In (1-2), the set S needs to be k/Q-closed to ensure that k_S/Q is Galois (see the definition of the *k/Q-closed* sets in Section 2), and the Γ action on the cohomology groups is defined via the conjugation by $\mathrm{Gal}(k/Q)$. In Section 7, we prove a generalized version of the global Euler–Poincaré characteristic formula (Theorem 7.1), from which we can compute $\delta_{k/Q,S}$ when S is nonempty and contains the primes above ∞ and ℓ if Q is a number field. The proof basically follows the original proof of the global Euler–Poincaré characteristic formula, but taking the Γ actions into account creates many technical difficulties.

In the work of Koch, when dealing with the case that $A = \mathbb{F}_\ell$ and S does not satisfy the assumptions in Theorem 7.1, the abelian group $\text{Б}_S(k)$ plays an important role in the computation of $\dim_{\mathbb{F}_\ell} H^i(G_S(k), \mathbb{F}_\ell)$ for $i = 1, 2$, and is defined to be the Pontryagin dual of the Kummer group

$$V_S(k) = \ker\Big(k^\times/k^{\times\ell} \to \prod_{\mathfrak{p}\in S} k_\mathfrak{p}^\times/k_\mathfrak{p}^{\times\ell} \times \prod_{\mathfrak{p}\notin S} k_\mathfrak{p}^\times/U_\mathfrak{p} k_\mathfrak{p}^{\times\ell}\Big),$$

where $k_\mathfrak{p}$ is the completion of k at $\mathfrak{p}$ and $U_\mathfrak{p}$ is the group of units of $k_\mathfrak{p}$. In Definition 8.1, we define a group $\text{Б}_S(k, A)$ in a cohomological way as

$$\mathrm{coker}\Big(\prod_{\mathfrak{p}\in S} H^1(k_\mathfrak{p}, A) \times \prod_{\mathfrak{p}\notin S} H^1_{nr}(k_\mathfrak{p}, A) \to H^1(k, A')^\vee\Big),$$

in order to generalize Koch's work to compute $\delta_{k/Q,S}(A)$ by replacing the trivial module $\mathbb{F}_\ell$ with an arbitrary finite simple module A. The definition of $\text{Б}_S(k, A)$ agrees with that of $\text{Б}_S(k)$ when $A = \mathbb{F}_\ell$ (Proposition 8.3). However, Koch's argument does not directly apply to $\text{Б}_S(k, A)$, because it uses the Hasse principle for $\mathbb{F}_\ell$ but the Hasse principle for arbitrary global fields and arbitrary Galois modules has not been proven (the Hasse principle holds for k and A if the Shafarevich group $\text{Ш}^1(k, A)$ is trivial). In Section 8, we modify Koch's work to overcome this obstacle, and show that most properties of $\text{Б}_S(k)$ also hold for $\text{Б}_S(k, A)$. In particular, one example, clearly showing that the failure of the Hasse principle makes a difference, is that there is a natural embedding $\text{Ш}^2_S(k, A) \hookrightarrow \text{Б}_S(k, A)$ for $A = \mathbb{F}_\ell$ but not for arbitrary A (Proposition 8.5 and Remark 8.6). In Section 9, we explicitly compute $\delta_{k/Q,S}(A)$ for all S by applying the results from Sections 7 and 8, and then we prove Theorem 1.2. In Section 10, we give the proof of Theorem 1.1. Finally, in Section 11, we apply our methods to the exceptional cases (i) and (ii) of Theorem 1.1. The proof of Theorem 1.1 uses results from Section 3 to Section 9; and the proof of Theorem 1.2 uses results from Sections 3, 7, 8, and 9.

1.2. ***Previous works.*** For an odd prime ℓ, the Cohen–Lenstra heuristics [1984] give predictions of the distribution of ℓ-primary parts of the class groups $\mathrm{Cl}(k)$ as k varies over quadratic number fields. Friedman and Washington [1989] formulated an analogous conjecture for global function fields. The probability measure used for the conjectural distributions in the Cohen–Lenstra heuristics matches the one defined by the random abelian group

$$\lim_{n\to\infty} \mathbb{Z}_\ell^{\oplus n}/(n+u \text{ random relations}), \tag{1-3}$$

where the random relations are taken with respect to the Haar measure, and u is chosen to be 0 and 1 respectively when k varies among imaginary quadratic fields and real quadratic fields. Ellenberg and Venkatesh [2010] theoretically explained the random group model (1-3) and the value of u, by viewing $\mathrm{Cl}(k)$ as the cokernel of the map sending the S-units of k to the group of fractional ideals of k generated by S with S running along an ascending sequence of finite sets of primes of k. Boston, Bush and Hajir [Boston et al. 2017; 2021] extended the Cohen–Lenstra heuristics to a nonabelian setting considering the distribution of ℓ-class tower groups (for odd ℓ). In their work, the probability measure in the heuristics is defined by a random pro-ℓ group generalizing (1-3), and the value of u (which is the deficiency in this setting) is obtained by applying Koch's argument. Notably, the moment versions of the function field analogs of the Cohen–Lenstra heuristics and the Boston–Bush–Hajir heuristics are both proven; see [Ellenberg et al. 2016; Boston and Wood 2017]. In [Liu et al. 2024], we constructed the random Γ-group

$$\lim_{n\to\infty} \mathcal{F}_n(\Gamma)/[r^{-1}\gamma(r)]_{r\in X,\gamma\in\Gamma}, \tag{1-4}$$

where X is a set of $n+u$ random elements of $\mathcal{F}_n(\Gamma)$. We showed that the moment proven in the function field case matches the moment of the probability measure defined by (1-4) exactly when $u=1$. With this evidence, we conjectured that the random group (1-4) gives the distribution of $\mathrm{Gal}(k^{\#}/k)$ in both the function field case and the number field case. Theorem 1.1 explains the theoretical reason behind $u=1$ in the Liu–Wood–Zureick-Brown conjecture.

Regarding the exceptional case (i), Cohen and Martinet [1987] provided a modification for the case that $Q=\mathbb{Q}$ and k/Q varies among imaginary Γ-extensions whose decomposition subgroup at ∞ is a fixed (conjugacy class of) subgroup of Γ. Wang and Wood [2021] proved some results about the probability measures described in the Cohen–Martinet heuristics. From these works, one can see that the decomposition subgroup Γ_∞ at ∞ of $k/\mathbb{Q}$ crucially affects the probability measures. In Lemma 11.1, we explicitly compute the upper bounds of multiplicities in a pro-ℓ admissible Γ-presentation of $G_\varnothing(k)(\ell)$, which shows how the multiplicities are determined by Γ_∞. Then in Corollary 11.2 and Remark 11.3, we prove that, when $k/\mathbb{Q}$ is an imaginary quadratic field, $G_\varnothing(k)(\ell)$ can be achieved by a random group model which defines a probability measure agreeing with the Boston–Bush–Hajir heuristics.

For the exceptional case (ii), when the base field Q contains the ℓ-th roots of unity, we give upper bounds for multiplicities in Lemma 11.4 and Corollary 11.5, which suggests that the distributions of $G_{\varnothing,\infty}(k)(\ell)$ should be different between the function field case and the number field case (Remark 11.6(2)). This difference is not surprising, as Malle [2010] observed that his conjecture regarding the class groups of number fields does not easily match the result for function fields. So the upper bounds obtained in Corollary 11.5 support Malle's observation. The phenomenon related to the presence of the roots of unity has been numerically computed in [Malle 2008; 2010], and the random matrices in this setting and their relation with function field counting has been studied in [Katz and Sarnak 1999; Achter 2006; 2008; Garton 2015; Adam and Malle 2015]. A correction for roots of unity, provided with empirical evidence, is presented in [Wood 2019].

1.3. ***Other applications and further questions.*** We expect that the techniques established in this paper will have many interesting and important applications. For example, the author applies the results in this paper to the following work. In [Liu 2022], the exceptional case (ii) is studied, where the moment conjecture in the number field case is inspired by the computation of $\delta_{k/Q,\varnothing}(A)$ similar to Section 11.2. In [Liu 2024], the abelian group $Б_S(k, A)$ is used to study the embedding problems with restricted ramification, which will be crucial for the forthcoming work on the generalized Cohen–Lenstra–Martinet–Gerth conjectures.

There are many further questions we would like to understand. First, the techniques in this paper work for any finite set S of primes. So we would like to ask whether the random group models (in the abelian, pro-ℓ and pro-$\mathcal{C}$ versions) can also be applied to predict the distributions of $G_S(k)$ as k/Q varies among certain families of Γ-extensions. Secondly, the group $Б_S(k, A)$, which is the generalization of $Б_S(k)$ that we construct in Section 8, has its own interest, because it could be applied to extend our knowledge of $G_S(k)$ from the pro-ℓ completion to the whole group, and moreover, it bounds the Shafarevich group via (see Proposition 8.5)

$$\#Ш^2_S(k, A) \leq \#Б_S(k, A). \tag{1-5}$$

We emphasize here that understanding when $\#Ш^2_\varnothing(k, A) = \#Б_\varnothing(k, A)$ holds can help us determine whether our upper bound of multiplicities is sharp or not (see how the inequality (1-5) is used in the proof of Proposition 9.4). Last but not least, the techniques established in Sections 3, 4 and 5, which use group cohomology to understand the presentation of a Γ-group, are purely group theoretical and independent of the number theory background, so we hope that they could have other interesting applications.

In this paper, we only study the maximal prime-to-$|\Gamma|$ quotient of $G_{\varnothing,\infty}(k)$ for a Galois Γ-extension k/Q, and one can see that this "prime-to-$|\Gamma|$" requirement is necessary in almost every crucial step. We would like to ask if the ideas of this paper can be generalized to the $|\Gamma|$-part of $G_{\varnothing,\infty}(k)$ too.

2. Notation and preliminaries

2.1. ***Profinite groups and modules.*** In this paper, groups are always profinite groups and subgroups are always closed subgroups. For a group G, a *G-group* is a group with a continuous G action. If $x_1, \dots$ are elements of a G-group H, we write $[x_1, \dots]$ for the closed normal G-subgroup of H topologically generated by $x_1, \dots$. If H is a G-group, then we write $H \rtimes G$ for the semidirect product induced by the G action on H, and its multiplication rule is given by $(h_1, g_1)(h_2, g_2) = (h_1 g_1(h_2), g_1 g_2)$ for $h_1, h_2 \in H$ and $g_1, g_2 \in G$. *Morphisms of G-groups* are G-equivariant group homomorphisms. We write $\simeq_G$ to represent isomorphism of G-groups, write Hom_G to represent the set of G-equivariant homomorphisms, and define G-subgroup and G-quotient accordingly. For a G-group H, we say a set of elements *G-generates* H if H is the smallest closed G-subgroup containing this set. We say that H is an *irreducible* G-group if it is a nontrivial G-group and has no proper, nontrivial normal G-subgroups. For a positive integer n, a *pro-n'*

group is a group such that every finite quotient has order relatively prime to n. The *pro-n' completion of G* is the inverse limit of all pro-n' quotients of G. For a prime ℓ, we denote the pro-ℓ and the pro-ℓ' completions of G by $G(\ell)$ and $G(\ell')$ respectively.

For a group G and a commutative ring R, we denote by $R[G]$ the completed R-group ring of G. We use the following notation of G-modules:

$$\begin{aligned}\mathrm{Mod}(G) &= \text{ the category of isomorphism classes of finite } G\text{-modules},\\ \mathrm{Mod}(R[G]) &= \text{ the category of isomorphism classes of finite } R[G]\text{-modules},\\ \mathrm{Mod}_n(G) &= \text{ the category of isomorphism classes of finite } \mathbb{Z}/n\mathbb{Z}[G]\text{-modules}.\end{aligned}$$

For a prime integer ℓ and a finite $\mathbb{F}_\ell[G]$-module A, we define $h_G(A)$ to be the $\mathbb{F}_\ell$-dimension of $\mathrm{Hom}_G(A, A)$. We consider the *Grothendieck group* $K_0'(R[G])$, which is the abelian group generated by the set $\{[A] \mid A \in \mathrm{Mod}(R[G])\}$ and the relations

$$[A]-[B]+[C]=0$$

arising from each exact sequence $0 \to A \to B \to C \to 0$ of modules in $\mathrm{Mod}(R[G])$. For $A, B \in \mathrm{Mod}(R[G])$, the tensor product $A \otimes_R B$ endowed with the diagonal action of G is an element of $\mathrm{Mod}(R[G])$. Then $K_0'(R[G])$ becomes a ring by linear extensions of the product $[A][B] = [A \otimes_R B]$. If H is a subgroup of G, then the action of taking induced modules Ind_G^H defines a map from $K_0'(R[H])$ to $K_0'(R[G])$, which we will also denote by Ind_G^H.

Let ℓ denote a prime integer. If H is a pro-ℓ' subgroup of G, then it follows by the Schur–Zassenhaus theorem that $H^1(H, A) = 0$ for any $A \in \mathrm{Mod}_\ell(G)$, and hence taking the H-invariants is an exact functor on $\mathrm{Mod}_\ell(G)$. Moreover, when G is a pro-ℓ' group, $\mathrm{Mod}_\ell(G)$ is the free abelian group generated by the isomorphism classes of finite simple $\mathbb{F}_\ell[G]$-modules, and elements $[A]$ and $[B]$ of $K_0'(\mathbb{F}_\ell[G])$ are equal if and only if A and B are isomorphic as $\mathbb{F}_\ell[G]$-modules. For an abelian group A, we let $A^\vee$ denote the Pontryagin dual of A.

2.2. ***Galois groups and Galois cohomology.*** For a field k, we write $\bar{k}$ for a fixed choice of separable closure of k, and write G_k for the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$. For a finite G_k-module A, we let $A' = \mathrm{Hom}(A, \bar{k}^\times)$. Let k/Q be a finite Galois extension of global fields. When v is a prime of the field Q, we define $S_v(k)$ to be the set of all primes of k lying above v. Note that the function field $\mathbb{F}_q(t)$ has an infinite place defined by the valuation $|\cdot|_\infty := q^{\deg(\cdot)}$, but this infinite place is nonarchimedean. We define $S_\infty(k)$ to be the set of all archimedean places of k, so it is the empty set if k is a function field. For a number field k, we let $S_\mathbb{R}(k)$ and $S_\mathbb{C}(k)$ denote the set of all real archimedean places and the set of all imaginary archimedean places of k respectively. We let $G_{\varnothing,\infty}(k)$ denote the Galois group of the maximal unramified extension of k that is split completely at every prime above ∞. So if k is a number field, then $G_{\varnothing,\infty}(k)$ is $G_\varnothing(k)$. If k is a function field, then $G_{\varnothing,\infty}(k)$ is the quotient of $G_\varnothing(k)$ by the decomposition subgroups of k at primes above ∞.

Let S be a set of places of k. We let k_S denote the maximal extension of k that is unramified outside S, and denote $\mathrm{Gal}(k_S/k)$ by $G_S(k)$ or just G_S when the choice of k is clear. The set S is called *k/Q-closed* if $S_v(k)$ either is contained in S or intersects emptily with S for any prime v of Q. When S is k/Q-closed, it is not hard to check by Galois theory that k_S is Galois over Q, and hence each element of $\mathrm{Gal}(k/Q)$ defines an outer automorphism of $G_S(k)$. We let

$$\mathbb{N}(S) = \{n \in \mathbb{N} \mid n \in \mathcal{O}_{k,S}^{\times}\},$$

where $\mathcal{O}_{k,S}^{\times}$ is the ring of S-integers of k. Explicitly, if k is a number field, then $\mathbb{N}(S)$ consists of the natural numbers such that $\mathrm{ord}_{\mathfrak{p}}(n) = 0$ for all $\mathfrak{p} \notin S$; and if k is a function field, then $\mathbb{N}(S)$ is the set of all natural numbers prime to $\mathrm{char}(k)$. For a group G, we define

$$\mathrm{Mod}_S(G) = \text{the category of finite } G\text{-modules whose order is in } \mathbb{N}(S).$$

In particular, if Q is a function field, then $\mathrm{Mod}_S(G)$ consists of modules of order prime to $\mathrm{char}(Q)$.

Let k be a global field, and $\mathfrak{p}$ a prime of k. The completion of k at $\mathfrak{p}$ is denoted by $k_{\mathfrak{p}}$, and the absolute Galois group and its inertia subgroup of $k_{\mathfrak{p}}$ are denoted by $\mathcal{G}_{\mathfrak{p}}(k)$ and $\mathcal{T}_{\mathfrak{p}}(k)$ respectively. When the choice of k is clear, we denote $\mathcal{G}_{\mathfrak{p}}(k)$ and $\mathcal{T}_{\mathfrak{p}}(k)$ by $\mathcal{G}_{\mathfrak{p}}$ and $\mathcal{T}_{\mathfrak{p}}$. Let k/Q be a Galois extension of global fields. For a prime v of Q and a prime $\mathfrak{p} \in S_v(k)$, the Galois group of $k_{\mathfrak{p}}/Q_v$, denoted by $\mathrm{Gal}_{\mathfrak{p}}(k/Q)$, is the decomposition subgroup of $\mathrm{Gal}(k/Q)$ at $\mathfrak{p}$. The subgroups $\mathrm{Gal}_{\mathfrak{p}}(k/Q)$ are conjugate to each other in $\mathrm{Gal}(k/Q)$ for all $\mathfrak{p} \in S_v(k)$, so we write $\mathrm{Gal}_v(k/Q)$ for a chosen representative of this conjugacy class. For a group G and an $A \in \mathrm{Mod}(G)$, we write $H^i(G, A)$ and $\widehat{H}^i(G, A)$ for the group cohomology and the Tate cohomology respectively. For a field k, we define $H^i(k, A) := H^i(G_k, A)$ and $\widehat{H}^i(k, A) := \widehat{H}^i(G_k, A)$. Let A be a module in $\mathrm{Mod}(G_Q)$, where G_Q is the absolute Galois group of Q. The Galois group $\mathrm{Gal}(k/Q)$ acts on $H^i(k, A)$ by conjugation. The conjugation map commutes with inflations, restrictions, cup products and connecting homomorphisms in a long exact sequence, and hence it is naturally compatible with spectral sequences and duality theorems used in the paper. For a prime v of Q, we consider the $\mathrm{Gal}(k/Q)$ action on $\bigoplus_{\mathfrak{p}\in S_v(k)} H^i(k_{\mathfrak{p}}, A)$ defined by the action on $\bigoplus_{\mathfrak{p}\in S_v(k)} H^i(k_{\mathfrak{p}}, \mathrm{Res}^{G_Q}_{\mathcal{G}_v(Q)} A)$. In other words, $\mathrm{Gal}(k/Q)$ acts on $\bigoplus_{\mathfrak{p}\in S_v(k)} H^i(k_{\mathfrak{p}}, A)$ by the permutation action on $S_v(k)$ and by the $\mathrm{Gal}_{\mathfrak{p}}(k/Q)$-conjugation on each summand. We similarly define the $\mathrm{Gal}(k/Q)$ action on the product when each of the local summands is $H^i(\mathcal{T}_{\mathfrak{p}}, A)$ or the unramified cohomology group $H^i_{nr}(k_{\mathfrak{p}}, A) := \mathrm{im}\big(H^i(\mathcal{G}_{\mathfrak{p}}/\mathcal{T}_{\mathfrak{p}}, A^{\mathcal{T}_{\mathfrak{p}}}) \xrightarrow{\mathrm{inf}} H^i(\mathcal{G}_{\mathfrak{p}}, A)\big)$. In particular, the product of restriction maps for v

$$H^i(k, A) \to \bigoplus_{\mathfrak{p}\in S_v(k)} H^i(k_{\mathfrak{p}}, A)$$

respects the $\mathrm{Gal}(k/Q)$ actions. Moreover, one can check that

$$\bigoplus_{\mathfrak{p}\in S_v(k)} H^i(k_{\mathfrak{p}}, A) \cong \mathrm{Ind}^{\mathrm{Gal}_{\mathfrak{q}}(k/Q)}_{\mathrm{Gal}(k/Q)} H^i(k_{\mathfrak{q}}, A)$$

as $\mathrm{Gal}(k/Q)$-modules for any $\mathfrak{q} \in S_v(k)$. The same statement holds for the Tate cohomology groups. For a set S of places of k, we use the following notation for Shafarevich groups:

$$Ш^i(k, A) = \ker\Big(H^i(k, A) \to \prod_{\mathfrak{p}\text{ all places}} H^i(k_{\mathfrak{p}}, A)\Big), \quad Ш^i_S(k, A) = \ker\Big(H^i(G_S(k), A) \to \prod_{\mathfrak{p}\in S} H^i(k_{\mathfrak{p}}, A)\Big),$$

and we set

$$\prod_{\mathfrak{p}\in S}{}' H^1(k_{\mathfrak{p}}, A) := \left\{ (f_{\mathfrak{p}})_{\mathfrak{p}\in S} \in \prod_{\mathfrak{p}\in S} H^1(k_{\mathfrak{p}}, A) \;\middle|\; f_{\mathfrak{p}} \text{ is unramified for all but finitely many primes in } S \right\}.$$

2.3. ***List of notation appearing in multiple sections.***

- $F_n(\Gamma)$: free profinite Γ-group on n generators (defined in Section 3).
- $F_n'(\Gamma)$: pro-$|\Gamma|'$ completion of $F_n(\Gamma)$.
- $\mathcal{F}_n(\Gamma)$: free admissible Γ-group on n generators (defined in Section 4).
- $m(\omega, \Gamma, H, A)$: multiplicity of A associated to a Γ-equivariant surjection ω to the Γ-group H (defined in Definition 3.1).
- $m(n, \Gamma, G, A)$: multiplicity of A associated to a pro-$|\Gamma|'$ Γ-equivariant surjection $F_n'(\Gamma) \to G$ (defined in Definition 3.6).
- $m_{\mathrm{ad}}(n, \Gamma, G, A)$: multiplicity of A associated to an admissible Γ-presentation $\mathcal{F}_n(\Gamma) \to G$ (defined in Definition 4.3).
- $m_{\mathrm{ad}}^{\mathcal{C}}(n, \Gamma, G, A)$: multiplicity of A associated to a level-$\mathcal{C}$ admissible Γ-presentation $\mathcal{F}_n(\Gamma)^{\mathcal{C}} \to G^{\mathcal{C}}$ (defined in Proposition 5.4).
- $\chi_{k/Q,S}(A)$: Euler characteristic (defined in Section 7).
- $\delta_{k/Q,S}(A) := \dim_{\mathbb{F}_\ell} H^2(G_S(k), A)^{\mathrm{Gal}(k/Q)} - \dim_{\mathbb{F}_\ell} H^1(G_S(k), A)^{\mathrm{Gal}(k/Q)}$ (defined in Definition 9.1).
- $\epsilon_{k/Q,S}(A)$: an invariant associated to the Galois module A (defined Proposition 9.4)

3. Presentations of finitely generated profinite Γ-groups

Let $F_n(\Gamma)$ denote the *free profinite* Γ*-group on n generators* defined in [Liu et al. 2024]. Explicitly, $F_n(\Gamma)$ is the free profinite group on $\{x_{i,\gamma} \mid i = 1, \dots, n \text{ and } \gamma \in \Gamma\}$ together with a Γ-action defined by

$$\sigma(x_{i,\gamma}) = x_{i,\sigma\gamma} \quad \text{for all } \gamma \in \Gamma.$$

If G is a profinite Γ-group that is Γ-generated by $g_1, \dots, g_n$, then there is a unique surjective Γ-equivariant homomorphism $F_n(\Gamma) \to G$ defined by sending x_{i,Id_Γ} to g_i for each i. So the universal property holds for $F_n(\Gamma)$, and that is why $F_n(\Gamma)$ is the free pro-Γ-group on n generators (namely, the generators are $x_{1,\mathrm{Id}_\Gamma}, \dots, x_{n,\mathrm{Id}_\Gamma}$).

When the choice of Γ is clear, we will denote $F_n(\Gamma)$ simply by F_n. Let G be a finitely generated Γ-group. Then when n is sufficiently large, there exists a short exact sequence

$$1 \to N \to F_n \rtimes \Gamma \xrightarrow{\pi} G \rtimes \Gamma \to 1, \tag{3-1}$$

where π is defined by mapping Γ identically to Γ, and $\{x_{i,1_\Gamma}\}_{i=1}^n$ to a set of n elements of G that generates G under the Γ action. Note that (3-1) can be viewed as a presentation of the group G that is compatible with Γ actions, and we will call it a Γ*-presentation of* G. The minimal number of relations in the presentation (3-1), which is one of the main objects studied in this paper, is related to the multiplicities of the irreducible $F_n \rtimes \Gamma$-quotients of N. We define the multiplicity as follows, and one can find that this quantity is similarly defined in [Lubotzky 2001; Liu and Wood 2020; Liu et al. 2024].

Definition 3.1. Given a short exact sequence $1 \to \ker\omega \to E \xrightarrow{\omega} H \to 1$ of Γ-groups, we let M be the intersection of all maximal proper $E \rtimes \Gamma$-normal subgroups of $\ker\omega$, and let $\bar{N} = \ker\omega/M$ and $\bar{E} = E/M$. Then one can show that $\bar{N}$ is a direct product of finite irreducible $\bar{E} \rtimes \Gamma$-groups. For any finite irreducible $\bar{E} \rtimes \Gamma$-group A, we define $m(\omega, \Gamma, H, A)$ to be the multiplicity of A appearing in $\bar{N}$. When the multiplicity is infinite, we let $m(\omega, \Gamma, H, A) = \infty$. When ω refers to the surjection $E \rtimes \Gamma \to H \rtimes \Gamma$ induced by the Γ-equivariant surjection $E \to H$, we use the notation $m(\omega, \Gamma, H, A)$ instead of $m(\omega|_E, \Gamma, H, A)$ for the sake of convenience.

Consider the short exact sequence (3-1). Let M be the intersection of all maximal proper $F_n \rtimes \Gamma$-normal subgroups of N, and define $R = N/M$ and $F = F_n/M$ (i.e., R and F are $\bar{N}$ and $\bar{E}$ in Definition 3.1) for the short exact sequence (3-1). Then we obtain a short exact sequence

$$1 \to R \to F \rtimes \Gamma \to G \rtimes \Gamma \to 1.$$

Note that $F \rtimes \Gamma$ acts on R by conjugation, and maps the factor $A^{m(\pi,\Gamma,G,A)}$ of R to itself. When A is abelian, then the conjugation action on A by elements in R is trivial, so the $F \rtimes \Gamma$ action on A factors through $G \rtimes \Gamma$, and hence A is a finite simple $G \rtimes \Gamma$-module.

Lemma 3.2. *Using the notation above, if A is a finite simple $G \rtimes \Gamma$-module such that* $\gcd(|\Gamma|, |A|) = 1$, *then*

$$m(\pi, \Gamma, G, A) = \frac{n \dim_{\mathbb{F}_\ell} A - \xi(A) + \dim_{\mathbb{F}_\ell} H^2(G \rtimes \Gamma, A) - \dim_{\mathbb{F}_\ell} H^1(G \rtimes \Gamma, A)}{h_{G\rtimes\Gamma}(A)},$$

where ℓ is the exponent of A and $\xi(A) := \dim_{\mathbb{F}_\ell} A^\Gamma / A^{G\rtimes\Gamma}$.

Remark 3.3. When Γ is the trivial group, the lemma is [Lubotzky 2001, Lemma 5.3]

Proof. Applying the inflation-restriction exact sequence to (3-1), we obtain

$$0 \to H^1(G \rtimes \Gamma, A^N) \to H^1(F_n \rtimes \Gamma, A) \to H^1(N, A)^{G\rtimes\Gamma} \to H^2(G \rtimes \Gamma, A^N) \to H^2(F_n \rtimes \Gamma, A). \quad (3\text{-}2)$$

Also by $\gcd(|A|, |\Gamma|) = 1$, the Hochschild–Serre spectural sequence $E^{ij} = H^i(\Gamma, H^j(F_n, A)) \Longrightarrow H^{i+j}(F_n \rtimes \Gamma, A)$ degenerates, so we have that

$$H^2(F_n \rtimes \Gamma, A) \cong H^2(F_n, A)^\Gamma,$$

which is trivial because F_n is a free profinite group. Note that N acts trivially on A, so

$$H^1(N, A)^{G\rtimes\Gamma} = \mathrm{Hom}_{F_n\rtimes\Gamma}(N, A) = \mathrm{Hom}_{G\rtimes\Gamma}(A^{m(\pi,\Gamma,G,A)}, A)$$

because A is a simple $\mathbb{F}_\ell[G \rtimes \Gamma]$-module and $m(\pi, \Gamma, G, A)$ is the maximal integer such that $A^{m(\pi,\Gamma,G,A)}$ is an $F_n \rtimes \Gamma$-equivariant quotient of N. Then it follows that

$$\dim_{\mathbb{F}_\ell} H^1(N, A)^{G\rtimes\Gamma} = m(\pi, \Gamma, G, A) \dim_{\mathbb{F}_\ell} \mathrm{Hom}_{G\rtimes\Gamma}(A, A).$$

Thus, by (3-2) it suffices to show $\dim_{\mathbb{F}_\ell} H^1(F_n \rtimes \Gamma, A) = n \dim_{\mathbb{F}_\ell} A - \xi(A)$.

Elements of $H^1(F_n \rtimes \Gamma, A)$ correspond to the A-conjugacy classes of homomorphic sections of $A \rtimes (F_n \rtimes \Gamma) \xrightarrow{\rho} F_n \rtimes \Gamma$. We write every element of $F_n \rtimes \Gamma$ in the form of (x, γ) for $x \in F_n$ and $\gamma \in \Gamma$, and similarly, write elements of $A \rtimes (F_n \rtimes \Gamma)$ as $(a; x, \gamma)$ for $a \in A$, $x \in F_n$ and $\gamma \in \Gamma$. Then ρ maps $(a; x, \gamma)$ to (x, γ) for any a, x and γ. Note that a section of ρ is completely determined by the images of $(x_{i,1_\Gamma}, 1)$ and $(1, \gamma)$ for $i = 1, \ldots, n$ and $\gamma \in \Gamma$, where $x_{i,1_\Gamma}$'s are the Γ-generators of F_n defined at the beginning of this section. Since $\gcd(|A|, |\Gamma|) = 1$, we have $H^1(\Gamma, A) = 0$ by the Schur–Zassenhaus theorem, which implies that the restrictions of all the sections of ρ to the subgroup Γ are conjugate to each other by A. So we only need to study the A-conjugacy classes of sections of ρ which map $(1, \gamma)$ to $(1; 1, \gamma)$ for any $\gamma \in \Gamma$, and such sections are totally determined by the images of $(x_{i,1_\Gamma}, 1)$ for $i = 1, \ldots, n$. Let s_1 and s_2 be two distinct sections of this type. Under the multiplication rule of semidirect product, the conjugation of $(a; x, \gamma)$ by an element $\alpha \in A$ is

$$\begin{aligned}(\alpha^{-1}; 1, 1)(a; x, \gamma)(\alpha; 1, 1) &= (\alpha^{-1} \cdot a \cdot (x, \gamma)(\alpha); x, \gamma)\\ &= (\alpha^{-1} \cdot (x, \gamma)(\alpha); 1, 1)(a; x, \gamma),\end{aligned}$$

where the last equality is because A is abelian. Therefore, because of the assumption that $s_1(1, \gamma) = s_2(1, \gamma) = (1; 1, \gamma)$ for any $\gamma \in \Gamma$, we see that s_1 and s_2 are A-conjugate if and only if there exists $\alpha \in A^\Gamma / A^{G \rtimes \Gamma}$ such that $s_2(x, \gamma) = (\alpha^{-1} \cdot (x, \gamma)(\alpha); 1, 1)s_1(x, \gamma)$ for any x, γ. So

$$\begin{aligned}\#\{A\text{-conjugacy classes of sections of } \rho\} &= |A^\Gamma / A^{G \rtimes \Gamma}|^{-1} \prod_{i=1}^{n} \#\rho^{-1}(x_{i,1_\Gamma}, 1)\\ &= |A^\Gamma / A^{G \rtimes \Gamma}|^{-1} |A|^n,\end{aligned}$$

which proves that $\dim_{\mathbb{F}_\ell} H^1(F_n \rtimes \Gamma, A) = n \dim_{\mathbb{F}_\ell} A - \dim_{\mathbb{F}_\ell}(A^\Gamma / A^{G \rtimes \Gamma})$. □

In this paper, instead of the Γ-presentations in the form of (3-1), we want to study the presentations of pro-$|\Gamma|'$ completions of Γ-groups. Recall that the pro-$|\Gamma|'$ completion of a group G is the inverse limit of all finite quotients of G whose order is prime to $|\Gamma|$. We denote the pro-$|\Gamma|'$ completions of $F_n(\Gamma)$ and G by $F'_n(\Gamma)$ and G' respectively, and write F'_n for $F'_n(\Gamma)$ when the choice of Γ is clear. Then F'_n and G' naturally obtain Γ actions from F_n and G, and we have a short exact sequence

$$1 \to N' \to F'_n \rtimes \Gamma \xrightarrow{\pi'} G' \rtimes \Gamma \to 1, \tag{3-3}$$

induced by (3-1), which will be called *a $|\Gamma|'$-Γ-presentation of G'*.

Proposition 3.4. *Use the notation above. Let A be a finite simple $G' \rtimes \Gamma$-module, and denote the exponent of A by ℓ. If ℓ divides $|\Gamma|$, then $m(\pi', \Gamma, G', A) = 0$. Otherwise,*

$$m(\pi', \Gamma, G', A) = \frac{n \dim_{\mathbb{F}_\ell} A - \xi(A) + \dim_{\mathbb{F}_\ell} H^2(G' \rtimes \Gamma, A) - \dim_{\mathbb{F}_\ell} H^1(G' \rtimes \Gamma, A)}{h_{G' \rtimes \Gamma}(A)} \tag{3-4}$$

$$\leq \frac{n \dim_{\mathbb{F}_\ell} A - \xi(A) + \dim_{\mathbb{F}_\ell} H^2(G, A)^\Gamma - \dim_{\mathbb{F}_\ell} H^1(G, A)^\Gamma}{h_{G \rtimes \Gamma}(A)}. \tag{3-5}$$

where in (3-5) A is viewed as a $G \rtimes \Gamma$-module via the surjection $G \rtimes \Gamma \to G' \rtimes \Gamma$. Moreover, the equality in (3-5) holds if $H^2(\ker(G \to G'), \mathbb{F}_\ell) = 0$.

Remark 3.5. We see from (3-5) that the multiplicity $m(\pi', \Gamma, G', A)$ depends on n, Γ, G and A, but not on the choice of the quotient map π'.

Proof. It is clear that if ℓ divides $|\Gamma|$, then $m(\pi', \Gamma, G', A) = 0$. For the rest of the proof, assume $\ell \nmid |\Gamma|$. We consider the commutative diagram

$$\begin{tikzcd} F_n \rtimes \Gamma \arrow[r, two heads, "\pi"] \arrow[d, two heads, "\rho"] \arrow[dr, two heads, "\varpi"] & G \rtimes \Gamma \arrow[d, two heads, "\rho_G"] \\ F'_n \rtimes \Gamma \arrow[r, two heads, "\pi'"] & G' \rtimes \Gamma \end{tikzcd}$$

where each of the vertical maps is taking the $|\Gamma|'$-completion of the first component in semidirect product. If U is a maximal proper $F'_n \rtimes \Gamma$-normal subgroup of $\ker \pi'$ such that $\ker \pi'/U \simeq_{G' \rtimes \Gamma} A$, then its full preimage $\rho^{-1}(U)$ in $F_n \rtimes \Gamma$ is a maximal proper $F_n \rtimes \Gamma$-normal subgroup of $\ker \varpi$ with $\ker \varpi / \rho^{-1}(U) \simeq_{G' \rtimes \Gamma} A$. So by definition of multiplicities, we have that $m(\pi', \Gamma, G, A) \leq m(\varpi, \Gamma, G, A)$. On the other hand, because $\gcd(|A|, |\Gamma|) = 1$, if V is a maximal proper $F_n \rtimes \Gamma$-normal subgroup of $\ker \varpi$ with $\ker \varpi / V \simeq_{G' \rtimes \Gamma} A$, then $F_n \rtimes \Gamma \twoheadrightarrow (F_n/V) \rtimes \Gamma$ factors through ρ, and hence we have shown that $m(\pi', \Gamma, G, A) = m(\varpi, \Gamma, G, A)$. Because ϖ defines a Γ-presentation of G', by Lemma 3.2 we obtain the equality (3-4).

Let W denote $\ker \rho_G = \ker(G \to G')$. Because G' is the pro-$|\Gamma|'$ completion of G and $\ell \nmid |\Gamma|$, the pro-ℓ completion of W is trivial. So as W acts trivially on A, we have that $H^1(W, A) = 0$. Then by considering the Hochschild–Serre spectral sequence associated to

$$1 \to W \to G \rtimes \Gamma \to G' \rtimes \Gamma \to 1,$$

we see that

$$H^1(G' \rtimes \Gamma, A) \cong H^1(G \rtimes \Gamma, A) \quad \text{and} \quad H^2(G' \rtimes \Gamma, A) \hookrightarrow H^2(G \rtimes \Gamma, A).$$

where the latter embedding is an isomorphism if $H^2(W, A) = 0$. Note that $H^2(W, A) = H^2(W, \mathbb{F}_\ell)^{\oplus \dim_{\mathbb{F}_\ell} A}$ because W acts trivially on A.

Finally, since $\gcd(|A|, |\Gamma|) = 1$, we have that $H^i(\Gamma, A) = 0$ for any $i \geq 1$, and hence by the Hochschild–Serre spectral sequence of

$$1 \to G \to G \rtimes \Gamma \to \Gamma \to 1$$

we have that $H^i(G \rtimes \Gamma, A) \cong H^i(G, A)^\Gamma$ for any i. Therefore, we have

$$\dim_{\mathbb{F}_\ell} H^1(G' \rtimes \Gamma, A) = \dim_{\mathbb{F}_\ell} H^1(G, A)^\Gamma \quad \text{and} \quad \dim_{\mathbb{F}_\ell} H^2(G' \rtimes \Gamma) \leq \dim_{\mathbb{F}_\ell} H^2(G, A)^\Gamma,$$

where the equality holds if $H^2(W, \mathbb{F}_\ell) = 0$. □

By Remark 3.5, we can define the multiplicities as follows.

Definition 3.6. Let Γ be a finite group, G' a finitely generated pro-$|\Gamma|'$ Γ-group, and A a finite irreducible $G' \rtimes \Gamma$-group. Assume that there exists a Γ-equivariant surjection $\pi' : F'_n \to G'$. We define $m(n, \Gamma, G', A)$ to be $m(\pi', \Gamma, G', A)$.

When A is abelian, $m(n, \Gamma, G', A)$ is bounded above by (3-5). The next proposition proves that the minimal number of relators in the presentation π' is determined by $m(n, \Gamma, G', A)$ for all abelian A.

Proposition 3.7. *Consider the short exact sequence (3-3). The minimal number of generators of* $\ker\pi'$ *as a closed normal* Γ*-subgroup of* F_n' *is*

$$\sup_{\ell\nmid|\Gamma|}\ \sup_{\substack{A:\,\textit{finite simple}\\ \mathbb{F}_\ell[G'\rtimes\Gamma]\textit{-modules}}}\left\lceil\frac{\dim_{\mathbb{F}_\ell}H^2(G'\rtimes\Gamma,A)-\dim_{\mathbb{F}_\ell}H^1(G'\rtimes\Gamma,A)-\xi(A)}{\dim_{\mathbb{F}_\ell}A}\right\rceil+n. \tag{3-6}$$

Moreover, this minimal number is

$$\sup_{\ell\nmid|\Gamma|}\ \sup_{\substack{A:\,\textit{finite simple}\\ \mathbb{F}_\ell[G'\rtimes\Gamma]\textit{-modules}}}\left\lceil\frac{\dim_{\mathbb{F}_\ell}H^2(G,A)^\Gamma-\dim_{\mathbb{F}_\ell}H^1(G,A)^\Gamma-\xi(A)}{\dim_{\mathbb{F}_\ell}A}\right\rceil+n \tag{3-7}$$

and the equality holds if $H^2(\ker(G\to G'),\mathbb{F}_\ell)=0$.

Proof. We let M be the intersection of all maximal proper $F_n'\rtimes\Gamma$-normal subgroups of $\ker\pi'$, and let $R=\ker\pi'/M$ and $F=F_n'/M$. Then R is isomorphic to a direct product of finite irreducible $F\rtimes\Gamma$-groups whose orders are coprime to $|\Gamma|$. A set of elements of $\ker\pi'$ generates $\ker\pi'$ as a normal subgroup of $F_n'\rtimes\Gamma$ if and only if their images generate R as a normal subgroup of $F\rtimes\Gamma$.

For positive integer m, r and a finite irreducible $F\rtimes\Gamma$-group A, by [Liu and Wood 2020, Corollaries 5.9 and 5.10], one can compute the probability that the $F\rtimes\Gamma$-closed group generated by r random elements of A^m is the whole A^m. Note that this probability is positive if and only if A^m can be generated by r elements as a $F\rtimes\Gamma$-group. It follows that the minimal number of elements generating A^m as an $F\rtimes\Gamma$-group is

$$\begin{cases}1 & \text{if } A \text{ is nonabelian,}\\ \left\lceil\dfrac{mh_{F\rtimes\Gamma}(A)}{\dim_{\mathbb{F}_\ell}A}\right\rceil & \text{if } A \text{ is abelian, where } \ell \text{ is the exponent of } A.\end{cases}$$

Recall that if A is an abelian simple factor appearing in R, then the $F\rtimes\Gamma$ action on A factors through $G'\rtimes\Gamma$, since the conjugation action of R on A is trivial. Therefore, by the argument above and [Liu and Wood 2020, Corollary 5.7], the minimal number of generators of R as an $F\rtimes\Gamma$-group is

$$\sup_{\ell\nmid|\Gamma|}\ \sup_{\substack{A:\text{ finite simple}\\ \mathbb{F}_\ell[G'\rtimes\Gamma]\text{-modules}}}\left\lceil\frac{m(n,\Gamma,G',A)h_{G'\rtimes\Gamma}(A)}{\dim_{\mathbb{F}_\ell}A}\right\rceil.$$

Then the proposition follows by Proposition 3.4 and the fact that $h_{G\rtimes\Gamma}(A)=h_{G'\rtimes\Gamma}(A)$. ☐

To end this section. we give a lemma that will be used later.

Lemma 3.8. *Let* E, F *and* G *be* Γ*-groups such that there exist* Γ*-equivariant surjections* $\alpha:E\to F$, $\beta:F\to G$ *and a* Γ*-equivariant homomorphic section* $s:F\to E$ *of* α. *Let* $\pi=\beta\circ\alpha$.

$$\begin{tikzcd} E \arrow[r, two heads, "\alpha"'] \arrow[rr, bend right, two heads, "\pi"'] & F \arrow[l, bend right, "s"'] \arrow[r, two heads, "\beta"] & G \end{tikzcd}$$

Let A *be a finite simple* $G\rtimes\Gamma$*-module. Then* $m(\pi,\Gamma,G,A)=m(\alpha,\Gamma,F,A)+m(\beta,\Gamma,G,A)$.

Proof. We first show $m(\pi, \Gamma, G, A) \geq m(\alpha, \Gamma, F, A) + m(\beta, \Gamma, G, A)$. By definition, the map β factors through an extension $\widetilde{G}$ of G satisfying the exact sequence

$$1 \to A^{m(\beta,\Gamma,G,A)} \to \widetilde{G} \to G \to 1.$$

Denote the composition of α and the quotient map $F \to \widetilde{G}$ by $\rho_1 : E \to \widetilde{G}$. Similarly, π factors through an extension $\widetilde{F}$ of F with kernel $A^{m(\alpha,\Gamma,F,A)}$. Because the section s identifies E as the semidirect product $\ker\alpha \rtimes s(F)$, we see that $\widetilde{F}$ has to be isomorphic to the semidirect product $A^{m(\alpha,\Gamma,F,A)} \rtimes F$. Note that the action of $F \rtimes \Gamma$ on A factors through $G \rtimes \Gamma$ (and similarly, factors through $\widetilde{G} \rtimes \Gamma$). So by composing with the surjection β, we have a Γ-equivariant quotient map

$$\rho_2 : E \to A^{m(\alpha,\Gamma,F,A)} \rtimes G.$$

Because ρ_2 factors through $A^{m(\alpha,\Gamma,F,A)} \rtimes \widetilde{G}$, we have the following fiber product diagram of Γ-equivariant quotients of E:

$$\begin{tikzcd}
A^{m(\alpha,\Gamma,F,A)} \rtimes \widetilde{G} = E/\ker\rho_1 \cap \ker\rho_2 \arrow[r, two heads] \arrow[d, two heads] & \widetilde{G} = E/\ker\rho_1 \arrow[d, two heads] \\
A^{m(\alpha,\Gamma,F,A)} \rtimes G = E/\ker\rho_2 \arrow[r, two heads] & G = E/\ker\rho_1 \ker\rho_2
\end{tikzcd}$$

So the diagram shows $m(\pi, \Gamma, G, A) \geq m(\alpha, \Gamma, F, A) + m(\beta, \Gamma, G, A)$.

Let $\mathcal{S}$ be the set of all maximal proper $E \rtimes \Gamma$-normal subgroups U of $\ker\pi$ with $\ker\pi/U \simeq_{G\rtimes\Gamma} A$. To prove the equality in the lemma, it suffices to show that, for each $U \in \mathcal{S}$,

$$\ker\rho_1 \cap \ker\rho_2 = \ker\rho_1 \cap \ker\rho_2 \cap U, \tag{3-8}$$

because (3-8) together with the preceding paragraph implies that $\cap_{U\in\mathcal{S}} U = \ker\rho_1 \cap \ker\rho_2$.

Let $U \in \mathcal{S}$. If $\ker\alpha \subset U$, then $\alpha(U)$ is a maximal proper $F \rtimes \Gamma$-normal subgroup of $\ker\beta$ such that $\ker\beta/\alpha(U) \simeq_{G\rtimes\Gamma} A$, so $\ker\rho_1 \subset U$ and therefore (3-8) holds. Otherwise, $\ker\alpha \not\subset U$. Then $\ker\alpha/(\ker\alpha \cap U) \simeq_{G\rtimes\Gamma} (\ker\alpha \cdot U)/U = \ker\pi/U \simeq_{G\rtimes\Gamma} A$ and similarly $\ker\rho_1/(\ker\rho_1 \cap U) \simeq_{G\rtimes\Gamma} A$, and we have the quotient map

$$E/\ker\alpha \cap U \simeq A \rtimes F \to E/\ker\rho_1 \cap U \simeq A \rtimes \widetilde{G}.$$

The domain of this quotient map is a quotient of $\widetilde{F}$ and the target is a quotient of $E/(\ker\rho_1 \cap \ker\rho_2)$. Then we see that $\ker\rho_1 \cap U \supset \ker\rho_1 \cap \ker\rho_2$; thus we prove (3-8) in this case. □

4. Presentations of finitely generated profinite admissible Γ-groups

We first recall the definition of the admissible Γ-groups and the free admissible Γ-groups in [Liu et al. 2024].

Definition 4.1. A profinite Γ-group G is called *admissible* if it is Γ-generated by elements $\{g^{-1}\gamma(g) \mid g \in G, \gamma \in \Gamma\}$ and is of order prime to $|\Gamma|$.

Recall that for each positive integer n, we defined F'_n to be the pro-$|\Gamma|'$ completion of F_n. We set $y_{i,\gamma}$ to be the image in F'_n of the generators $x_{i,\gamma}$ of F_n, and therefore F'_n is the free pro-$|\Gamma|'$ group on $\{y_{i,\gamma} \mid i = 1, \ldots, n \text{ and } \gamma \in \Gamma\}$, where $\sigma \in \Gamma$ acts on F'_n by $\sigma(y_{i,\gamma}) = y_{i,\sigma\gamma}$. We fix a generating set $\{\gamma_1, \ldots, \gamma_d\}$ of the finite group Γ throughout the paper. We set $y_i := y_{i,\mathrm{id}_\Gamma}$ and define $\mathcal{F}_n(\Gamma)$ to be the closed Γ-subgroup of F'_n that is generated as a Γ-subgroup by the elements

$$\{y_i^{-1}\gamma_j(y_i) \mid i = 1, \ldots, n \text{ and } j = 1, \ldots, d\}.$$

We will denote $\mathcal{F}_n(\Gamma)$ by $\mathcal{F}_n$ when the choice of Γ is clear. The following is a list of properties of $\mathcal{F}_n(\Gamma)$ proven in [Liu et al. 2024, Lemma 3.1, Corollary 3.8 and Lemma 3.9]:

(1) $\mathcal{F}_n$ is an admissible Γ-group and it does not depend on the choice of the generating set $\{\gamma_1, \ldots, \gamma_d\}$.

(2) There is a Γ-equivariant quotient map $\rho_n : F'_n \to \mathcal{F}_n$ such that the composition of the inclusion $\mathcal{F}_n \subset F'_n$ with ρ_n is the identity map on $\mathcal{F}_n$.

(3) Define a set function for any Γ-group G

$$Y : G \to G^d, \quad g \mapsto (g^{-1}\gamma_1(g), g^{-1}\gamma_2(g), \ldots, g^{-1}\gamma_d(g)).$$

Then the function

$$Y(G)^n \to \mathrm{Hom}_\Gamma(\mathcal{F}_n, G)$$

taking $(Y(g_1), \ldots, Y(g_n))$ to the restriction of the map $F'_n \to G$ with $y_i \mapsto g_i$ is a bijection.

Let G be an admissible Γ-group with a Γ-presentation defined by $F_n \rtimes \Gamma \overset{\pi}{\twoheadrightarrow} G \rtimes \Gamma$ such that the reduced map $F'_n \rtimes \Gamma \overset{\pi'}{\twoheadrightarrow} G \rtimes \Gamma$ satisfies that

$$G \text{ is } \Gamma\text{-generated by coordinates of } Y(y_i), \quad i = 1, \ldots, n. \tag{4-1}$$

Under the condition (4-1), the restriction of π' to the admissible subgroup $\mathcal{F}_n$ of F'_n is surjective, so π' that factors through the quotient map $\rho_n : F'_n \to \mathcal{F}_n$ in (2) above. We let $\pi_{\mathrm{ad}} = \pi'|_{\mathcal{F}_n \rtimes \Gamma}$ and obtain a short exact sequence

$$1 \to N \to \mathcal{F}_n \rtimes \Gamma \xrightarrow{\pi_{\mathrm{ad}}} G \rtimes \Gamma \to 1, \tag{4-2}$$

and we call it an *admissible* Γ*-presentation of* G.

Similarly to the previous section, we are interested in the multiplicities of the simple factors appearing as the quotients of N.

Lemma 4.2. *Let G be an admissible Γ-group with an admissible Γ-presentation (4-2) and A a finite simple $G \rtimes \Gamma$-module with* $\gcd(|A|, |\Gamma|) = 1$. *Then*

$$m(\pi_{\mathrm{ad}}, \Gamma, G, A) = m(n, \Gamma, G, A) - m(n, \Gamma, \mathcal{F}_n, A).$$

Proof. We let $\rho_n : F'_n \to \mathcal{F}_n$ be the quotient map described in property (2). Let ϖ be the composition of the following Γ-equivariant surjections and then ϖ defines a $|\Gamma|'$-Γ-presentation of G. Let $\iota : \mathcal{F}_n \to F'_n$ be the natural embedding. Then we have the diagram

$$\begin{tikzcd} F'_n \arrow[r, two heads, "\rho_n"'] \arrow[rr, bend right, two heads, "\varpi"'] & \mathcal{F}_n \arrow[l, bend right, "\iota"'] \arrow[r, two heads, "\pi_{\mathrm{ad}}|_{\mathcal{F}_n}"] & G, \end{tikzcd}$$

The lemma follows by Lemma 3.8. $\square$

Definition 4.3. Let G be a Γ-group with an admissible Γ-presentation (4-2). For a finite simple $G \rtimes \Gamma$-module A with $\gcd(|A|, |\Gamma|) = 1$, we define $m_{\mathrm{ad}}(n, \Gamma, G, A)$ to be $m(\pi_{\mathrm{ad}}, \Gamma, G, A)$. By Lemma 4.2, $m_{\mathrm{ad}}(n, \Gamma, G, A) = m(n, \Gamma, G, A) - m(n, \Gamma, \mathcal{F}_n, A)$ does not depend on the choice of π_{ad}.

Lemma 4.4. *Let A be a finite simple $\mathcal{F}_n \rtimes \Gamma$-module such that* $\gcd(|A|, |\Gamma|) = 1$. *Then*

$$\dim_{\mathbb{F}_\ell} H^1(\mathcal{F}_n \rtimes \Gamma, A) = n \dim_{\mathbb{F}_\ell}(A/A^\Gamma) - \xi(A).$$

Proof. We use the idea in the proof of Lemma 3.2. Elements of $H^1(\mathcal{F}_n \rtimes \Gamma, A)$ correspond to the A-conjugacy classes of homomorphic sections of $A \rtimes (\mathcal{F}_n \rtimes \Gamma) \xrightarrow{\rho} \mathcal{F}_n \rtimes \Gamma$. We use (g, γ) to represent elements of $\mathcal{F}_n \rtimes \Gamma$, and $(a; g, \gamma)$ to represent elements of $A \rtimes (\mathcal{F}_n \rtimes \Gamma)$. Again, by the Schur–Zassenhaus theorem, we only need to count the A-conjugacy classes of sections of ρ that maps $(1; 1, \gamma)$ to $(1, \gamma)$. In other words, we only need to study the A-conjugacy classes of Γ-equivariant sections of $A \rtimes \mathcal{F}_n \to \mathcal{F}_n$.

By property (3) of $\mathcal{F}_n$, there is a bijection $Y(A \rtimes \mathcal{F}_n)^n \to \mathrm{Hom}_\Gamma(\mathcal{F}_n, A \rtimes \mathcal{F}_n)$ taking $(Y(g_1), \ldots, Y(g_n))$ to the restriction of the map $F'_n \to A \rtimes \mathcal{F}_n$ with $y_i \mapsto g_i$. For a Γ-equivariant section s of $A \rtimes \mathcal{F}_n \to \mathcal{F}_n$, the elements $s(y_i^{-1}\gamma_j(y_i))$ in $A \rtimes \mathcal{F}_n$ must map to $y_i^{-1}\gamma_j(y_i) \in \mathcal{F}_n$ for each $i = 1, \ldots, n$ and $j = 1, \ldots, d$. Therefore, the Γ-equivariant sections of $A \rtimes \mathcal{F}_n \to \mathcal{F}_n$ are in one-to-one correspondence with elements in $Y(A \rtimes \mathcal{F}_n)^n$ which map to $(Y(y_1), \ldots, Y(y_n)) \in Y(\mathcal{F}_n)^n$ under the natural quotient map $A \rtimes \mathcal{F}_n \to \mathcal{F}_n$ on each component.

Let's consider $Y(y_i)$ and its preimages in $Y(A \rtimes \mathcal{F}_n)$. Note that there is also a natural embedding $Y(\mathcal{F}_n) \hookrightarrow Y(A \rtimes \mathcal{F}_n)$ defined by the obvious section of split extension $A \rtimes \mathcal{F}_n \twoheadrightarrow \mathcal{F}_n$. So we can fix a $g \in A \rtimes \mathcal{F}_n$ such that $Y(g)$ is the image of $Y(y_i)$ under this embedding, and then $Y(g)$ is a preimage of $Y(y_i)$ under φ, where φ is the quotient map $(A \rtimes \mathcal{F}_n)^d \to \mathcal{F}_n^d$. The self-bijection

$$(A \rtimes \mathcal{F}_n)^d \to (A \rtimes \mathcal{F}_n)^d, \quad (a_1, \ldots, a_d) \mapsto (g a_1 \gamma_1(g)^{-1}, \ldots, g a_d \gamma_d(g)^{-1})$$

maps $Y(A \rtimes \mathcal{F}_n)$ to itself and $\varphi^{-1}(Y(y_i))$ to A^d. Thus,

$$\#Y(A \rtimes \mathcal{F}_n) \cap \varphi^{-1}(Y(y_i)) = \#Y(A \rtimes \mathcal{F}_n) \cap A^d = \#Y(A) = |A/A^\Gamma|,$$

where the second equality above uses [Liu et al. 2024, Lemma 3.4] and the last uses [Liu et al. 2024, Lemma 3.5]. So we've shown that there are $|A/A^\Gamma|$ elements in $Y(A \rtimes \mathcal{F}_n)$ mapping to $Y(y_i)$, and it follows that the number of Γ-equivariant sections of $A \rtimes \mathcal{F}_n \to \mathcal{F}_n$ is $|A/A^\Gamma|^n$.

Finally, recall that two sections s_1, s_2 of $A \rtimes (\mathcal{F}_n \rtimes \Gamma) \to \mathcal{F}_n \rtimes \Gamma$ are A-conjugate if and only if $s_1(g,\gamma) = (\alpha^{-1} \cdot (g,\gamma)(\alpha); 1, 1) s_1(g,\gamma)$ for some $\alpha \in A^{\Gamma}/A^{\mathcal{F}_n \rtimes \Gamma}$, by the computation in the proof of Lemma 3.2. Therefore,

$$\# H^1(\mathcal{F}_n \rtimes \Gamma, A) = \frac{|A/A^{\Gamma}|^n}{|A^{\Gamma}/A^{\mathcal{F}_n \rtimes \Gamma}|}. \qquad \square$$

Corollary 4.5. *Under the assumptions in Lemma 4.2, we have*

$$m_{\mathrm{ad}}(n, \Gamma, G, A) = m(n, \Gamma, G, A) - \frac{n \dim_{\mathbb{F}_\ell} A^{\Gamma}}{h_{G \rtimes \Gamma}(A)}.$$

Proof. By Proposition 3.4 and Lemma 4.4, we have

$$m(n, \Gamma, \mathcal{F}_n, A) = \frac{n \dim_{\mathbb{F}_\ell} A^{\Gamma} + \dim_{\mathbb{F}_\ell} H^2(\mathcal{F}_n, A)^{\Gamma}}{h_{G \rtimes \Gamma}(A)}.$$

Note that, forgetting the Γ-action, $\mathcal{F}_n$ is a projective profinite group, because by definition it is a closed subgroup of the free pro-$|\Gamma|'$ group F'_n. So $H^2(\mathcal{F}_n, A) = 0$, and then the corollary follows immediately by Lemma 4.2. $\square$

We point out in the next lemma that A^{Γ} is strictly smaller than A when $G \rtimes \Gamma$ acts nontrivially on A.

Lemma 4.6. *If G is an admissible Γ-group and A is a $G \rtimes \Gamma$-group such that Γ acts trivially on A, then $G \rtimes \Gamma$ acts trivially on A.*

Proof. The $G \rtimes \Gamma$ action on A induces a group homomorphism $G \rtimes \Gamma \to \mathrm{Aut}(A)$. So it suffices to show that Γ is not contained in any proper normal subgroup of $G \rtimes \Gamma$. Suppose M is a proper normal subgroup containing Γ. Then $B := (G \rtimes \Gamma)/M$ is a Γ-quotient of G and Γ acts trivially on B. However, G is admissible, so is generated by elements $g^{-1}\gamma(g)$ for $g \in G$ and $\gamma \in \Gamma$. Then the images of all $g^{-1}\gamma(g)$ in the Γ-quotient B generate B but each of these images is 1, and hence we obtain the contradiction. $\square$

5. Presentations of finitely generated profinite Γ-groups of level $\mathcal{C}$

Let $\mathcal{C}$ be a set of isomorphism classes of finite Γ-groups. The *variety of Γ-groups generated by $\mathcal{C}$* is defined to be the smallest set $\overline{\mathcal{C}}$ of isomorphism classes of Γ-groups containing $\mathcal{C}$ that is closed under taking finite direct products, Γ-quotients and Γ-subgroups. For a given Γ-group G, we define the pro-$\mathcal{C}$ completion of G to be

$$G^{\mathcal{C}} = \varprojlim_{M} G/M,$$

where the inverse limit runs over all closed normal Γ-subgroups M of G such that the Γ-group G/M is contained in $\overline{\mathcal{C}}$. We call a Γ-group G *level* $\mathcal{C}$ if $G^{\mathcal{C}} = G$.

We want to emphasize that we do not require $\overline{\mathcal{C}}$ to be closed under taking group extensions, and it is different from most of works in the literature about completions of groups. For example, if we set $\mathcal{C}$ to be the set containing only the group $\mathbb{Z}/\ell\mathbb{Z}$ with the trivial Γ action, then $G^{\mathcal{C}}$ is the maximal quotient of G that is isomorphic to a direct product of $\mathbb{Z}/\ell\mathbb{Z}$ on which Γ acts trivially. If we want $G^{\mathcal{C}}$ to give us the pro-ℓ completion of G, then we need to let $\mathcal{C}$ contain all the finite Γ-groups of order a power of ℓ. Similarly, $G^{\mathcal{C}}$ is the pro-$|\Gamma|'$ completion of G if $\mathcal{C}$ consists of all finite Γ-groups of order prime to $|\Gamma|$.

Lemma 5.1. *Let F, G be Γ-groups and $\omega : F \to G$ a Γ-equivariant surjection. Let $\mathcal{C}$ be a set of isomorphism classes of finite Γ-groups, and φ the pro-$\mathcal{C}$ completion map $F \to F^{\mathcal{C}}$. Then we have the following commutative diagram of Γ-equivariant surjections*:

$$\begin{tikzcd} F \arrow[r, two heads, "\omega"] \arrow[d, two heads, "\varphi"] & G \arrow[d, two heads, "\alpha"] \\ F^{\mathcal{C}} \arrow[r, two heads, "\omega^{\mathcal{C}}"] & G^{\mathcal{C}} \end{tikzcd}$$

where $\omega^{\mathcal{C}}$ is the quotient map by $\varphi(\ker\omega)$.

Proof. By the set-up, $\operatorname{im}\omega^{\mathcal{C}}$ naturally fits into the right-lower position of this diagram, so it's enough to show that $\operatorname{im}\omega^{\mathcal{C}} \simeq G^{\mathcal{C}}$. First, $\operatorname{im}\omega^{\mathcal{C}}$ is a quotient of G and a quotient of $F^{\mathcal{C}}$, so it is of level $\mathcal{C}$ and hence is a quotient of $G^{\mathcal{C}}$. On the other hand, we consider the natural pro-$\mathcal{C}$ completion map $\alpha : G \to G^{\mathcal{C}}$, and the composition $\alpha \circ \omega : F \to G^{\mathcal{C}}$. Because $G^{\mathcal{C}}$ is of level $\mathcal{C}$, it follows that $\ker(\alpha\circ\omega) \supseteq \ker\varphi$. Also, because $\ker\omega \subseteq \ker(\alpha\circ\omega)$, we have that $\operatorname{im}(\alpha\circ\omega) = G^{\mathcal{C}}$ is a quotient of $F/(\ker\omega\ker\varphi) = (F/\ker\varphi)/(\ker\omega/\ker\omega\cap\ker\varphi) = F^{\mathcal{C}}/\ker\omega^{\mathcal{C}} = \operatorname{im}\omega^{\mathcal{C}}$. So we have proved that $\operatorname{im}\omega^{\mathcal{C}} \simeq G^{\mathcal{C}}$. □

Definition 5.2. For any Γ-equivariant surjection $\omega : F \to G$, we define the pro-$\mathcal{C}$ completion of ω to be $\omega^{\mathcal{C}} : F^{\mathcal{C}} \to G^{\mathcal{C}}$ in Lemma 5.1.

Corollary 5.3. *Under the assumptions in Lemma 5.1, for any finite simple $G^{\mathcal{C}} \rtimes \Gamma$-module A, we have $m(\omega^{\mathcal{C}}, \Gamma, G^{\mathcal{C}}, A) \leq m(\omega, \Gamma, G, A)$.*

Proof. By definition of $\omega^{\mathcal{C}}$, $\ker\omega^{\mathcal{C}}$ is the quotient of $\ker\omega$ by $\ker\omega\cap\ker\varphi$, and we denote this quotient map by $\phi : \ker\omega \to \ker\omega^{\mathcal{C}}$. If N is a maximal proper $F^{\mathcal{C}} \rtimes \Gamma$-normal subgroup of $\ker\omega^{\mathcal{C}}$ such that $\ker\omega^{\mathcal{C}}/N \simeq A$ as $G^{\mathcal{C}} \rtimes \Gamma$-modules, then its preimage $\phi^{-1}(N)$ in F is a maximal proper $F \rtimes \Gamma$-normal subgroup of $\ker\omega$ with $\ker\omega/\phi^{-1}(N) \simeq A$. The corollary follows by the definition of the multiplicity. □

Proposition 5.4. *Let G be an admissible Γ-group, $\mathcal{C}$ a set of isomorphism classes of finite Γ-groups and A a finite simple $G^{\mathcal{C}} \rtimes \Gamma$-module with $\gcd(|A|, |\Gamma|) = 1$. Then, for a fixed positive integer n such that there exists an admissible Γ-presentation of G as (4-2), the multiplicity $m(\pi_{\mathrm{ad}}^{\mathcal{C}}, \Gamma, G^{\mathcal{C}}, A)$ does not depend on the choice of π_{ad}, and so we denote $m(\pi_{\mathrm{ad}}^{\mathcal{C}}, \Gamma, G^{\mathcal{C}}, A)$ by $m_{\mathrm{ad}}^{\mathcal{C}}(n, \Gamma, G, A)$. Then*

$$m_{\mathrm{ad}}^{\mathcal{C}}(n, \Gamma, G, A) \leq m_{\mathrm{ad}}(n, \Gamma, G, A).$$

Moreover, if $m_{\mathrm{ad}}(n, \Gamma, G, A)$ is finite, then the equality holds for sufficiently large $\mathcal{C}$.

Proof. Since A is finite, we can find a finite set $\mathcal{C}_1 \subset \mathcal{C}$ of isomorphism classes of finite Γ-groups such that the map $G^{\mathcal{C}} \rtimes \Gamma \to \operatorname{Aut}(A)$ induced by the $G^{\mathcal{C}} \rtimes \Gamma$ action on A factors through $G^{\mathcal{C}_1} \rtimes \Gamma$, and hence A is a simple $G^{\mathcal{C}_1} \rtimes \Gamma$-module. Let $\mathcal{C}_1 \subset \mathcal{C}_2 \subset \cdots$ be an ascending sequence of finite sets of isomorphism classes of finite Γ-groups with $\cup\mathcal{C}_i=\mathcal{C}$. For each $i\leq j$, we have that $m(\pi_{\mathrm{ad}}^{\mathcal{C}_i},\Gamma,G^{\mathcal{C}_i},A)\leq m(\pi_{\mathrm{ad}}^{\mathcal{C}_j},\Gamma,G^{\mathcal{C}_j},A)\leq m(\pi_{\mathrm{ad}}^{\mathcal{C}},\Gamma,G^{\mathcal{C}},A)$ by Corollary 5.3, and hence

$$m(\pi_{\mathrm{ad}}^{\mathcal{C}},\Gamma,G^{\mathcal{C}},A)=\lim_{i\to\infty} m(\pi_{\mathrm{ad}}^{\mathcal{C}_i},\Gamma,G^{\mathcal{C}_i},A).$$

Since $\mathcal{C}_i$ is a finite set of Γ-groups, [Liu et al. 2024, Remark 4.9] shows that the multiplicity $m(\pi_{\mathrm{ad}}^{\mathcal{C}_i},\Gamma,G^{\mathcal{C}_i},A)$ does not depend on the choice of π_{ad}. So we obtained that $m(\pi_{\mathrm{ad}}^{\mathcal{C}},\Gamma,G^{\mathcal{C}},A)$ also does not depend on the choice of π_{ad}. The inequality in the proposition follows by $m(\pi_{\mathrm{ad}}^{\mathcal{C}},\Gamma,G^{\mathcal{C}},A)\leq m(\pi_{\mathrm{ad}},\Gamma,G,A)$.

The last statement in the proposition then automatically follows because

$$m_{\mathrm{ad}}(n,\Gamma,G,A)=\sup_{\substack{\mathcal{D}\text{: finite set}\\ \text{of }\Gamma\text{-groups}}} m_{\mathrm{ad}}^{\mathcal{D}}(n,\Gamma,G,A).\qquad\square$$

6. The heights of pro-$\mathcal{C}$ groups

Definition 6.1. For a finite group H, we define $\mathfrak{h}(H)$ to be the smallest integer n such that there exists a length-n sequence of normal subgroups of H,

$$1=H_0\lhd H_1\lhd\cdots\lhd H_n=H,$$

where H_{i+1}/H_i is isomorphic to a direct product of minimal normal subgroups of H/H_i. We define the height of H to be

$$\hat{\mathfrak{h}}(H)=\max\{\mathfrak{h}(U)\mid U\text{ is a subquotient of }H\}.$$

For a profinite group H, the height is defined as

$$\hat{\mathfrak{h}}(H)=\sup_{\substack{U\text{: finite}\\ \text{quotient of }H}}\hat{\mathfrak{h}}(U).$$

Lemma 6.2. *Let G and H be two finite groups. Then $\hat{\mathfrak{h}}(G\times H)=\max\{\hat{\mathfrak{h}}(G),\hat{\mathfrak{h}}(H)\}$.*

Proof. Note that a subquotient of G or H is a subquotient of $G\times H$, so $\hat{\mathfrak{h}}(G\times H)\geq\max\{\hat{\mathfrak{h}}(G),\hat{\mathfrak{h}}(H)\}$. It suffices to show that $\mathfrak{h}(U)\leq\max\{\hat{\mathfrak{h}}(G),\hat{\mathfrak{h}}(H)\}$ for any subquotient U of $G\times H$. Each subquotient U of $G\times H$ is a quotient of a subgroup V of $G\times H$. Then because a sequence of normal subgroups of V induces a sequence of normal subgroups of U, and a minimal normal subgroup is mapped to a product of minimal normal subgroups or the trivial subgroup under any quotient map. We see that $\mathfrak{h}(U)\leq\mathfrak{h}(V)$, so we only need to show that $\mathfrak{h}(V)\leq\max\{\hat{\mathfrak{h}}(G),\hat{\mathfrak{h}}(H)\}$ for any subgroup $V\subset G\times H$.

We let Proj_G and Proj_H be the projections mapping $G\times H$ to G and H respectively, and denote $V_G=\mathrm{Proj}_G(V)$ and $V_H=\mathrm{Proj}_H(V)$. Then $\mathrm{Proj}_G\times\mathrm{Proj}_H$ maps V injectively into $V_G\times V_H$. Let n denote $\max\{\hat{\mathfrak{h}}(G),\hat{\mathfrak{h}}(H)\}$, and then there exists a sequence

$$1\lhd V_{G,1}\times V_{H,1}\lhd V_{G,2}\times V_{H,2}\lhd\cdots\lhd V_{G,n}\times V_{H,n}=V_G\times V_H.$$

of normal subgroups of $V_G\times V_H$ of length n, where $\{V_{*,i}\}$ for $*=G$ or H is a sequence of normal subgroups of V_* such that $V_{*,i+1}/V_{*,i}$ is a direct product of minimal normal subgroups of $V_*/V_{*,i}$.

Assume that A is a minimal normal subgroup of $V_G \times V_H$ contained in $V_{G,1} \times V_{H,1}$ such that $A \cap V \neq 1$. Since V is a subgroup of $V_G \times V_H$, we have that $A \cap V$ is normal in V. Then $\mathrm{Proj}_G \times \mathrm{Proj}_H$ sends $A \cap V$ to a normal subgroup of $V_G \times V_H$ that is contained in $\mathrm{Proj}_G \times \mathrm{Proj}_H(A) \subset V_{G,1} \times V_{H,1}$. We see that $A \cap V$ is A, because $A \cap V \neq 1$ and A is minimal normal in $V_G \times V_H$. In particular, $A \cap V$ is a minimal normal subgroup of V, because otherwise Proj_G would map a minimal normal subgroup of V contained in $A \cap V$ to a normal subgroup of V_G that is properly contained in A which contradicts to the assumption that A is minimal normal. Thus, we have shown that $V \cap (V_{G,1} \times V_{H,1})$ is a direct product of minimal normal subgroups of V. Then by induction on i, we see that $\{V_i := V \cap (V_{G,i} \times V_{H,i})\}_{i=1}^n$ forms a sequence of normal subgroups of V such that V_{i+1}/V_i is a direct product of minimal normal subgroups of V/V_i, and hence $\mathfrak{h}(V) \leq \max\{\hat{\mathfrak{h}}(G), \hat{\mathfrak{h}}(H)\}$. □

Proposition 6.3. *Let Γ be a finite group and $\mathcal{C}$ a finite set of isomorphism classes of finite Γ-groups. For any Γ-group G, we have that $\hat{\mathfrak{h}}(G^{\mathcal{C}})$ is at most*

$$\hat{\mathfrak{h}}_{\mathcal{C}} := \max\{\hat{\mathfrak{h}}(H) \mid H \in \mathcal{C}\}.$$

Proof. By definition of $\hat{\mathfrak{h}}(G^{\mathcal{C}})$, it suffices to prove $\hat{\mathfrak{h}}(G) \leq \hat{\mathfrak{h}}_{\mathcal{C}}$ for any $G \in \overline{\mathcal{C}}$. So we just need to show that the three actions,

(1) taking Γ-quotients,

(2) taking Γ-subgroups, and

(3) taking finite direct products,

do not produce groups with larger value of $\hat{\mathfrak{h}}$. For the first two actions, it is obvious that if H is a Γ-quotient or a Γ-subgroup of G, then it is a quotient or a subgroup of G by forgetting the Γ actions, and hence $\hat{\mathfrak{h}}(H) \leq \hat{\mathfrak{h}}(G)$ by definition of heights. The last action follows by Lemma 6.2. □

We finish this section by applying Proposition 6.3 to prove the following number theory theorem.

Theorem 6.4. *Let k/Q be a Galois global field extension with $\mathrm{Gal}(k/Q) \simeq \Gamma$ and S a finite k/Q-closed set of places of k. Let $\mathcal{C}$ be a finite set of isomorphism classes of finite Γ-groups. Then $G_S(k)^{\mathcal{C}}$ is a finite group.*

Proof. By Proposition 6.3, we have that

$$h := \hat{\mathfrak{h}}(G_S(k)^{\mathcal{C}}) \leq \hat{\mathfrak{h}}_{\mathcal{C}}$$

is finite. So there exists a sequence of normal subgroups of $G_S(k)^{\mathcal{C}}$,

$$1 = H_0 \lhd H_1 \lhd \cdots \lhd H_h = G_S(k)^{\mathcal{C}},$$

such that H_{i+1}/H_i is isomorphic to a direct product of minimal normal subgroups of H_h/H_i. Note that each of the minimal normal subgroups is a (not necessarily finite) direct product of isomorphic finite simple groups. So, for each i, H_{i+1}/H_i as a group is a direct product of finite simple groups. On the other hand, $G_S(k)^{\mathcal{C}}$ is a quotient of $G_S(k)$, so is the Galois group of an extension of k that is unramified outside S. Therefore, H_{i+1}/H_i is the Galois group of an extension K_i/K_{i+1} of some intermediate fields between k_S and k. We denote by S_i the set of primes of K_i lying above S.

For a prime $\mathfrak{P}$ of K_i, the local absolute Galois group $\mathcal{G}_{\mathfrak{P}}(K_i)$ is finitely generated, so there are finitely many Galois extensions of $(K_i)_{\mathfrak{P}}$ having a fixed Galois group. Then for a simple group E, there exists an integer $N_{E,\mathfrak{P}}(K_i)$ for each $\mathfrak{P} \in S_i$, such that any Galois extension of $(K_i)_{\mathfrak{P}}$ whose Galois group is a subgroup of E has discriminant at most $N_{E,\mathfrak{P}}(K_i)$. Let $N_{E,S}(K_i)$ denote the product $\prod_{\mathfrak{P}\in S_i} N_{E,\mathfrak{P}}(K_i)$. By the Hermite-Minkowski theorem (see [Goss 1996, Theorem 8.23.5(3)] for the function field version of this theorem), for each finite simple group E, there are only finitely many extensions of K_i that have Galois group E and of discriminant at most $N_{E,S}(K_i)$. Therefore, there are finitely many extensions of K_i that are of Galois group E and unramified outside S_i.

Since $\mathcal{C}$ is finite, there are only finitely many simple groups that appear as composition factors of groups in $\bar{\mathcal{C}}$ (see [Liu and Wood 2020, Corollary 6.12]). Now we consider the tower of extensions K_i. Note that $K_h = k$ and $\mathrm{Gal}(K_{h-1}/K_h) \simeq H_h/H_{h-1}$. By the above argument, we conclude that H_h/H_{h-1} is a direct product of finite simple groups, that there are finitely many choices of these finite simple groups, and that for each of them there are finitely many copies of this simple group appearing in H_h/H_{h-1}. So we obtain that H_h/H_{h-1} is finite, and hence K_{h-1} is a finite extension of k. By induction, we see that H_{i+1}/H_i is finite for each $i = h-1, \dots, 0$, and it follows that $G_S(k)^{\mathcal{C}}$ is finite. □

7. A generalized version of global Euler–Poincaré characteristic formula

Throughout this section, we let k/Q be a finite Galois extension of global fields, and S be a *finite nonempty* k/Q-closed set of primes of k such that $S_\infty(k) \subseteq S$. For each $A \in \mathrm{Mod}(\mathrm{Gal}(k_S/Q))$, we define

$$\chi_{k/Q,S}(A) = \frac{\#H^2(G_S(k), A)^{\mathrm{Gal}(k/Q)} \#H^0(G_S(k), A)^{\mathrm{Gal}(k/Q)}}{\#H^1(G_S(k), A)^{\mathrm{Gal}(k/Q)}},$$

where $\mathrm{Gal}(k/Q)$ acts on $H^i(G_S(k), A)$ by conjugation. We will prove the following theorem.

Theorem 7.1. *Use the assumption at the beginning of this section. If $A \in \mathrm{Mod}_S(\mathrm{Gal}(k_S/Q))$ has order prime to $[k : Q]$, then*

$$\chi_{k/Q,S}(A) = \#\Big(\bigoplus_{v\in S_\infty(Q)} \widehat{H}^0(Q_v, A')\Big) \Big/ \#\Big(\bigoplus_{v\in S_\infty(Q)} H^0(Q_v, A')\Big).$$

Remark 7.2. (1) If k is a function field, then the theorem says that $\chi_{k/Q,S}(A) = 1$ since $S_\infty(k) = \varnothing$.

(2) When $k = Q$, the theorem is exactly the global Euler–Poincaré characteristic formula [Neukirch et al. 2008, Theorem (8.7.4)].

(3) When Q is a number field, a similar result is proven in [Clozel et al. 2008, Lemma 2.3.3].

7.1. *Preparation for the proof.*

Lemma 7.3. *Let G be a profinite group and U an open normal subgroup of G. Let H be an open subgroup of G and V denote $U \cap H$. Then H/V is naturally a subgroup of G/U, and for an H-module A we have*

$$H^i(U, \mathrm{Ind}_G^H A) \cong \mathrm{Ind}_{G/U}^{H/V} H^i(V, A)$$

as G/U-modules for each $i \geq 0$.

Proof. Under the quotient map $G \twoheadrightarrow G/U$, H/V is the image of H, so it is a subgroup of G/U. Then

$$\operatorname{Ind}_G^H A = \operatorname{Ind}_G^{UH} \operatorname{Ind}_{UH}^H A = \bigoplus_{\sigma \in G/UH} \sigma(\operatorname{Ind}_{UH}^H A),$$

where we denote by $\sigma(\operatorname{Ind}_{UH}^H A)$ the $\sigma UH\sigma^{-1}$-module, whose underlying group is $\operatorname{Ind}_{UH}^H A$ and the action of $\tau \in \sigma UH\sigma^{-1}$ is given by $a \mapsto \sigma^{-1}\tau\sigma a$. So

$$\begin{aligned} H^i(U, \operatorname{Ind}_G^H A) &= \bigoplus_{\sigma \in G/UH} H^i(U, \sigma(\operatorname{Ind}_{UH}^H A)) \\ &= \bigoplus_{\sigma \in G/UH} \sigma_* H^i(U, \operatorname{Ind}_{UH}^H A) \\ &= \operatorname{Ind}_{G/U}^{H/V} H^i(U, \operatorname{Ind}_{UH}^H A), \end{aligned} \tag{7-1}$$

where the second equality follows by $U \trianglelefteq G$ and the definition of the conjugation action σ_* on cohomology groups, and the last equality is because the quotient map $G \to G/U$ maps a set of representatives of G/UH to a set of representatives of $(G/U)/(H/V)$. Since A is an H-module, UH acts on $\operatorname{Ind}_U^V A$, and moreover, it follows by $V = H \cap U$ that $\operatorname{Ind}_U^V A = \operatorname{Ind}_{UH}^H A$ as UH-modules. So we have the following identity of H/V-modules:

$$H^i(U, \operatorname{Ind}_{UH}^H A) = H^i(U, \operatorname{Ind}_U^V A) \cong H^i(V, A), \tag{7-2}$$

where the last isomorphism follows by Shapiro's lemma. The lemma follows from (7-1) and (7-2). □

For the rest of this section, we assume S is a nonempty k/Q-closed set of primes of k containing S_∞ and let $G = \operatorname{Gal}(k_S/Q)$ and $U = G_S(k)$. For each open subgroup H of $\operatorname{Gal}(k_S/Q)$ we let $V = U \cap H$ and K be the fixed field of V, and define a map

$$\varphi_{H,S} : \operatorname{Mod}(H) \to K_0'(\mathbb{Z}[H/V]),$$

$$A \mapsto [H^0(V, A)] - [H^1(V, A)] + [H^2(V, A)] - \Big[\bigoplus_{\mathfrak{P} \in S_\infty(K)} \widehat{H}^0(K_{\mathfrak{P}}, A')\Big]^\vee + \Big[\bigoplus_{\mathfrak{P} \in S_\infty(K)} H^0(K_{\mathfrak{P}}, A')\Big]^\vee,$$

where H/V acts on $\bigoplus_{\mathfrak{P} \in S_\infty(K)} H^0(K_{\mathfrak{P}}, A')$ (similarly on Tate cohomology) by its permutation action on $S_\infty(K)$ and by the $\operatorname{Gal}_{\mathfrak{P}}(K/Q) \cap H$ on each summand, and the Pontryagin dual is taking on the classes of $K_0'(\mathbb{Z}[H/V])$.

Lemma 7.4. *Using the notation above, we have the following isomorphisms of G/U-modules for any $A \in \operatorname{Mod}(H)$:*

$$\bigoplus_{\mathfrak{p} \in S_\infty(k)} H^0(k_{\mathfrak{p}}, \operatorname{Ind}_G^H A) \cong \operatorname{Ind}_{G/U}^{H/V} \bigoplus_{\mathfrak{P} \in S_\infty(K)} H^0(K_{\mathfrak{P}}, A), \tag{7-3}$$

$$\bigoplus_{\mathfrak{p} \in S_\infty(k)} \widehat{H}^0(k_{\mathfrak{p}}, \operatorname{Ind}_G^H A) \cong \operatorname{Ind}_{G/U}^{H/V} \bigoplus_{\mathfrak{P} \in S_\infty(K)} \widehat{H}^0(K_{\mathfrak{P}}, A). \tag{7-4}$$

Proof. It suffices to fix a $v \in S_\infty(Q)$ and prove (7-3) and (7-4) for places above v. For each $\mathfrak{p} \in S_v(k)$, $\operatorname{Ind}_G^H A$ as a $\mathcal{G}_v(Q)$-module has the following canonical decomposition (see [Neukirch et al. 2008, §1.5, Example 5]):

$$\operatorname{Res}_{\mathcal{G}_v}^G \operatorname{Ind}_G^H A = \bigoplus_{\sigma \in \mathcal{G}_v \backslash G/H} \operatorname{Ind}_{\mathcal{G}_v}^{\mathcal{G}_v \cap \sigma H \sigma^{-1}} \sigma \operatorname{Res}_{\sigma^{-1}\mathcal{G}_v\sigma \cap H}^H A. \tag{7-5}$$

If v splits completely in k/Q, then $\mathrm{Gal}_v(k/Q)=1$ and $\mathcal{G}_{\mathfrak{p}}(k)=\mathcal{G}_v(Q)$. So we have the following identities of $\mathrm{Gal}_v(k/Q)$-modules:

$$\begin{aligned} H^0(k_{\mathfrak{p}}, \mathrm{Ind}_G^H A) &= \bigoplus_{\sigma\in\mathcal{G}_v\backslash G/H} H^0(\mathcal{G}_v\cap\sigma H\sigma^{-1}, \sigma\,\mathrm{Res}^H_{\sigma^{-1}\mathcal{G}_v\sigma\cap H} A) \\ &= \bigoplus_{\sigma\in\mathcal{G}_v\backslash G/H} \sigma_* H^0(\sigma\mathcal{G}_v\sigma^{-1}\cap H, \mathrm{Res}^H_{\sigma^{-1}\mathcal{G}_v\sigma\cap H} A), \end{aligned} \tag{7-6}$$

where the first equality uses (7-5) and Shapiro's lemma, and the second follows by definition of the conjugation action on cohomology groups. We let L denote the fixed field of H. Then, the set $\{\sigma\mathcal{G}_{\mathfrak{p}}\sigma^{-1}\cap H \mid \sigma\in\mathcal{G}_{\mathfrak{p}}\backslash G/H\}$ is exactly the set $\{\mathcal{G}_w(L)\mid w\in S_v(L)\}$. Therefore, we have the identity of abelian groups (hence of $\mathrm{Gal}_v(k/Q)$-modules since $\mathrm{Gal}_v(k/Q)=1$)

$$H^0(k_{\mathfrak{p}}, \mathrm{Ind}_G^H A) = \bigoplus_{w\in S_v(L)} H^0(L_w, A),$$

and hence

$$\bigoplus_{\mathfrak{p}\in S_v(k)} H^0(k_{\mathfrak{p}}, \mathrm{Ind}_G^H A) = \mathrm{Ind}^1_{G/U}\Bigl(\bigoplus_{w\in S_v(L)} H^0(L_w, A)\Bigr) \tag{7-7}$$

because the $\mathrm{Gal}(k/Q)$-action on this direct sum is determined by its permutation action on places above v. On the other hand, because $K=kL$, the assumption that v splits completely in k/Q implies that w splits completely in K for any $w\in S_v(L)$ and then we obtain

$$\bigoplus_{\mathfrak{P}\in S_v(K)} H^0(K_{\mathfrak{P}}, A) = \mathrm{Ind}^1_{H/V}\Bigl(\bigoplus_{w\in S_v(L)} H^0(L_w, A)\Bigr). \tag{7-8}$$

Thus, (7-7) and (7-8) prove (7-3) in this case. The isomorphism in (7-4) can be proven using the exactly same argument.

Otherwise, v is ramified in k/Q, so $\mathrm{Gal}_v(k/Q)\simeq\mathbb{Z}/2\mathbb{Z}$, $\mathcal{G}_{\mathfrak{p}}(k)=1$ and $\mathcal{G}_{\mathfrak{P}}(K)=1$ for each $\mathfrak{p}\in S_v(k)$ and $\mathfrak{P}\in S_v(K)$. Then (7-4) automatically follows because of $\widehat{H}^0(k_{\mathfrak{p}}, \mathrm{Ind}_G^H A)=\widehat{H}^0(K_{\mathfrak{P}}, A)=0$. The set of right cosets G/H naturally acts on $S_v(L)$, and moreover, for any $w\in S_v(L)$ and $\sigma_1,\sigma_2\in G/H$, $\sigma_1^{-1}\sigma_2$ is contained in $\mathcal{G}_w(L)\subset\mathrm{Gal}(K/L)$ if and only if $\sigma_1(w)=\sigma_2(w)$. So by (7-5), we have the following identities of $\mathrm{Gal}_{\mathfrak{p}}(k/Q)$-modules:

$$H^0(k_{\mathfrak{p}}, \mathrm{Ind}_G^H A) = \mathrm{Res}^G_{\mathcal{G}_v(Q)}\mathrm{Ind}_G^H A = \bigoplus_{w\in S_{\mathbb{R}}(L)} A_w \oplus \bigoplus_{w\in S_{\mathbb{C}}(L)} (A_w\oplus\tau A_w),$$

where $A_w := \mathrm{Res}^H_{\mathcal{G}_w(L)} A$ and τ denotes the nontrivial element in $\mathrm{Gal}_v(k/Q)$. So we have the following identity of $\mathrm{Gal}(k/Q)$-modules:

$$\bigoplus_{\mathfrak{p}\in S_v(k)} H^0(k_{\mathfrak{p}}, \mathrm{Ind}_G^H A) = \bigoplus_{w\in S_{\mathbb{R}}(L)} \mathrm{Ind}^{\mathrm{Gal}_v(k/Q)}_{\mathrm{Gal}(k/Q)} A_w \oplus \bigoplus_{w\in S_{\mathbb{C}}(L)} \mathrm{Ind}^1_{\mathrm{Gal}(k/Q)} A_w. \tag{7-9}$$

Finally, because $w\in S_v(L)$ is imaginary if and only if $\mathrm{Gal}_w(K/L)=1$, we have

$$\begin{aligned}\operatorname{Ind}_{G/U}^{H/V} \bigoplus_{\mathfrak{P}\in S_v(K)} H^0(K_{\mathfrak{P}}, A) &= \operatorname{Ind}_{G/U}^{H/V}\Big(\bigoplus_{w\in S_v(L)}\bigoplus_{\mathfrak{P}\in S_w(K)} A_w\Big)\\ &= \operatorname{Ind}_{G/U}^{H/V}\Big(\bigoplus_{w\in S_{\mathbb{R}}(L)} \operatorname{Ind}_{\mathrm{Gal}(K/L)}^{\mathrm{Gal}_w(K/L)} A_w \oplus \bigoplus_{w\in S_{\mathbb{C}}(L)} \operatorname{Ind}_{\mathrm{Gal}(K/L)}^{1} A_w\Big)\\ &= \bigoplus_{w\in S_{\mathbb{R}}(L)} \operatorname{Ind}_{\mathrm{Gal}(k/Q)}^{\mathrm{Gal}_v(k/Q)} A_w \oplus \bigoplus_{w\in S_{\mathbb{C}}(L)} \operatorname{Ind}_{\mathrm{Gal}(k/Q)}^{1} A_w. \end{aligned} \tag{7-10}$$

Thus, (7-3) follows by (7-9) and (7-10). □

The corollary below immediately follows by Lemmas 7.3, 7.4 and the fact $\operatorname{Ind}_G^H A' = (\operatorname{Ind}_G^H A)'$.

Corollary 7.5. *For any open subgroup H of G and $A \in \operatorname{Mod}(H)$, we have*

$$\varphi_{G,S}(\operatorname{Ind}_G^H A) \simeq \operatorname{Ind}_{G/U}^{H/V} \varphi_{H,S}(A).$$

Lemma 7.6. *The map $\varphi_{G,S}$ is additive on short exact sequences of modules in $\operatorname{Mod}_S(G)$.*

Proof. Denote $G_S(k)$ by G_S. Let $0 \to A_1 \to A_2 \to A_3 \to 0$ be an exact sequence of finite modules in $\operatorname{Mod}_S(G)$. By considering the associated long exact sequence of group cohomology, we have the following identity of elements in $K_0'(\mathbb{Z}[\mathrm{Gal}(k/Q)])$:

$$\sum_{i=0}^{2}\sum_{j=1}^{3}(-1)^{i+j+1}[H^i(G_S, A_j)] = \sum_{i=3}^{4}\sum_{j=1}^{3}(-1)^{i+j}[H^i(G_S, A_j)] + [\delta H^4(G_S, A_3)], \tag{7-11}$$

where δ denotes the connecting map $H^i \to H^{i+1}$ (or $\widehat{H}^i \to \widehat{H}^{i+1}$ for Tate cohomology groups) in the long exact sequence. By [Neukirch et al. 2008, Theorem (8.6.10)(ii)], for $i \geq 3$ and any j, the restriction map $H^i(G_S, A_j) \to \bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)} H^i(k_{\mathfrak{p}}, A_j)$ is an isomorphism. Note that for $\mathfrak{p} \in S_{\mathbb{R}}(k)$, we have $\mathcal{G}_{\mathfrak{p}}(k) = \mathbb{Z}/2\mathbb{Z}$, so by [Neukirch et al. 2008, Propositions (1.7.1) and (1.7.2)] we have

$$\begin{aligned}\sum_{i=3}^{4}\sum_{j=1}^{3}(-1)^{i+j}[H^i(G_S, A_j)] &= \sum_{i=3}^{4}\sum_{j=1}^{3}(-1)^{i+j}\Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)} H^i(k_{\mathfrak{p}}, A_j)\Big]\\ &= \sum_{\mathfrak{p}\in S_{\mathbb{R}}(k)}\sum_{i=-1}^{0}\sum_{j=1}^{3}(-1)^{i+j}[\widehat{H}^i(k_{\mathfrak{p}}, A_j)] = 0.\end{aligned}$$

So (7-11) gives

$$\begin{aligned}\sum_{i=0}^{2}\sum_{j=1}^{3}(-1)^{i+j+1}[H^i(G_S, A_j)] &= [\delta H^4(G_S, A_3)]\\ &= \Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)} \delta H^4(k_{\mathfrak{p}}, A_3)\Big] = \Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)} \delta \widehat{H}^0(k_{\mathfrak{p}}, A_3)\Big]\\ &= \Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)} \ker(\widehat{H}^1(k_{\mathfrak{p}}, A_1) \to \widehat{H}^1(k_{\mathfrak{p}}, A_2))\Big]\\ &= \Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)} \operatorname{coker}(\widehat{H}^1(k_{\mathfrak{p}}, A_2') \to \widehat{H}^1(k_{\mathfrak{p}}, A_1'))\Big]^{\vee}\\ &= \Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)} \delta \widehat{H}^1(k_{\mathfrak{p}}, A_1')\Big]^{\vee},\end{aligned} \tag{7-12}$$

where the fourth and last equalities use the long exact sequence of Tate cohomology groups, and the fifth uses the local duality theorem [Neukirch et al. 2008, Theorem (7.2.17)]. On the other hand, again by [Neukirch et al. 2008, Propositions (1.7.1) and (1.7.2)], the long exact sequence induced by

$$0 \to A_3' \to A_2' \to A_1' \to 0 \tag{7-13}$$

implies

$$\begin{aligned}\sum_{j=1}^{3}(-1)^{j+1}\Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)}\widehat{H}^0(k_{\mathfrak{p}}, A_j')\Big] &= \sum_{j=1}^{3}(-1)^{j+1}\Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)}\widehat{H}^1(k_{\mathfrak{p}}, A_j')\Big]\\ &= \sum_{j=1}^{3}(-1)^{j+1}\Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)}H^0(k_{\mathfrak{p}}, A_j')\Big]+\Big[\bigoplus_{\mathfrak{p}\in S_{\mathbb{R}}(k)}\delta H^1(k_{\mathfrak{p}}, A_1')\Big],\end{aligned} \tag{7-14}$$

where the last equality follows by the long exact sequence of group cohomology induced by (7-13). Therefore, combining (7-12) and (7-14), we obtain

$$\varphi_{G,S}(A_1)-\varphi_{G,S}(A_2)+\varphi_{G,S}(A_3)=0. \qquad \square$$

Lemma 7.7. *If $\ell\in\mathbb{N}(S)$ is a prime, then we have the following identities of elements in $K_0'(\mathbb{F}_\ell[\mathrm{Gal}(K/Q)])$ for any Galois extension K of Q with $k(\mu_\ell)\subset K\subset k_S$:*

$$\begin{aligned}&[H^0(\mathrm{Gal}(k_S/K),\mu_\ell)]=[\mu_\ell],\\ &[H^1(\mathrm{Gal}(k_S/K),\mu_\ell)]=[\mathcal{O}_{K,S}^\times/\ell]+[\mathrm{Cl}_S(K)[\ell]],\\ &[H^2(\mathrm{Gal}(k_S/K),\mu_\ell)]=[\mathrm{Cl}_S(K)/\ell]-[\mathbb{F}_\ell]+\Big[\bigoplus_{\mathfrak{P}\in S\setminus S_\infty(K)}\mathbb{F}_\ell\Big]+\Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)}\widehat{H}^0(\mathcal{G}_{\mathfrak{P}},\mathbb{F}_\ell)\Big],\end{aligned}$$

where $\mathrm{Cl}_S(K)$ is the S-class group of K, $\mathrm{Cl}_S(K)[\ell]$ is the ℓ-torsion subgroup of $\mathrm{Cl}_S(K)$, and $\mathcal{O}_{K,S}^\times/\ell$ and $\mathrm{Cl}_S(K)/\ell$ denote the maximal exponent-ℓ quotients of $\mathcal{O}_{K,S}^\times$ and $\mathrm{Cl}_S(K)$ respectively.

Proof. The lemma follows directly from the claims (i)–(iii) in the proof of [Neukirch et al. 2008, Theorem 8.7.4]. Though the proof of those claims only shows these identities when each terms are treated as Grothendieck group elements of $\mathrm{Gal}(K/k)$-modules, one can check that the ideas there work generally for the base field Q instead of k. $\square$

Proof of Theorem 7.1. For any G-module A and $v\in S_\infty(Q)$,

$$\bigoplus_{\mathfrak{p}\in S_v(k)}H^0(k_{\mathfrak{p}},A')\cong\mathrm{Ind}_{\mathrm{Gal}(k/Q)}^{\mathrm{Gal}_{\mathfrak{p}}(k/Q)}H^0(k_{\mathfrak{p}},A')$$

as $\mathrm{Gal}(k/Q)$-modules, where $\mathfrak{p}$ on the right-hand side is an arbitrarily chosen place in $S_v(k)$. So by Shapiro's lemma, we have

$$\Big(\bigoplus_{\mathfrak{p}\in S_v(k)}H^0(k_{\mathfrak{p}},A')\Big)^{\mathrm{Gal}(k/Q)}\cong H^0(k_{\mathfrak{p}},A')^{\mathrm{Gal}_{\mathfrak{p}}(k/Q)}=H^0(Q_v,A'). \tag{7-15}$$

If $\mathrm{Gal}_{\mathfrak{p}}(k/Q)=\mathbb{Z}/2\mathbb{Z}$, then $\widehat{H}^0(k_{\mathfrak{p}}, A')=\widehat{H}^0(Q_v, A')=0$ because $|A'|$ has to be odd as $\gcd(|A|, [k:Q])=1$. If $\mathrm{Gal}_{\mathfrak{p}}(k/Q)=1$, then $\widehat{H}^0(k_{\mathfrak{p}}, A')=\widehat{H}^0(Q_v, A')$. So

$$\Big(\bigoplus_{\mathfrak{p}\in S_v(k)} \widehat{H}^0(k_{\mathfrak{p}}, A')\Big)^{\mathrm{Gal}(k/Q)} \cong \widehat{H}^0(k_{\mathfrak{p}}, A')^{\mathrm{Gal}_{\mathfrak{p}}(k/Q)} = \widehat{H}^0(Q_v, A'). \tag{7-16}$$

Note that for any $M\in \mathrm{Mod}(\mathrm{Gal}(k/Q))$, we have $(M^\vee)^{\mathrm{Gal}(k/Q)}=\mathrm{Hom}_{\mathrm{Gal}(k/Q)}(M, \mathbb{Q}/\mathbb{Z})\simeq M_{\mathrm{Gal}(k/Q)}$. When M has order prime to $[k:\mathbb{Q}]$, $M^{\mathrm{Gal}(k/\mathbb{Q})}$ and $M_{\mathrm{Gal}(k/\mathbb{Q})}$ are isomorphic. So the $\mathrm{Gal}(k/Q)$-invariants of

$$\Big(\bigoplus_{\mathfrak{p}\in S_v(k)} H^0(k_{\mathfrak{p}}, A')\Big)^\vee \quad\text{and}\quad \Big(\bigoplus_{\mathfrak{p}\in S_v(k)} \widehat{H}^0(k_{\mathfrak{p}}, A')\Big)^\vee$$

are $H^0(Q_v, A')$ and $\widehat{H}^0(Q_v, A')$ respectively.

We let R denote the ring $\prod_{p\nmid[k:Q]}\mathbb{Z}_p$. Let $\Theta: K_0'(R[\mathrm{Gal}(k/Q)])\to\mathbb{Z}$ be the map defined by sending the class $[A]$ to the size of $A^{\mathrm{Gal}(k/Q)}$, which is a group homomorphism because taking $\mathrm{Gal}(k/Q)$-invariants is an exact functor in the category of $R[\mathrm{Gal}(k/Q)]$-modules. So we want to show that $\Theta\circ\varphi_{G,S}$ is the zero map when restricted to modules in $\mathrm{Mod}_S(\mathrm{Gal}(k_S/Q))$ with order prime to $[k:Q]$. By Lemma 7.6 we just need to show

$$\Theta\circ\varphi_{G,S}(K_0'(\mathbb{F}_\ell[\mathrm{Gal}(E/Q)]))=0 \tag{7-17}$$

for any prime integer $\ell\in\mathbb{N}(S)$ with $\ell\nmid[k:Q]$ and any finite extension E of k that is Galois over Q. Because the codomain of the map Θ is free, (7-17) is equivalent to the vanishing of $\Theta\circ\varphi_{G,S}$ on the torsion-free part of $K_0'(\mathbb{F}_\ell[\mathrm{Gal}(E/Q)])$. Note that, by [Neukirch et al. 2008, Lemma (7.3.4)], the $\mathbb{Q}$-linear space $K_0'(\mathbb{F}_\ell[\mathrm{Gal}(E/Q)])\otimes_{\mathbb{Z}}\mathbb{Q}$ is generated by classes in the form of $\mathrm{Ind}^{\overline{C}}_{\mathrm{Gal}(E/Q)} A$, where $\overline{C}$ runs over all cyclic subgroups of $\mathrm{Gal}(E/Q)$ of order prime to ℓ and A runs over classes of $K_0'(\mathbb{F}_\ell[\overline{C}])$. For such $\overline{C}$ and A, we denote by C the full preimage of $\overline{C}$ in $G=\mathrm{Gal}(k_S/Q)$, and then by Corollary 7.5 and $\mathrm{Ind}^{\overline{C}}_{\mathrm{Gal}(E/Q)} A=\mathrm{Ind}^C_G A$, we have that $\Theta\circ\varphi_{G,S}(\mathrm{Ind}^C_G A)=0$ if and only if $\Theta\circ\varphi_{C,S}(A)=0$. By setting G to be C, U to be $C\cap U$, Q to be $(k_S)^C$ and k to be $(k_S)^{C\cap U}$, we finally reduce the problem to the statement that we will prove in the rest of this section:

$$\Theta\circ\varphi_{G,S}(A)=0 \text{ for all } A\in\mathrm{Mod}_\ell(G) \text{ such that } k(A)/Q \text{ is a cyclic extension of } Q \text{ of order relatively prime to } \ell. \tag{7-18}$$

We let $K=k(A,\mu_\ell)$. So under the assumption in (7-18), we have that $\mathrm{Gal}(K/Q)$ is an abelian group of order relatively prime to ℓ, in which case the Hochschild–Serre spectral sequence for the group extension

$$1\to\mathrm{Gal}(k_S/K)\to\mathrm{Gal}(k_S/k)\to\mathrm{Gal}(K/k)\to 1$$

and the module A degenerates, and then for each $i\geq 0$ we have that

$$H^i(\mathrm{Gal}(k_S/k), A)\cong H^i(\mathrm{Gal}(k_S/K), A)^{\mathrm{Gal}(K/k)}. \tag{7-19}$$

We first consider the module $A=\mu_\ell$, then $K=k(\mu_\ell)$ and we let $\overline{G}=\mathrm{Gal}(K/Q)$. As $\ell\nmid\mathrm{Gal}(K/Q)$, in both the number field case (by [Neukirch et al. 2008, Corollary (8.7.3)]) and the function field case (by a standard argument using the divisor group), we have that

$$[\mathcal{O}_{K,S}^\times/\ell]=\Big[\bigoplus_{\mathfrak{P}\in S(K)}\mathbb{F}_\ell\Big]+[\mu_\ell]-[\mathbb{F}_\ell]$$

in $K_0'(\mathbb{F}_\ell[\overline{G}])$. Then since $[\mathrm{Cl}_S(K)[\ell]]=[\mathrm{Cl}_S(K)/\ell]$ as they are the kernel and the cokernel of the map $\mathrm{Cl}_S(K)\xrightarrow{\times\ell}\mathrm{Cl}_S(K)$, by Lemma 7.7 we have

$$\sum_{i=0}^{2}(-1)^i[H^i(\mathrm{Gal}(k_S/K),\mu_\ell)]=\Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)}\widehat{H}^0(K_\mathfrak{P},\mathbb{F}_\ell)\Big]-\Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)}H^0(K_\mathfrak{P},\mathbb{F}_\ell)\Big],\tag{7-20}$$

and hence $\varphi_{G,S}(\mu_\ell)=0$ follows easily by (7-19) and by the arguments in the first paragraph of this subsection. Thus $\Theta\circ\varphi_{G,S}(\mu_\ell)=0$.

For a general finite module $A\in\mathrm{Mod}_\ell(G)$, we again let $K=k(A,\mu_\ell)$ and $\overline{G}=\mathrm{Gal}(K/Q)$. We define

$$\chi:\mathrm{Mod}_\ell(\overline{G})\to K_0'(\mathbb{F}_\ell[\overline{G}]),\qquad M\mapsto\sum_{i=0}^{2}(-1)^i[H^i(\mathrm{Gal}(k_S/K),M)].$$

Because A and μ_ℓ are both trivial $\mathrm{Gal}(k_S/K)$-modules, the pairing

$$\mu_\ell\times\mathrm{Hom}(A',\mathbb{F}_\ell)\to\mathrm{Hom}(A',\mu_\ell)=A,\qquad(\zeta,f)\mapsto(x\mapsto\zeta^{f(x)})$$

defines $\overline{G}$-isomorphisms via the cup product

$$H^i(\mathrm{Gal}(k_S/K),\mu_\ell)\otimes_\mathbb{Z}\mathrm{Hom}(A',\mathbb{F}_\ell)\xrightarrow{\sim}H^i(\mathrm{Gal}(k_S/K),A).$$

So we have $\chi(A)=[A'^\vee]\chi(\mu_\ell)$, and hence by (7-20) we have

$$\chi(A)=[A'^\vee]\Big(\Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)}\widehat{H}^0(K_\mathfrak{P},\mathbb{F}_\ell)\Big]-\Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)}H^0(K_\mathfrak{P},\mathbb{F}_\ell)\Big]\Big).$$

If Q is a function field, then (7-18) follows immediately after taking the $\overline{G}$-invariants on both sides above.

For the rest of the proof we consider the number field case. Let $S_\infty^-(Q)$ be the set of archimedean places of Q lying below the imaginary places of K if $\ell=2$, and be the set $S_\infty(Q)$ if ℓ is odd. One can check by definition of $\widehat{H}^0$ that for any module $M\in\mathrm{Mod}_\ell(\overline{G})$ (for example, $M=A'$ and $M=\mathbb{F}_\ell$), we have

$$\Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)}\widehat{H}^0(K_\mathfrak{P},M)\Big]-\Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)}H^0(K_\mathfrak{P},M)\Big]=\sum_{v\in S_\infty^-(Q)}-[\mathrm{Ind}_{\overline{G}}^{\overline{G}_v}M],$$

where the group $\overline{G}_v$ is the decomposition subgroup $G_v(K/Q)$. Also, note that $(\mathrm{Ind}_{\overline{G}}^{\overline{G}_v}\mathbb{F}_\ell)\otimes_\mathbb{Z}M\cong\mathrm{Ind}_{\overline{G}}^{\overline{G}_v}M$ for any $M\in\mathrm{Mod}_\ell(\overline{G})$ and that

$$(\mathrm{Ind}_{\overline{G}}^{\overline{G}_v}M)^{\overline{G}}=H^0(\overline{G},\mathrm{Ind}_{\overline{G}}^{\overline{G}_v}M)=H^0(\overline{G}_v,M)=M^{\overline{G}_v}.$$

So we have

$$\begin{aligned}\Theta\circ\varphi_{G,\ell}(A) &= \#\Big(\sum_{i=0}^{2}(-1)^i[H^i(G_S(k),A)] - \Big[\bigoplus_{\mathfrak{p}\in S_\infty(k)}\widehat{H}^0(k_\mathfrak{p},A')\Big]^\vee + \Big[\bigoplus_{\mathfrak{p}\in S_\infty(k)}H^0(k_\mathfrak{p},A')\Big]^\vee\Big)^{\mathrm{Gal}(k/Q)}\\ &= \#\Big(\chi(A) - \Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)}\widehat{H}^0(K_\mathfrak{P},A')\Big]^\vee + \Big[\bigoplus_{\mathfrak{P}\in S_\infty(K)}H^0(K_\mathfrak{P},A')\Big]^\vee\Big)^{\overline{G}}\\ &= \sum_{v\in S_\infty^-(Q)}\#\big(-[A'^\vee][\mathrm{Ind}_{\overline{G}}^{\overline{G}_v}\mathbb{F}_\ell]+[\mathrm{Ind}_{\overline{G}}^{\overline{G}_v}A']^\vee\big)^{\overline{G}}\\ &= \sum_{v\in S_\infty^-(Q)}\#\big(-[\mathrm{Ind}_{\overline{G}}^{\overline{G}_v}A'^\vee]+[\mathrm{Ind}_{\overline{G}}^{\overline{G}_v}A']^\vee\big)^{\overline{G}}=0,\end{aligned}$$

completing the proof of Theorem 7.1. □

8. Definition and properties of $Б_S(k, A)$

Throughout this section, we assume that k/Q is a finite Galois extension of global fields, and that S is a k/Q-closed set of primes of k (not necessarily nonempty or containing S_∞).

Let $\mathfrak{p}$ be a prime of the global field k. We let $\mathcal{G}_\mathfrak{p}=\mathcal{G}_\mathfrak{p}(k)$ and $\mathcal{T}_\mathfrak{p}=\mathcal{T}_\mathfrak{p}(k)$. Recall that for a $\mathcal{G}_\mathfrak{p}$-module A of order not divisible by $\mathrm{char}(k)$, the unramified cohomology group is defined to be

$$H^i_{nr}(k_\mathfrak{p},A)=\mathrm{im}(H^i(\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p},A^{\mathcal{T}_\mathfrak{p}})\to H^i(k_\mathfrak{p},A)),$$

where the map is the inflation map. Then we consider the following homomorphism of cohomology groups:

$$\prod_{\mathfrak{p}\in S}H^1(k_\mathfrak{p},A)\times\prod_{\mathfrak{p}\notin S}H^1_{nr}(k_\mathfrak{p},A)\hookrightarrow\prod_{\mathfrak{p}}H^1(k_\mathfrak{p},A)\xrightarrow{\sim}\prod_{\mathfrak{p}}H^1(k_\mathfrak{p},A')^\vee\to H^1(k,A')^\vee. \tag{8-1}$$

The first map is the natural embedding of cohomology groups. The second map is an isomorphism because of the local Tate duality theorem [Neukirch et al. 2008, Theorems 7.2.6 and 7.2.17]. The last map is defined by the Pontryagin dual of the product of restriction map $H^1(k,A')\to H^1(k_\mathfrak{p},A')$ for each prime $\mathfrak{p}$ of k. In particular, the restriction of the composition of the last two maps in (8-1) to the restricted product is the map

$$\prod_{\mathfrak{p}}{}'H^1(k_\mathfrak{p},A)\to H^1(k,A')^\vee$$

used in the long exact sequence of Poitou–Tate [Neukirch et al. 2008, (8.6.10)(i)]. Here the restricted product $\prod'_\mathfrak{p}H^1(k_\mathfrak{p},A)$ is the subgroup of $\prod_\mathfrak{p}H^1(k_\mathfrak{p},A)$ consisting of all $(x_\mathfrak{p})$ such that $x_\mathfrak{p}\in H^1_{nr}(k_\mathfrak{p},A)$ for almost all $\mathfrak{p}$.

Definition 8.1. For a global field k, a set S of primes of k, and $A\in\mathrm{Mod}(G_k)$ of order not divisible by $\mathrm{char}(k)$, we define

$$Б_S(k,A)=\mathrm{coker}\Big(\prod_{\mathfrak{p}\in S}H^1(k_\mathfrak{p},A)\times\prod_{\mathfrak{p}\notin S}H^1_{nr}(k_\mathfrak{p},A)\to H^1(k,A')^\vee\Big),$$

where the map is the composition of maps in (8-1).

Remark 8.2. (1) When A is a finite G_Q-module and S is k/Q-closed, the maps in (8-1) are compatible with the conjugation action of $\mathrm{Gal}(k/Q)$ on cohomology groups, so $\text{Б}_S(k, A)$ is naturally a $\mathrm{Gal}(k/Q)$-module.

(2) Using the language of the Selmer groups, $\text{Б}_S(k, A)$ is the Pontryagin dual of the Selmer group of the Galois module A' consisting of elements of $H^1(k, A')$ that have images inside the subgroup

$$\prod_{\mathfrak{p}\in S} 1 \times \prod_{\mathfrak{p}\notin S} \ker(H^1(k_\mathfrak{p}, A') \to H^1_{nr}(k_\mathfrak{p}, A)^\vee) \subset \prod_{\mathfrak{p}} H^1(k_\mathfrak{p}, A').$$

under the product of local restriction maps.

Proposition 8.3. *If $A = \mathbb{F}_\ell$ is the trivial G_k-module with $\ell \neq \mathrm{char}(k)$, then $\text{Б}_S(k, \mathbb{F}_\ell)$ is the Pontryagin dual of the Kummer group*

$$V_S(k, \ell) = \ker\Big(k^\times/k^{\times\ell} \to \prod_{\mathfrak{p}\in S} k_\mathfrak{p}^\times/k_\mathfrak{p}^{\times\ell} \times \prod_{\mathfrak{p}\notin S} k_\mathfrak{p}^\times/U_\mathfrak{p}k_\mathfrak{p}^{\times\ell}\Big).$$

Proof. By the class field theory, we have

$$H^1(k, \mu_\ell) \cong k^\times/k^{\times\ell}, \quad H^1(k_\mathfrak{p}, \mu_\ell) \cong k_\mathfrak{p}^\times/k_\mathfrak{p}^{\times\ell}, \quad \text{and} \quad H^1_{nr}(k_\mathfrak{p}, \mathbb{F}_\ell)^\vee \cong k_\mathfrak{p}^\times/U_\mathfrak{p}k_\mathfrak{p}^{\times\ell}.$$

Then the proposition follows directly from Definition 8.1. □

The following lemma is a generalization of [Neukirch et al. 2008, Lemma(10.7.4)(i)]

Lemma 8.4. *Let k/Q be a finite Galois extension of global fields, $T \supseteq S$ be k/Q-closed sets of primes of k, and $A \in \mathrm{Mod}(\mathrm{Gal}(k_S/Q))$ be of order not divisible by $\mathrm{char}(k)$. Then we have the following exact sequence that is compatible with the conjugation by $\mathrm{Gal}(k/Q)$:*

$$H^1(G_S(k), A) \hookrightarrow H^1(G_T(k), A) \to \bigoplus_{\mathfrak{p}\in T\setminus S} H^1(\mathcal{T}_\mathfrak{p}(k), A)^{\mathcal{G}_\mathfrak{p}(k)} \to \text{Б}_S(k, A) \twoheadrightarrow \text{Б}_T(k, A).$$

Proof. We consider the commutative diagram

$$\begin{tikzcd}
 & Ш^1(k, A) \arrow[dl, dashed, hook'] \arrow[d, hook] & \\
H^1(G_S, A) \arrow[r, hook] & H^1(k, A) \arrow[r] \arrow[d] & H^1(G_{k_S}, A)^{G_S} \arrow[d, hook] \\
\prod'_{\mathfrak{p}\in S} H^1(k_\mathfrak{p}, A) \times \prod_{\mathfrak{p}\notin S} H^1_{nr}(k_\mathfrak{p}, A) \arrow[r, hook] \arrow[d] & \prod'_{\mathfrak{p}} H^1(k_\mathfrak{p}, A) \arrow[r, two heads] \arrow[d] & \bigoplus_{\mathfrak{p}\notin S} H^1(\mathcal{T}_\mathfrak{p}, A)^{\mathcal{G}_\mathfrak{p}} \\
H^1(k, A')^\vee \arrow[r, equal] \arrow[d, two heads] & H^1(k, A')^\vee \arrow[d, two heads] & \\
\text{Б}_S(k, A) & Ш^2(k, A') &
\end{tikzcd}$$

The exactnesses of the second row and the third row follow from the Hochschild–Serre spectral sequence, and last arrow in the third row is surjective because of the fact that $H^2_{nr}(\mathcal{G}_\mathfrak{p}, A) = 0$ as $\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p} \simeq \widehat{\mathbb{Z}}$ when $\mathfrak{p}$

is nonarchimedean and 1 when $\mathfrak{p}$ is archimedean. The exact sequence of the first column follows from the definition of $Б_S(k, A)$, and the second column follows from the long exact sequence of Poitou–Tate [Neukirch et al. 2008, (8.6.10)]. The right vertical map is injective since G_{k_S} is generated by the inertia groups of primes outside S.

We consider the map $H^1(k, A) \to \bigoplus_{\mathfrak{p}\notin S} H^1(\mathcal{T}_\mathfrak{p}, A)^{\mathcal{G}_\mathfrak{p}}$ in the diagonal of the square diagram on the right. Since $H^1(G_S, A)$ is the kernel of this map and $Ш^1(k, A)$ is contained in this kernel, the top dashed arrow exists and is injective. Then by diagram chasing, we have an exact sequence

$$Ш^1(k, A) \hookrightarrow H^1(G_S, A) \to \prod_{\mathfrak{p}\in S}{}' H^1(k_\mathfrak{p}, A) \times \prod_{\mathfrak{p}\notin S} H^1_{nr}(k_\mathfrak{p}, A) \to H^1(k, A')^\vee \twoheadrightarrow Б_S(k, A). \tag{8-2}$$

We apply the snake lemma to the diagram

$$\begin{tikzcd}
\prod'_{\mathfrak{p}\in S} H^1(k_\mathfrak{p}, A) \times \prod_{\mathfrak{p}\notin S} H^1_{nr}(k_\mathfrak{p}, A) \arrow[r] \arrow[d, hook] & H^1(k, A')^\vee \arrow[d, equal] \\
\prod'_{\mathfrak{p}\in T} H^1(k_\mathfrak{p}, A) \times \prod_{\mathfrak{p}\notin T} H^1_{nr}(k_\mathfrak{p}, A) \arrow[r] \arrow[d, two heads] & H^1(k, A')^\vee \\
\bigoplus_{\mathfrak{p}\in T\setminus S} H^1(\mathcal{T}_\mathfrak{p}, A)^{\mathcal{G}_\mathfrak{p}} &
\end{tikzcd}$$

where the horizontal map above is from (8-2), and we obtain the exact sequence

$$\frac{H^1(G_S, A)}{Ш^1(k, A)} \hookrightarrow \frac{H^1(G_T, A)}{Ш^1(k, A)} \to \bigoplus_{\mathfrak{p}\in T\setminus S} H^1(\mathcal{T}_\mathfrak{p}, A)^{\mathcal{G}_\mathfrak{p}} \to Б_S(k, A) \twoheadrightarrow Б_T(k, A).$$

Note that the inflation map $H^1(G_S, A) \hookrightarrow H^1(G_T, A)$ maps the submodule $Ш^1(k, A)$ to itself, because $Ш^1(k, A)$ is the kernel of $H^1(G_*, A) \to \prod_\mathfrak{p} H^1(k_\mathfrak{p}, A)$ for $* = S, T$. Therefore we proved the exact sequence in the lemma, and it is naturally compatible with the conjugation action by $\mathrm{Gal}(k/Q)$. □

Proposition 8.5. *Let k/Q be a finite Galois extension of global fields and S a k/Q-closed set of primes of k. Then for any $A \in \mathrm{Mod}(\mathrm{Gal}(k_S/Q))$ of order not divisible by $\mathrm{char}(k)$, we have the following inequality of elements in $K'_0(\mathrm{Gal}(k/Q))$:*

$$[Ш^2_S(k, A)] \le [Б_S(k, A)].$$

Proof. We consider the commutative diagram

$$\begin{tikzcd}
H^1(G_S, A) \arrow[r, hook] & H^1(k, A) \arrow[r] & H^1(k_S, A)^{G_S} \arrow[r, "\alpha"] & H^2(G_S, A) \arrow[r, "\beta"] \arrow[d, "\rho_S"] & H^2(k, A) \arrow[d, "\rho"] \\
 & & & \prod_{\mathfrak{p}\in S} H^2(k_\mathfrak{p}, A) \arrow[r, hook] & \prod_{\mathfrak{p}} H^2(k_\mathfrak{p}, A)
\end{tikzcd} \tag{8-3}$$

where the first row is the Hochschild–Serre long exact sequence of $1 \to G_{k_S} \to G_k \to G_S \to 1$. Because $\operatorname{im}\alpha = \ker\beta \subseteq \ker \rho\circ\beta = \ker\rho_S = Ш^2_S(k, A)$, we have an exact sequence

$$H^1(G_S, A) \hookrightarrow H^1(k, A) \to H^1(G_{k_S}, A)^{G_S} \to Ш^2_S(k, A) \twoheadrightarrow \beta(Ш^2_S(k, A)).$$

Comparing this exact sequence to Lemma 8.4 using $T = \{\text{all primes}\}$, we have

$$\begin{tikzcd}
H^1(k, A) \arrow[r] \arrow[d, equal] & H^1(k_S, A)^{G_S} \arrow[r] \arrow[d, hook] & Ш^2_S(k, A) \arrow[r, two heads] & \beta(Ш^2_S(k, A)) \\
H^1(k, A) \arrow[r] & \bigoplus_{\mathfrak{p}\notin S} H^1(\mathcal{T}_\mathfrak{p}, A)^{\mathcal{G}_\mathfrak{p}} \arrow[r] & Б_S(k, A) \arrow[r, two heads] & Б_{\{\text{all primes}\}}(k, A)
\end{tikzcd}$$

So by the vertical injection above, we have $\ker\beta \hookrightarrow N := \ker(Б_S(k, A) \to Б_{\{\text{all primes}\}}(k, A))$. By the diagram in (8-3), we have $\beta(\ker\rho_S) \subseteq \ker\rho$, which means $\beta(Ш^2_S(k, A)) \subseteq Ш^2(k, A)$. Also, note that by Definition 8.1 and the Poitou–Tate duality we have $Б_{\{\text{all primes}\}}(k, A) = Ш^1(k, A')^\vee \cong Ш^2(k, A)$. Then we consider the two short exact sequence

$$0 \to \ker\beta \to Ш^2_S(k, A) \to \beta(Ш^2_S(k, A)) \to 0,$$
$$0 \to N \to Б_S(k, A) \to Б_{\{\text{all primes}\}}(k, A) \to 0,$$

Because $\ker\beta \hookrightarrow N$, $\beta(Ш^2_S(k, A)) \hookrightarrow Б_{\{\text{all primes}\}}(k, A)$ and every map respects the conjugation action by $\mathrm{Gal}(k/Q)$, we have the desired inequality $[Ш^2_S(k, A)] \le [Б_S(k, A)]$. □

Remark 8.6. When $A = \mathbb{F}_\ell$ is the trivial module, then $Б_{\{\text{all primes}\}}(k, \mathbb{F}_\ell)$ vanishes [Neukirch et al. 2008, Proposition 9.1.12(ii)], so there is an embedding $Ш^2_S(k, \mathbb{F}_\ell) \hookrightarrow Б_S(k, \mathbb{F}_\ell)$. However, for an arbitrary A, Proposition 8.5 does not give such an embedding.

Lemma 8.7. *Let k be a global field and S a set of primes of k containing $S_\infty(k)$. Then for any $A \in \mathrm{Mod}_S(G_S(k))$ of order not divisible by* $\mathrm{char}(k)$, *we have* $Ш^1_S(k, A') \cong Б_S(k, A)^\vee$.

Proof. We consider the commutative diagram

$$\begin{tikzcd}
\prod_{\mathfrak{p}} H^1(k_\mathfrak{p}, A') \arrow[r] \arrow[d, "\sim"] & \prod_{\mathfrak{p}\in S} H^1(k_\mathfrak{p}, A') \times \prod_{\mathfrak{p}\notin S} H^1(\mathcal{T}_\mathfrak{p}, A')^{\mathcal{G}_\mathfrak{p}} \arrow[d, "\sim"] \\
\prod_{\mathfrak{p}} H^1(k_\mathfrak{p}, A)^\vee \arrow[r] & \prod_{\mathfrak{p}\in S} H^1(k_\mathfrak{p}, A)^\vee \times \prod_{\mathfrak{p}\notin S} H^1_{nr}(k_\mathfrak{p}, A)^\vee
\end{tikzcd}$$

where the two vertical arrows are isomorphisms by the Tate local duality theorem and its consequence that $H^1(\mathcal{T}_\mathfrak{p}, A')^{\mathcal{G}_\mathfrak{p}} \xrightarrow{\sim} H^1_{nr}(k_\mathfrak{p}, A)^\vee$ when A is unramified at $\mathfrak{p}$ and $\#\mathrm{tor}(A)$ is prime to the characteristic of the residue field of $k_{\mathfrak{p}}$ (see the proof of [Neukirch et al. 2008, Theorem 7.2.15]). Then by definition, we have

$$\begin{aligned}\text{Б}_S(k, A)^\vee &= \ker\Big(H^1(k, A') \to \prod_{\mathfrak{p}\in S} H^1(k_{\mathfrak{p}}, A)^\vee \times \prod_{\mathfrak{p}\notin S} H^1_{nr}(k_{\mathfrak{p}}, A)^\vee\Big) \\ &= \ker\Big(H^1(k, A') \to \prod_{\mathfrak{p}\in S} H^1(k_{\mathfrak{p}}, A') \times \prod_{\mathfrak{p}\notin S} H^1(\mathcal{T}_{\mathfrak{p}}, A')^{\mathcal{G}_p}\Big).\end{aligned}$$

So by applying the snake lemma to the commutative diagram

$$\begin{tikzcd}
\text{Ш}^1_S(k, A') \arrow[r, hook] & H^1(G_S, A') \arrow[r] \arrow[d, hook] & \prod_{\mathfrak{p}\in S} H^1(k_{\mathfrak{p}}, A') \arrow[d, hook] \\
\text{Б}_S(k, A)^\vee \arrow[r, hook] & H^1(k, A') \arrow[r] \arrow[d] & \prod_{\mathfrak{p}\in S} H^1(k_{\mathfrak{p}}, A') \times \prod_{\mathfrak{p}\notin S} H^1(\mathcal{T}_{\mathfrak{p}}, A')^{\mathcal{G}_{\mathfrak{p}}} \arrow[d, two heads] \\
 & H^1(k_S, A')^{G_S} \arrow[r, hook] & \prod_{\mathfrak{p}\notin S} H^1(\mathcal{T}_{\mathfrak{p}}, A')^{\mathcal{G}_{\mathfrak{p}}}
\end{tikzcd}$$

we obtain the desired isomorphism $\text{Ш}^1_S(k, A') \xrightarrow{\sim} \text{Б}_S(k, A)^\vee$. ☐

Corollary 8.8. *For any set S of primes of a global field k and any $A \in \mathrm{Mod}(G_S(k))$ of order not divisible by* $\mathrm{char}(k)$, *we have that $\text{Б}_S(k, A)$ is finite.*

Proof. Define $T = S \cup S_\infty(k) \cup S_{|A|}(k)$. By applying Lemma 8.4, we have

$$\bigoplus_{\mathfrak{p}\in T\setminus S} H^1(\mathcal{T}_{\mathfrak{p}}, A)^{\mathcal{G}_{\mathfrak{p}}} \to \text{Б}_S(k, A) \twoheadrightarrow \text{Б}_T(k, A). \tag{8-4}$$

Since $A \in \mathrm{Mod}_T(G_T)$, by Lemma 8.7 and [Neukirch et al. 2008, Theorem 8.6.4], we have that $\text{Б}_T(k, A)^\vee \cong \text{Ш}^1_T(k, A')$ is finite. Also note that $H^1(k_{\mathfrak{p}}, A)$ is finite [Neukirch et al. 2008, Theorem 7.1.8(iv)] and $H^1(\mathcal{T}_{\mathfrak{p}}, A)^{\mathcal{G}_{\mathfrak{p}}}$ is a quotient of $H^1(k_{\mathfrak{p}}, A)$. Thus, the direct product $\prod_{\mathfrak{p}\in T\setminus S} H^1(\mathcal{T}_{\mathfrak{p}}, A)^{\mathcal{G}_{\mathfrak{p}}}$ is finite, and hence the corollary follows by (8-4). ☐

9. Determination of $\delta_{k/Q,S}(A)$

Definition 9.1. Let k/Q be a finite Galois extension of global fields, S a finite k/Q-closed set of primes of k, $\ell \neq \mathrm{char}(k)$ a prime integer not dividing $[k : Q]$, and $A \in \mathrm{Mod}_\ell(\mathrm{Gal}(k_S/Q))$. We define

$$\delta_{k/Q,S}(A) = \dim_{\mathbb{F}_\ell} H^2(G_S(k), A)^{\mathrm{Gal}(k/Q)} - \dim_{\mathbb{F}_\ell} H^1(G_S(k), A)^{\mathrm{Gal}(k/Q)}.$$

We will use the notation and assumption in Definition 9.1 throughout this section. When $\ell \in \mathbb{N}(S)$ and $S_\infty(k) \subset S$, by Theorem 7.1, we have our first case for which $\delta_{k/Q,S}(A)$ can be determined.

Proposition 9.2. *Assume $\ell \in \mathbb{N}(S)$ and $S \supset S_\infty(k)$ is nonempty. Then*

$$\delta_{k/Q,S}(A) = \sum_{v\in S_\infty(Q)} \big(\dim_{\mathbb{F}_\ell} \widehat{H}^0(Q_v, A') - \dim_{\mathbb{F}_\ell} H^0(Q_v, A')\big) - \dim_{\mathbb{F}_\ell} A^{\mathrm{Gal}(k_S/Q)}.$$

So in this section, we will consider the cases that are not covered by Proposition 9.2. In Section 9.1, we will deal with the case that Q is a function field and $S=\varnothing$, and obtain a formula for $\delta_{k/Q,\varnothing}(A)$ (Proposition 9.3). Then in Section 9.2, we will give an upper bound of $\delta_{k/Q,S}(A)$ when k is a number field with $S_\ell(k)\cup S_\infty(k)\not\subset S$ (Proposition 9.4). In Section 9.2, we will prove Theorem 1.2 by setting $k=Q$ and applying Propositions 9.2 and 9.4.

9.1. *Function field case with S = ∅.*

Proposition 9.3. *Assume k and Q are function fields. Let $g=g(k)$ be the genus of the curve corresponding to k.*

(1) *If $g=0$, then $\delta_{k/Q,\varnothing}(A)=-\dim_{\mathbb{F}_\ell} A_{\mathrm{Gal}(k_\varnothing/Q)}$.*

(2) *If $g>0$, then $\delta_{k/Q,\varnothing}(A)=\dim_{\mathbb{F}_\ell}(A')^{\mathrm{Gal}(k_\varnothing/Q)}-\dim_{\mathbb{F}_\ell} A^{\mathrm{Gal}(k_\varnothing/Q)}$.*

Proof. When $g=0$, we have $G_\varnothing(k)\cong\widehat{\mathbb{Z}}$ by [Neukirch et al. 2008, Corollary 10.1.3(i)]. So $H^2(G_\varnothing,A)=0$ as $\widehat{\mathbb{Z}}$ has cohomological dimension 1 and $H^1(G_\varnothing,A)\cong A_{G_\varnothing}$ by [Neukirch et al. 2008, Proposition 1.7.7(i)]. Then we see that

$$\delta_{k/Q,\varnothing}(A)=-\dim_{\mathbb{F}_\ell}(A_{G_\varnothing})^{\mathrm{Gal}(k/Q)}=-\dim_{\mathbb{F}_\ell}(A_{G_\varnothing})_{\mathrm{Gal}(k/Q)}=-\dim_{\mathbb{F}_\ell} A_{\mathrm{Gal}(k_\varnothing/Q)},$$

where the second equality uses $\ell\nmid[k:Q]$, so we proved (1).

For the rest, we assume $g>0$. Let κ be the finite field of constants of k and $C=\mathrm{Gal}(\bar\kappa/\kappa)\cong\widehat{\mathbb{Z}}$. Then there exists an exact sequence, for each j,

$$H^j(G_\varnothing(k\bar\kappa),A)^C\hookrightarrow H^j(G_\varnothing(k\bar\kappa),A)\xrightarrow{\mathrm{Frob}-1}H^j(G_\varnothing(k\bar\kappa),A)\twoheadrightarrow H^j(G_\varnothing(k\bar\kappa),A)_C,\tag{9-1}$$

where Frob is the Frobenius action on the cohomology groups defined by conjugation. Note that $\mathrm{Gal}(k\bar\kappa/Q)$ acts on cohomology groups in (9-1), and

$$1\to C\cong\mathrm{Gal}(k\bar\kappa/k)\to\mathrm{Gal}(k\bar\kappa/Q)\to\mathrm{Gal}(k/Q)\to 1$$

is a central group extension because $\mathrm{Gal}(k/Q)$ acts trivially on the generator Frob of C. So the map $\mathrm{Frob}-1$ in (9-1) respects the $\mathrm{Gal}(k\bar\kappa/Q)$ actions. It follows that $H^j(G_\varnothing(k\bar\kappa),A)^C$ and $H^j(G_\varnothing(k\bar\kappa),A)_C$ are in the same class in $K_0'(\mathbb{F}_\ell[\mathrm{Gal}(k\bar\kappa/Q)])$, and hence they are in the same class in $K_0'(\mathbb{F}_\ell[\mathrm{Gal}(k/Q)])$. Because $\ell\nmid[k:Q]$ implies $\mathbb{F}_\ell[\mathrm{Gal}(k/Q)]$ is semisimple, we have

$$H^j(G_\varnothing(k\bar\kappa),A)^C\simeq H^j(G_\varnothing(k\bar\kappa),A)_C\tag{9-2}$$

as $\mathrm{Gal}(k/Q)$-modules. Therefore, as C is cyclic,

$$\begin{aligned}H^1(C,H^j(G_\varnothing(k\bar\kappa),A))&\simeq\widehat{H}^{-1}(C,H^j(G_\varnothing(k\bar\kappa),A))\simeq H^j(G_\varnothing(k\bar\kappa),A)_C\\&\simeq H^0(C,H^j(G_\varnothing(k\bar\kappa),A))\end{aligned}\tag{9-3}$$

as $\mathrm{Gal}(k/Q)$-modules. Then we consider the Hochschild–Serre spectral sequence

$$E_2^{ij}=H^i(C,H^j(G_\varnothing(k\bar\kappa),A))\Rightarrow H^{i+j}(G_\varnothing(k),A).$$

As C has cohomological dimension 1, $E_2^{ij} = 0$ for each $i > 1$, and hence by [Neukirch et al. 2008, Lemma 2.1.3(ii)] we have the following exact sequence for every $j \geq 1$:

$$H^1(C, H^{j-1}(G_\varnothing(k\bar{\kappa}), A)) \hookrightarrow H^j(G_\varnothing(k), A) \twoheadrightarrow H^0(C, H^j(G_\varnothing(k\bar{\kappa}), A)). \tag{9-4}$$

Note that $G_\varnothing(k)$ has strict cohomological ℓ-dimension 3 by [Neukirch et al. 2008, Corollary 10.1.3(ii)]. Then as $\ell \nmid [k : Q]$, taking $\mathrm{Gal}(k/Q)$-invariants is exact on (9-4), and by computing the alternating sum of (9-4) for $j = 1, 2, 3$ and applying (9-3), we have

$$\begin{aligned}\sum_{j=1}^{3}(-1)^j \dim_{\mathbb{F}_\ell} H^j(G_\varnothing(k), A)^{\mathrm{Gal}(k/Q)} &= -\dim_{\mathbb{F}_\ell} H^1(C, H^0(G_\varnothing(k\bar{\kappa}), A))^{\mathrm{Gal}(k/Q)} \\ &= -\dim_{\mathbb{F}_\ell} H^0(C, H^0(G_\varnothing(k\bar{\kappa}), A))^{\mathrm{Gal}(k/Q)} \\ &= -\dim_{\mathbb{F}_\ell} H^0(\mathrm{Gal}(k_\varnothing/Q), A).\end{aligned}$$

Also, [Neukirch et al. 2008, Corollary 10.1.3(ii)] shows that $G_\varnothing(k)$ is a Poincaré group of dimension 3 with dualizing module μ, so we have a functorial isomorphism $H^3(G_\varnothing(k), A) \cong H^0(G_\varnothing(k), A')^\vee$. Combining the above computations, we see that

$$\begin{aligned}\delta_{k/Q,\varnothing}(A) &= \dim_{\mathbb{F}_\ell}(H^0(G_\varnothing(k), A')^\vee)^{\mathrm{Gal}(k/Q)} - \dim_{\mathbb{F}_\ell} H^0(\mathrm{Gal}(k_\varnothing/Q), A) \\ &= \dim_{\mathbb{F}_\ell} H^0(G_\varnothing(k), A')^{\mathrm{Gal}(k/Q)} - \dim_{\mathbb{F}_\ell} H^0(\mathrm{Gal}(k_\varnothing/Q), A) \\ &= \dim_{\mathbb{F}_\ell}(A')^{\mathrm{Gal}(k_\varnothing/Q)} - \dim_{\mathbb{F}_\ell} A^{\mathrm{Gal}(k_\varnothing/Q)},\end{aligned}$$

where the second equality is because the $\mathrm{Gal}(k/Q)$-invariants of M and $M^\vee$ have the same dimension for any $M \in \mathrm{Mod}_\ell(\mathrm{Gal}(k/Q))$. □

9.2. *Number field case with $S_\ell \cup S_\infty \not\subset S$.*

Proposition 9.4. *Assume k and Q are number fields. Let $T = S \cup S_\ell(k) \cup S_\infty(k)$. Then*

$$\delta_{k/Q,S}(A) \leq \log_\ell(\chi_{k/Q,T}(A)) + \dim_{\mathbb{F}_\ell}(A')^{\mathrm{Gal}(k_T/Q)} - \dim_{\mathbb{F}_\ell} A^{\mathrm{Gal}(k_S/Q)} + \epsilon_{k/Q,S}(A),$$

where $\epsilon_{k/Q,S}(A) = -\sum_{v\in I} \log_\ell \|\#A\|_v$[1] *with*

$$I = \{v \in S_\ell(Q) \text{ such that } S_v(k) \not\subset S\}.$$

In particular, when $S = \varnothing$, the equality holds if and only if $Ш^2_\varnothing(k, A)$ and $Б_\varnothing(k, A)$ are in the same class of $K'_0(\mathbb{F}_\ell[\mathrm{Gal}(k/Q)])$.

Remark 9.5. For an arbitrary S, the equality holds if and only if the equalities in (9-5) hold. So when $S \neq \varnothing$, if the equality holds then $[Ш^2_\varnothing(k, A)] = [Б_\varnothing(k, A)]$, but the converse is false.

Proof. First of all, by definition of $Ш^2_S$ and Proposition 8.5, we have the following inequalities of elements in $K'_0(\mathbb{F}_\ell[\mathrm{Gal}(k/Q)])$:

$$[H^2(G_S, A)] \leq [Ш^2_S(k, A)] + \Big[\bigoplus_{\mathfrak{p}\in S} H^2(k_\mathfrak{p}, A)\Big] \leq [Б_S(k, A)] + \Big[\bigoplus_{\mathfrak{p}\in S} H^2(k_\mathfrak{p}, A)\Big]. \tag{9-5}$$

[1] $\|x\|_v = q^{-\mathrm{ord}_v(x)}$ where q is the cardinality of the residue field of v and ord_v is the additive valuation with value group $\mathbb{Z}$.

By applying Lemma 8.4, we have

$$[\text{Б}_S(k, A)] - [H^1(G_S, A)] = [\text{Б}_T(k, A)] - [H^1(G_T, A)] + \Big[\bigoplus_{\mathfrak{p}\in T\setminus S} H^1(\mathcal{T}_{\mathfrak{p}}, A)^{\mathcal{G}_{\mathfrak{p}}}\Big]. \tag{9-6}$$

Since T contains $S_\ell(k) \cup S_\infty(k)$, it follows that $[\text{Б}_T(k, A)] = [\text{Ш}^2_T(k, A)]$ by Lemma 8.7 and the Poitou–Tate duality theorem. Also, note that the long exact sequence of Poitou–Tate [Neukirch et al. 2008, (8.6.10)] induces an exact sequence

$$\text{Ш}^2_T(k, A) \hookrightarrow H^2(G_T, A) \to \bigoplus_{\mathfrak{p}\in T} H^2(k_{\mathfrak{p}}, A) \twoheadrightarrow H^0(G_T, A')^\vee.$$

Therefore

$$[\text{Б}_T(k, A)] = [H^2(G_T, A)] + [H^0(G_T, A')^\vee] - \Big[\bigoplus_{\mathfrak{p}\in T} H^2(k_{\mathfrak{p}}, A)\Big]. \tag{9-7}$$

Combining (9-5), (9-6) and (9-7), we have

$$\begin{aligned}&[H^2(G_S, A)] - [H^1(G_S, A)]\\ &\quad\le [H^2(G_T, A)] - [H^1(G_T, A)] + [H^0(G_T, A')^\vee] + \Big[\bigoplus_{\mathfrak{p}\in T\setminus S} H^1(\mathcal{T}_{\mathfrak{p}}, A)^{\mathcal{G}_{\mathfrak{p}}}\Big] - \Big[\bigoplus_{\mathfrak{p}\in T\setminus S} H^2(k_{\mathfrak{p}}, A)\Big].\end{aligned}$$

The dimension of $\mathrm{Gal}(k/Q)$-invariants of the left-hand side above is $\delta_{k/Q,S}(A)$. On the right-hand side, the dimension of $\mathrm{Gal}(k/Q)$-invariants of $[H^2(G_T, A)] - [H^1(G_T, A)]$ is

$$\log_\ell(\chi_{k/Q,T}(A)) - \dim_{\mathbb{F}_\ell} H^0(G_T, A)^{\mathrm{Gal}(k/Q)} = \log_\ell(\chi_{k/Q,T}(A)) - \dim_{\mathbb{F}_\ell} A^{\mathrm{Gal}(k_S/Q)}$$

by the definition of $\chi_{k/Q,T}$ and the assumption that A is a $\mathrm{Gal}(k_S/Q)$-module. Also,

$$\dim_{\mathbb{F}_\ell}(H^0(G_T, A')^\vee)^{\mathrm{Gal}(k/Q)} = \dim_{\mathbb{F}_\ell} H^0(G_T, A')^{\mathrm{Gal}(k/Q)} = \dim_{\mathbb{F}_\ell}(A')^{\mathrm{Gal}(k_T/Q)}.$$

So to prove the inequality in the proposition, it suffices to show

$$\epsilon_{k/Q,S}(A) = \dim_{\mathbb{F}_\ell}\Big(\bigoplus_{\mathfrak{p}\in T\setminus S} H^1(\mathcal{T}_{\mathfrak{p}}, A)^{\mathcal{G}_{\mathfrak{p}}}\Big)^{\mathrm{Gal}(k/Q)} - \dim_{\mathbb{F}_\ell}\Big(\bigoplus_{\mathfrak{p}\in T\setminus S} H^2(k_{\mathfrak{p}}, A)\Big)^{\mathrm{Gal}(k/Q)}. \tag{9-8}$$

We first consider $v \in S_\infty(Q)$ such that $S_v(k) \not\subset S$. Since $\mathcal{T}_{\mathfrak{p}}(k) = \mathcal{G}_{\mathfrak{p}}(k)$, we know that $H^1(\mathcal{T}_{\mathfrak{p}}, A)^{\mathcal{G}_{\mathfrak{p}}} = H^1(k_{\mathfrak{p}}, A)$ for each $\mathfrak{p} \in S_v(k)$. For $i = 1, 2$, we have

$$\Big(\bigoplus_{\mathfrak{p}\in S_v(k)} H^i(k_{\mathfrak{p}}, A)\Big)^{\mathrm{Gal}(k/Q)} = \big(\mathrm{Ind}_{\mathrm{Gal}(k/Q)}^{\mathrm{Gal}_{\mathfrak{p}}(k/Q)} H^i(k_{\mathfrak{p}}, A)\big)^{\mathrm{Gal}(k/Q)} = H^i(k_{\mathfrak{p}}, A)^{\mathrm{Gal}_{\mathfrak{p}}(k/Q)} = H^i(Q_v, A),$$

where the second equality uses Shapiro's lemma and the last one follows by the assumption that $\ell \nmid [k : Q]$ and the same argument for (7-15). Therefore

$$\begin{aligned}&\dim_{\mathbb{F}_\ell}\Big(\bigoplus_{\mathfrak{p}\in S_v(k)} H^1(\mathcal{T}_{\mathfrak{p}}, A)^{\mathcal{G}_{\mathfrak{p}}}\Big)^{\mathrm{Gal}(k/Q)} - \dim_{\mathbb{F}_\ell}\Big(\bigoplus_{\mathfrak{p}\in S_v(k)} H^2(k_{\mathfrak{p}}, A)\Big)^{\mathrm{Gal}(k/Q)}\\ &\qquad = \dim_{\mathbb{F}_\ell} H^1(Q_v, A) - \dim_{\mathbb{F}_\ell} H^2(Q_v, A),\end{aligned}$$

which always equals 0 since Q_v is a cyclic group [Neukirch et al. 2008, Proposition 1.7.6].

Finally, we consider $v \in S_\ell(Q)$ such that $S_v(k) \not\subset S$. Because $\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}$ is procyclic, we have that $H^1(\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}, A) \cong A_{\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}}$; and by the same argument from (9-1) to (9-2), we have an isomorphism $H^1(\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}, A) \simeq A^{\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}} = A^{\mathcal{G}_\mathfrak{p}}$ that is compatible with the conjugation action by $\mathrm{Gal}_\mathfrak{p}(k/Q)$. So we see that

$$\begin{aligned}\dim_{\mathbb{F}_\ell}\Bigl(\bigoplus_{\mathfrak{p}\in S_\mathfrak{p}(k)} H^1(\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}, A)\Bigr)^{\mathrm{Gal}(k/Q)} &= \dim_{\mathbb{F}_\ell}\bigl(\mathrm{Ind}_{\mathrm{Gal}(k/Q)}^{\mathrm{Gal}_\mathfrak{p}(k/Q)} H^1(\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}, A)\bigr)^{\mathrm{Gal}(k/Q)}\\ &= \dim_{\mathbb{F}_\ell} H^1(\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}, A)^{\mathrm{Gal}_\mathfrak{p}(k/Q)}\\ &= \dim_{\mathbb{F}_\ell} A^{\mathcal{G}_\mathfrak{p}(Q)}. \end{aligned} \tag{9-9}$$

Therefore, we compute

$$\begin{aligned}&\dim_{\mathbb{F}_\ell}\Bigl(\bigoplus_{\mathfrak{p}\in S_v(k)} H^1(\mathcal{T}_\mathfrak{p}, A)^{\mathcal{G}_\mathfrak{p}}\Bigr)^{\mathrm{Gal}(k/Q)} - \dim_{\mathbb{F}_\ell}\Bigl(\bigoplus_{\mathfrak{p}\in S_v(k)} H^2(k_\mathfrak{p}, A)\Bigr)^{\mathrm{Gal}(k/Q)}\\ &\qquad= \dim_{\mathbb{F}_\ell}\Bigl(\bigoplus_{\mathfrak{p}\in S_v(k)} H^1(k_\mathfrak{p}, A)\Bigr)^{\mathrm{Gal}(k/Q)} - \dim_{\mathbb{F}_\ell}\Bigl(\bigoplus_{\mathfrak{p}\in S_v(k)} H^2(k_\mathfrak{p}, A)\Bigr)^{\mathrm{Gal}(k/Q)} - \dim_{\mathbb{F}_\ell} A^{\mathcal{G}_v(Q)}\\ &\qquad= \dim_{\mathbb{F}_\ell} H^1(k_\mathfrak{p}, A)^{\mathrm{Gal}_\mathfrak{p}(k/Q)} - \dim_{\mathbb{F}_\ell} H^2(k_\mathfrak{p}, A)^{\mathrm{Gal}_\mathfrak{p}(k/Q)} - \dim_{\mathbb{F}_\ell} A^{\mathcal{G}_v(Q)}\\ &\qquad= \dim_{\mathbb{F}_\ell} H^1(Q_v, A) - \dim_{\mathbb{F}_\ell} H^2(Q_v, A) - \dim_{\mathbb{F}_\ell} A^{\mathcal{G}_v(Q)}\\ &\qquad= -\log_\ell \|\#A\|_v.\end{aligned}$$

The first equality above uses (9-9) and the exact sequence $H^1(\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}, A) \hookrightarrow H^1(k_\mathfrak{p}, A) \twoheadrightarrow H^1(\mathcal{T}_\mathfrak{p}, A)^{\mathcal{G}_\mathfrak{p}}$, the second uses the Shapiro's lemma, the third uses the assumption that $\ell \nmid [k : Q]$, and the last uses the Tate's local Euler–Poincaré characteristic formula [Neukirch et al. 2008, Theorem 7.3.1]. We have proved (9-8).

When $S = \varnothing$, we have $Ш^2_\varnothing(k, A) = H^2(G_\varnothing, A)$, so the first inequality in (9-5) is an equality, and hence we have the last statement in the proposition. □

Proof of Theorem 1.2. We apply the above results to the case $k = Q$. Let $G = G_S(k)$. Let A be a finite simple G-module and ℓ denote the exponent of A. Since $\widehat{H}^0(k_\mathfrak{p}, A')$ is naturally a quotient of $H^0(k_\mathfrak{p}, A')$ for each $\mathfrak{p} \in S_\infty(k)$, we have $\log_\ell \chi_{k/k,T}(A) \le 0$ for $T = S \cup S_\ell(k) \cup S_\infty(k)$. When $S \supset S_\ell(k) \cup S_\infty(k)$, applying Proposition 9.2 to the case $k = Q$, we have $\delta_{k/k,S}(A) \le 0$. It follows by definition of $\epsilon_{k/k,S}(A)$ in Proposition 9.4 that $\epsilon_{k/k,S}(A) \le [k : \mathbb{Q}] \dim_{\mathbb{F}_\ell} A$. Also, note that, when $S \not\supset S_\ell(k) \cup S_\infty(k)$ and $A \not\simeq \mu_\ell$, we have $\dim_{\mathbb{F}_\ell}(A')^{G_T(k)} - \dim_{\mathbb{F}_\ell} A^{G_S(k)} \le 0$. When $S \not\supset S_\ell(k) \cup S_\infty(k)$ and $A = \mu_\ell$ (assume $\mu_\ell \not\simeq \mathbb{F}_\ell$), we have $\dim_{\mathbb{F}_\ell}(A')^{G_T(k)} - \dim_{\mathbb{F}_\ell} A^{G_S(k)} = 1$ but $\log_\ell \chi_{k/k,T}(A) \le -1$. So in both cases, Proposition 9.4 shows that $\delta_{k/k,S}(A) \le [k : \mathbb{Q}] \dim_{\mathbb{F}_\ell} A$, and hence the theorem follows by Proposition 3.7. □

10. Proof of Theorem 1.1

In this section, we will prove Theorem 1.1. We assume that Γ is a nontrivial finite group, $Q = \mathbb{Q}$ or $\mathbb{F}_q(t)$ with $\gcd(q, |\Gamma|) = 1$, and let k/Q be a Galois extension with $\mathrm{Gal}(k/Q) \simeq \Gamma$. By Theorem 6.4, $G_\varnothing(k)^{\mathcal{C}}$ is a finite Γ-group when $\mathcal{C}$ is finite, so for a sufficiently large n there is a Γ-presentation $F_n(\Gamma) \to G_\varnothing(k)^{\mathcal{C}}$. In Section 10.1, we construct a finitely generated Γ-quotient G of $G_\varnothing(k)$ such that $G^{\mathcal{C}} \simeq G_\varnothing(k)^{\mathcal{C}}$ as Γ-groups. With the help of the group G, we employ the cohomology of $G_\varnothing$ to compute the multiplicities in a pro-$\mathcal{C}$ admissible Γ-presentation of $G_\varnothing(k)^{\mathcal{C}}$. In Section 10.2, we compute the multiplicities $m_{\mathrm{ad}}^{\mathcal{C}}(n, \Gamma, G_\varnothing(k)^{\mathcal{C}}, A)$, and then compute the multiplicities $m_{\mathrm{ad}}^{\mathcal{C}}(n, \Gamma, G_{\varnothing,\infty}(k)^{\mathcal{C}}, A)$ for a finite simple $G_{\varnothing,\infty}(k)^{\mathcal{C}} \rtimes \Gamma$-module A. Using these multiplicities, finally in Section 10.3, we show that the kernel of a pro-$\mathcal{C}$ admissible Γ-presentation $\mathcal{F}_n(\Gamma)^{\mathcal{C}} \to G_{\varnothing,\infty}(k)^{\mathcal{C}}$ can be normally generated by elements $\{r^{-1}\gamma(r)\}_{r\in X,\gamma\in\Gamma}$ with X a subset of $\mathcal{F}_n(\Gamma)$ of cardinality $n+1$.

Note that in Theorem 1.1, k/Q is assumed to be split completely at ∞, and the Γ-groups in $\mathcal{C}$ are of order prime to $|\mu(Q)|$, $|\Gamma|$ and $\mathrm{char}(Q)$. However, in the proof, we do not use these assumptions until Section 10.2. So right now, we only assume that k/Q is a Galois field extension with $\mathrm{Gal}(k/Q) \simeq \Gamma$ and that $\mathcal{C}$ is a finite set of isomorphism classes of finite Γ-groups of order prime to $|\Gamma|$.

10.1. ***Construction of a specific finitely generated quotient of $G_\varnothing(k)$.*** Because $G_\varnothing(k)^{\mathcal{C}}$ is finite, when n is sufficiently large, there exists a Γ-equivariant surjection $\pi : F_n(\Gamma) \to G_\varnothing(k)^{\mathcal{C}}$, where $F_n(\Gamma)$ is the free profinite Γ-group defined in Section 3. Then π factors through $\pi^{\mathcal{C}} : F_n(\Gamma)^{\mathcal{C}} \to G_\varnothing(k)^{\mathcal{C}}$ as defined in Definition 5.2.

Lemma 10.1. *Use the notation above. If A is a finite simple $G_\varnothing(k)^{\mathcal{C}} \rtimes \Gamma$-module with*

$$m(\pi^{\mathcal{C}}, \Gamma, G_\varnothing(k)^{\mathcal{C}}, A) > 0,$$

then $A \rtimes G_\varnothing(k)^{\mathcal{C}} \in \overline{\mathcal{C}}$.

Proof. We denote $G_\varnothing(k)^{\mathcal{C}}$ by G_0 for convenience purposes. If $m(\pi^{\mathcal{C}}, \Gamma, G_0, A) > 0$, then there is a Γ-group extension

$$1 \to A \to H \xrightarrow{\varpi} G_0 \to 1$$

such that H is a quotient of $F_n^{\mathcal{C}}$, and so $H \in \overline{\mathcal{C}}$. We let E be the fiber product $H \times_{G_0} H$ defined by ϖ, i.e., $E = \{(x, y) \in H \times H \mid \varpi(x) = \varpi(y)\}$. Note that E is a subgroup of $H \times H$, so is in $\overline{\mathcal{C}}$. There is a natural diagonal embedding $H \hookrightarrow E$ mapping x to (x, x), and a normal subgroup $\{(a, 1) \mid a \in A\}$ of E that is isomorphic to A. From this, one can check that the diagonal subgroup H and the normal subgroup A are disjoint and they generate E, so $E \simeq A \rtimes H$ where the H action on A factors through $\varpi(H) = G_0$. So by taking the quotient map ϖ on the subgroup H of E, we obtain that $A \rtimes G_0$ is a quotient of E, and therefore we proved the lemma. $\square$

Now we fix a finite simple $G_\varnothing(k)^{\mathcal{C}} \rtimes \Gamma$-module A with $m(\pi^{\mathcal{C}}, \Gamma, G_\varnothing(k)^{\mathcal{C}}, A) > 0$, and construct the desired quotient of $G_\varnothing(k)$ for A. We let φ_0 denote the quotient map $G_\varnothing(k) \to G_\varnothing(k)^{\mathcal{C}}$, and again let G_0 denote $G_\varnothing(k)^{\mathcal{C}}$. We define G_1 to be the quotient of $G_\varnothing(k)$ satisfying the following Γ-group extension:

$$1 \to A^{m(\varphi_0,\Gamma,G_0,A)} \to G_1 \xrightarrow{\varpi_0} G_0 \to 1. \tag{10-1}$$

By definition of the multiplicities, G_1 is well-defined. Since G_1 is a quotient of $G_\varnothing(k)$, we have that $G_1^{\mathcal{C}}$ is exactly G_0. Then we claim that the extension (10-1) is "completely nonsplit" (that is, if a subgroup of G_1 maps surjectively onto G_0, then it has to be G_1 itself). Indeed, if it's not completely nonsplit, then G_1 has a Γ-quotient isomorphic to $A \rtimes G_0$, and hence by Lemma 10.1 we have $A \rtimes G_0 \in \overline{\mathcal{C}}$, which contradicts that $G_1^{\mathcal{C}} = G_0$.

Similarly, we define $G_2, G_3, \ldots$ to be the Γ-quotients of $G_\varnothing(k)$ inductively via

$$1 \to A^{m(\varphi_i,\Gamma,G_i,A)} \to G_{i+1} \xrightarrow{\varpi_i} G_i \to 1,$$

where the map φ_i is the quotient map $G_\varnothing(k) \to G_i$. Using the argument in the previous paragraph, we see that each of these group extensions is completely nonsplit, and $G_i^{\mathcal{C}} = G_0$ for each i. Then we take the inverse limit

$$G := \varprojlim_i G_i.$$

Then the profinite group G is the maximal extension of G_0 in $G_\varnothing(k)$ that can be obtained via group extensions by A.

Lemma 10.2. (1) *A subset of G is a generator set if and only if its image in G_0 generates G_0.*

(2) *The map $\pi : F_n(\Gamma) \to G_0$ defined at the beginning of this subsection factors through G.*

(3) *Let φ be the natural quotient map $G_\varnothing(k) \to G$ defined by inverse limit of φ_i. Then*

$$\mathrm{Hom}_{G \rtimes \Gamma}((\ker \varphi)^{ab}, A) = 0.$$

Proof. The group extension $\varpi_i : G_{i+1} \to G_i$ is completely nonsplit, so any lift of a generator set of G_i is a generator set of G_{i+1}. So we have (1) by taking inverse limit, and then (2) follows.

Note that G acts on the abelianization $(\ker \varphi)^{ab}$ of $\ker \varphi$ by conjugation. Suppose that

$$\mathrm{Hom}_{G \rtimes \Gamma}((\ker \varphi)^{ab}, A) \neq 0.$$

Then it means that φ factors through a Γ-equivariant group extension H of G by a kernel A. However, G does not have such a group extension in $G_\varnothing(k)$ by definition. So we proved (3). □

10.2. *Determination of the multiplicity of A.* We continue to use notation and assumptions given previously in this section. In particular, we remind the reader that A is a fixed finite simple $G_\varnothing(k)^{\mathcal{C}} \rtimes \Gamma$-module where $\Gamma \simeq \mathrm{Gal}(k/Q)$, and G depends on A. The goal of this subsection is to compute the multiplicity of A in an admissible Γ-presentation of $G_{\varnothing,\infty}(k)^{\mathcal{C}}$. The Γ-group G plays a very important role in this computation.

Lemma 10.3. *Let ℓ be the exponent of A and assume that $\ell \neq \mathrm{char}(Q)$ is prime to $|\Gamma|$. Then*

$$\dim_{\mathbb{F}_\ell} H^2(G, A)^\Gamma - \dim_{\mathbb{F}_\ell} H^1(G, A)^\Gamma \leq \delta_{k/Q,\varnothing}(A).$$

Proof. We consider the Γ-equivariant short exact sequence

$$1 \to M \to G_\varnothing(k) \xrightarrow{\varphi} G \to 1.$$

By the Hochschild–Serre exact sequence, we have

$$0 \to H^1(G, A) \to H^1(G_\varnothing(k), A) \to H^1(M, A)^G \to H^2(G, A) \to H^2(G_\varnothing(k), A), \tag{10-2}$$

which is compatible with the conjugation action by Γ. Since M acts trivially on A, we see that $H^1(M, A)^{G \rtimes \Gamma} = \mathrm{Hom}_{G \rtimes \Gamma}(M^{ab}, A) = 0$ by Lemma 10.2(3). So by taking the Γ-invariants on (10-2) and computing the dimensions, we have that

$$\dim_{\mathbb{F}_\ell} H^2(G, A)^\Gamma - \dim_{\mathbb{F}_\ell} H^1(G, A)^\Gamma \leq \dim_{\mathbb{F}_\ell} H^2(G_\varnothing(k), A)^\Gamma - \dim_{\mathbb{F}_\ell} H^1(G_\varnothing(k), A)^\Gamma = \delta_{k/Q,\varnothing}(A). \quad \square$$

Starting from now, we assume that $\mathcal{C}$ is a finite set of isomorphism classes of finite Γ-groups all of whose orders are prime to $|\Gamma|$, char Q and $|\mu(Q)|$. Let $\widehat{\pi}$ denote the Γ-equivariant surjective map $F_n(\Gamma) \to G$ used in Lemma 10.2(2). Then the pro-$\mathcal{C}$ completion of $\widehat{\pi}$ is $\pi^{\mathcal{C}} : F_n^{\mathcal{C}} \twoheadrightarrow G_\varnothing(k)^{\mathcal{C}}$. If $Q = \mathbb{Q}$, then $G_\varnothing(k)^{\mathcal{C}}$ is exactly $G_{\varnothing,\infty}(k)^{\mathcal{C}}$. If Q is a function field, then $k_\varnothing/k$ is not split completely at primes over ∞. Instead, $G_{\varnothing,\infty}(k)$ is the Γ-quotient of $G_\varnothing(k)$ obtained via modulo the decomposition subgroup $\mathrm{Gal}_{\mathfrak{p}}(k_\varnothing/k)$ of one prime $\mathfrak{p}$ of k above ∞ (because Γ acts transitively on all the primes of k above ∞). Since this decomposition subgroup $\mathrm{Gal}_{\mathfrak{p}}(k_\varnothing/k)$ is isomorphic to $\widehat{\mathbb{Z}}$ and G is a quotient of $G_\varnothing(k)$, we can define g_n to be an element of G that is the image of one generator of $\mathrm{Gal}_{\mathfrak{p}}(k_\varnothing/k)$. In other words, denoting $G^\#$ the quotient of G by the Γ-closed normal subgroup generated by g_n, we have the diagram

$$\begin{tikzcd}
F_n \arrow[r, two heads, "\widehat{\pi}"] \arrow[rr, bend left, two heads, "\varpi"] \arrow[d, two heads] \arrow[dr, two heads, "\pi"] & G \arrow[r, two heads, "\eta", "/[g_n]"'] \arrow[d, two heads] & G^\# \arrow[d, two heads] \\
F_n{}^{\mathcal{C}} \arrow[r, two heads, "\pi^{\mathcal{C}}"] \arrow[rr, bend right, two heads, "\varpi^{\mathcal{C}}"'] & G_\varnothing(k)^{\mathcal{C}} \arrow[r, two heads, "\eta^{\mathcal{C}}"] & G_{\varnothing,\infty}(k)^{\mathcal{C}}
\end{tikzcd} \tag{10-3}$$

where the vertical maps are taking pro-$\mathcal{C}$ completions. To make the notation consistent between the number field and the function field cases, when $Q = \mathbb{Q}$, we let $g_n = 1$, and hence η and $\eta^{\mathcal{C}}$ in (10-3) are both identity maps. First of all, we want to determine $m(\widehat{\pi}, \Gamma, G, A)$.

Proposition 10.4. *Let ℓ be the exponent of A. Assume $\ell \neq \mathrm{char}(Q)$ is relatively prime to $|\mu(Q)||\Gamma|$. If $Q = \mathbb{Q}$, then*

$$m(\widehat{\pi}, \Gamma, G, A) \leq \frac{(n+1)\dim_{\mathbb{F}_\ell} A - \dim_{\mathbb{F}_\ell} A^\Gamma}{h_{G \rtimes \Gamma}(A)}.$$

If $Q = \mathbb{F}_q(t)$ and $A \neq \mu_\ell$, then

$$m(\widehat{\pi}, \Gamma, G, A) \leq \frac{n \dim_{\mathbb{F}_\ell} A - \dim_{\mathbb{F}_\ell} A^\Gamma}{h_{G \rtimes \Gamma}(A)}.$$

Remark 10.5. Recall that in Theorem 1.1 we assume that k/Q is split completely at ∞. In the function field case, μ_ℓ is a $\mathrm{Gal}(k_\varnothing/Q)$-module but not a $\mathrm{Gal}(k_{\varnothing,\infty}/Q)$-module, so we exclude the case that $A = \mu_\ell$.

Proof. By the assumptions, we can apply Proposition 3.4 to compute the multiplicities. Because $\ell \nmid |\Gamma|$, we have for $i = 1, 2$ that $H^i(G \rtimes \Gamma, A) = H^i(G, A)^\Gamma$. Then by Lemma 10.3, we have

$$m(\widehat{\pi}, \Gamma, G, A) \leq \frac{n \dim_{\mathbb{F}_\ell} A - \xi(A) + \delta_{k/Q,\varnothing}(A)}{h_{G \rtimes \Gamma}(A)}. \tag{10-4}$$

So we just need to compute $\delta_{k/Q,\varnothing}(A)$.

In the function field case, recall that A is a simple $\mathbb{F}_\ell[\mathrm{Gal}(k_\varnothing/Q)]$-module that is not μ_ℓ, so by Proposition 9.3 we see that $\delta_{k/Q,\varnothing}(A)$ is -1 if $A = \mathbb{F}_\ell$, and is 0 otherwise. So we proved the result in function field case.

In the number field case that $Q = \mathbb{Q}$, we need to compute each of the terms in the formula in Proposition 9.4. Let $T = S_\ell(k) \cup S_\infty(k)$. In this case, ℓ is odd as $\mu_2 \subset Q$. First, we apply Theorem 7.1

$$\log_\ell \chi_{k/Q,T}(A) = -\dim_{\mathbb{F}_\ell} H^0(\mathbb{Q}_\infty, A') = -\dim_{\mathbb{F}_\ell} (A')^{\mathrm{Gal}(\mathbb{C}/\mathbb{R})},$$

where the first equality uses $\widehat{H}^0(\mathbb{Q}_\infty, A') = 0$ because $\#\mathcal{G}_\infty(\mathbb{Q}) = 2$ and [Neukirch et al. 2008, Proposition 1.6.2(a)]. Then because A is a simple $\mathbb{F}_\ell[\mathrm{Gal}(k_\varnothing/Q)]$-module, $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acts trivially on A, and hence $(A')^{\mathrm{Gal}(\mathbb{C}/\mathbb{R})} = \mathrm{Hom}_{\mathrm{Gal}(\mathbb{C}/\mathbb{R})}(A, \mu_\ell) = 0$. So we have $\log_\ell \chi_{k/Q,T}(A) = 0$. Then note that $\epsilon_{k/Q,\varnothing}(A)$ in the formula in Proposition 9.4 is $\dim_{\mathbb{F}_\ell} A$ in this case, and we obtain

$$\delta_{k/Q,\varnothing}(A) \le \dim_{\mathbb{F}_\ell} \mathrm{Hom}_{\mathrm{Gal}(k_T/Q)}(A, \mu_\ell) - \dim_{\mathbb{F}_\ell} A^{\mathrm{Gal}(k_\varnothing/Q)} + \dim_{\mathbb{F}_\ell} A,$$

where the right-hand side is 0 if $A = \mathbb{F}_\ell$ and is $\dim_{\mathbb{F}_\ell} A$ otherwise. So we proved the number field case. □

Lemma 10.6. *Use the assumptions in Proposition 10.4. Consider the function field case and the diagram (10-3). When n is sufficiently large, we have*

$$m(\varpi, \Gamma, G^\#, A) \le \frac{(n+1)\dim_{\mathbb{F}_\ell} A - \dim_{\mathbb{F}_\ell} A^\Gamma}{h_{G^\# \rtimes \Gamma}(A)}.$$

Proof. Again, we use $x_1, \dots, x_n$ to denote the generators of F_n. We can make n large to assume $\widehat{\pi}(x_n) = g_n$ (recall that the multiplicity depends on n but not on the choice of ϖ). Then we have a commutative diagram

$$\begin{tikzcd} F_n \arrow[r, two heads, "\lambda", "/{[x_n]}"'] \arrow[d, two heads, "\widehat{\pi}"] \arrow[dr, two heads, "\varpi"'] & F_{n-1} \arrow[d, two heads, "\phi"] \\ G \arrow[r, two heads, "\eta", "/{[g_n]}"'] & G^\# \end{tikzcd}$$

where the top map is defined by taking the quotient by the Γ-closed normal subgroup generated by x_n. Note that the composition of the top and the right arrows satisfies the conditions of Lemma 3.8, so we have

$$m(\varpi, \Gamma, G^\#, A) = m(\lambda, \Gamma, F_{n-1}, A) + m(\phi, \Gamma, G^\#, A).$$

By the statement and the computation of $H^i(F_n \rtimes \Gamma, A)$ in the proof of Lemma 3.2, we see that

$$m(\lambda, \Gamma, F_{n-1}, A) = \frac{\dim_{\mathbb{F}_\ell} A}{h_{G^\# \rtimes \Gamma}(A)}.$$

So by Proposition 10.4, it suffices to prove

$$m(\phi, \Gamma, G^\#, A) \le m(\widehat{\pi}, \Gamma, G, A), \tag{10-5}$$

which will immediately follow after we prove the embedding

$$\begin{aligned} &\{U \mid \text{max. proper } F_{n-1} \rtimes \Gamma\text{-normal subgroup of } \ker\phi \text{ such that } \ker\phi/U \simeq_{G^\# \rtimes \Gamma} A\} \\ &\qquad \xhookrightarrow{\kappa} \{V \mid \text{max. proper } F_n \rtimes \Gamma\text{-normal subgroup of } \ker\widehat{\pi} \text{ such that } \ker\widehat{\pi}/V \simeq_{G \rtimes \Gamma} A\} \end{aligned}$$

mapping U to $\lambda^{-1}(U) \cap \ker\widehat{\pi}$.

Since $\ker\varpi = \ker\widehat{\pi}\ker\lambda$, for each U in the first set, we have

$$\ker\widehat{\pi}/(\lambda^{-1}(U)\cap\ker\widehat{\pi}) = \lambda^{-1}(U)\ker\widehat{\pi}/\lambda^{-1}(U) = \ker\varpi/\lambda^{-1}(U) \simeq_{G^{\#}\rtimes\Gamma} A,$$

so the map κ is well-defined. Also, if $V = \kappa(U)$, then

$$\ker\varpi/V\ker\lambda = (\ker\widehat{\pi})(V\ker\lambda)/V\ker\lambda = \ker\widehat{\pi}/(\ker\widehat{\pi}\cap(V\ker\lambda)). \tag{10-6}$$

Since $V\subset\ker\widehat{\pi}$ and $\ker\widehat{\pi}/V$ is a simple module, the last quotient is either 1 or isomorphic to A. On the other hand, both of V and $\ker\lambda$ are contained in $\lambda^{-1}(U)$, so is $V\ker\lambda$. Then (10-6) implies that $V\ker\lambda = \lambda^{-1}(U)$. So we see that if $\kappa(U_1)=\kappa(U_2)=V$, then $\lambda^{-1}(U_1)=\lambda^{-1}(U_2)$ and hence $U_1=U_2$. So we conclude that κ is injective. □

Proposition 10.7. *Let $\mathcal{C}$ be a finite set of isomorphism classes of finite Γ-groups all of whose orders are prime to $|\mu(Q)||\Gamma|$ and $\operatorname{char}(Q)$ (if nonzero). Let A be a finite simple $G_{\varnothing,\infty}(k)^{\mathcal{C}}\rtimes\Gamma$-module of exponent $\ell\neq\operatorname{char}(k)$ relatively prime to $|\mu(Q)||\Gamma|$. When n is sufficiently large, there exists an admissible Γ-presentation $\mathcal{F}_n(\Gamma)\twoheadrightarrow G_{\varnothing,\infty}(k)^{\mathcal{C}}$, and*

$$m_{\mathrm{ad}}^{\mathcal{C}}(n,\Gamma,G_{\varnothing,\infty}(k)^{\mathcal{C}},A)\le m_{\mathrm{ad}}(n,\Gamma,G^{\#},A)\le\frac{(n+1)(\dim_{\mathbb{F}_\ell}A-\dim_{\mathbb{F}_\ell}A^{\Gamma})}{h_{G_{\varnothing,\infty}(k)^{\mathcal{C}}\rtimes\Gamma}(A)}.$$

Remark 10.8. The proposition shows that $m_{\mathrm{ad}}^{\mathcal{C}}(n,\Gamma,G_{\varnothing,\infty}(k)^{\mathcal{C}},\mathbb{F}_\ell)=0$. In other words, $G_{\varnothing,\infty}(k)^{\mathcal{C}}$ does not admit any nonsplit central group extension

$$1\to\mathbb{F}_\ell\to\widetilde{G}\rtimes\Gamma\to G_{\varnothing,\infty}(k)^{\mathcal{C}}\rtimes\Gamma\to 1,$$

such that $\widetilde{G}$ is of level $\mathcal{C}$. This is equivalent to the solvability (i.e., the existence of the dashed arrow) of the embedding problem

$$\begin{tikzcd} & & & G_{\varnothing,\infty}(k)^{\mathcal{C}}\rtimes\Gamma \arrow[dl, dashed] \arrow[d, two heads, "\alpha"] & \\ 1 \arrow[r] & \mathbb{F}_\ell \arrow[r] & \widetilde{H}\rtimes\Gamma \arrow[r] & H\rtimes\Gamma \arrow[r] & 1 \end{tikzcd}$$

for any nonsplit central group extension in the lower row with $\widetilde{H}$ of level $\mathcal{C}$, and for any surjection α. In [Liu et al. 2024], this solvability is called the *Property E* of $G_{\varnothing,\infty}(k)$ and is proven using the classical techniques of embedding problems. So Proposition 10.7 provides a new proof of the Property E by counting multiplicities.

Proof. By [Liu et al. 2024, Proposition 2.2], the pro-prime-to-($|\Gamma|\operatorname{char}Q$) completion of $G_{\varnothing,\infty}(k)$ is an admissible Γ-group, so its Γ-quotient $G^{\#}$ is also admissible. Since $G_{\varnothing,\infty}(k)^{\mathcal{C}}$ is finite, when n is large, there exist elements $a_1,\dots,a_n$ of $G_{\varnothing,\infty}(k)^{\mathcal{C}}$ such that $\{Y(a_i)\}_{i=1}^n$ forms a generator sets of $G_{\varnothing,\infty}(k)^{\mathcal{C}}$. Note that $G_{\varnothing,\infty}(k)^{\mathcal{C}}$ is a quotient of $G^{\#}$ as described in (10-3). We choose a preimage $b_i\in G^{\#}$ of a_i for each i, and then $\{Y(b_i)\}_{i=1}^n$ generates $G^{\#}$ by Lemma 10.2(1). Recall that the multiplicity does not depend on the choice of presentation, so we assume ϖ in (10-3) maps $y_i\in F_n$ to $b_i\in G^{\#}$ for each $i=1,\dots,n$.

Then the restriction $\varpi|_{\mathcal{F}_n}$ is an admissible Γ-presentation of $G^\#$. We have by Corollary 4.5 that

$$m_{\mathrm{ad}}(n,\Gamma,G^\#,A)=m(n,\Gamma,G^\#,A)-\frac{n\dim_{\mathbb{F}_\ell}A^\Gamma}{h_{G^\#\rtimes\Gamma}(A)}.$$

Then the desired result follows by Propositions 5.4, 10.4 and Lemma 10.6. □

10.3. ***Existence of the presentation (1-1).*** Finally, we will prove that when n is sufficiently large, there exists a subset X of $\mathcal{F}_n^{\mathcal{C}}$ containing $n+1$ elements for which the following isomorphism, which is (1-1) in Theorem 1.1, holds:

$$G_{\varnothing,\infty}(k)^{\mathcal{C}}\simeq\mathcal{F}_n(\Gamma)^{\mathcal{C}}/[r^{-1}\gamma(r)]_{r\in X,\gamma\in\Gamma}.$$

In Proposition 10.7, we showed that when n is sufficiently large, there is an admissible Γ-presentation, denoted by

$$1\to N\to\mathcal{F}_n^{\mathcal{C}}\xrightarrow{\varpi_{\mathrm{ad}}^{\mathcal{C}}}G_{\varnothing,\infty}(k)^{\mathcal{C}}\to 1.$$

Let M be the intersection of all maximal proper $\mathcal{F}_n^{\mathcal{C}}\rtimes\Gamma$-normal subgroups of N, and define $R=N/M$ and $F=\mathcal{F}_n^{\mathcal{C}}/M$. Note that because $\mathcal{C}$ is finite, we have that $\mathcal{F}_n^{\mathcal{C}}$ is finite [Neumann 1967, Corollary 15.72]. Then R is a finite direct product $\prod_{i=1}^t A_i^{m_i}$ of finite irreducible $F\rtimes\Gamma$-groups A_i. Assume A_i and A_j are not isomorphic as $F\rtimes\Gamma$-groups if $i\neq j$. When a factor A_i is abelian, its multiplicity m_i is $m_{\mathrm{ad}}^{\mathcal{C}}(n,\Gamma,G_{\varnothing,\infty}(k)^{\mathcal{C}},A_i)$ computed in Proposition 10.7.

Let X be a subset of $\mathcal{F}_n^{\mathcal{C}}$. Then the closed $\mathcal{F}_n^{\mathcal{C}}\rtimes\Gamma$-normal subgroup generated by $\{r^{-1}\gamma(r)\}_{r\in X,\gamma\in\Gamma}$ is N if and only if the closed $F\rtimes\Gamma$-normal subgroup generated by $\{\bar{r}^{-1}\gamma(\bar{r})\}_{\bar{r}\in\overline{X},\gamma\in\Gamma}$ is R, where $\overline{X}$ and $\bar{r}$ are the images of X and r in R respectively. Recall the properties of $\mathcal{F}_n$ listed at the beginning of Section 4. Because of the property (1), in the definition of Y in (3), we can take the generator set $\{\gamma_1,\dots,\gamma_d\}$ to be the whole group Γ, then

$$\{r^{-1}\gamma(r)\}_{r\in X,\gamma\in\Gamma}=Y(\{r\}_{r\in X})\quad\text{and}\quad\{\bar{r}^{-1}\gamma(\bar{r})\}_{\bar{r}\in\overline{X},\gamma\in\Gamma}=Y(\{\bar{r}\}_{\bar{r}\in\overline{X}}).$$

By [Liu et al. 2024, Proposition 4.3], for a fixed integer u, the probability that the images under the map Y of $n+u$ random elements of R generate R as an $F\rtimes\Gamma$-normal subgroup is

$$\begin{aligned}\mathrm{Prob}([Y(\{r_1,\dots,r_{n+u}\})]_{F\rtimes\Gamma}=R)\\&=\prod_{\substack{1\le i\le t\\ A_i\text{ abelian}}}\prod_{j=0}^{m_i-1}(1-h_{F\rtimes\Gamma}(A_i)^j|Y(A_i)|^{-n-u})\prod_{\substack{1\le i\le t\\ A_i\text{ nonabelian}}}(1-|Y(A_i)|^{-n-u})^{m_i}.\end{aligned}$$

This product in the formula is a finite product. By [Liu et al. 2024, Lemma 3.5], we have $|Y(A_i)|=|A_i|/|A_i^\Gamma|$ for each i. Note that Lemma 4.6 shows that $|Y(A_i)|>1$ when A_i is nonabelian, so the product over nonabelian factors in the above formula is always positive. The term for an abelian factor A_i is positive if and only if

$$m_i\le\frac{(n+u)\log_\ell|Y(A_i)|}{h_{G_{\varnothing,\infty}(k)^{\mathcal{C}}\rtimes\Gamma}(A_i)}=\frac{(n+u)(\dim_{\mathbb{F}_\ell}A_i-\dim_{\mathbb{F}_\ell}A_i^\Gamma)}{h_{G_{\varnothing,\infty}(k)^{\mathcal{C}}\rtimes\Gamma}(A_i)}.$$

Therefore, by Proposition 10.7, R can be $F\rtimes\Gamma$-normally generated by the Y-values of $n+1$ elements, and hence we finish the proof of Theorem 1.1.

11. Exceptional cases

We will discuss the cases that are not covered by the Liu–Wood–Zureick-Brown conjecture, using the techniques developed in this paper. In this section, the base field Q can be any global field. If Q is a number field, we denote by r_1 and r_2 the number of real and pairs of complex embeddings of Q.

Again, we let Γ be a nontrivial finite group and k/Q a Galois extension of global fields with $\mathrm{Gal}(k/Q) \simeq \Gamma$, such that $\mathrm{char}(Q)$ and $|\Gamma|$ are relatively prime. We assume that ℓ is a prime integer that is not $\mathrm{char}(Q)$ and is prime to $|\Gamma|$. Recall that $G_\varnothing(k)(\ell)$ denotes the pro-ℓ completion of $G_\varnothing(k)$. So $G_\varnothing(k)(\ell)$ is the Galois group of the maximal unramified pro-ℓ extension of k, which we will denote by $k_\varnothing(\ell)/k$. Note that $G_\varnothing(k)(\ell)$ is finitely generated, because $\dim_{\mathbb{F}_\ell} H^1(k_\varnothing, \mathbb{F}_\ell)$ is the minimal number of generators of $G_\varnothing(k)(\ell)$ and is finite. So when n is sufficiently large, there is a Γ-presentation $\pi : F'_n(\Gamma) \to G_\varnothing(k)(\ell)$. Moreover, we assume, throughout this section, that the ℓ-primary part of the class group of Q is trivial. Then $G_{\varnothing,\infty}(k)(\ell)$ is admissible by the proof of [Liu et al. 2024, Proposition 2.2], and hence we can assume that the presentation π induces an admissible presentation, i.e., $\pi^{\mathrm{ad}} := \pi|_{\mathcal{F}_n}$ is surjective.

In this section, we use the assumptions above and study the multiplicities from the presentation π^{ad} in the following two cases:

(1) When Q is a number field with $\mu_\ell \not\subset Q$, and k/Q is not required to be split completely at $S_\infty(Q)$ (see Section 11.1).

(2) When Q contains the ℓ-roots of unity μ_ℓ (see Section 11.2).

We will compare the multiplicities in these two cases with the multiplicities from Theorem 1.1, to see why the random group model used in the Liu–Wood–Zureick-Brown conjecture cannot be applied to these two exceptional cases.

We point out that we study only $G_\varnothing(k)(\ell)$ instead of $G_\varnothing(k)^{\mathcal{C}}$ for a general $\mathcal{C}$, simply because we want to keep the computation easy in this section and there is no previous work discussing these two exceptional cases beyond the distribution of ℓ-class tower groups. One can generalize the argument in this section to any finite set $\mathcal{C}$.

11.1. ***Other signatures.*** Assume Q is a number field with $\mu_\ell \not\subset Q$ (so ℓ is odd), and k is a Γ-extension of Q. For each $v \in S_\infty(Q)$, we set Γ_v to be the decomposition subgroup at v of the extension k/Q.

Lemma 11.1. *For a finite simple $\mathbb{F}_\ell[\mathrm{Gal}(k_\varnothing(\ell)/Q)]$-module A, we have*

$$m_{\mathrm{ad}}(n, \Gamma, G_\varnothing(k)(\ell), A) \le \begin{cases} r_1 + r_2 - 1 & \text{if } A = \mathbb{F}_\ell, \\ n + r_2 + 1 & \text{if } A = \mu_\ell, \\ \dfrac{(n+r_1+r_2)\dim_{\mathbb{F}_\ell} A - \sum_{v \in S_{\mathbb{R}}(Q)} \dim_{\mathbb{F}_\ell} A/A^{\Gamma_v} - (n+1)\dim_{\mathbb{F}_\ell} A^\Gamma}{h_{\mathrm{Gal}(k_\varnothing(\ell)/Q)}(A)} & \text{otherwise.} \end{cases}$$

Proof. Let T be $S_\infty(k) \cup S_\ell(k)$. Since ℓ is odd, $\widehat{H}^0(Q_v, A') = 0$ for any $v \in S_\infty(Q)$, and hence by applying Theorem 7.1 with $S = T$ we have

$$\begin{aligned}\log_\ell(\chi_{k/Q,T}(A)) &= -\sum_{v \in S_\infty(Q)} \dim_{\mathbb{F}_\ell} H^0(Q_v, A') \\ &= -\sum_{v \in S_\mathbb{C}(Q)} \dim_{\mathbb{F}_\ell} A - \sum_{v \in S_\mathbb{R}(Q)} \dim_{\mathbb{F}_\ell} A/A^{\Gamma_v}.\end{aligned}$$

The last equality is because:

(1) If $v \in S_\mathbb{C}(Q)$, then $\mathcal{G}_v(Q) = 1$ acts trivially on both μ_ℓ and A.

(2) If $v \in S_\mathbb{R}(Q)$, then $\mathcal{G}_v(Q) \simeq \mathbb{Z}/2\mathbb{Z}$ acts on μ_ℓ as taking inverse. Since the action of $\mathcal{G}_v(Q)$ on A factors through Γ_v, and Γ_v acts on A/A^{Γ_v} as taking inverse, we have $\dim_{\mathbb{F}_\ell}(A')^{\mathcal{G}_v(Q)} = \dim_{\mathbb{F}_\ell} \operatorname{Hom}_{\mathcal{G}_v(Q)}(A, \mu_\ell) = \dim_{\mathbb{F}_\ell} \operatorname{Hom}_{\mathcal{G}_v(Q)}(A/A^{\Gamma_v}, \mu_\ell) = \dim_{\mathbb{F}_\ell} A/A^{\Gamma_v}$.

By Proposition 9.4, we have

$$\delta_{k/Q,S}(A) \le \begin{cases} \epsilon_{k/Q,\varnothing}(A) - r_2 - 1 & \text{if } A = \mathbb{F}_\ell, \\ \epsilon_{k/Q,\varnothing}(A) - r_2 - r_1 + 1 & \text{if } A = \mu_\ell, \\ \epsilon_{k/Q,\varnothing}(A) - r_2 \dim_{\mathbb{F}_\ell} A - \sum_{v \in S_\mathbb{R}(Q)} \dim_{\mathbb{F}_\ell} A/A^{\Gamma_v} & \text{otherwise,} \end{cases}$$

where A can be μ_ℓ only if $\mu_\ell \subset k$. Note that by definition, $\epsilon_{k/Q,\varnothing}(A)$ is equal to $[Q : \mathbb{Q}] \dim_{\mathbb{F}_\ell} A$. So the desired result follows by Proposition 3.4, Corollary 4.5, and Proposition 5.4. □

Corollary 11.2. *Let $k/\mathbb{Q}$ be an imaginary quadratic field such that $k \neq \mathbb{Q}(\sqrt{-3})$, and γ denote the nontrivial element of $\Gamma = \operatorname{Gal}(k/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$. For an odd prime ℓ, we have the following isomorphism of Γ-groups*:

$$G_\varnothing(k)(\ell) \simeq \mathcal{F}_n(\Gamma)(\ell)/[r^{-1}\gamma(r)]_{r \in X} \tag{11-1}$$

for a sufficiently large positive integer n and some set X consisting of n elements of $\mathcal{F}_n(\Gamma)(\ell)$.

Remark 11.3. If we choose the n elements of set X randomly with respect to the Haar measure, then the quotient in (11-1) gives a random group that defines a probability measure on all n-generated pro-ℓ admissible Γ-groups. By taking $n \to \infty$, there is a limit probability measure, which can be computed using formulas in [Liu et al. 2024]. The discussion in [Liu et al. 2024, §7.2 and Theorem 7.5] shows that this limit probability measure agrees with the probability measure used in the Boston–Bush–Hajir heuristics [Boston et al. 2017].

Proof. When $Q = \mathbb{Q}$ and k is imaginary quadratic, we have $r_1 = 1$, $r_2 = 0$, and $\Gamma_\infty = \Gamma$. Let A be a finite simple $\mathbb{F}_\ell[\operatorname{Gal}(k_\varnothing(\ell)/\mathbb{Q})]$-module. Also, $\mu_\ell \not\subset k$ for any odd ℓ because $k \neq \mathbb{Q}(\sqrt{-3})$, so $A \neq \mu_\ell$. By Lemma 11.1 , when n is sufficiently large, we have:

$$m_{\mathrm{ad}}(n, \Gamma, G_\varnothing(k)(\ell), A) \le \begin{cases} 0 & \text{if } A = \mathbb{F}_\ell, \\ \dfrac{n(\dim_{\mathbb{F}_\ell} A - \dim_{\mathbb{F}_\ell} A^\Gamma)}{h_{\operatorname{Gal}(k_\varnothing(\ell)/\mathbb{Q})} A} & \text{otherwise.} \end{cases}$$

Note that $\Gamma \simeq \mathbb{Z}/2\mathbb{Z}$ implies that the normal subgroup of $\mathcal{F}_n(\Gamma)(\ell) \rtimes \Gamma$ generated by $Y(X)$ is exactly $[r^{-1}\gamma(r)]_{r \in X}$. Thus, the corollary follows by [Liu et al. 2024, Proposition 4.3]. □

11.2. ***When Q contains the ℓ-th roots of unity.*** In this subsection, we assume $\mu_\ell \subset Q$. In this case, μ_ℓ becomes the trivial $\mathrm{Gal}(k_\varnothing/Q)$-module $\mathbb{F}_\ell$, which makes the multiplicities in a presentation of $G_\varnothing(k)(\ell)$ significantly different from the previous cases.

Lemma 11.4. *Assume $\mu_\ell \subset Q$. For a finite simple $\mathbb{F}_\ell[\mathrm{Gal}(k_\varnothing(\ell)/Q)]$-module A, we have*

(1) *If Q is a function field and the genus of k is not* 0, *then $\delta_{k/Q,\varnothing}(A) = 0$.*

(2) *If Q is a number field, then $\delta_{k/Q,\varnothing}(A) \le (r_1 + r_2)\dim_{\mathbb{F}_\ell} A$.*

Proof. Because of the assumption $\mu_\ell \subset Q$, we have

$$\dim_{\mathbb{F}_\ell}(A')^{\mathrm{Gal}(k_\varnothing/Q)} = \dim_{\mathbb{F}_\ell}(A^\vee)^{\mathrm{Gal}(k_\varnothing/Q)} = \dim_{\mathbb{F}_\ell} A_{\mathrm{Gal}(k_\varnothing/Q)} = \dim_{\mathbb{F}_\ell} A^{\mathrm{Gal}(k_\varnothing/Q)}. \tag{11-2}$$

Then the first statement follows directly by Proposition 9.3(2). For the rest we assume that Q is a number field and let $T = S_\ell(k) \cup S_\infty(k)$. If ℓ is odd, then the assumption $\mu_\ell \subset Q$ implies that Q is totally imaginary. Then we can easily see by Theorem 7.1 that $\log_\ell \chi_{k/Q,T}(A) = -r_2 \dim_{\mathbb{F}_\ell} A$, and hence the statement for odd ℓ follows by Proposition 9.4 and (11-2). If $\ell = 2$, then we first want to compute, for each $v \in S_\infty(Q)$,

$$\dim_{\mathbb{F}_\ell} \widehat{H}^0(Q_v, A') - \dim_{\mathbb{F}_\ell} H^0(Q_v, A'). \tag{11-3}$$

For each $v \in S_\mathbb{C}(Q)$, we have $\mathcal{G}_v(Q) = 1$, and hence (11-3) becomes $-\dim_{\mathbb{F}_\ell} A$. For each $v \in S_\mathbb{R}(Q)$, the assumption $\ell \nmid |\Gamma|$ implies that $|\Gamma|$ is odd. So for each $\mathfrak{p} \in S_v(k)$, $\mathfrak{p}$ is real, and so is any prime of $k_\varnothing(\ell)$ lying above $\mathfrak{p}$. Thus, $\mathcal{G}_\mathfrak{p}(k)$ acts trivially on A, so it also acts trivially on A', which implies that $\widehat{H}^0(k_\mathfrak{p}, A') = H^0(k_\mathfrak{p}, A')$. Then (11-3) equals 0, and we obtain the statement for $\ell = 2$ by Proposition 9.4 and (11-2). □

Then by the same arguments in Section 10, we obtain the following bounds for the multiplicity of A.

Corollary 11.5. *Assume $\mu_\ell \subset Q$. When k is a function field, we assume that $Q = \mathbb{F}_q(t)$ for some prime power q such that $\ell \mid q - 1$ and k/Q is split completely at ∞. Let A be a finite simple $\mathbb{F}_\ell[\mathrm{Gal}(k_\varnothing(\ell)/Q)]$-module. Then for a sufficiently large n, we have*

$$m_{\mathrm{ad}}(n, \Gamma, G_{\varnothing,\infty}(k)(\ell), A) \le \begin{cases} \dfrac{(n+1)\dim_{\mathbb{F}_\ell} A - \xi(A) - n\dim_{\mathbb{F}_\ell} A^\Gamma}{h_{G_{\varnothing,\infty}(k)(\ell)\rtimes\Gamma}(A)} & \text{if } Q \text{ is a function field,} \\[2ex] \dfrac{(n+r_1+r_2)\dim_{\mathbb{F}_\ell} A - \xi(A) - n\dim_{\mathbb{F}_\ell} A^\Gamma}{h_{G_{\varnothing,\infty}(k)(\ell)\rtimes\Gamma}(A)} & \text{if } Q \text{ is a number field.} \end{cases}$$

Remark 11.6. (1) Readers can compare the corollary with Proposition 10.7. When $A = \mathbb{F}_\ell$ and Q is $\mathbb{Q}(\zeta_\ell)$ or $\mathbb{F}_q(t)$ with $\ell \mid q - 1$, one can check that the upper bound of the multiplicity is positive, which suggests the failure of the Property E of $G_{\varnothing,\infty}(k)$. Therefore, the random group model used in the Liu–Wood–Zureick-Brown conjecture is not expected to work in this exceptional case.

(2) If the upper bounds in Corollary 11.5 are sharp, then it also suggests that we should not expect the coincidence of the distributions of $G_{\varnothing,\infty}(k)(\ell)$ between the function field case and the number field case.

For example, when $Q=\mathbb{Q}$, $\ell=2$ or $Q=\mathbb{Q}(\zeta_3)$, $\ell=3$, the upper bound in the corollary equals the one for function fields. However, when $Q=\mathbb{Q}(\zeta_\ell)$ with $\ell>3$, the upper bound is

$$\frac{(n+(\ell-1)/2)\dim_{\mathbb{F}_\ell} A-\xi(A)-n\dim_{\mathbb{F}_\ell} A^\Gamma}{h_{G_{\varnothing,\infty}(k)(\ell)\rtimes\Gamma}(A)},$$

which is strictly larger than the upper bound for function fields.

Acknowledgements

I would like to thank Nigel Boston and Melanie Matchett Wood for helpful conversations and encouragement which inspired me to work on the questions studied in this paper. I also thank Nigel Boston, Yufan Luo, Mark Shusterman, Preston Wake, Ken Willyard and Melanie Matchett Wood for comments on and corrections to an early draft of the paper. I am grateful to the referee for suggestions and comments that improved the exposition of the paper. I am partially supported by NSF Grant DMS-2200541.

References

[Achter 2006] J. D. Achter, "The distribution of class groups of function fields", *J. Pure Appl. Algebra* **204**:2 (2006), 316–333. MR Zbl

[Achter 2008] J. D. Achter, "Results of Cohen–Lenstra type for quadratic function fields", pp. 1–7 in *Computational arithmetic geometry* (San Francisco, CA, 2006), edited by K. E. Lauter and K. A. Ribet, Contemp. Math. **463**, Amer. Math. Soc., Providence, RI, 2008. MR Zbl

[Adam and Malle 2015] M. Adam and G. Malle, "A class group heuristic based on the distribution of 1-eigenspaces in matrix groups", *J. Number Theory* **149** (2015), 225–235. MR Zbl

[Boston and Wood 2017] N. Boston and M. M. Wood, "Non-abelian Cohen–Lenstra heuristics over function fields", *Compos. Math.* **153**:7 (2017), 1372–1390. MR Zbl

[Boston et al. 2017] N. Boston, M. R. Bush, and F. Hajir, "Heuristics for p-class towers of imaginary quadratic fields", *Math. Ann.* **368**:1-2 (2017), 633–669. MR Zbl

[Boston et al. 2021] N. Boston, M. R. Bush, and F. Hajir, "Heuristics for p-class towers of real quadratic fields", *J. Inst. Math. Jussieu* **20**:4 (2021), 1429–1452. MR Zbl

[Clozel et al. 2008] L. Clozel, M. Harris, and R. Taylor, "Automorphy for some l-adic lifts of automorphic mod l Galois representations", *Publ. Math. Inst. Hautes Études Sci.* **108** (2008), 1–181. MR Zbl

[Cohen and Lenstra 1984] H. Cohen and H. W. Lenstra, Jr., "Heuristics on class groups of number fields", pp. 33–62 in *Number theory* (Noordwijkerhout, Netherlands, 1983), edited by H. Jager, Lecture Notes in Math. **1068**, Springer, 1984. MR Zbl

[Cohen and Martinet 1987] H. Cohen and J. Martinet, "Class groups of number fields: numerical heuristics", *Math. Comp.* **48**:177 (1987), 123–137. MR Zbl

[Ellenberg et al. 2016] J. S. Ellenberg, A. Venkatesh, and C. Westerland, "Homological stability for Hurwitz spaces and the Cohen–Lenstra conjecture over function fields", *Ann. of Math.* (2) **183**:3 (2016), 729–786. MR Zbl

[Friedman and Washington 1989] E. Friedman and L. C. Washington, "On the distribution of divisor class groups of curves over a finite field", pp. 227–239 in *Théorie des nombres* (Quebec, 1987), edited by J.-M. De Koninck and C. Levesque, de Gruyter, Berlin, 1989. MR Zbl

[Garton 2015] D. Garton, "Random matrices, the Cohen–Lenstra heuristics, and roots of unity", *Algebra Number Theory* **9**:1 (2015), 149–171. MR Zbl

[Golod and Shafarevich 1964] E. S. Golod and I. R. Shafarevich, "On the class field tower", *Izv. Akad. Nauk SSSR Ser. Mat.* **28** (1964), 261–272. In Russian. MR Zbl

[Goss 1996] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Math. (3) **35**, Springer, 1996. MR Zbl

[Katz and Sarnak 1999] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, Amer. Math. Soc. Colloq. Publ. **45**, Amer. Math. Soc., Providence, RI, 1999. MR Zbl

[Koch 2002] H. Koch, *Galois theory of p-extensions*, Springer, 2002. MR Zbl

[Liu 2022] Y. Liu, "Non-abelian Cohen–Lenstra heuristics in the presence of roots of unity", preprint, 2022. arXiv 2202.09471

[Liu 2024] Y. Liu, "On the p-rank of class groups of p-extensions", *Int. Math. Res. Not.* **2024**:6 (2024), 5274–5325. MR Zbl

[Liu and Wood 2020] Y. Liu and M. M. Wood, "The free group on n generators modulo $n+u$ random relations as n goes to infinity", *J. Reine Angew. Math.* **762** (2020), 123–166. MR Zbl

[Liu et al. 2024] Y. Liu, M. M. Wood, and D. Zureick-Brown, "A predicted distribution for Galois groups of maximal unramified extensions", *Invent. Math.* **237**:1 (2024), 49–116. MR Zbl

[Lubotzky 2001] A. Lubotzky, "Pro-finite presentations", *J. Algebra* **242**:2 (2001), 672–690. MR Zbl

[Malle 2008] G. Malle, "Cohen–Lenstra heuristic and roots of unity", *J. Number Theory* **128**:10 (2008), 2823–2835. MR Zbl

[Malle 2010] G. Malle, "On the distribution of class groups of number fields", *Exp. Math.* **19**:4 (2010), 465–474. MR Zbl

[Neukirch et al. 2008] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, 2nd ed., Grundl. Math. Wissen. **323**, Springer, 2008. MR Zbl

[Neumann 1967] H. Neumann, *Varieties of groups*, Springer, 1967. MR Zbl

[Shusterman 2022] M. Shusterman, "Balanced presentations for fundamental groups of curves over finite fields", *Math. Res. Lett.* **29**:4 (2022), 1251–1259. MR Zbl

[Venkatesh and Ellenberg 2010] A. Venkatesh and J. S. Ellenberg, "Statistics of number fields and function fields", pp. 383–402 in *Proceedings of the International Congress of Mathematicians*, *II* (Hyderabad, India, 2010), edited by R. Bhatia et al., Hindustan Book Agency, New Delhi, 2010. MR

[Wang and Wood 2021] W. Wang and M. M. Wood, "Moments and interpretations of the Cohen–Lenstra–Martinet heuristics", *Comment. Math. Helv.* **96**:2 (2021), 339–387. MR Zbl

[Wood 2019] M. M. Wood, "Nonabelian Cohen–Lenstra moments", *Duke Math. J.* **168**:3 (2019), 377–427. MR Zbl

Communicated by Akshay Venkatesh
Received 2023-02-04 Revised 2023-12-17 Accepted 2024-07-16

yyyliu@illinois.edu *Department of Mathematics, University of Illinois Urbana-Champaign, Urbana, IL, United States*

ALGEBRA AND NUMBER THEORY 19:5 (2025)
https://doi.org/10.2140/ant.2025.19.883

Motivic distribution of rational curves and twisted products of toric varieties

Loïs Faisant

This work concerns asymptotical stabilisation phenomena occurring in the moduli space of sections of certain algebraic families over a smooth projective curve, whenever the generic fibre of the family is a smooth projective Fano variety, or not far from being Fano.

We describe the expected behaviour of the class, in a ring of motivic integration, of the moduli space of sections of given numerical class. Up to an adequate normalisation, it should converge, when the class of the sections goes arbitrarily far from the boundary of the dual of the effective cone, to an effective element given by a motivic Euler product. Such a principle can be seen as an analogue for rational curves of the Batyrev–Manin–Peyre principle for rational points.

The central tool of this article is the property of equidistribution of curves. We show that this notion does not depend on the choice of a model of the generic fibre, and that equidistribution of curves holds for smooth projective split toric varieties. As an application, we study the Batyrev–Manin–Peyre principle for curves on a certain kind of twisted products.

Introduction

The aim of this work is to describe the expected behaviour of moduli spaces of morphisms from a smooth projective curve to a smooth Fano variety when the numerical class of the curves goes to infinity. More generally, we study sections of a faithfully flat morphism to such a curve. What we consider are the classes of these moduli spaces in a variant of the Grothendieck ring of varieties.

This is related to the classical subject of homological stability. Recent developments concern homological stability for moduli spaces, as described for example by Ellenberg, Venkatesh and Westerland [29]. The underlying philosophy is that given a sequence (X_n) of algebraic varieties defined over the finite

MSC2020: primary 14H10, 14E18, 11G50; secondary 11M41, 14G40.
Keywords: Manin's conjectures, rational curves, motivic Euler products, toric varieties, equidistribution, twisted products, motivic stabilisation.

field $\mathbb{F}_q$ of growing dimension with respect to n — for instance, a sequence of moduli spaces — the quantity $|X_n(\mathbb{F}_q)|q^{-\dim(X_n)}$ should admit a limit as $n \to \infty$ precisely when the cohomology groups of X_n stabilise [29, Section 1.8]. For example, when the X_n are smooth and geometrically irreducible varieties of dimension n, Deligne's proof of the Weil conjecture [25] provides an upper bound on the eigenvalues of the Frobenius morphism, acting on the étale cohomology groups of X_n, and the Grothendieck–Lefschetz formula allows one to pass from homological stabilisation to point-counting stabilisation.

The study of the asymptotic behaviour of the number of $\mathbb{F}_q(t)$-rational points of bounded height on Fano varieties over $\mathbb{F}_q$, in the framework suggested by Manin and his collaborators in the late 1980s, is expected to be an illustrative instance of this phenomenon: in that case, $\mathbb{F}_q(t)$-points can be interpreted as $\mathbb{F}_q$-points of the moduli space of morphisms from $\mathbb{P}^1_{\mathbb{F}_q}$ to the variety. One of the goals of this article is to formulate a motivic analogue of this framework which allows "point-counting" in any characteristic (in particular, of $\mathbb{C}(t)$-points). Actually, the motivic point of view tends to incorporate both the homological approach and the point-counting approach. Then, techniques coming from arithmetic help one get answers to questions concerning geometry and topology: dimension, number of components, homological stabilisation, or even stabilisation of Hodge structures.

Let us now recall that the modern formulation of a Batyrev–Manin–Peyre principle *over number fields* is the sum of works carried out by Franke–Manin–Tschinkel [32], Batyrev–Manin [1], Batyrev–Tschinkel [2], Peyre [51], Salberger [59], Lehmann–Tanimoto [40] and Lehmann–Sengupta–Tanimoto [43], among many others. This principle admits many variants, for example when one works *over a function field of positive characteristic* [52], when one considers *integral points* [18] or *Campana points* [55], or counts rational points on stacks [22; 30].

This literature is a rich source of inspiration for anyone wishing to consider a geometric analogue of this principle, namely the asymptotic behaviour of *rational curves* of arbitrarily large degree — which corresponds to rational points of varieties defined *over a function field of arbitrary characteristic*. This is no longer strictly speaking a counting problem if the characteristic is zero, but a quite natural framework is provided by the theory of motivic integration, introduced by Kontsevich (during his talk in Orsay, 1995) and then developed and expanded by Denef, Loeser [26], Looijenga [45] and their collaborators [19; 47; 60]. Then *counting curves* means taking the classes, in the ring of motivic integration, of the components of the moduli space of rational curves.

Following remarks by Batyrev about the dimension of the moduli space and a question raised by Peyre in the early 2000s, one may ask whether the class of the moduli space of curves of a given degree stabilises when the degree, which is an element of the dual of the Picard group of the variety, goes arbitrarily far away from the boundary of the dual of the effective cone.

Any positive answer to this question for a given class of varieties would be in the spirit of a larger family of recent stabilisation results in motivic statistics, such as those appearing in several works by Vakil and Wood concerning moduli of hypersurfaces [64], by Bilu and Howe about moduli of sections of vector bundles [5], by Bilu, Das and Howe about configuration spaces and Hadamard convergence [6], and by Landesman, Vakil and Wood regarding low-degree Hurwitz spaces [39], to cite a few of them.

Until recently, an obstruction to a precise formulation of a geometric or motivic Batyrev–Manin–Peyre principle was the absence of a sufficiently robust *notion of motivic Euler product* which would play the role of Peyre's adelic constant. A path was opened up by Bourqui [12; 13; 14] in the late 2000s and the notion reached a certain degree of maturity and robustness quite recently with Bilu's thesis [3]. In this article we make extensive use of this notion in order to formulate a motivic Batyrev–Manin–Peyre principle for curves, as well as a stronger notion of equidistribution of curves. We test the validity of these concepts on smooth split projective toric varieties and twisted products of toric varieties, in a continuation of [6; 11; 12; 15; 16].

Framework. We fix once and for all a smooth projective and geometrically integral curve $\mathscr{C}$ over a base field k, with function field $F = k(\mathscr{C})$.

Definition 1. If V is a smooth (irreducible) projective variety over F, we will say that V is a *Fano-like variety* if

- $V(F)$ is Zariski dense in V;
- both cohomology groups $H^1(V, \mathscr{O}_V)$ and $H^2(V, \mathscr{O}_V)$ are trivial;
- the Picard group of V coincides with its geometric Picard group;
- the geometric Picard group of V has no torsion, and its geometric Brauer group is trivial;
- the class of the anticanonical line bundle of V lies in the interior of the effective cone $\mathrm{Eff}(V)$, which itself is rational polyhedral: there exists a finite set of effective line bundles spanning it.

In the case of a projective variety V defined over the base field k, F-points of V correspond to morphisms $f : \mathscr{C} \to V$. Such a morphism will be somewhat abusively called a *rational curve* if $\mathscr{C}$ is the projective line $\mathbb{P}^1_k$. In general, we will consider sections of models $\pi : \mathscr{V} \to \mathscr{C}$ of V. By *model*, we mean a separated and faithfully flat morphism of finite type whose generic fibre is isomorphic to V. If furthermore π is proper, F-points of V will correspond to sections of π. For the sake of conciseness, in this Introduction we start by assuming that V is actually defined over the base field k.

Multidegrees of curves. If L is a invertible sheaf on V and $f : \mathscr{C} \to V$ is a morphism, then a relevant invariant of f is its degree with respect to L, that is, the degree

$$\deg(f^*L)$$

of the pull-back of L to $\mathscr{C}$ through f. However, except for the canonical sheaf ω_V of V, there is no canonical choice for L, and the canonical degree has no particular reason to be an invariant sharp enough, as the analogy with the arithmetic setting may suggest (see for example [53, Section 4]). A way of addressing this issue would be to introduce more invariants.

Our approach consists in taking *all the degrees* in the following manner: actually, a morphism $f : \mathscr{C} \to V$ defines an element of the dual of the Picard group of V

$$\mathbf{deg}\, f : [L] \in \mathrm{Pic}(V) \mapsto \deg(f^*L),$$

called the *multidegree*. Given a class $\delta \in \mathrm{Pic}(V)^\vee$, one can show that morphisms $f : \mathscr{C} \to V$ of multidegree δ are parametrised by a quasiprojective scheme $\mathrm{Hom}_k^\delta(\mathscr{C}, V)$ [23, Chapter 2]. The dimension of $\mathrm{Hom}_k^\delta(\mathscr{C}, V)$ admits the lower bound

$$\delta \cdot \omega_V^{-1} + \dim(V)(1 - g(\mathscr{C}))$$

called the *expected dimension*.

In this paper, we are interested in the behaviour of this sequence of moduli spaces when δ belongs to the dual of the effective cone $\mathrm{Eff}(V)$ and goes arbitrarily far from its boundaries. More precisely, we study the sequence of the corresponding *classes* in a ring of varieties.

The ring of motivic integration. Let S be a scheme. The Grothendieck group of S-varieties

$$K_0\mathbf{Var}_S$$

is defined as the abelian group generated by the isomorphism classes of S-*varieties* (by this, we mean S-schemes of finite presentation), together with *scissors relations*

$$X - Y - U$$

whenever X is an S-variety, Y is a closed subscheme of X and U is its open complement in X. The class of an S-variety X is denoted by $[X]$. The class of the affine line $\mathbb{A}^1_S$ is denoted by $\mathbb{L}_S$ and when the base scheme is clear from the context we may drop the index. Any constructible subset X of an S-variety admits a class $[X]$ in such a group [19, p. 59]. In our case, a constructible subset is a finite union of locally closed subsets of an S-variety.

The product $[X][Y] = [X \times_S Y]$ defines a ring structure on $K_0\mathbf{Var}_S$ with unit element the class of S over itself with natural structural map. The localised Grothendieck ring of varieties $\mathscr{M}_S$ is by definition the ring $K_0\mathbf{Var}_S$ localised at the class $\mathbb{L}_S$ of the affine line.

The ring $\mathscr{M}_S$ admits a decreasing filtration by the virtual dimension: for $m \in \mathbb{Z}$, let $\mathcal{F}^m\mathscr{M}_S$ be the subgroup of $\mathscr{M}_S$ generated by elements of the form

$$[X]\,\mathbb{L}_S^{-i},$$

where X is an S-variety and i is an integer such that $\dim_S(X) - i \leqslant -m$. The completion of $\mathscr{M}_S$ with respect to this decreasing dimensional filtration is the projective limit

$$\widehat{\mathscr{M}_S}^{\dim} = \varprojlim \mathscr{M}_S / \mathcal{F}^m \mathscr{M}_S,$$

which comes with a morphism $\mathscr{M}_S \to \widehat{\mathscr{M}_S}^{\dim}$. The dimensional filtration is one of the filtrations we are going to use, another one being the filtration by the weight of the Hodge realisation; see Section 2.1.

In positive characteristic, we will work with modified versions of $K_0\mathbf{Var}_S$ and $\mathscr{M}_S$ (see Section 4.4 of [19, Chapter 2]). An S-morphism $f : X \to Y$ between S-varieties is called a *universal homeomorphism* if for any S-morphism $Y' \to Y$ the induced morphism $X \times_Y Y' \to Y'$ is a homeomorphism. Then the modified ring of varieties $K_0^{\mathrm{uh}}\mathbf{Var}_S$ is the quotient of $K_0\mathbf{Var}_S$ by the ideal given by differences $[X] - [Y]$

of classes of S-varieties such that there exists an S-morphism $X \to Y$ which is a universal homeomorphism. If S is a $\mathbb{Q}$-scheme, this ideal is trivial so that $K_0^{\mathrm{uh}}\mathbf{Var}_S \simeq K_0\mathbf{Var}_S$ [19, Chapter 2, Corollary 4.4.7]. An equivalent description is given by the quotient of $K_0\mathbf{Var}_S$ by *radicial surjective morphisms*; see [5, Remark 2.1.4]. Note that we will systematically drop the "uh" exponent in this article.

Expected asymptotical behaviour. Now we are able to formulate a first version of what could be a *motivic Batyrev–Manin–Peyre principle for curves*. Again by analogy with the arithmetical side, one has to take into account the hypothetical existence of *accumulating subsets*. A description of these subsets in the geometric context is given in the works of Lehmann, Tanimoto and Tschinkel [41; 42]. In particular, we will have to focus on curves intersecting a well-chosen nonempty open subset U of V, denoting by $\mathrm{Hom}_k^\delta(\mathscr{C}, V)_U$ the corresponding moduli space.

Let $\mathrm{Eff}(V)^\vee_{\mathbb{Z}}$ be the subset of $\mathrm{Eff}(V)^\vee$ consisting of points in $\mathrm{Pic}(V)^\vee$. In characteristic zero, curves whose class belongs to this subset are *moveable* by [8]. With Question 5.4 in [53], Peyre raised the following question.

Question 1. *Assume that V is a Fano-like variety, defined over the base field k. Does the symbol*

$$[\mathrm{Hom}_k^\delta(\mathscr{C}, V)_U]\,\mathbb{L}_k^{-\delta\cdot\omega_V^{-1}}$$

converge in $\widehat{\mathscr{M}_k}^{\dim}$ as the class $\delta \in \mathrm{Eff}(V)^\vee_{\mathbb{Z}}$ goes arbitrarily far from the boundaries of $\mathrm{Eff}(V)^\vee$?

Note that in some cases this formulation is too optimistic, in particular the convergence may only hold for a filtration by the weight, which is finer than the one by the dimension, as it is the case, for example, in [3; 4; 31], rather than for the coarser dimensional filtration. We refer to Question 2 on page 917 for a more accurate version.

In what follows, we will say that V satisfies the motivic Batyrev–Manin–Peyre principle for curves if the answer to the previous question is positive for V. We now give a few examples for which it is the case.

Example 1. The first and simplest example is given by the projective space of dimension $n \geqslant 1$. Since its Picard group is generated by the class of a hyperplane H, the class of a moveable curve is given by a degree $d \in \mathbb{N}$ while an anticanonical divisor is $(n+1)H$, so that the normalisation factor is $\mathbb{L}_k^{(n+1)d}$. One can easily compute the class of the moduli space $\mathrm{Hom}_k^d(\mathbb{P}_k^1, \mathbb{P}_k^n)$ in $\mathscr{M}_k$ and show that for $d \geqslant 1$

$$[\mathrm{Hom}_k^d(\mathbb{P}_k^1, \mathbb{P}_k^n)]\,\mathbb{L}_k^{-(n+1)d} = [\mathbb{P}_k^n](1-\mathbb{L}_k^{-n});$$

see [53, Proposition 5.5]. The answer to Question 1 is positive in this case.

Example 2. More generally, Question 1 has a positive answer for smooth projective split toric varieties over any field k. The work of Bourqui [12], together with the unpublished notes [14] only provided the result in the ring of Chow motives, when k has characteristic zero. Bilu, Das and Howe [6, Section 5] checked a residue-type result at the level of the ring of varieties and we finally show in Section 5 that Bourqui's study actually provides convergence of the normalised class $[\mathrm{Hom}_k^\delta(\mathbb{P}_k^1, V)]\,\mathbb{L}_k^{-\delta\cdot\omega_V^{-1}}$ in $\widehat{\mathscr{M}_k}^{\dim}$ (see Theorem B below and Theorem 5.4 on page 930).

Example 3. Building on previous works by Chambert-Loir and Loeser [15] and Bilu [3], we show in [31] that the answer to Question 1 is positive for equivariant compactifications of vector spaces, when k is algebraically closed of characteristic zero and one considers the finer filtration on the ring of motivic integration given by the weight of the mixed Hodge realisation. See Example 3.9.

Example 4. Bilu and Browning developed in [4] a motivic circle method and applied it to show that the answer to Question 1 is positive when $V \subset \mathbb{P}^{n-1}_{\mathbb{C}}$ is a hypersurface of degree $d \geqslant 3$ with $n > 2^d(d-1)$, if one considers the filtration on $\mathscr{M}_{\mathbb{C}}$ coming from the weight of the mixed Hodge realisation.

Main results and structure of the paper. In this article we show that our motivic Batyrev–Manin–Peyre principle for curves is compatible with a certain kind of twisted product [17]. A little bit more precisely, we show:

Theorem A (Theorem 6.9). *If $\mathscr{B}$ is a Fano-like variety over k satisfying the motivic Batyrev–Manin–Peyre principle for curves, X is a smooth projective split toric variety over k, with torus T, and $\mathscr{T}$ is a Zariski-locally trivial T-torsor over $\mathscr{B}$, then the twisted product*

$$\mathscr{X} = X \times^{\mathscr{T}} \mathscr{B}$$

satisfies the motivic Batyrev–Manin–Peyre principle as well: the answer to Question 1 is positive for rational curves on $\mathscr{X}$.

The proof of this result is to be found in the very last section. It requires two ingredients.

Formulating a Batyrev–Manin–Peyre principle for curves. The first ingredient is presented in Section 3 and consists in a precise formulation of a motivic Batyrev–Manin–Peyre principle in a nonconstant setting, namely when one considers a proper model $\mathscr{V} \to \mathscr{C}$ of an F-variety V and studies the moduli space of its sections $\sigma : \mathscr{C} \to \mathscr{V}$ generically intersecting a convenient open subset U of V, as is done for example in [3; 15; 31] for equivariant compactifications of vector spaces. Fixing line bundles forming a basis of $\mathrm{Pic}(V)$ and choosing models of them over $\mathscr{V}$, one is able to define the multidegree of a section, generalising the previous notion (see Definition 1.5 on page 891). If $\mathscr{V}$ is projective over the base field k, we show in the first section of this article that the corresponding moduli space of sections $\mathrm{Hom}^{\delta}_{\mathscr{C}}(\mathscr{C}, \mathscr{V})_U$ *of multidegree* δ exists as a quasiprojective k-scheme, and formulate a relative geometric Batyrev–Manin–Peyre principle concerning the behaviour of the class

$$[\mathrm{Hom}^{\delta}_{\mathscr{C}}(\mathscr{C}, \mathscr{V})_U]\, \mathbb{L}_k^{-\delta \cdot \omega_V^{-1}} \tag{1}$$

when the multidegree δ *becomes arbitrarily large* (see Question 2 on page 917).

Let $\tau(\mathscr{V})$ be the expected limit of (1). We give an explicit description of $\tau(\mathscr{V})$ as a motivic Euler product, using Bilu's construction [3] of such an object. This motivic Tamagawa number can be interpreted as a motivic analogue of Peyre's constant [51]. For a constant family $\mathscr{V} = V \times_k \mathscr{C}$, where V is actually defined over k, it takes the form

$$\tau(\mathscr{V}) = \mathbb{L}_k^{(1-g(\mathscr{C}))\dim(V)} \left(\frac{[\mathrm{Pic}^0(\mathscr{C})]\mathbb{L}_k^{-g(\mathscr{C})}}{1-\mathbb{L}_k^{-1}} \right)^{\mathrm{rk}(\mathrm{Pic}(V))} \prod_{p\in\mathscr{C}} (1-\mathbb{L}_p^{-1})^{\mathrm{rk}(\mathrm{Pic}(V))} \frac{[V_p]}{\mathbb{L}_p^{\dim(V)}},$$

where $g(\mathscr{C})$ is the genus of the curve $\mathscr{C}$ and $\mathrm{Pic}^0(\mathscr{C})$ is the connected component of the Picard group of $\mathscr{C}$. Note that the class $(1-\mathbb{L}_p^{-1})^{\mathrm{rk}(\mathrm{Pic}(V))}([V_p]/\mathbb{L}_p^{\dim(V)})$ can be rewritten as

$$[\mathcal{T}_V]\,\mathbb{L}^{-(\dim(V)+\mathrm{rk}(\mathrm{Pic}(V)))},$$

where $\mathcal{T}_V$ is the[1] universal torsor of V.

However, the definition of $\tau(\mathscr{V})$ may require the use of a finer filtration on $\mathscr{M}_k$, namely the filtration by the weight of the Hodge realisation of $\mathscr{V}/\mathscr{C}$, when k is a subfield of $\mathbb{C}$. We refer to Definition 3.2 on page 915.

Equidistribution of curves and models. The second ingredient is a change-of-model theorem, given by Theorem C below. Such a result is grounded on the central idea of this article, which is the concept of equidistribution of curves. This notion, which is presented in Section 4, describes the behaviour of constrained curves of large multidegree: if $\mathscr{S}$ is a zero-dimensional subscheme of the curve $\mathscr{C}$, and $\varphi : \mathscr{S} \to \mathscr{V}$ a $\mathscr{C}$-morphism, broadly, the equidistribution principle says that the class of the moduli space of curves of multidegree δ whose restriction to $\mathscr{S}$ is φ, normalised $\mathbb{L}_k^{\delta\cdot\omega_V^{-1}}$, converges to the restriction of the product $\tau(\mathscr{V})$ to the complement of the closed points of $\mathscr{S}$. More generally, one considers curves whose restriction to $\mathscr{S}$ belongs to any constructible subset of $\mathrm{Hom}_{\mathscr{C}}(\mathscr{S},\mathscr{V})$. In particular, the notion of equidistribution is much stronger than the Batyrev–Manin–Peyre principle, see Definition 4.3 on page 921. Smooth projective split toric varieties provide a first example of varieties for which this principle holds (see Section 5).

Theorem B (Theorem 5.6). *The principle of equidistribution of curves holds for smooth and projective split toric varieties defined over any base field k, with respect to the dimensional filtration on $\mathscr{M}_k$.*

In particular, for such varieties, the answer to Question 1 is positive.

Our main fundamental result allows us to switch between models, whenever one has equidistribution of curves on one of them.

Theorem C (Theorem 4.6). *Assume that two proper models $\mathscr{V}/\mathscr{C}$ and $\mathscr{V}'/\mathscr{C}$ of the same Fano-like F-variety V are given, together with models of a $\mathbb{Z}$-basis of* $\mathrm{Pic}(V)$ *on each of them, defining two multidegrees δ and δ', for sections of $\mathscr{V}$ and $\mathscr{V}'$, respectively.*

Then there is equidistribution of curves on $\mathscr{V}$ with respect to δ if and only if there is equidistribution of curves on $\mathscr{V}'$ with respect to δ'.

Convention. In this article, without explicit mention, if R is a discrete valuation ring, we will always assume that it has equal characteristic.

[1] Since $\mathrm{Pic}(V)=\mathrm{Pic}(\overline{V})$, the universal torsor of V is unique up to isomorphism. For more about this alternative definition of the local factor in a more general framework, see Peyre's talk [54, around 23′].

1. Models and moduli spaces of sections

1.1. ***Global models and degrees.*** Let $\mathscr{C}$ be a smooth projective and geometrically integral curve over a field k, with function field F, and let V be a smooth F-variety. As in the Introduction, a *model of V over $\mathscr{C}$* is a separated, faithfully flat and finite-type $\mathscr{C}$-scheme $\mathscr{V}$ whose generic fibre is isomorphic to V.

Example 1.1. Let $V \hookrightarrow \mathbb{P}^N_F$ be an embedding of V in some projective space. Take $\mathscr{V}$ to be the Zariski closure of V in $\mathbb{P}^N_{\mathscr{C}}$. Then the composition $\mathscr{V} \to \mathbb{P}^N_{\mathscr{C}} \to \mathscr{C}$ is a projective model of V.

Remark 1.2. If $\pi : \mathscr{V} \to \mathscr{C}$ is a proper model, the functors $\pi_!$ and π_* from the category of sheaves on $\mathscr{V}$ to the ones on $\mathscr{C}$ coincide [46, Chapter 6, Section 3]. Since $\mathscr{C}$ is integral, by [38, Theorem 4.18.2] there exists a nonempty Zariski open subset $\mathscr{C}' \subset \mathscr{C}$ such that the Picard scheme $\mathrm{Pic}_{\mathscr{V}_{\mathscr{C}'}/\mathscr{C}'}$ representing the Picard functor $\mathbf{Pic}_{(\mathscr{V}_{\mathscr{C}'}/\mathscr{C}')\,(\mathrm{fppf})}$ exists and is a disjoint union of open quasiprojective subschemes. Here we recall that $\mathbf{Pic}_{(X/S)\,(\mathrm{fppf})}$ is the sheaf associated to the functor

$$(T/S) \mapsto \mathrm{Pic}(X \times_S T)/\,\mathrm{Pic}(T)$$

in the fppf (faithfully flat of finite type) topology, given a separated map of finite type $X \to S$ between locally Noetherian schemes [38, Definition 2.2].

Moreover, we assume that π has (local) sections, so that the Picard functor $\mathbf{Pic}_{(\mathscr{V}_{\mathscr{C}}/\mathscr{C})\,(\mathrm{fppf})}$ is actually

$$\mathbf{Pic}_{\mathscr{V}/\mathscr{C}}(T) = H^0(T, \mathcal{R}^1\pi_*(\boldsymbol{G}_m))$$

for the Zariski topology [7, p. 204].

Remark 1.3. Assume there exists a closed point $p_0 \in \mathscr{C}$ such that $H^1(\mathscr{V}_{p_0}, \mathscr{O}_{\mathscr{V}_{p_0}}) = H^2(\mathscr{V}_{p_0}, \mathscr{O}_{\mathscr{V}_{p_0}}) = 0$. By the semicontinuity theorem [27, (7.7.5-I)], there exists an open neighborhood $\mathscr{C}''$ of p_0 such that $H^1(\mathscr{V}_p, \mathscr{O}_{\mathscr{V}_p}) = H^2(\mathscr{V}_p, \mathscr{O}_{\mathscr{V}_p}) = 0$ for all $p \in \mathscr{C}''$. This shows in particular that $(R^1\pi_!\mathscr{O}_{\mathscr{V}})_{|\mathscr{C}''} = (R^2\pi_!\mathscr{O}_{\mathscr{V}})_{|\mathscr{C}''} = 0$. By flat base-change [62, Lemma 02KH] applied to the generic fibre

$$\begin{array}{ccc} V & \longrightarrow & \mathscr{V} \\ \downarrow & & \downarrow{\scriptstyle \pi} \\ \mathrm{Spec}(F) & \longrightarrow & \mathscr{C} \end{array}$$

we have $(R^i\pi_!\mathscr{O}_{\mathscr{V}})_\eta = H^i(V, \mathscr{O}_V)$ for all i and in particular $H^1(V, \mathscr{O}_V) = H^2(V, \mathscr{O}_V) = 0$. Conversely, if $H^1(V, \mathscr{O}_V)$ and $H^2(V, \mathscr{O}_V)$ are both trivial, then there exists a nonempty open subset of $\mathscr{C}$ above which $R^1\pi_!\mathscr{O}_{\mathscr{V}}$ and $R^2\pi_!\mathscr{O}_{\mathscr{V}}$ are both trivial. This argument actually shows that the assumptions on the first and second cohomology groups of the structure sheaf of a Fano-like variety, in Definition 1, can be done indifferently with respect to V or to a special fibre of $\mathscr{V}$.

Moreover, by [38, Proposition 5.19], $\mathrm{Pic}_{\mathscr{V}_{\mathscr{C}'}/\mathscr{C}'}$ is smooth over $\mathscr{C}' \cap \mathscr{C}''$ and by [38, Corollary 5.13] each fibre $\mathrm{Pic}_{\mathscr{V}_p/\kappa_p}$ above $p \in \mathscr{C}' \cap \mathscr{C}''$ is discrete, given by $H^2(\mathscr{V}_p, \mathbb{Z})$. From this point of view, $\mathbf{Pic}_{\mathscr{V}_{\mathscr{C}'}/\mathscr{C}'}$ is a constructible sheaf on $\mathscr{C}$ and can be seen as a variation of mixed Hodge structure; see the proof of Proposition 2.6 on page 905.

Setting 1.4. Let $\mathscr{V} \to \mathscr{C}$ be a proper model of a Fano-like F-variety V. We fix a finite set $L_1, \dots, L_r$ of invertible sheaves on V whose linear classes form a basis of the torsion-free $\mathbb{Z}$-module $\operatorname{Pic}(V)$, as well as invertible sheaves $\mathscr{L}_1, \dots, \mathscr{L}_r$ on $\mathscr{V}$ extending respectively $L_1, \dots, L_r$.

Definition 1.5 (multidegree). Let $\mathscr{V} \to \mathscr{C}$ and $\underline{\mathscr{L}} = (\mathscr{L}_1, \dots, \mathscr{L}_r)$ be as in Setting 1.4. A section $\sigma : \mathscr{C} \to \mathscr{V}$ defines an element $\mathbf{deg}_{\underline{\mathscr{L}}}(\sigma)$ of the dual $\operatorname{Pic}(V)^\vee$ by sending an effective invertible sheaf of the form

$$\bigotimes_{i=1}^{r} L_i^{\otimes \lambda_i}$$

to the linear combination of degree

$$\sum_{i=1}^{r} \lambda_i \deg(\sigma^* \mathscr{L}_i).$$

This element $\mathbf{deg}_{\underline{\mathscr{L}}}(\sigma)$ is called the *multidegree of σ with respect to the model $\underline{\mathscr{L}}$.*

1.2. *Moduli spaces of curves.* Again, let $\mathscr{V} \to \mathscr{C}$ and $\underline{\mathscr{L}} = (\mathscr{L}_1, \dots, \mathscr{L}_r)$ be as in Setting 1.4. For every class $\delta \in \operatorname{Pic}(V)^\vee$, we consider the functor

$$\mathbf{Hom}^{\delta}_{\mathscr{C}}(\mathscr{C}, \mathscr{V})$$

sending a k-scheme T to the set of maps $\sigma \in \operatorname{Hom}_{\mathrm{Sch}/T}(\mathscr{C} \times_k T, \mathscr{V} \times_k T)$ such that

$$\pi_T \circ \sigma = \mathrm{id}_{\mathscr{C} \times_k T},$$
$$\text{for all } t \in T, \quad \mathbf{deg}_{\underline{\mathscr{L}}}(\sigma_t) = \delta.$$

If U is a dense open subset of the generic fibre V, we define

$$\mathbf{Hom}^{\delta}_{\mathscr{C}}(\mathscr{C}, \mathscr{V})_U$$

to be the subfunctor of $\mathbf{Hom}^{\delta}_{\mathscr{C}}(\mathscr{C}, \mathscr{V})$ sending a k-scheme T to the T-families of maps sending the generic point of $\mathscr{C}$ into $U(F)$.

The moduli space of sections of a proper model $\mathscr{V} \to \mathscr{C}$ is well-defined: adapting the ideas of [12, Lemme 4.1] and [15, Proposition 2.2.2] we get the following general representability lemma. Here we assume that $\mathscr{V}$ is projective over the base field k.

Lemma 1.6. *For any nonempty open subset $U \subset V$ and any class $\delta \in \operatorname{Pic}(V)^\vee$, the functor $\mathbf{Hom}^{\delta}_{\mathscr{C}}(\mathscr{C}, \mathscr{V})_U$ is representable by a quasiprojective scheme.*

Proof. Let $\mathscr{L}$ be an ample invertible sheaf on $\mathscr{V}$. For every $d \geqslant 1$, let

$$\mathbf{Hom}^{d}_{k}(\mathscr{C}, \mathscr{V})$$

be the functor of morphisms $\varsigma : \mathscr{C} \to \mathscr{V}$ such that $\deg(\varsigma^* \mathscr{L}) = d$ and

$$\mathbf{Hom}^{d}_{\mathscr{C}}(\mathscr{C}, \mathscr{V})$$

be the functor of sections $\sigma : \mathscr{C} \to \mathscr{V}$ such that $\deg(\sigma^* \mathscr{L}) = d$.

By the existence theorems of Hilbert schemes [34, 4.c], there exists a quasiprojective k-scheme $\mathrm{Hom}_k^d(\mathscr{C},\mathscr{V})$ representing $\mathbf{Hom}_k^d(\mathscr{C},\mathscr{V})$. The condition $\pi\circ\sigma=\mathrm{id}_{\mathscr{C}}$ is closed and thus $\mathbf{Hom}_{\mathscr{C}}^d(\mathscr{C},\mathscr{V})$ is a closed subfunctor of $\mathbf{Hom}_k^d(\mathscr{C},\mathscr{V})$. Therefore it is represented by a quasiprojective scheme $\mathrm{Hom}_{\mathscr{C}}^d(\mathscr{C},\mathscr{V})$.

Let U be a nonempty open subset of V and let $\mathrm{Hom}_{\mathscr{C}}^d(\mathscr{C},\mathscr{V})_U$ be the complement of the closed subscheme of $\mathrm{Hom}_{\mathscr{C}}^d(\mathscr{C},\mathscr{V})$ defined by the condition $\sigma(\mathscr{C})\subset|\mathscr{V}\setminus U|$. This open subscheme $\mathrm{Hom}_{\mathscr{C}}^d(\mathscr{C},\mathscr{V})_U$ parametrises sections $\sigma:\mathscr{C}\to\mathscr{V}$ such that $f(\eta_{\mathscr{C}})\in U(F)$ and $\deg(\sigma^*(\mathscr{L}))=d$. It is again a quasiprojective scheme, since $\mathrm{Hom}_{\mathscr{C}}^d(\mathscr{C},\mathscr{V})$ is.

The restriction L of $\mathscr{L}$ to V is isomorphic to a linear combination

$$\bigotimes_{i=1}^{r} L_i^{\otimes\lambda_i}$$

of the L_i. Let $\mathscr{L}'$ be the invertible sheaf

$$\bigotimes_{i=1}^{r} \mathscr{L}_i^{\otimes\lambda_i}$$

on $\mathscr{V}$.

Let $\delta\in\mathrm{Pic}(V)^\vee$ be a multidegree and $\sigma:\mathscr{C}\to\mathscr{V}$ a section such that $\mathbf{deg}_{\underline{\mathscr{L}}}(\sigma)=\delta$ and $\sigma(\eta_{\mathscr{C}})\in U(F)$. Then

$$\begin{aligned}\deg(\sigma^*\mathscr{L})&=\deg(\sigma^*\mathscr{L})-\deg(\sigma^*\mathscr{L}')+\deg(\sigma^*\mathscr{L}')\\&=\deg(\sigma^*\mathscr{L})-\deg(\sigma^*\mathscr{L}')+\delta\cdot L.\end{aligned}$$

Since the restriction of $\mathscr{L}\otimes(\mathscr{L}')^{-1}$ to the generic fibre is trivial, there exist vertical divisors E and E' such that

$$\mathscr{L}\otimes(\mathscr{L}')^{-1}\simeq\mathscr{O}_{\mathscr{V}}(E'-E).$$

In particular, the difference $\deg(\sigma^*\mathscr{L})-\deg(\sigma^*\mathscr{L}')$ only takes a finite number of values, since σ has intersection of degree 1 with any fibre of π. Let a be its maximal value. Moreover, by flatness, the r conditions given by $\mathbf{deg}_{\underline{\mathscr{L}}}=\delta$ are open and closed in the Hilbert scheme of $\mathscr{V}$. Therefore $\mathbf{Hom}_{\mathscr{C}}^\delta(\mathscr{C},\mathscr{V})_U$ can be identified with an open subfunctor of

$$\coprod_{0\leqslant d\leqslant a+\delta\cdot L}\mathbf{Hom}_{\mathscr{C}}^d(\mathscr{C},\mathscr{V})_U,$$

and hence the lemma. $\square$

1.3. ***Greenberg schemes and motivic integrals.*** A reference for this subsection is given by Chapters 4 to 6 of [19].

If R is a complete discrete valuation ring, with field of fractions F and residue field κ such that F and κ have equal characteristic, then the choice of a uniformiser π of R together with a section of $R\to\kappa$ provides a morphism of κ-algebras

$$\kappa[\![t]\!]\to R,\quad t\mapsto\pi,$$

which is an isomorphism by Theorem 2 of [10, Chapter IX, Section 3].

Example 1.7. If p is a closed point of the smooth projective k-curve $\mathscr{C}$, the previous result applies to the completed local ring $R_p = \widehat{\mathscr{O}}_{\mathscr{C},p}$.

Definition 1.8 (Greenberg schemes). Let R be a complete discrete valuation ring, with maximal ideal $\mathfrak{m}$ and residue field $\kappa = R/\mathfrak{m}$. Assume that R has equal characteristic and fix a section of $R \to \kappa$.

Let $\mathscr{X}$ be an R-variety. For any nonnegative integer m, the Greenberg scheme of order m of $\mathscr{X}$ is the κ-scheme $\mathrm{Gr}_m(\mathscr{X})$ representing the functor

$$A \mapsto \mathrm{Hom}_R(\mathrm{Spec}(R_m \otimes_\kappa A), \mathscr{X})$$

on the category of κ-algebras [19, Chapter 4, Section 2.1], where $R_m = R/\mathfrak{m}^{m+1}$ for all $m \geqslant 0$. There are canonical affine projection morphisms

$$\theta_m^{m+1} : \mathrm{Gr}_{m+1}(\mathscr{X}) \to \mathrm{Gr}_m(\mathscr{X}),$$

given by truncation, and the Greenberg scheme is the κ-proscheme

$$\mathrm{Gr}_\infty(\mathscr{X}) = \varprojlim \mathrm{Gr}_m(\mathscr{X})$$

(or more concisely $\mathrm{Gr}(\mathscr{X})$) which represents the functor

$$A \mapsto \mathrm{Hom}_\kappa(\mathrm{Spec}(A \otimes_\kappa R), X)$$

on the category of κ-algebras. This scheme carries a canonical projection

$$\theta_m^\infty : \mathrm{Gr}_\infty(\mathscr{X}) \to \mathrm{Gr}_m(\mathscr{X})$$

for every nonnegative integer m, called the truncation of level m.

Example 1.9. If $\mathscr{V} \to \mathscr{C}$ is a model of a projective variety V over $F = k(\mathscr{C})$, let $\mathscr{V}_{R_p}$ be the schematic fibre over the completed local ring $R_p = \widehat{\mathscr{O}}_{\mathscr{C},p}$. If $\mathfrak{m}_p$ is the maximal ideal of R_p, then the κ_p-points respectively of $\mathrm{Gr}_m(\mathscr{V}_{R_p})$ and $\mathrm{Gr}(\mathscr{V}_{R_p})$ are in bijection respectively with the sets of points $\mathscr{V}_{R_p}(R_p/\mathfrak{m}_p^{m+1})$ and $\mathscr{V}_{R_p}(R_p)$. Moreover, if $\mathscr{V} \to \mathscr{C}$ is proper, by the valuative criterion of properness the set $\mathscr{V}_{R_p}(R_p)$ is in one-to-one correspondence with the set $V_{F_p}(F_p)$, where F_p is the completion of F at p.

By [19, Chapter 4, Lemma 4.2.2], the constructible subsets of $\mathrm{Gr}(\mathscr{X})$ are exactly the subsets C of the form

$$C = (\theta_m^\infty)^{-1}(C_m)$$

for a certain level m and a constructible subset C_m of $\mathrm{Gr}_m(\mathscr{X})$. Moreover, if C is Zariski closed, respectively Zariski open, then C_m can be chosen to be closed, respectively open. Then, a map

$$f : C \to \mathbb{Z} \cup \{\infty\}$$

on a constructible subset C of $\mathrm{Gr}(\mathscr{X})$ is said to be constructible if $f^{-1}(n)$ is constructible for every $n \in \mathbb{Z}$.

By [19, Chapter 6, Section 2], there is an additive motivic measure

$$\mu_{\mathscr{X}} : \mathrm{Cons}_{\mathrm{Gr}(\mathscr{X})} \to \widehat{\mathscr{M}}_{\mathscr{X}_0}^{\dim}$$

(where $\mathscr{X}_0$ is the special fibre of $\mathscr{X}$) called the *motivic volume* or *motivic density*, which extends to a countably additive motivic measure $\mu^*_{\mathscr{X}}$ on a class $\mathrm{Cons}^*_{\mathrm{Gr}(\mathscr{X})}$ of measurable subsets of $\mathrm{Gr}(\mathscr{X})$; see [19, Chapter 6, Section 3]. For example, if $\mathscr{X}$ is smooth of pure relative dimension d over R, then

$$\mu_{\mathscr{X}}(\mathrm{Gr}(\mathscr{X})) = [\mathscr{X}_0]\,\mathbb{L}^{-d}.$$

If A is a measurable subset of $\mathrm{Gr}(\mathscr{X})$ and $f : A \to \mathbb{Z} \cup \{\infty\}$ has measurable fibres (by this we mean that $f^{-1}(n)$ is measurable for all $n \in \mathbb{Z}$) such that the series

$$\sum_{n\in\mathbb{Z}} \mu^*_{\mathscr{X}}(f^{-1}(n))\mathbb{L}^{-n}$$

is convergent in $\widehat{\mathscr{M}}^{\dim}_{\mathscr{X}_0}$, then the motivic integral of $\mathbb{L}^{-f}$

$$\int_A \mathbb{L}^{-f}\,\mathrm{d}\mu^*_{\mathscr{X}} = \sum_{n\in\mathbb{Z}} \mu^*_{\mathscr{X}}(f^{-1}(n))\mathbb{L}^{-n}$$

is well-defined.

Remark 1.10. By the quasicompactness of the constructible topology, a constructible function f which does not reach infinity is bounded and thus only takes a finite number of values. In particular, if f is bounded constructible, then f is measurable and $\mathbb{L}^{-f}$ is integrable; see Example 4.1.3 in [19, Chapter 6].

As explained in [19, Chapter 4, (3.3.7)], one can go from points on $\mathscr{X}$ with coordinates in extensions of R of ramification index 1 to points on the Greenberg schemes of $\mathscr{X}$. For this it is convenient to use the functors from κ-algebras to rings given by

$$\mathscr{R}_m : A \mapsto R_m \otimes_\kappa A$$

for any nonnegative integer m, which form a system of functors whose limit is

$$\mathscr{R}_\infty : A \mapsto R \,\widehat{\otimes}_\kappa\, A = \varprojlim R_m \otimes_\kappa A.$$

Such functors are represented respectively by $\mathbb{A}^m_k$, $m \in \mathbb{N}$, and $\mathbb{A}^{\mathbb{N}}_k$. If k' is a field extension of k, then $R' = \mathscr{R}_\infty(k')$ is an extension of R with ramification index 1 (the only one up to unique isomorphism if k'/k is unramified), by Proposition 2.3.2 of [19, Chapter 4]. Then by the definition of $\mathrm{Gr}_\infty(\mathscr{X})$ there is a canonical bijection

$$\mathrm{Gr}_\infty(\mathscr{X})(k') \xrightarrow{\sim} \mathscr{X}(\mathscr{R}_\infty(k'))$$

which is compatible with the truncation morphisms. Thus, if one wants to define functions at the level of Greenberg schemes, it is enough to define them on R'-points for any extension R' of ramification index 1 over the complete valuation ring R. This will allow one to use such functions on Greenberg schemes of weak Néron models later in Section 1.5, thanks to Proposition 1.25 stated a few pages below.

Definition 1.11 [19, Chapter 5, Section 3.1]. Let $f : \mathscr{Y} \to \mathscr{X}$ be a morphism of flat R-schemes of finite type and pure relative dimension d. Let R' be an extension of R and $q \in \mathscr{Y}(R')$. Consider the morphism

$$\alpha(q) : ((f \circ q)^{*}\Omega^{d}_{\mathscr{X}/R'})/(\text{torsion}) \to (q^{*}\Omega^{d}_{\mathscr{Y}/R'})/(\text{torsion})$$

of free R'-modules of finite rank induced by f.

The *order of the Jacobian of f along q* is defined by

$$\operatorname{ordjac}_f(q) = \operatorname{length}_{R'} \operatorname{coker}(\alpha(q)).$$

This provides a function

$$\operatorname{ordjac}_f : \operatorname{Gr}(\mathscr{Y}) \to \mathbb{N}.$$

Note that by Proposition 3.1.4 of [19, Chapter 5], if $\mathscr{Y}$ is smooth over R and the restriction of f to generic fibres is étale, then ordjac_f is constructible and bounded.

Proposition 1.12 (smooth change of variable). *Let $\mathscr{X}$ and $\mathscr{Y}$ be two R-schemes of finite type and pure relative dimension d, with singular loci respectively $\mathscr{X}_{\text{sing}}$ and $\mathscr{Y}_{\text{sing}}$. Let $f : \mathscr{Y} \to \mathscr{X}$ be a morphism of R-schemes. Let A and B be constructible subsets respectively of* $\operatorname{Gr}(\mathscr{X}) - \operatorname{Gr}(\mathscr{X}_{\text{sing}})$ *and* $\operatorname{Gr}(\mathscr{Y}) - \operatorname{Gr}(\mathscr{Y}_{\text{sing}})$. *Assume that f induces a bijection*

$$B(\kappa') \to A(\kappa')$$

for every extension κ' of κ, and that $B \cap \operatorname{ordjac}_f^{-1}(+\infty)$ is empty.

Let $\alpha : A \to \mathbb{Z}$ be a constructible function on A. Then the function

$$\beta : y \in B \mapsto (\alpha \circ \operatorname{Gr}(f))(y) + \operatorname{ordjac}_f(y)$$

is constructible and

$$\int_A \mathbb{L}^{-\alpha}\, \mathrm{d}\mu_{\mathscr{X}} = f_{0!} \int_B \mathbb{L}^{-\beta}\, \mathrm{d}\mu_{\mathscr{Y}}$$

in $\mathscr{M}_{\mathscr{X}_0}$.

Proof. See Theorem 1.2.5 in [19, Chapter 6]. □

Remark 1.13. Here the symbol $\mathbb{L}^{-\operatorname{ordjac}_f}$ plays the role of the absolute value of the determinant $|\det((\partial x_i/\partial y_j)_{i,j})|$ in the usual change-of-variable formula.

1.4. ***Local intersection degrees.*** Let L be an invertible sheaf on V. A coherent sheaf on $\mathscr{V}$ whose restriction to V is isomorphic to L is called a *model* of L. In this subsection we define local intersection degrees on L of a section $\mathscr{C} \to \mathscr{V}$ at a closed point $p \in \mathscr{C}$, with respect to a model of L, and study the difference between the degrees given by two different models of L. This is a reformulation, in the framework of Greenberg schemes and motivic integration [19], of the p-adic and adelic metrics of [52, Section 1.2]. Let us first recall the local definition of such metrics.

Definition 1.14. Let R be a complete discrete valuation ring with fraction field K. Let $\mathscr{X}$ be an R-scheme of pure dimension, X its generic fibre, L an invertible sheaf on X and $\mathscr{L}$ a model of L on $\mathscr{X}$ (not necessarily invertible).

For any extension R' of R, of ramification index 1 over R, with uniformiser ϖ and field of fractions K', we define order functions on $\mathscr{X}(R')$ as follows: let $\tilde{q} : \mathrm{Spec}(R') \to \mathscr{X}$ be an R'-point of $\mathscr{X}$, q be its restriction to the generic fibre and y a point of the K'-vector space $q^*L = (\tilde{q}^*\mathscr{L}) \otimes_{R'} K'$. Then we set, if $q^*y \neq 0$,

$$\mathrm{ord}_{\tilde{q}}(y) = \max\{n \in \mathbb{Z} \mid \varpi^{-n} y \in \tilde{q}^*\mathscr{L}/(\text{torsion})\}$$

(the unique integer ℓ such that $\varpi^{-\ell} y$ is a generator of the R'-lattice $\tilde{q}^*\mathscr{L}/(\text{torsion})$), and

$$\mathrm{ord}_{\tilde{q}}(y) = \infty$$

if $q^*y = 0$.

In other words, $\mathrm{ord}_{\tilde{q}}(y)$ is the valuation of y with respect to the lattice $\tilde{q}^*\mathscr{L}/(\text{torsion})$: given a generator y_0 of $\tilde{q}^*\mathscr{L}/(\text{torsion})$,

$$\mathrm{ord}_{\tilde{q}}(y) = v_{R'}(y/y_0) \in \mathbb{Z} \cup \{\infty\},$$

where $v_{R'}$ is the normalised discrete valuation extended to K'. In particular, this definition does not depend on the choice of the uniformiser ϖ nor on the choice of the generator y_0.

If s is a section of L on an open set containing q, then

$$\mathrm{ord} \circ s : \mathscr{X}(R') \to \mathbb{Z} \cup \{\infty\}$$

is the function sending $\tilde{q} \in \mathscr{X}(R')$ to $\mathrm{ord}_{\tilde{q}}(s(q))$.

Remark 1.15. We are going to apply the previous definition as follows. Let $\mathscr{V}$ be a proper model of a smooth F-variety V. We fix a closed point $p \in \mathscr{C}$ and work with the R_p-scheme $\mathscr{V}_{R_p}$, identifying the sets $V(F_p)$ and $\mathscr{V}(R_p)$ by properness. We take L to be an invertible sheaf on V and $\mathscr{L}$ a model of L on $\mathscr{V}$.

If q is an F_p-point of V, the function $\mathrm{ord}_{\tilde{q}}$ is well-defined on $L_q(F_p)$. Of course, any F_p-point of L belongs to the fibre of a unique F_p-point of V, so that this function extends to a function

$$\mathrm{ord}_p : L(F_p) \to \mathbb{Z} \cup \{\infty\}, \quad y \mapsto \mathrm{ord}_{\tilde{q}}(y) \text{ whenever } y \in L_q.$$

If $s \in \Gamma(U, L)$ is a section of L above an open subset $U \subset V$, by composition one gets a map

$$\mathrm{ord}_p \circ s : U(F_p) \to \mathbb{Z} \cup \{\infty\}, \quad x \mapsto \mathrm{ord}_{\tilde{x}}(s(x)).$$

If $\mathscr{D}$ is a Cartier divisor on $\mathscr{V}$ given by a rational section of $\mathscr{L}$ and s is the restriction of this section to V, defined on an open subset $U \subset V$, then $\mathrm{ord}_p(s(x))$ coincides with the intersection number $(x, \mathscr{D})_p = \deg(\tilde{x}^*\mathscr{D})$ for all $x \in U(F_p)$ not in $\mathscr{D}$. Besides, both take an infinite value whenever x lies in $\mathscr{D}$.

By the product formula, for all $x \in V(F)$ the (finite) sum on closed points

$$\sum_{p \in |\mathscr{C}|} \mathrm{ord}_p(s(x)) \in \mathbb{Z}$$

does not depend on the choice of a local section s of L such that $s(x) \neq 0$, and if $\sigma : \mathscr{C} \to \mathscr{V}$ is the section of the proper model $\mathscr{V}$ given by the point $x \in V(F)$, then

$$\deg(\sigma^*\mathscr{L}) = \sum_{p\in|\mathscr{C}|} \mathrm{ord}_p(s(x)).$$

We go back to the notation of Definition 1.14.

Lemma 1.16. *Let $\mathscr{X}$ be a model of X and $\mathscr{L}$, $\mathscr{L}'$ be two models of L, and* ord, ord$'$ *the corresponding order functions given by Definition 1.14. For all $\tilde{x} \in \mathscr{X}(R')$, the difference*

$$y \mapsto \mathrm{ord}'_{\tilde{x}}(y) - \mathrm{ord}_{\tilde{x}}(y)$$

is constant on the stalks of L. This constant value defines a function

$$\varepsilon_{\mathscr{L}'-\mathscr{L}} : \mathrm{Gr}_\infty(\mathscr{X}) \to \mathbb{Z}.$$

Proof. The difference of the two corresponding valuations is

$$\mathrm{ord}'_{\tilde{x}}(y) - \mathrm{ord}_{\tilde{x}}(y) = v_{R'}(y/y'_0) - v_{R'}(y/y_0) = v_{R'}(y_0/y'_0)$$

for every $\tilde{x} \in \mathscr{X}(R')$ and $y \in x^*L$, where y_0 and y'_0 are generators respectively of $\tilde{x}^*\mathscr{L}$ and $\tilde{x}^*\mathscr{L}'$ in x^*L. Consequently, this difference induces a map

$$\tilde{x} \in \mathscr{X}(R') \mapsto v_{R'}(y_0/y'_0)$$

which does not depend on the choices of the generators y_0 and y'_0 of $\tilde{x}^*\mathscr{L}$ and $\tilde{x}^*\mathscr{L}'$, since the quotient of two generators has valuation zero. □

Remark 1.17. Note that if $\mathscr{L}$, $\mathscr{L}'$ and $\mathscr{L}''$ are three models of L, we have the relation

$$\varepsilon_{\mathscr{L}''-\mathscr{L}} = \varepsilon_{\mathscr{L}''-\mathscr{L}'} + \varepsilon_{\mathscr{L}'-\mathscr{L}}.$$

Remark 1.18. If $\mathscr{I}$ is a coherent sheaf of ideals on $\mathscr{X}$, an order function

$$\mathrm{ord}_{\mathscr{I}} : \mathrm{Gr}_\infty(\mathscr{X}) \to \mathbb{N} \cup \{+\infty\}$$

can be obtained by taking

$$\mathrm{ord}_{\mathscr{I}}(\tilde{x}) = \inf_{f\in\mathscr{I}_{\tilde{x}}} v_{R'}(f(\tilde{x}))$$

for all points $\tilde{x} \in \mathscr{X}(R')$, where $v_{R'}(f(\tilde{x})) = v_{R'}(\tilde{x}^*f)$; see (4.4.3) of [19, Chapter 4]. By Corollary 4.4.8 of [19, Chapter 4] this defines a constructible function $\mathrm{Gr}_\infty(\mathscr{X}) \to \mathbb{N} \cup \{+\infty\}$.

The affine local description of this function [19, Chapter 4, Example 4.4.4] shows that $\mathrm{ord}_{\mathscr{I}}(\tilde{x})$ is given by the smallest $v_{R'}(f(\tilde{x}))$ for f belonging to a finite set of generators of the ideal corresponding to $\mathscr{I}$. In particular, if $\mathscr{I}$ and $\mathscr{I}'$ are two coherent sheaves of ideals, with local generators respectively $y_0 \in \mathscr{I}_{\tilde{x}}$ and $y'_0 \in \mathscr{I}'_{\tilde{x}}$, and whose restrictions I and I' to X are invertible and isomorphic, then $\mathrm{ord}_{\mathscr{I}}(\tilde{x}) = v_{R'}(\tilde{x}^*y_0)$

and for all $y \in I_x \simeq I'_x$

$$\begin{aligned}\operatorname{ord}'_{\tilde{x}}(y) - \operatorname{ord}_{\tilde{x}}(y) &= v_{R'}(y/(1/y'_0)) - v_{R'}(y/(1/y_0)) = v_{R'}(y'_0/y_0)\\ &= v_{R'}(\tilde{x}^* y'_0) - v_{R'}(\tilde{x}^* y_0)\\ &= \operatorname{ord}_{\mathscr{I}'}(\tilde{x}) - \operatorname{ord}_{\mathscr{I}}(\tilde{x}).\end{aligned}$$

The $(1/y_0)$ here comes from the fact that the ideal sheaf associated to an effective Cartier divisor D on X is $\mathscr{O}_X(-D)$.

Lemma 1.19. *The difference $\varepsilon_{\mathscr{L}'-\mathscr{L}}$ is a constructible function on $\operatorname{Gr}_\infty(\mathscr{X})$. By the quasicompactness of the constructible topology, it takes only finitely many values.*

Proof. Let $n \in \mathbb{Z}$. Assume first that $n \geqslant 0$. Then $\varepsilon_{\mathscr{L}'-\mathscr{L}}(\tilde{x}) > n$ if and only if y_0/y'_0 belongs to the $(n{+}1)$-th power of the maximal ideal of R if and only if its class in R_n is zero.

We claim that there exists $n_0 \in \mathbb{Z}$ such that $\varepsilon_{\mathscr{L}'-\mathscr{L}}(\tilde{x}) \geqslant n_0$ for all $\tilde{x} \in \mathscr{X}(R')$. We choose generators y_0 and y'_0 of $\tilde{x}^*\mathscr{L}$ and $\tilde{x}^*\mathscr{L}'$. Then the rational section $y_0/y'_0 \in K'$ of $(\mathscr{L}')^\vee \otimes \mathscr{L}$ has a vertical divisor of poles E which is the pull-back of a formal multiple of the closed point of R', and $(\mathscr{L}')^\vee \otimes \mathscr{L} \otimes \mathscr{O}_{\mathscr{X}}(-E)$ is effective. Let z_0 be a generator of E; then $z_0(y_0/y'_0) \in R'$ and

$$\varepsilon_{\mathscr{L}'-\mathscr{L}}(\tilde{x}) = v_{R'}(y_0/y'_0) = v_{R'}\left(\frac{y_0 z_0}{y'_0}\cdot\frac{1}{z_0}\right) = v_{R'}\left(\frac{y_0 z_0}{y'_0}\right) - v_{R'}(z_0) \geqslant -v_{R'}(z_0).$$

We take $n_0 = -v_{R'}(z_0)$ so that

$$\varepsilon_{\mathscr{L}'-\mathscr{L}}(\tilde{x}) = v_{R'}(\varpi^{-n_0} y'_0/y_0) + n_0$$

for all $\tilde{x}$. Then for a given $n \geqslant n_0$, one has $\varepsilon_{\mathscr{L}'-\mathscr{L}}(\tilde{x}) > n$ if and only if $\varpi^{-n_0} y'_0/y_0$ belongs to the $(n{-}n_0{+}1)$-th power of the maximal ideal of R if and only if its class in R_{n-n_0} is zero. Thus

$$\{\xi \in \operatorname{Gr}(\mathscr{X}) \mid \varepsilon_{\mathscr{L}'-\mathscr{L}}(\xi) > n\}$$

is constructible of level $\leqslant (n-n_0)$.

Moreover it follows from the definition that $\varepsilon_{\mathscr{L}'-\mathscr{L}}$ does not reach infinity. Thus it takes only a finite number of values by the quasicompactness of the constructible topology (see for example Theorem 1.2.4 in [19, Appendix A]). □

Remark 1.20. Note that this difference is trivial if $\mathscr{L}$ and $\mathscr{L}'$ are already isomorphic above R. In particular, if $\mathscr{L}$ and $\mathscr{L}'$ are two different models on $\mathscr{V} \to \mathscr{C}$ of the same L on V, there exists a dense open subset of $\mathscr{C}$ above which they are isomorphic. Its complement S is a finite set of closed points of $\mathscr{C}$ and

$$\deg_{\mathscr{L}'} - \deg_{\mathscr{L}} = \sum_{p \in \mathsf{S}} \varepsilon_{\mathscr{L}'_{R_p} - \mathscr{L}_{R_p}}$$

is bounded.

Definition 1.21 (motivic density associated to a model of the anticanonical sheaf). Let $\mathscr{X}$ be an R-scheme of pure relative dimension n.

Assume that the generic fibre X is smooth over K and take a model $\mathscr{L}_{\mathscr{X}}$ of the anticanonical sheaf ω_X^{-1} over $\mathscr{X}$.

The sheaf $\Omega^1_{\mathscr{X}/R}$ of relative differentials of $\mathscr{X}$ over R [36, p. 175] is a coherent sheaf of $\mathscr{O}_{\mathscr{X}}$-modules and the dual of its determinant $(\Lambda^n\Omega^1_{\mathscr{X}/R})^\vee$ is a model of ω_X^{-1}.

By Lemma 1.19 the local difference function $\varepsilon_{\mathscr{L}_{\mathscr{X}}-(\Lambda^n\Omega^1_{\mathscr{X}/R})^\vee}$ is a constructible function.

Its motivic integral over any measurable subset A avoiding the singular locus of $\mathscr{X}$ will be written

$$\mu^*_{\mathscr{L}_{\mathscr{X}}}(A) = \int_A \mathbb{L}^{-\varepsilon_{\mathscr{L}_{\mathscr{X}}-(\Lambda^n\Omega^1_{\mathscr{X}/R})^\vee}} \,\mathrm{d}\mu^*_{\mathscr{X}}$$

and $\mu^*_{\mathscr{L}_{\mathscr{X}}}$ will be called *motivic density associated to $\mathscr{L}_{\mathscr{X}}$.*

1.5. ***Weak Néron models and smoothening.*** In order to prove our result about invariance by change of model (see Theorem 4.6 below), we need to collect a few additional definitions and results about weak Néron models and relations between them. References for this subsection are the third chapter of the book of Bosch, Lütkebohmert and Raynaud [7], together with the reminder of Section 7.1 in [19, Chapter 7], as well as Section 3.4 in [19, Chapter 4].

1.5.1. *Local models.* We keep the notation of the previous subsection, except that we do not need to assume that R is complete.

Definition 1.22. Let X be a K-variety.

A model for X is a flat separated R-scheme of finite type $\mathscr{X}$ together with an isomorphism $\mathscr{X}_K \to X$.

A *weak Néron model*[2] of X is a model $\mathscr{X}$ of X such that $\mathscr{X}$ is smooth over R and every K'-point of X extends to an R'-point of $\mathscr{X}$ for every unramified extension R' of R with fraction field K'. Since by definition $\mathscr{X}$ is separated, such an R'-point is unique.

Let $\mathscr{Y}$ be a flat separated R-scheme of finite type with smooth generic fibre. A *Néron smoothening* of $\mathscr{Y}$ is a smooth R-scheme $\mathscr{X}$ of finite type together with an R-morphism $\mathscr{X} \to \mathscr{Y}$ inducing an isomorphism $\mathscr{X}_K \to \mathscr{Y}_K$ and such that $\mathscr{X}(R') \to \mathscr{Y}(R')$ is bijective for every unramified extension R' of R.

Given $\mathscr{X}$ and $\mathscr{X}'$ two weak Néron models of X, a morphism of weak Néron models is a R-morphism $\mathscr{X}' \to \mathscr{X}$ whose restriction to the generic fibre commutes with the isomorphisms with X. In that case we say that $\mathscr{X}'$ dominates $\mathscr{X}$.

The following is a short reformulation of Theorem 3 and Corollary 4 of [7, p. 61]:

Theorem 1.23. *Every R-scheme of finite type whose generic fibre is smooth over K admits a Néron smoothening, given by the R-smooth locus of a composition of admissible blow-ups.*

Even if the result is formulated in the language of formal schemes, the proof of Proposition 3.4.7 in [19, Chapter 3], which is a variant of the Néron smoothening algorithm of [7], gives the following useful proposition.

[2]We adopt the terminology used by Chambert-Loir, Nicaise and Sebag in [19]. For the comparison of this definition of weak Néron models with the one given by Bosch, Lütkebohmert and Raynaud in [7], see Remark 7.1.6 in [19, Chapter 7]. The main difference is a properness assumption.

Proposition 1.24. *Let X be a smooth K-variety. If $\mathscr{X}'$ and $\mathscr{X}''$ are two models of X, then there exists another model $\mathscr{X}''$ of X above $\mathscr{X}$ and $\mathscr{X}'$ whose R-smooth locus $(\mathscr{X}'')^\circ$ is a Néron smoothening of both models*:

$$\begin{tikzcd}
 & (\mathscr{X}'')^\circ \arrow[ddl] \arrow[d] \arrow[ddr] & \\
 & \mathscr{X}'' \arrow[dl] \arrow[dr] \arrow[dd] & \\
\mathscr{X} \arrow[dr] & & \mathscr{X}' \arrow[dl] \\
 & \mathrm{Spec}(R) &
\end{tikzcd}$$

In the equal characteristic case, we have the following correspondence of points of Greenberg schemes; see Proposition 3.5.1 of [19, Chapter 4]. It allows one to apply the motivic change of variable formula, Proposition 1.12, to Néron smoothenings.

Proposition 1.25. *Let $\mathscr{Y} \to \mathscr{X}$ be a morphism of separated flat R-schemes of finite type, restricting to an immersion on generic fibres and such that $\mathscr{Y}$ is smooth.*

Then $\mathscr{Y} \to \mathscr{X}$ is a Néron smoothening if and only if the induced map

$$\mathrm{Gr}(\mathscr{Y})(\kappa') \to \mathrm{Gr}(\mathscr{X})(\kappa')$$

is a bijection for every separable extension κ' of κ.

Proposition 1.26. *Let $\mathscr{X}$ be an R-model of a smooth K-variety X, of pure relative dimension n, and $f : \mathscr{Y} \to \mathscr{X}$ a Néron smoothening of $\mathscr{X}$.*

Then

$$\varepsilon_{(\Omega^n_{\mathscr{Y}/R})^\vee - f^*(\Omega^n_{\mathscr{X}/R})^\vee} = \mathrm{ordjac}_f$$

on $\mathrm{Gr}(\mathscr{Y})$.

Proof. This is given by the argument of the chain rule (5.2.2) in [19, Chapter 7] and the fact that in our situation the function ordjac_f coincides with the order function of the Jacobian ideal of f. See Lemma 3.1.3 in [19, Chapter 5] as well. □

1.5.2. *From local models to global ones.* We will need the following gluing result, which is a variant of [7, p. 18, Proposition 1].

Proposition 1.27. *Let $\mathscr{V} \to \mathscr{C}$ be a model of V above $\mathscr{C}$. Let $\mathscr{C}_0$ be a dense open subset of $\mathscr{C}$ and $\mathscr{V}_0', \mathscr{V}_1', \dots, \mathscr{V}_s'$ be a finite number of models of V respectively over $\mathscr{C}_0$ and over the local rings of the closed points $p_1, \dots, p_s$ not in $\mathscr{C}_0$. Assume that these models dominate respectively the restriction of $\mathscr{V}$ to $\mathscr{C}_0$ and to these local rings. In particular, they induce isomorphisms on generic fibres.*

Then there exists a model $\mathscr{V}' \to \mathscr{C}$ of V extending $\mathscr{V}_0, \dots, \mathscr{V}_s$, as well as a $\mathscr{C}$-morphism $\mathscr{V}' \to \mathscr{V}$ extending the local ones. If moreover the local models are smooth, then $\mathscr{V}' \to \mathscr{C}$ is smooth as well.

Proof. Let R_i be the local ring of $\mathscr{C}$ at the point $p_i \in \mathscr{C} \setminus \mathscr{C}_0$ for $i = 1, \dots, s$. The morphism $\mathscr{V}_i' \to \mathscr{V}_{R_i}$ uniquely extends to a $\mathscr{C}_i$-morphism for a certain open neighbourhood $\mathscr{C}_i$ of p_i by [28, Théorème 8.8.2].

Since $(\mathscr{V}'_i)_F \simeq (\mathscr{V}_{R_i})_F \simeq V$, such a model coincides with $\mathscr{V}'_0 \to \mathscr{C}_0$ above a nonempty open subset $\mathscr{C}'_0 \subset \mathscr{C}_0$. Then, up to removing a finite number of points of $\mathscr{C}'_i$ so that $\mathscr{C}_i \cap (\mathscr{C} - \mathscr{C}'_0) = \{s_i\}$, we can assume that they coincide above $\mathscr{C}_i \cap \mathscr{C}'_0$ and glue them above each $\mathscr{C}_i \cap \mathscr{C}'_0$, obtaining a model extending the starting data and dominating $\mathscr{V} \to \mathscr{C}$. $\square$

For us, a weak Néron model of V above $\mathscr{C}$ will be a smooth $\mathscr{C}$-scheme $\mathscr{V}$ of finite type, together with an isomorphism $\mathscr{V}_F \to V$ and satisfying the following property concerning étale integral points: for any closed point p and any étale local $\mathscr{O}_{\mathscr{C},p}$-algebra R' with field of fractions F', the canonical map $\mathscr{V}(R') \to \mathscr{V}_F(F')$ is surjective (see p. 7, Definition 1, as well as the end of p. 12, and p. 60–61 in [7]).

Corollary 1.28. *Let $\mathscr{V}$ and $\mathscr{V}'$ be two models of V above $\mathscr{C}$. Then there exists a third model $\mathscr{V}''$ of V above $\mathscr{C}$ whose $\mathscr{C}$-smooth locus is a Néron smoothening of both $\mathscr{V}$ and $\mathscr{V}'$ above $\mathscr{C}$:*

$$\begin{tikzcd} & \mathscr{V}'' \arrow[dl] \arrow[dr] \arrow[dd] & \\ \mathscr{V} \arrow[dr] & & \mathscr{V}' \arrow[dl] \\ & \mathscr{C} & \end{tikzcd}$$

Moreover, if $\mathscr{V}$ and $\mathscr{V}'$ are proper, then $\mathscr{V}''$ can be taken proper as well.

Proof. By spreading-out [28, Théorème 8.8.2] applied to the generic point of $\mathscr{C}$, we know the existence of a nonempty open subset $\mathscr{C}' \subset \mathscr{C}$ such that the restrictions of $\mathscr{V}$ and $\mathscr{V}'$ above $\mathscr{C}'$ are isomorphic as $\mathscr{C}'$-schemes:

$$\begin{tikzcd} \mathscr{V}_{\mathscr{C}'} \arrow[rr, "\sim"] \arrow[d] \arrow[dr] & & \mathscr{V}'_{\mathscr{C}'} \arrow[d] \arrow[dl] \\ \mathscr{V} \arrow[dr] & \mathscr{C}' \arrow[d] & \mathscr{V}' \arrow[dl] \\ & \mathscr{C} & \end{tikzcd}$$

Then, for each closed point p in the complement of $\mathscr{C}'$, by Proposition 1.24 we can find a weak Néron model which dominates both restrictions of $\mathscr{V}$ and $\mathscr{V}'$ to $\operatorname{Spec}(\mathscr{O}_{\mathscr{C},p})$. One can use Proposition 1.27 to glue $\mathscr{V}_{\mathscr{C}'}$ together with these models and get the desired new weak Néron model. These operations preserve properness, by the valuative criterion. $\square$

1.6. *Piecewise trivial fibrations.* In this subsection S is a Noetherian scheme. We recall definitions and properties of (classes in $K_0\mathbf{Var}_S$) of piecewise trivial fibrations, following [19, Chapter 2, Section 2.3].

Definition 1.29. Let F be an S-variety. A *piecewise trivial fibration with fibre F* is a morphism of schemes $f : X \to Y$ between two S-varieties such that there exists a finite partition $(Y_i)_{i\in I}$ of Y into locally closed subsets together with an isomorphism of $(Y_i)_{\mathrm{red}}$-schemes between $(X \times_Y Y_i)_{\mathrm{red}}$ and $(F \times_S Y_i)_{\mathrm{red}}$ for all $i \in I$.

Proposition 1.30. *Let F be an S-variety and $f : X \to Y$ a piecewise trivial fibration with fibre F. Then*

$$[X] = [F][Y]$$

in $K_0\mathbf{Var}_S$.

Proof. See Corollary 1.4.9 and Proposition 2.3.3 of [19, Chapter 2]. □

We will make extensive use of the following criterion.

Proposition 1.31. *Let F be an S-variety and $f : X \to Y$ a morphism of S-varieties. Then f is a piecewise trivial fibration with fibre F if and only if, for every point $y \in Y$, the $\kappa(y)$-schemes $f^{-1}(y)_{\mathrm{red}}$ and $(F \otimes_k \kappa(y))_{\mathrm{red}}$ are isomorphic.*

Proof. See Proposition 2.3.4 of [19, Chapter 2] (one proceeds by Noetherian induction and applies [28, Théorème 8.10.5]). □

2. Motivic Euler products

2.1. ***The weight filtration.*** In this S is a variety over a subfield k of the field $\mathbb{C}$ of complex numbers. We fix once and for all an embedding of k in $\mathbb{C}$ and consider that S is actually defined over $\mathbb{C}$ by extension of scalars. We briefly recall the construction of a weight filtration on the Grothendieck ring of varieties over S. We use [49] as a general reference for mixed Hodge modules, as well as the summaries of [3, Chapter 4] and [19, Chapter 2, Section 3.1–3.3].

2.1.1. *Mixed Hodge modules.* The category $\mathbf{MHM}_S$ of mixed Hodge modules over S was introduced by Saito in [56; 57]. It is an abelian category which provides a cohomological realisation of the Grothendieck group $K_0\mathbf{Var}_S$ of S-varieties. Its derived category is endowed with a six-functor formalism à la Grothendieck. When $S = \mathrm{Spec}(\mathbb{C})$ is a point, mixed Hodge modules over S coincide with polarisable Hodge structures as defined by Deligne [24]; see [49, Lemma 14.8].

The Grothendieck group $K_0(\mathbf{MHM}_S)$ of mixed Hodge modules over S is the quotient of the free abelian group of isomorphism classes of mixed Hodge modules over S by the relations

$$[E] - [F] + [G]$$

whenever there is a split exact sequence

$$0 \to E \to F \to G \to 0$$

for E, F and G objects of $\mathbf{MHM}_S$. There is a notion of weight of a mixed Hodge module, morphisms are strict for the weight filtration and the Grothendieck group $K_0(\mathbf{MHM}_S)$ is generated by the classes of pure Hodge modules.

The tensor product operation in the bounded derived category of $\mathbf{MHM}_S$ provides a multiplicative structure on $K_0(\mathbf{MHM}_S)$ as follows. The Grothendieck group $K_0^{\mathrm{tri}}(D^b(\mathbf{MHM}_S))$ is defined similarly to $K_0(\mathbf{MHM}_S)$ by taking distinguished triangles

$$E^\bullet \to F^\bullet \to G^\bullet \to E^\bullet[1]$$

of complexes as relations, in the place of exact sequences [35, Exposé VIII]. By the theorem of decomposition of mixed Hodge modules [49, Corollary 14.4], there is an isomorphism of groups

$$K_0(\mathbf{MHM}_S) \to K_0^{\mathrm{tri}}(D^b(\mathbf{MHM}_S))$$

sending the class of a mixed Hodge module M to the class of the complex with M in degree zero. Indeed, the inverse is given by the morphism

$$[M^\bullet] \mapsto \sum_{i\in\mathbb{Z}} (-1)^i [\mathcal{H}^i(M^\bullet)]$$

from $K_0^{\mathrm{tri}}(D^b(\mathbf{MHM}_S))$ to $K_0(\mathbf{MHM}_S)$. The tensor product on $D^b(\mathbf{MHM}_S)$ induces a ring structure on $K_0^{\mathrm{tri}}(D^b(\mathbf{MHM}_S))$ and on $K_0(\mathbf{MHM}_S)$ through the previous isomorphism.

The faithful and exact functor

$$\mathrm{rat}_S : \mathbf{MHM}_S \to \mathbf{Perv}_S$$

to perverse sheaves on S sends the six-functor formalism of $\mathbf{MHM}_S$ to the one of the bounded derived category of constructible sheaves $D_c^b(S)$. In order to prove an isomorphism between two mixed Hodge modules, it will be enough to check it at the level of perverse sheaves. Indeed, a mixed Hodge module M is given by the data of filtrations on a $\mathcal{D}$-module isomorphic to $\mathbb{C} \otimes_{\mathbb{Q}} \mathrm{rat}_S(M)$ by the Riemann–Hilbert correspondence (comparison isomorphism [49, Section 14.1]). Moreover, the Verdier duality functor $\boldsymbol{D}_S$ on $D_c^b(S)$ lifts to $\mathbf{MHM}_S$ so that $\mathrm{rat}_S \circ \boldsymbol{D}_S = \boldsymbol{D}_S \circ \mathrm{rat}_S$.

2.1.2. *The Hodge realisation of* $K_0\mathbf{Var}_S$. For every integer d we denote by $\mathbb{Q}_S^{\mathrm{Hdg}}(-d)$ the complex of mixed Hodge modules obtained by pulling back to S the Hodge structure $\mathbb{Q}_{\mathrm{pt}}^{\mathrm{Hdg}}(-d)$ of type (d,d) through the structure morphism $S \to \mathrm{Spec}(\mathbb{C})$. If $p : X \to S$ is an S-variety, let $\mathbb{Q}_X^{\mathrm{Hdg}}$ be the complex $p^*\mathbb{Q}_S^{\mathrm{Hdg}}$ of mixed Hodge modules.

Definition 2.1. The *Hodge realisation*

$$\chi_S^{\mathrm{Hdg}} : K_0\mathbf{Var}_S \to K_0\,\mathbf{MHM}_S,$$

sometimes called the *motivic Hodge–Grothendieck characteristic*, sends a class $[X \xrightarrow{p} S]$ to

$$[p_!\,\mathbb{Q}_X^{\mathrm{Hdg}}] = \sum_{i\in\mathbb{Z}} (-1)^i [\mathcal{H}^i(p_!\,\mathbb{Q}_X^{\mathrm{Hdg}})],$$

where the equality comes from the isomorphism

$$K_0(\mathbf{MHM}_S) \xrightarrow{\sim} K_0^{\mathrm{tri}}(D^b(\mathbf{MHM}_S))$$

described in the previous subsection.

The perverse realisation $K_0\mathbf{Var}_S \to K_0(D^b(\mathbf{Perv}_S))$ factors through this morphism as $\mathrm{rat}_S \circ \chi_S^{\mathrm{Hdg}}$ [19, Chapter 2, Proposition 3.3.7]. If $S = \mathrm{Spec}(\mathbb{C})$, this is the class, in the Grothendieck group of mixed Hodge structures, of the cohomology with compact support of X and rational coefficients, together with its Hodge structure. This homomorphism is well-defined (see [49, Lemma 16.61] or Proposition 3.3.7 in [19, Chapter 2] for a proof). Since χ_S^{Hdg} sends $\mathbb{L}_S$ to $[\mathbb{Q}_S^{\mathrm{Hdg}}(-1)]$, which is invertible in $K_0(\mathbf{MHM}_S)$, it is a morphism of rings compatible with the localisation $K_0\mathbf{Var}_S \to \mathscr{M}_S$.

2.1.3. *The weight filtration on* $K_0\mathbf{Var}_S$. In this subsection we collect definitions and properties from [3, Section 4.6] and develop a few useful examples about weights.

Definition 2.2. The weight function $w_S : \mathscr{M}_S \to \mathbb{Z}$ is given by the composition of χ_S^{Hdg} together with the weight function on mixed Hodge modules.

Proposition 2.3. *Let S be a complex variety. The weight function $w_S : \mathscr{M}_S \to \mathbb{Z}$ satisfies the following properties*:

(1) $w_S(0) = -\infty$.

(2) $w_S(\mathfrak{a} + \mathfrak{a}') \leqslant \max(w_S(\mathfrak{a}), w_S(\mathfrak{a}'))$ *with equality if* $w_S(\mathfrak{a}) \neq w_S(\mathfrak{a}')$ *for any* $\mathfrak{a}, \mathfrak{a}' \in \mathscr{M}_S$.

(3) *If* $\mathscr{Y} \to S$ *is a variety over S then*

$$w_S(\mathscr{Y}) = 2\dim_S(\mathscr{Y}) + \dim(S).$$

For proofs of these properties, see Lemmas 4.5.1.3, 4.6.2.1 and 4.6.3.1 of [3, Chapter 4]. This weight function induces a filtration $(W_{\leqslant n}\mathscr{M}_S)_{n\in\mathbb{Z}}$ on $\mathscr{M}_S$ given by

$$W_{\leqslant n}\mathscr{M}_S = \{\mathfrak{a} \in \mathscr{M}_S \mid w_S(\mathfrak{a}) \leqslant n\}$$

for all $n \in \mathbb{Z}$.

Definition 2.4. The *completion of $\mathscr{M}_S$ with respect to the weight topology* is the projective limit

$$\widehat{\mathscr{M}_S}^{w} = \varprojlim(\mathscr{M}_S / W_{\leqslant n}\mathscr{M}_S).$$

2.1.4. *Useful examples and vanishing properties.* Let n be the dimension of the complex variety $S \xrightarrow{a_S} \operatorname{Spec}(\mathbb{C})$. If S is smooth, the complex $\mathbb{Q}_S^{\mathrm{Hdg}}$ of mixed Hodge modules is concentrated in degree n and $\mathcal{H}^n\mathbb{Q}_S^{\mathrm{Hdg}}$ is given by the pure Hodge module of weight n associated to the constant one-dimensional variation of Hodge structure on S of weight zero. Furthermore, we have the relation $a_S^! \cong a_S^*(n)[2n]$, in particular

$$\mathbb{Q}_S^{\mathrm{Hdg}}(n)[2n] \cong a_S^!\mathbb{Q}_{\operatorname{Spec}(\mathbb{C})}^{\mathrm{Hdg}}.$$

The class of $\mathbb{A}_S^d = \mathbb{A}_{\mathbb{C}}^d \times_{\mathbb{C}} S$ is sent by χ_S^{Hdg} to

$$\begin{aligned} \chi_S^{\mathrm{Hdg}}(\mathbb{L}_S^d) &= (\chi_S^{\mathrm{Hdg}}(\mathbb{L}_S))^{\otimes d} \\ &= (\mathrm{pr}_! \,\mathbb{Q}_{\mathbb{A}_S^1}^{\mathrm{Hdg}})^{\otimes d} = \mathbb{Q}_S^{\mathrm{Hdg}}(-d). \end{aligned}$$

More generally, we have the following proposition on top-graded parts.

Proposition 2.5 [3, Lemma 4.6.3.4]. *Let S be a smooth and connected complex variety of dimension n. Let $p : \mathscr{Y} \to S$ and $\mathscr{Z} \to S$ be two smooth S-varieties with irreducible fibres of dimension $d \geqslant 0$. Then*

$$w_S([\mathscr{Y}] - [\mathscr{Z}]) \leqslant 2d + n - 1.$$

Proof. Since p is smooth, one has $p^! \simeq p^*(d)[2d]$ and there is a morphism of mixed Hodge modules

$$\mathcal{H}^{2d+n}(p_! \mathbb{Q}_{\mathscr{Y}}^{\mathrm{Hdg}}) \to \mathcal{H}^{2d+n}(\mathbb{Q}_S^{\mathrm{Hdg}}(-d)[-2d])$$

which induces an isomorphism on the $(2d+n)$-th graded parts [3, Remark 4.1.5.5]. This means that if $\mathscr{X} \to S$ is another smooth S-variety with irreducible fibres of dimension d, the corresponding top-weight graded parts cancel out and the weight of $\chi_S^{\mathrm{Hdg}}([\mathscr{Y}]-[\mathscr{X}])$ is at most $2d+n-1$. □

Proposition 2.6. *Let S be a smooth and connected complex variety of dimension n. Let $p : \mathscr{Y} \to S$ be a proper smooth morphism whose fibres are smooth projective varieties of dimension $\dim_S(\mathscr{Y}) = d$. Assume that*

$$\mathcal{R}^1 p_! \mathscr{O}_{\mathscr{Y}} = \mathcal{R}^2 p_! \mathscr{O}_{\mathscr{Y}} = 0$$

and that p has local sections.

Then there exists an open subset $S' \subset S$ above which the relative Picard scheme exists, is smooth with discrete fibres of rank r, and such that the class

$$\chi_{S'}^{\mathrm{Hdg}}(\mathscr{Y}) - \chi_{S'}^{\mathrm{Hdg}}(\mathbb{L}_{S'}^d) - \chi_{S'}^{\mathrm{Hdg}}(r\mathbb{L}_{S'}^{d-1}) = [p_! \mathbb{Q}_{\mathscr{Y}_{|S'}}^{\mathrm{Hdg}}] - [\mathbb{Q}_{S'}^{\mathrm{Hdg}}(-d)[-2d]] - [\mathbb{Q}_{S'}^{\mathrm{Hdg}}(-(d-1))[-2(d-1)]^{\oplus r}]$$

has S'-weight at most $2d+n-3$.

Proof. Recall that if a complex M is concentrated in degree n, then its shifting

$$M[k]^\bullet = M^{\bullet + k}$$

is concentrated in degree n' such that $n'+k = n$, that is to say, in degree $n-k$ (in what follows, we will use this with $k = -2d$).

Since S is smooth and connected, the complex $\mathbb{Q}_S^{\mathrm{Hdg}}$ is concentrated in degree $n = \dim(S)$ and

$$\mathcal{H}^{2d+n}(\mathbb{Q}_S^{\mathrm{Hdg}}(-d)[-2d])$$

is a pure Hodge module of weight $2d+n$. As complexes, $\mathbb{Q}_{\mathscr{Y}}^{\mathrm{Hdg}}$ and $\mathbb{Z}_{\mathscr{Y}}^{\mathrm{Hdg}}$ are both concentrated in degree $d+n$, which will explain the shift in what follows. The morphism p induces functors $p_! : D^b(\mathscr{Y}) \to D^b(S)$ and p_* between the bounded derived categories of sheaves respectively over $\mathscr{Y}$ and S, compatible with the ones on mixed Hodge modules. Since p is proper, p_* and $p_!$ coincide. By [3, Lemma 4.1.4.2], the functor $p_! : D^b(\mathbf{MHM}_{\mathscr{Y}}) \to D^b(\mathbf{MHM}_S)$ has cohomological amplitude $\leqslant d$, which means that the complex $p_! \mathbb{Q}_{\mathscr{Y}}^{\mathrm{Hdg}}$ only has cohomology in degree at most $(d+n)+d = 2d+n$. We deduce that only terms of weight $\leqslant 2d+n$ occur in $\chi_{S'}^{\mathrm{Hdg}}(\mathscr{Y})$. Hence, to prove the proposition, we have to compute the terms of weights $2d+n$, $2d+n-1$ and $2d+n-2$. By Proposition 2.5 and its proof, we already know what is the part of weight $2d+n$.

The exponential exact sequence of sheaves of abelian groups over $\mathscr{Y}$

$$0 \to \mathbb{Z}_{\mathscr{Y}}(1) \to \boldsymbol{G}_{a,\mathscr{Y}} \to \boldsymbol{G}_{m,\mathscr{Y}} \to 0$$

gives rise to an exact sequence of cohomology sheaves over S

$$\begin{tikzcd}
\cdots \arrow[r] & \mathcal{H}^n(p_!\,\mathbb{Z}_{\mathscr{Y}}(1)) \arrow[r] & \mathcal{H}^n(p_!\,\mathscr{O}_{\mathscr{Y}}[-n]) \arrow[r] & \mathcal{H}^n(p_!\,\mathscr{O}_{\mathscr{Y}}^{\times}[-n]) \arrow[dll, rounded corners] \\
& \mathcal{H}^{n+1}(p_!\,\mathbb{Z}_{\mathscr{Y}}(1)) \arrow[r] & \mathcal{H}^{n+1}(p_!\,\mathscr{O}_{\mathscr{Y}}[-n]) \arrow[r] & \mathcal{H}^{n+1}(p_!\,\mathscr{O}_{\mathscr{Y}}^{\times}[-n]) \arrow[dll, rounded corners] \\
& \mathcal{H}^{n+2}(p_!\,\mathbb{Z}_{\mathscr{Y}}(1)) \arrow[r] & \mathcal{H}^{n+2}(p_!\,\mathscr{O}_{\mathscr{Y}}[-n]) \arrow[r] & \cdots
\end{tikzcd} \tag{2.1.1}$$

which on stalks specialises to the well-known exact sequence of abelian groups

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}(1) \arrow[r] & \mathbb{C} \arrow[r] & \mathbb{C}^* \arrow[dll, rounded corners] \\
& H^1(\mathscr{Y}_s(\mathbb{C}), \mathbb{Z}(1)) \arrow[r] & H^1(\mathscr{Y}_s, \mathscr{O}_{\mathscr{Y}_s}) \arrow[r] & H^1(\mathscr{Y}_s, \mathscr{O}_{\mathscr{Y}_s}^{\times}) \arrow[dll, rounded corners] \\
& H^2(\mathscr{Y}_s(\mathbb{C}), \mathbb{Z}(1)) \arrow[r] & H^2(\mathscr{Y}_s, \mathscr{O}_{\mathscr{Y}_s}) \arrow[r] & \cdots
\end{tikzcd}$$

where $\mathbb{Z}(1)$ is the $\mathbb{Z}$-Hodge structure with underlying $\mathbb{Z}$-module $2i\pi\mathbb{Z}$ and Hodge type $(-1,-1)$. Since $\mathcal{H}^{n+i}(p_!\,\mathscr{O}_{\mathscr{Y}}[-n]) = \mathcal{R}^i p_!\,\mathscr{O}_{\mathscr{Y}} = 0$ for $i = 1, 2$, the map

$$\mathrm{Pic}_{\mathscr{Y}/S} = \mathcal{H}^{n+1}(p_!\,\mathscr{O}_{\mathscr{Y}}^{\times}[-n]) \to \mathcal{H}^{n+2}(p_!\,\mathbb{Z}_{\mathscr{Y}}(1))$$

is an isomorphism. In particular, the map it induces on stalks

$$\mathrm{Pic}(\mathscr{Y}_s) = H^1(\mathscr{Y}_s, \mathscr{O}_{\mathscr{Y}_s}^{\times}) \to H^2(\mathscr{Y}_s(\mathbb{C}), \mathbb{Z}(1))$$

is an isomorphism. Since we assumed that S and $\mathscr{Y} \to S$ are smooth, this means that

$$\mathrm{Pic}_{\mathscr{Y}/S} \otimes \mathbb{Q}_S^{\mathrm{Hdg}} \simeq \mathcal{H}^{n+2}(p_!\,\mathbb{Q}_{\mathscr{Y}}^{\mathrm{Hdg}}(1)) \tag{2.1.2}$$

is a variation of Hodge structure, of rank r, above S.

By surjectivity of the exponential map, the arrow $\mathbb{C}^* \to H^1(\mathscr{Y}_s(\mathbb{C}), \mathbb{Z}(1))$ is trivial. Thus $H^1(\mathscr{Y}_s(\mathbb{C}), \mathbb{Z}(1))$ injects into $H^1(\mathscr{Y}_s, \mathscr{O}_{\mathscr{Y}_s})$, which is trivial by assumption; thus $H^1(\mathscr{Y}_s(\mathbb{C}), \mathbb{Z}(1))$ is trivial as well for all $s \in S$, which means that $\mathcal{H}^{n+1}(p_!\,\mathbb{Z}_{\mathscr{Y}}(1))$ is trivial.

We use the exact involutive dual functor

$$\boldsymbol{D} : \mathbf{MHM} \to \mathbf{MHM}^{\mathrm{opp}}$$

of Verdier duality on mixed Hodge modules, which extends to the derived bounded category $D_c^b(\mathbf{MHM})$, by the formula

$$\boldsymbol{D}M^\bullet = \mathcal{H}om(M^\bullet, \boldsymbol{D}\mathbb{Q}^{\mathrm{Hdg}})$$

in $D_c^b(\mathbf{MHM})$, where $\boldsymbol{D}\mathbb{Q}^{\mathrm{Hdg}}$ is the dualizing complex. Here since S is smooth,

$$\boldsymbol{D}_S\mathbb{Q}_S^{\mathrm{Hdg}} \simeq \mathbb{Q}_S^{\mathrm{Hdg}}(n)[2n];$$

see for example [58, Appendix A]. It sends mixed Hodge modules of weight w to mixed Hodge modules of weight $-w$, and interchanges p_* and $p_!$. In our situation, it gives

$$\boldsymbol{D}_S(p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}) = p_*(\boldsymbol{D}_{\mathscr{Y}}\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}) = p_!\,(\boldsymbol{D}_{\mathscr{Y}}\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}) = p_!\,(\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}(n+d)[2(n+d)]);$$

thus

$$\begin{aligned}\mathrm{Gr}^W_i\,\mathcal{H}^j(p_!\,\boldsymbol{D}_{\mathscr{Y}}\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}) &= \mathrm{Gr}^W_i\,\mathcal{H}^j(p_!\,(\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}(n+d)[2(n+d)]))\\ &= \mathrm{Gr}^W_{i+2(n+d)}\,\mathcal{H}^{j+2(n+d)}(p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}})\end{aligned} \tag{2.1.3}$$

for all integers i and j (recall that the $(n+d)$-th Tate twist translates into a double shift $2(n+d)$ of the weight). On the other hand the decomposition theorem [49, Corollary 14.4]

$$p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}} \simeq \bigoplus_k \mathcal{H}^k(p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}})[-k]$$

in $D^b(\mathbf{MHM}_S)$ gives

$$\boldsymbol{D}_S(p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}) \simeq \bigoplus_k (\boldsymbol{D}_S\mathcal{H}^k(p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}))[k].$$

We apply [57, Proposition 2.6], which says that

$$\boldsymbol{D}_S\,\mathrm{Gr}^W_i\,M = \mathrm{Gr}^W_{-i}\,\boldsymbol{D}_S M$$

for all $M \in \mathbf{MHM}_S$, which gives

$$\begin{aligned}\mathrm{Gr}^W_{i+2(n+d)}\,\mathcal{H}^{j+2(n+d)}(p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}) &= \mathrm{Gr}^W_i\,\mathcal{H}^j(\boldsymbol{D}_S(p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}))\\ &\simeq \mathrm{Gr}^W_i\,\boldsymbol{D}_S(\mathcal{H}^{-j}\,p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}) \qquad \text{(by (2.1.3))}\\ &\simeq \boldsymbol{D}_S\,\mathrm{Gr}^W_{-i}\,\mathcal{H}^{-j}(p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}),\end{aligned}$$

which, in turn, for $j \in \{-(n+1), -(n+2)\}$ and $i = j$, specialises to

$$\begin{aligned}\mathrm{Gr}^W_{n+2d-1}\,\mathcal{H}^{n+2d-1}(p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}) &\simeq \boldsymbol{D}_S\,\mathrm{Gr}^W_{n+1}\,\mathcal{H}^{n+1}(p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}),\\ \mathrm{Gr}^W_{n+2(d-1)}\,\mathcal{H}^{n+2(d-1)}(p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}) &\simeq \boldsymbol{D}_S\,\mathrm{Gr}^W_{n+2}\,\mathcal{H}^{n+2}(p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}).\end{aligned}$$

We previously showed (in the paragraph right after (2.1.2)) that $\mathcal{H}^{n+1}(p_!\,\mathbb{Z}^{\mathrm{Hdg}}_{\mathscr{Y}}(1))$ is trivial; we have in particular

$$\mathcal{H}^{n+1}(p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}) = 0$$

and the first line is zero. Finally, since by (2.1.2)

$$\mathcal{H}^{n+2}(p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}) \simeq \mathrm{Pic}_{\mathscr{Y}/S} \otimes \mathbb{Q}^{\mathrm{Hdg}}_S(-1)$$

is pure, the local rank of

$$\begin{aligned}\mathrm{Gr}^W_{n+2(d-1)}\,\mathcal{H}^{n+2(d-1)}(p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}}) &\simeq \boldsymbol{D}_S\,\mathrm{Gr}^W_{n+2}\,\mathcal{H}^{n+2}(p_!\,\mathbb{Q}^{\mathrm{Hdg}}_{\mathscr{Y}})\\ &\simeq \boldsymbol{D}_S\,\mathrm{Gr}^W_{n+2}(\mathrm{Pic}_{\mathscr{Y}/S} \otimes \mathbb{Q}^{\mathrm{Hdg}}_S(-1))\end{aligned}$$

is given by the one of $\mathrm{Pic}_{\mathscr{Y}/S'} \otimes \mathbb{Q}^{\mathrm{Hdg}}_{S'}$ above an open subset $S' \subset S$, and hence the result. ∎

2.2. ***Motivic Euler product.*** Formal motivic Euler products have been introduced by Margaret Bilu [3], as a *notation* generalising the Kapranov zeta function and *behaving like a product*. For our purpose we will only need a particular case of this construction, but we will state a few useful properties of this object in a general framework. We mostly follow the exposition one can find in Sections 3 and 6 of [5].

2.2.1. *Symmetric products and configuration spaces.* Let S be a k-variety and X an S-variety. The m-th symmetric product of X relative to S is by definition the quotient

$$\mathrm{Sym}^m_{/S}(X) = (\underbrace{X \times_S \cdots \times_S X}_{m \text{ times}})/\mathfrak{S}_m.$$

Let $\mathscr{X} = (X_i)_{i \in I}$ be a family of quasiprojective varieties above X, where I is an arbitrary set. Let $\mu = (m_i)_{i \in I} \in \mathbb{N}^{(I)}$ be a family of nonnegative integers with finite support, which we call a *partition* (if $I = \mathbb{N}^*$, then a partition of a nonnegative integer n is a family $(m_i)_{i \geqslant 1}$ such that $\sum_{i \geqslant 1} i m_i = n$).[3] For such a partition, we define

$$\mathrm{Sym}^\mu_{/S}(X) = \prod_{i \in I} \mathrm{Sym}^{m_i}_{/S}(X),$$

as well as

$$\mathrm{Sym}^\mu_{X/S}(\mathscr{X}) = \prod_{i \in I} \mathrm{Sym}^{m_i}_{X/S}(X_i),$$

which is a variety over $\mathrm{Sym}^\mu_{/S}(X)$. These constructions extend to elements of $K_0\mathbf{Var}_X$, using Cauchy products; for details, see for example [5, Section 6.1.1].

Given a partition $\mu \in \mathbb{N}^{(I)}$, one can construct the restricted μ-th symmetric product

$$\mathrm{Sym}^\mu_{X/S}(\mathscr{X})_*$$

as follows. If we write $\left(\prod_{i \in I} X^{m_i}\right)_{*,X/S}$ for the complement of the diagonal (points having at least two equal coordinates) in $\prod_{i \in I} X^{m_i}$, then the restricted symmetric product

$$\mathrm{Sym}^\mu_{/S}(X)_*,$$

sometimes abbreviated

$$\mathrm{S}^\mu_{/S}(X)_*,$$

is by definition the image of $\left(\prod_{i \in I} X^{m_i}\right)_{*,X/S}$ in $\mathrm{Sym}^\mu_{/S} X$. Furthermore, there is a Cartesian diagram

$$\begin{array}{ccc} \left(\prod_{i \in I} X_i^{m_i}\right)_{*,X/S} & \hookrightarrow & \prod_{i \in I} X_i^{m_i} \\ \downarrow & & \downarrow \\ \left(\prod_{i \in I} X^{m_i}\right)_{*,X/S} & \hookrightarrow & \prod_{i \in I} X^{m_i} \end{array}$$

[3]Note that such partitions admit holes and that this set $\mathbb{N}^{(I)}$ of generalised partitions is denoted by $\mathcal{P}(I)$ in [5; 6; 37; 64], while the set of partitions with no hole is written $\mathcal{Q}(I)$. We will adopt the notation $\mathcal{P}$ and $\mathcal{Q}$ only for partitions of integers, that is to say, elements of $\mathbb{N}^{(\mathbb{N}^*)}$.

defining an open subset $\left(\prod_{i\in I} X_i^{m_i}\right)_{*,X/S}$ of points of $\prod_{i\in I} X_i^{m_i}$ mapping to points of $\prod_{i\in I} X^{m_i}$ with pairwise distinct coordinates. Then one defines[4]

$$\mathrm{S}^{\mu}_{X/S}(\mathscr{X})_* = \mathrm{Sym}^{\mu}_{X/S}(\mathscr{X})_* = \left(\prod_{i\in I} X_i^{m_i}\right)_{*,X/S} / \prod_{i\in I} \mathfrak{S}_{m_i},$$

that is to say, the image of $\left(\prod_{i\in I} X_i^{m_i}\right)_{*,X/S}$ in $\mathrm{Sym}^{\mu}_{X/S}(\mathscr{X})$.

Example 2.7. In the case where I is a singleton, and $\mathscr{X} = (Y \to X)$, then any partition μ is given by a nonnegative integer n and $\mathrm{Sym}^{\mu}_{X/S}(\mathscr{X})_* = \mathrm{Sym}^{n}_{X/S}(Y)_*$ is the scheme parametrising étale zero-cycles of degree n above X, with labels in Y.

Example 2.8. If $I = \mathbb{N}^r \setminus \{\mathbf{0}\}$, then for any $\boldsymbol{n} \in \mathbb{N}^r \setminus \{\mathbf{0}\}$ the disjoint union

$$\mathrm{Sym}^{\boldsymbol{n}}_{X/S}(\mathscr{X})_* = \coprod_{\substack{\mu=(n_{\boldsymbol{m}})\in\mathbb{N}^{((\mathbb{N}^r)^*)}\\ \sum_{\boldsymbol{m}} n_{\boldsymbol{m}}\boldsymbol{m}=\boldsymbol{n}}} \mathrm{Sym}^{\mu}_{X/S}(\mathscr{X})_*$$

parametrises r-tuples of zero-cycles of degree $\boldsymbol{n}$ with labels in $\mathscr{X}$.

As well, this construction extends to families of elements of $K_0\mathbf{Var}_X$ and $\mathscr{M}_X$ [5, Definition 6.1.7]: if $\mathscr{A} = (\mathfrak{a}_i)_{i\in I}$ is such a family, then

$$\mathrm{Sym}^{\mu}_{X/S}(\mathscr{A}) = \boxtimes_{i\in I} \mathrm{Sym}^{m_i}_{X/S}(\mathfrak{a}_i) \in K_0\mathbf{Var}_{\mathrm{Sym}^{\mu}_{/S} X}$$

and

$$\mathrm{S}^{\mu}_{X/S}(\mathscr{A})_* = \mathrm{Sym}^{\mu}_{X/S}(\mathscr{A})_* \in K_0\mathbf{Var}_{\mathrm{Sym}^{\mu}_{/S}(X)_*}$$

is the restriction to $\mathrm{S}^{\mu}_{/S}(X)_* = \mathrm{Sym}^{\mu}_{/S}(X)_* \subset \mathrm{Sym}^{\mu}_{/S}(X)$ of $\mathrm{Sym}^{\mu}_{X/S}(\mathscr{A})$. More generally, if K is a class in $K_0\mathbf{Var}_{\mathrm{Sym}^{\mu}_{/S} X}$, we will denote by K_* its image in $K_0\mathbf{Var}_{\mathrm{Sym}^{\mu}_{/S}(X)_*}$ by the restriction morphism.

2.2.2. *Formal and effective motivic Euler products.*

Notation 2.9 (formal motivic Euler product). Let X be a variety over S and $\mathscr{X} = (X_i)_{i\in I}$ be a family of elements of $K_0\mathbf{Var}_X$ or $\mathscr{M}_X$ indexed by a set I. Let $(t_i)_{i\in I}$ be a family of indeterminates. Then the product

$$\prod_{x\in X/S}\left(1 + \sum_{i\in I} X_{i,x} t_i\right)$$

is defined as a *notation* for the formal series

$$\sum_{\mu\in\mathbb{N}^{(I)}} [\mathrm{Sym}^{\mu}_{X/S}(\mathscr{X})_*]\boldsymbol{t}^{\mu},$$

where $\boldsymbol{t}^{\mu} = \prod_{i\in I} t_i^{m_i}$ whenever $\mu = (m_i)_{i\in I} \in \mathbb{N}^{(I)}$.

[4]Denoted by $S^{\mu}(\mathscr{X}/S)$ in [3] and $C^{\mu}_{X/S}(\mathscr{X})$ or $\left(\prod_{i\in I} \mathrm{Sym}^{m_i} X_i\right)_{*,X/S}$ in [5; 6].

Example 2.10 (formal motivic Euler product with one indeterminate over a curve). The simplest kind of motivic Euler products we are going to use is the following. Assume that I is made of a single element. Then a family $\mathscr{X}$ is given by a single class Y and $\mu = [\underbrace{1, \ldots, 1}_{m \text{ times}}]$ is the only relevant partition type for a given positive integer m. In this setting,

$$\prod_{p \in \mathscr{C}} (1 + Yt)$$

is the formal series

$$\sum_{m \in \mathbb{N}} [\mathrm{Sym}^m_{\mathscr{C}}(Y)_*]\, t^m,$$

where $\mathrm{Sym}^m_{\mathscr{C}}(Y)_* = \mathrm{Sym}^{[1,\ldots,1]}_{\mathscr{C}}(Y)_*$ parametrises étale zero cycles of $\mathscr{C}$ of degree m with labels in Y (whenever Y is a variety).

Proposition 2.11 [3, Section 3.8.1]. *The Euler product notation is compatible with the cut-and-paste relations*: *if* $X = U \cup Y$ *with* Y *a closed subscheme of* X *and* U *its complement*, *then for any family* $\mathscr{X} = (X_i)_{i \in I}$ *of elements of* $K_0\mathbf{Var}_X$ *or* $\mathscr{M}_X$

$$\prod_{x \in X/S} \Big(1 + \sum_{i \in I} X_{i,x} t_i\Big) = \Big(\prod_{u \in U/S} \Big(1 + \sum_{i \in I} X_{i,u} t_i\Big)\Big)\Big(\prod_{y \in Y/S} \Big(1 + \sum_{i \in I} X_{i,y} t_i\Big)\Big)$$

when considering the motivic Euler products of the restrictions

$$\mathscr{Y} = (X_i \times_X Y)_{i \in I} \quad \textit{and} \quad \mathscr{U} = (X_i \times_X U)_{i \in I}.$$

We will need the following generalisation of [3, Proposition 3.9.2.4].

Proposition 2.12. *We assume that* I *is of the form* $I_0 \setminus \{0\}$, *where* I_0 *is a commutative monoid*, *and that* $(t_i)_{i \in I}$ *is a collection of indeterminates*, *such that*[5]

(1) I_0 *is endowed with a total order* $<$ *such that* $p + q = i$, *where* $q \neq 0$, *implies* $p < i$;

(2) *for all* $i \in I$, *the set* $\{p \in I \mid p < i\}$ *is finite*;

(3) *the collection of indeterminates* $(t_i)_{i \in I}$ *satisfies* $t_p t_q = t_{p+q}$.

Let S *be a variety*, X *a variety over* S, $\mathscr{A} = (A_i)_{i \in I}$ *and* $\mathscr{B} = (B_i)_{i \in I}$ *any pair of families of elements of* $K_0\mathbf{Var}_X$ *or* $\mathscr{M}_X$. *Then*, *under the above hypotheses on* I *and* $(t_i)_{i \in I}$,

$$\prod_{x \in X/S} \Big(\Big(1 + \sum_{i \in I} A_{i,x} t_i\Big)\Big(1 + \sum_{i \in I} B_{i,x} t_i\Big)\Big) = \prod_{x \in X/S} \Big(1 + \sum_{i \in I} A_{i,x} t_i\Big) \prod_{x \in X/S} \Big(1 + \sum_{i \in I} B_{i,x} t_i\Big).$$

Remark 2.13. In [3, Proposition 3.9.2.4], the family $\mathscr{A}$ is assumed to be made of *effective* elements. In order to check that the motivic Tamagawa number of a product of two Fano-like varieties is the product of the two motivic Tamagawa numbers, or, more generally, to compute the motivic Tamagawa number of a fibration, we need to drop the effectiveness assumption.

[5] We refer the reader to the notion of *algèbre large d'un monoïde* in [9, Chapter III, p. 27].

Proof of Proposition 2.12. I thank Margaret Bilu for having pointed out that it is actually a direct application of [3, Corollary 3.9.2.5]. One proceeds exactly as in [3, p. 89–90], where Proposition 2.12 is proved for families of varieties.

Indeed, [3, Corollary 3.9.2.5] tells us that if X' is a variety over X, and $\mathscr{X}' = (X'_i)_{i\in I}$ is a family of classes in $K_0\mathbf{Var}_{X'}$, then

$$\prod_{x\in X/S}\left(\prod_{x'\in X'/X}\left(1+\sum_{i\in I} X'_{i,x'}t_i\right)\right)_x = \prod_{x'\in X'/X}\left(1+\sum_{i\in I} X'_{i,u}t_i\right)$$

(see [3, Section 3.9.1] for the definition of this double-product notation). Taking X' to be the disjoint union of two copies of X, and $\mathscr{A}$, $\mathscr{B}$ to be the restrictions of $\mathscr{X}$ respectively to the first and to the second copies, we get the expected identity. □

Example 2.14 [64, Proposition 3.7]. The Kapranov zeta function of X/S is defined as

$$Z^{\mathrm{Kapr}}_{X/S}(t) = \sum_{m\in\mathbb{N}}[\mathrm{Sym}^m_{/S} X]\, t^m.$$

If the characteristic of the base field is zero, it can be rewritten

$$Z^{\mathrm{Kapr}}_{X/S}(t) = \prod_{x\in X/S}((1-t)^{-1})$$

and then by Proposition 2.12

$$Z^{\mathrm{Kapr}}_{X/S}(t)^{-1} = \prod_{x\in X/S}(1-t).$$

In positive characteristic, this equality only holds in the modified Grothendieck ring $K_0\mathbf{Var}^{\mathrm{uh}}_S$; see [5, Example 6.1.11].

Notation 2.15 (effective motivic Euler product). Let Y be an element of $K_0\mathbf{Var}_X$ or $\mathscr{M}_X$. The motivic Euler product

$$\prod_{x\in X/S}(1+Y_x)$$

is by definition the series

$$\sum_{m\geqslant 0}[\mathrm{Sym}^m_{X/S}(Y)_*].$$

When this series converges in a convenient completion of $K_0\mathbf{Var}_X$ or $\mathscr{M}_X$, its sum is written $\prod_{x\in X/S}(1+Y_x)$ as well.

Remark 2.16. Since abstract motivic Euler products are compatible with changes of variable of the form $t' = \mathbb{L}^a t$ [3, Section 3.6.4], this notation can be seen as the specialisation of

$$\prod_{x\in X/S}(1+Y_x\mathbb{L}^a_x t) = \sum_{m\geqslant 0}[\mathrm{Sym}^m_{X/S}(Y\times_X \mathbb{A}^a_X)_*]\, t^m = \sum_{m\geqslant 0}[\mathrm{Sym}^m_{X/S}(Y)_*]\, \mathbb{L}^{ma}_S t^m$$

at $t = \mathbb{L}^{-a}_S$ for any nonnegative integer a.

2.2.3. *Specialising products.* The previous multiplicative property specialises.

Proposition 2.17. *Assume that* $\prod_{x\in X/S}(1+A_x)$ *and* $\prod_{x\in X/S}(1+B_x)$ *converge. Then*

$$\prod_{x\in X/S}(1+A_x)(1+B_x)$$

converges and

$$\prod_{x\in X/S}(1+A_x)\prod_{x\in X/S}(1+B_x)=\prod_{x\in X/S}(1+A_x)(1+B_x).$$

Proof. Let us consider the two formal motivic Euler products

$$P(t)=\prod_{x\in X/S}(1+(A_x+B_x+A_xB_x)t^2),$$
$$P_{1,2}(t_1,t_2)=\prod_{x\in X/S}(1+t_1A_x)(1+t_2B_x)=\prod_{x\in X/S}(1+t_1A_x+t_2B_x+t_1t_2A_xB_x).$$

We have to check that

$$P(1)=P_{1,2}(1,1).$$

We introduce the following intermediate Euler product:

$$\begin{aligned}P_{0,1,2}(t_0,t_1,t_2)&=\prod_{x\in X/S}(1+t_0t_1A_x+t_0t_2B_x+t_1t_2A_xB_x)\\&=\prod_{x\in X/S}(1+t_0(t_1A_x+t_2B_x)+t_1t_2A_xB_x).\end{aligned}$$

Then by Proposition 2.12,

$$P_{1,2}(t_1,t_2)=\prod_{x\in X/S}(1+t_1A_x)\prod_{x\in X/S}(1+t_2B_x)$$

and by [5, Proposition 6.4.5]

$$P_{0,1,2}(1,t_1,t_2)=\prod_{x\in X/S}(1+t_1A_x+t_2B_x+t_1t_2A_xB_x)=P_{1,2}(t_1,t_2).$$

Moreover, by [5, Lemma 6.5.1]

$$P_{0,1,2}(t,t,t)=P(t).$$

Taking $t=1$ everywhere one gets

$$P(1)=P_{0,1,2}(1,1,1)=P_{1,2}(1,1)$$

as expected. □

2.2.4. *Convergence criterion with respect to the weight filtration.* When k is a subfield of $\mathbb{C}$, we have a convergence criterion for motivic Euler products of families over a curve $\mathscr{C}$. It is a particular case of [31, Proposition 2.6], which itself is a multivariable variant of [3, Proposition 4.7.2.1].

Proposition 2.18. *Fix an integer $r \geqslant 1$ and an r-tuple $\rho \in (\mathbb{N}^*)^r$. For any tuple $\boldsymbol{m}$ of nonnegative integers, we write $\langle \rho, \boldsymbol{m} \rangle = \sum_{i=1}^r m_i \rho_i$.*

Assume that $\mathscr{X} = (X_{\boldsymbol{m}})_{\boldsymbol{m} \in (\mathbb{N}^r)^*}$ is a family of elements of $\mathscr{M}_{\mathscr{C}}$ such that there exist an integer $M \geqslant 0$ and real numbers $\alpha < 1$ and β such that

- *$w_{\mathscr{C}}(X_{\boldsymbol{m}}) \leqslant 2\langle \rho, \boldsymbol{m} \rangle - 2$ whenever $1 \leqslant \langle \rho, \boldsymbol{m} \rangle \leqslant M$;*
- *$w_{\mathscr{C}}(X_{\boldsymbol{m}}) \leqslant 2\alpha \langle \rho, \boldsymbol{m} \rangle + \beta - 1$ whenever $\langle \rho, \boldsymbol{m} \rangle > M$.*

Then there exists $\delta \in \,]0, 1]$ and $\delta' > 0$ such that

$$w_{\mathbb{C}}(\mathrm{Sym}^{\pi}_{\mathscr{C}/k}(\mathscr{X})_* \cdot \mathfrak{a}_1^{\rho_1 m_1} \cdots \mathfrak{a}_r^{\rho_r m_r}) \leqslant -\delta' \langle \rho, \boldsymbol{m} \rangle$$

for all $\boldsymbol{m} \in (\mathbb{N}^r)^*$, partitions π of $\boldsymbol{m}$ and elements $\mathfrak{a}_1, \ldots, \mathfrak{a}_r \in \mathscr{M}_{\mathbb{C}}$ such that $w(\mathfrak{a}_i) < -2 + \delta - \beta/(M+1)$ for all $1 \leqslant i \leqslant r$.

If we specialise the previous proposition to the polynomial $F(T) = 1 + Y\mathbb{L}T$ and consider the convergence at $T = \mathbb{L}^{-1}$ we get the following criterion.

Proposition 2.19. *Assume that $Y \in \mathscr{M}_{\mathscr{C}}$ is such that $w_{\mathscr{C}}(Y) \leqslant -2$. Then the series $\sum_{m \geqslant 0} [\mathrm{Sym}^m_{\mathscr{C}}(Y)_*]$ converges in $\widehat{\mathscr{M}_k}^w$ and the Euler product*

$$\prod_{p \in \mathscr{C}} (1 + Y_p)$$

is well-defined.

Example 2.20. Recall that $w_{\mathscr{C}}(\mathbb{L}_{\mathscr{C}}^{-2}) = -2 \dim_{\mathscr{C}}(\mathbb{A}^2_{\mathscr{C}}) + \dim(\mathscr{C}) = -3$; thus

$$\prod_{p \in \mathscr{C}} (1 - \mathbb{L}_p^{-2})$$

converges in $\widehat{\mathscr{M}_k}^w$. Moreover, one can show that this convergence actually holds in $\widehat{\mathscr{M}_k}^{\dim}$ for any k.

Let $p : Y \to \mathscr{C}$ be a smooth $\mathscr{C}$-variety with irreducible fibres of dimension $d \geqslant 0$. Then,

$$\prod_{p \in \mathscr{C}} (1 + ([Y_p] - \mathbb{L}_p^d)\mathbb{L}_p^{-(d+1)})$$

converges in $\widehat{\mathscr{M}_k}^w$, since

$$w_{\mathscr{C}}([Y] - \mathbb{L}^d_{\mathscr{C}}) \leqslant 2d$$

by Proposition 2.5; thus $w_{\mathscr{C}}(([Y] - \mathbb{L}^d_{\mathscr{C}})\mathbb{L}_{\mathscr{C}}^{-(d+1)}) \leqslant -2$.

The following little lemma will help us to explicitly control error terms when studying the case of toric varieties. One can replace the dimension by the weight or any other filtration compatible with finite sums.

Lemma 2.21. *Let $(\mathfrak{c}_{\boldsymbol{m}})_{\boldsymbol{m} \in \mathbb{N}^r}$ be a family of elements of $\mathscr{M}_k$. Assume that there exists a constant $a > 0$ such that*

$$\dim(\mathfrak{c}_{\boldsymbol{m}}) \leqslant -a|\boldsymbol{m}|$$

for every $\boldsymbol{m} \in \mathbb{N}^r$, where $|\boldsymbol{m}| = \sum_{i=1}^r m_i$.

Then, for any nonempty subset $A \subset \{1, \dots, r\}$ and nonnegative integer b,

$$\dim\Big(\sum_{\boldsymbol{m}' \leqslant \boldsymbol{m}-\boldsymbol{b}} \mathfrak{c}_{\boldsymbol{m}'} \mathbb{L}^{\boldsymbol{m}'_A - \boldsymbol{m}_A}\Big) \leqslant -\tfrac{1}{2}\min(1,a)\min_{\alpha \in A}(m_\alpha) - \tfrac{1}{2}b\min(1, 2|A|-a)$$

for all $\boldsymbol{m} \in \mathbb{N}^r_{\geqslant b}$, where $\boldsymbol{m}_A$ is the restriction of $\boldsymbol{m}$ to A and $\boldsymbol{b} = (b, \dots, b)$.

Proof. If $\boldsymbol{m}'_A \nleqslant \frac{1}{2}(\boldsymbol{m}_A - \boldsymbol{b})$ then the coarse upper bound

$$\dim(\mathfrak{c}_{\boldsymbol{m}'}\mathbb{L}^{\boldsymbol{m}'_A - \boldsymbol{m}_A}) \leqslant -a|\boldsymbol{m}'| - b|A|$$

for $\boldsymbol{m}' \leqslant \boldsymbol{m} - b$ gives

$$\dim(\mathfrak{c}_{\boldsymbol{m}'}\mathbb{L}^{\boldsymbol{m}'_A - \boldsymbol{m}_A}) < -\tfrac{1}{2}a\min_{\alpha\in A}(m_\alpha - b) - b|A| = -\tfrac{1}{2}a\min_{\alpha\in A}(m_\alpha) - \tfrac{1}{2}b(2|A|-a),$$

while if $\boldsymbol{m}'_A \leqslant \frac{1}{2}(\boldsymbol{m}_A - \boldsymbol{b})$ then $\boldsymbol{m}'_A - \boldsymbol{m}_A \leqslant -\frac{1}{2}(\boldsymbol{m}_A + \boldsymbol{b}_A)$ and

$$\dim(\mathfrak{c}_{\boldsymbol{m}'}\mathbb{L}^{\boldsymbol{m}'_A - \boldsymbol{m}_A}) \leqslant -a|\boldsymbol{m}'| - \tfrac{1}{2}|\boldsymbol{m}_A| - \tfrac{1}{2}b \leqslant -\tfrac{1}{2}\min_{\alpha\in A}(m_\alpha) - \tfrac{1}{2}b. \qquad \square$$

3. Batyrev–Manin–Peyre principle for curves

3.1. ***A convergence lemma in characteristic zero.*** In this subsection we assume that k is a subfield of $\mathbb{C}$ and choose once and for all an embedding $k \hookrightarrow \mathbb{C}$, as in Section 2.1.

Lemma 3.1. *Let $\mathscr{V} \to \mathscr{C}$ be a proper model of a Fano-like variety V. Then for any dense open subset $\mathscr{C}' \subset \mathscr{C}$, the motivic Euler product*

$$\prod_{p\in\mathscr{C}'}\bigg(\frac{[\mathscr{V}_p]}{\mathbb{L}_p^{\dim(V)}}(1-\mathbb{L}_p^{-1})^{\mathrm{rk}(\mathrm{Pic}(V))}\bigg)$$

converges in the completion of $\mathscr{M}_k$ with respect to the weight filtration.

Proof. By the multiplicative property of motivic Euler products Proposition 2.11, it is enough to find some dense open subset $\mathscr{C}' \subset \mathscr{C}$ such that the product above converges. Let r be the Picard rank of V. In $\mathscr{M}_{\mathscr{C}}$, we have

$$\begin{aligned}[\mathscr{V}]\mathbb{L}_{\mathscr{C}}^{-\dim_{\mathscr{C}}\mathscr{V}}(1-\mathbb{L}_{\mathscr{C}}^{-1})^r &= \big(1+([\mathscr{V}]-\mathbb{L}_{\mathscr{C}}^{\dim_{\mathscr{C}}(\mathscr{V})})\mathbb{L}_{\mathscr{C}}^{-\dim_{\mathscr{C}}(\mathscr{V})}\big)\bigg(1+\sum_{k=1}^{r}\binom{r}{k}(-1)^k\mathbb{L}_{\mathscr{C}}^{-k}\bigg)\\ &= 1 + \frac{[\mathscr{V}]-\mathbb{L}_{\mathscr{C}}^{\dim_{\mathscr{C}}(\mathscr{V})} - r\mathbb{L}_{\mathscr{C}}^{\dim_{\mathscr{C}}(\mathscr{V})-1}}{\mathbb{L}_{\mathscr{C}}^{\dim_{\mathscr{C}}(\mathscr{V})}} + \mathscr{R},\end{aligned}$$

where

$$\mathscr{R} = -r\frac{[\mathscr{V}]-\mathbb{L}_{\mathscr{C}}^{\dim_{\mathscr{C}}(\mathscr{V})}}{\mathbb{L}_{\mathscr{C}}^{\dim_{\mathscr{C}}(\mathscr{V})+1}} + \frac{[\mathscr{V}]}{\mathbb{L}_{\mathscr{C}}^{\dim_{\mathscr{C}}(\mathscr{V})}}\sum_{k=2}^{r}\binom{r}{k}(-1)^k\mathbb{L}_{\mathscr{C}}^{-k}.$$

By Notation 2.15 of the motivic Euler product, we are interested in the series

$$\sum_{m\geqslant 0}[S_*^m(\mathscr{Y})],$$

where

$$\mathscr{Y} = \frac{[\mathscr{V}] - \mathbb{L}_{\mathscr{C}}^{\dim_{\mathscr{C}}(\mathscr{V})} - r\mathbb{L}_{\mathscr{C}}^{\dim_{\mathscr{C}}(\mathscr{V})-1}}{\mathbb{L}_{\mathscr{C}}^{\dim_{\mathscr{C}}(\mathscr{V})}} + \mathscr{R} \in \mathscr{M}_{\mathscr{C}}$$

and in order to prove convergence, it is enough to check that $w_{\mathscr{C}}(\mathscr{Y}) \leqslant -2$. Since the motivic Euler product is compatible with finite products, up to replacing $\mathscr{C}$ by a nonempty open subset we can assume that $\mathscr{V} \to \mathscr{C}$ is smooth with irreducible fibres. Then by Proposition 2.5 we have a first bound on the weight

$$w_{\mathscr{C}}\big(([\mathscr{V}] - \mathbb{L}_{\mathscr{C}}^{\dim_{\mathscr{C}}(\mathscr{V})})\mathbb{L}_{\mathscr{C}}^{-\dim_{\mathscr{C}}(\mathscr{V})-1}\big) \leqslant -2$$

and the expression of $\mathscr{R}$ shows that

$$w_{\mathscr{C}}(\mathscr{R}) \leqslant -2$$

as well. In order to show that $w_{\mathscr{C}}(\mathscr{Y} - \mathscr{R}) \leqslant -2$, we use the fact that V is Fano-like. By Remark 1.3, we are in the situation of Proposition 2.6: up to restricting to an open subset of $\mathscr{C}$, we have a decomposition

$$\chi_{\mathscr{C}}^{\mathrm{Hdg}}([\mathscr{V}]) = (\chi_{\mathscr{C}}^{\mathrm{Hdg}}(\mathbb{L}_{\mathscr{C}}))^{\dim_{\mathscr{C}}(\mathscr{V})} + r(\chi_{\mathscr{C}}^{\mathrm{Hdg}}(\mathbb{L}_{\mathscr{C}}))^{\dim_{\mathscr{C}}(\mathscr{V})-1} + \mathscr{W} \in K_0(\mathbf{MHM}_{\mathscr{C}}),$$

with $w_{\mathscr{C}}(\mathscr{W}) \leqslant 2(\dim_{\mathscr{C}}(\mathscr{V}) - 1)$. Hence $w_{\mathscr{C}}(\mathscr{Y} - \mathscr{R}) \leqslant -2$ and, by the property of the weight, one has $w_{\mathscr{C}}(\mathscr{Y}) \leqslant -2$. By the convergence criterion of Proposition 2.19, this shows that the motivic Euler product we are considering converges in $\widehat{\mathscr{M}_k}^{w}$. □

3.2. *Motivic Tamagawa number of a model.* Let V be a Fano-like F-variety of dimension n and $\mathscr{V}$ a proper model of V. We are now able to give a precise meaning to the motivic analogue of the Tamagawa number.

Up to replacing $\mathscr{V}$ by a dominating model, we can always assume that it is a *good model*, that is to say, a proper model of V whose smooth locus $\mathscr{V}^{\circ}$ is a weak Néron model of V, by Theorem 1.23 and Proposition 1.27.

Furthermore, we assume that $\mathscr{C}$ admits a divisor of degree 1, which is the case for example if $k = \mathbb{F}_q$ by the Lang–Weil estimate, or more trivially if $k = \mathbb{C}$ or if $\mathscr{C}$ is the projective line.

Definition 3.2. The motivic constant $\tau_{\mathscr{L}}(\mathscr{V})$ of the proper model $\mathscr{V} \to \mathscr{C}$ with respect to a model $\mathscr{L}$ of ω_V^{-1} is the effective element of $\widehat{\mathscr{M}_k}^{\dim}$ or $\widehat{\mathscr{M}_k}^{w}$ given by the motivic Euler product

$$\mathbb{L}_k^{(1-g)\dim(V)}(\operatorname{res}_{t=\mathbb{L}_k^{-1}} Z_{\mathscr{C}}^{\mathrm{Kapr}}(t))^{\mathrm{rk}(\mathrm{Pic}(V))} \prod_{p\in\mathscr{C}} (1 - \mathbb{L}_p^{-1})^{\mathrm{rk}(\mathrm{Pic}(V))} \mu^*_{\mathscr{L}|\mathscr{V}_{R_p}}(\mathrm{Gr}(\mathscr{V}^{\circ}_{R_p})),$$

where the motivic density

$$\mu^*_{\mathscr{L}|\mathscr{V}_{R_p}}$$

is given by Definition 1.21 and

$$\operatorname{res}_{t=\mathbb{L}_k^{-1}}(Z_{\mathscr{C}}^{\mathrm{Kapr}}(t)) = \big((1 - \mathbb{L}_k t)Z_{\mathscr{C}}^{\mathrm{Kapr}}(t)\big)_{t=\mathbb{L}_k^{-1}},$$

with $Z_{\mathscr{C}}^{\mathrm{Kapr}}(t)$ being the Kapranov zeta function of $\mathscr{C}$ as defined in Example 2.14.

If $\mathscr{V}$ is a constant model of the form $\mathscr{V} = V \times_k \mathscr{C}$, with V a nice variety defined over k, $\mathscr{L} = \mathrm{pr}_1^*(\omega_V^{-1})$ and $\pi = \mathrm{pr}_2$, then the constant $\tau_{\mathscr{L}}(\mathscr{V})$ will be written $\tau(V/\mathscr{C})$. If moreover $\mathscr{C}$ is clear from the context, it will be simply written $\tau(V)$.

Remark 3.3. The use of the motivic Euler product notation in this definition is licit. Indeed, there exists a dense open subset $\mathscr{C}'$ of $\mathscr{C}$ on which π is smooth, $(\Omega^n_{\mathscr{V}/\mathscr{C}})^\vee$ is invertible and isomorphic to $\mathscr{L}$. For points p in $\mathscr{C}'$,

$$\mu^*_{\mathscr{L}}(\mathrm{Gr}(\mathscr{V}^\circ_{R_p})) = \mu_{\mathscr{V}_{R_p}}(\mathrm{Gr}(\mathscr{V}_{R_p})) = [\mathscr{V}_{\kappa_p}]\,\mathbb{L}^{-\dim(V)}.$$

Then the motivic Euler product

$$\prod_{p\in\mathscr{C}'} (1-\mathbb{L}_p^{-1})^{\mathrm{rk}(\mathrm{Pic}(V))}\,\mu_{\mathscr{V}_{R_p}}(\mathrm{Gr}(\mathscr{V}_{R_p}))$$

is obtained by applying Notation 2.15 to the family

$$(1-\mathbb{L}_{\mathscr{C}'}^{-1})^{\mathrm{rk}(\mathrm{Pic}(V))}[\mathscr{V}_{\mathscr{C}'}]\,\mathbb{L}_{\mathscr{C}'}^{-\dim(V)} - 1 \in \mathscr{M}_{\mathscr{C}'}.$$

Remark 3.4. By Lemma 3.1, when k is a subfield of $\mathbb{C}$, this class is well-defined in $\widehat{\mathscr{M}_k}^{w}$. When V is a smooth split projective toric variety, the convergence holds in $\widehat{\mathscr{M}_k}^{\dim}$, without any assumption on k (see Theorem 5.4).

Remark 3.5. Since we assume that $\mathscr{C}$ admits a divisor of degree 1, we know that the series

$$(1-t)(1-\mathbb{L}_k t)Z_{\mathscr{C}}^{\mathrm{Kapr}}(t)$$

is actually a polynomial $P_{\mathscr{C}}(t)$ of degree $2g$ such that

$$P_{\mathscr{C}}(\mathbb{L}_k^{-1}) = [\mathrm{Pic}^0(\mathscr{C})]\,\mathbb{L}_k^{-g};$$

see, e.g., Section 1.3 in [15, Chapter 6]. Hence in that case

$$\mathrm{res}_{t=\mathbb{L}_k^{-1}} Z_{\mathscr{C}}^{\mathrm{Kapr}}(t) = \left(\frac{P_{\mathscr{C}}(t)}{1-t}\right)_{t=\mathbb{L}_k^{-1}} = \frac{[\mathrm{Pic}^0(\mathscr{C})]\,\mathbb{L}_k^{-g}}{1-\mathbb{L}^{-1}}.$$

In general, Daniel Litt showed in [44] that if d is the minimum degree of a divisor on $\mathscr{C}$, then $(1-t^d)(1-\mathbb{L}_k^d t^d)Z_{\mathscr{C}}^{\mathrm{Kapr}}(t)$ is a polynomial. Note that if $d>1$, then in general $(1-t)(1-\mathbb{L}_k t)Z_{\mathscr{C}}^{\mathrm{Kapr}}(t)$ is *not* a polynomial; see, e.g., Remark 1.3.4 of [15, Chapter 7]. Thus one should modify the previous definitions according to that fact. This more general situation is beyond the scope of this paper.

It is possible to define variants of the motivic constant $\tau_{\mathscr{L}}(\mathscr{V})$, related to components of the moduli space.

Definition 3.6. Let β be a choice of vertical components E_β of multiplicity 1, that is to say, over a finite number of closed points p, the choice of an irreducible component of $\mathscr{V}_p$ of multiplicity 1.

If $E^\circ_{\beta_p} = E_{\beta_p} \cap \mathscr{V}^\circ$ for all p, then

$$\tau_{\mathscr{L}}(\mathscr{V})^\beta$$

is the motivic Tamagawa number

$$\mathbb{L}_k^{(1-g)\dim(V)}\left(\frac{[\mathrm{Pic}^0(\mathscr{C})]\,\mathbb{L}_k^{-g}}{1-\mathbb{L}^{-1}}\right)^{\mathrm{rk}(\mathrm{Pic}(V))}\prod_{p\in\mathscr{C}}(1-\mathbb{L}_p^{-1})^{\mathrm{rk}(\mathrm{Pic}(V))}\mu^*_{\mathscr{L}_{|\mathscr{V}_{R_p}}}(\mathrm{Gr}(E^\circ_{\beta_p})).$$

Note that $\tau_{\mathscr{L}}(\mathscr{V})$ equals the finite sum of the $\tau_{\mathscr{L}}(\mathscr{V})^\beta$ for β running over the finite set of choices of vertical components E_β above each closed point of $\mathscr{C}$.

Definition 3.7. If $\mathscr{C}'$ is a nonempty open subset of $\mathscr{C}$, we will call restriction of $\tau_{\mathscr{L}}(\mathscr{V})^\beta$ to $\mathscr{C}'$, written $\tau_{\mathscr{L}}(\mathscr{V})^\beta_{|\mathscr{C}'}$, the element

$$\mathbb{L}_k^{(1-g)\dim(V)}(\mathrm{res}_{t=\mathbb{L}_k^{-1}} Z_{\mathscr{C}'}(t))^{\mathrm{rk}(\mathrm{Pic}(V))}\prod_{p\in\mathscr{C}'}(1-\mathbb{L}_p^{-1})^{\mathrm{rk}(\mathrm{Pic}(V))}\mu^*_{\mathscr{L}_{|\mathscr{V}_{R_p}}}(\mathrm{Gr}(E^\circ_{\beta_p})).$$

3.3. ***Motivic Batyrev–Manin–Peyre principle for curves.*** In order to deal with different good models of a projective variety V over F, we need a refined version of Question 1. The previous tools make the adaptation straightforward.

We use the notation introduced in Setting 1.4: we fix a finite set $L_1,\dots,L_r$ of invertible sheaves on V whose linear classes form a $\mathbb{Z}$-basis of $\mathrm{Pic}(V)$, as well as invertible sheaves $\mathscr{L}_1,\dots,\mathscr{L}_r$ on $\mathscr{V}$ extending respectively $L_1,\dots,L_r$.

There exists a unique r-tuple of integers $(\lambda_1,\dots,\lambda_r)$ such that

$$\omega_V^{-1}\simeq\bigotimes_{i=1}^r L_i^{\otimes\lambda_i}.$$

Consequently, we have a model of ω_V^{-1} given by

$$\mathscr{L}_{\mathscr{V}}=\bigotimes_{i=1}^r \mathscr{L}_i^{\otimes\lambda_i}. \tag{3.3.4}$$

For any choice β of irreducible vertical components of multiplicity 1 of $\mathscr{V}$, and for every nonempty open subset U of V, the space

$$\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}}=\delta}(\mathscr{V},\mathscr{C})_U^\beta$$

parametrizing curves of multidegree $\mathbf{deg}_{\underline{\mathscr{L}}}=\delta$ intersecting the components given by β exists as a quasiprojective scheme, and the space

$$\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}}=\delta}(\mathscr{V},\mathscr{C})_U \tag{1.6}$$

is then the finite disjoint union over β of these subspaces.

Recall that $\mathrm{Eff}(V)^\vee_{\mathbb{Z}}$ is the intersection of $\mathrm{Eff}(V)^\vee$ and $\mathrm{Pic}(V)^\vee$ in $\mathrm{Pic}(V)^\vee\otimes_{\mathbb{Z}}\mathbb{Q}$.

Question 2 (relative geometric Batyrev–Manin–Peyre). *Let $\mathscr{V}$ and $\underline{\mathscr{L}}$ be as in Setting 1.4 on page 891. Does the symbol*

$$[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}}=\delta}(\mathscr{V},\mathscr{C})_U]\,\mathbb{L}_k^{-\delta\cdot\omega_V^{-1}}\in\mathscr{M}_k$$

converge to $\tau_{\mathscr{L}_{\mathscr{V}}}(\mathscr{V})$ *in* $\widehat{\mathscr{M}_k}^{w}$ *(or even more optimistic, in* $\widehat{\mathscr{M}_k}^{\dim}$*), as* $\delta \in \mathrm{Eff}(V)^{\vee}_{\mathbb{Z}}$ *goes arbitrarily far away from the boundaries of the dual cone* $\mathrm{Eff}(V)^{\vee}$*?*

Remark 3.8. We can refine the previous question as follows: given a choice β of vertical components of multiplicity 1: does the symbol

$$[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\mathscr{L}}=\delta}(\mathscr{V},\mathscr{C})_U^{\beta}]\,\mathbb{L}_k^{-\delta\cdot\omega_V^{-1}} \in \mathscr{M}_k$$

converge to $\tau(\mathscr{V})^{\beta}$ in $\widehat{\mathscr{M}_k}^{w}$, or even $\widehat{\mathscr{M}_k}^{\dim}$, as $\delta \in \mathrm{Eff}(V)^{\vee}_{\mathbb{Z}}$ goes arbitrarily far away from the boundaries of the dual cone $\mathrm{Eff}(V)^{\vee}$?

Example 3.9. Starting from previous works by Chambert-Loir and Loeser [15] and Bilu [3], we show in [31] that the conjecture of Remark 3.8 is true when V is an equivariant compactification of a vector space and k is algebraically closed with characteristic zero.

Example 3.10. Bilu and Browning show in [4] that the answer to Question 2 is positive whenever $\mathscr{C} = \mathbb{P}^1_{\mathbb{C}}$, $V \subset \mathbb{P}^{n-1}_{\mathbb{C}}$ is a hypersurface of degree $d \geqslant 3$ such that $n > 2^d(d-1)$, and $\mathscr{V} = \mathbb{P}^1_{\mathbb{C}} \times_{\mathbb{C}} V$.

3.4. *Products of Fano-like varieties.*

Proposition 3.11. *Let* V_1 *and* V_2 *be two Fano-like varieties over* F*. Let* $\mathscr{V}_1$ *(respectively* $\mathscr{V}_2$*) be a model of* V_1 *above* $\mathscr{C}$ *and* $\mathscr{L}_1$ *be a model of* $\omega_{V_1}^{-1}$ *(resp.* V_2*,* $\mathscr{L}_2$ *and* $\omega_{V_2}^{-1}$*). Then* $\mathscr{V}_1 \times_{\mathscr{C}} \mathscr{V}_2$ *is a model of* $V_1 \times_F V_2$ *above* $\mathscr{C}$*,* $(\mathrm{pr}_1^* \mathscr{L}_1) \otimes (\mathrm{pr}_2^* \mathscr{L}_2)$ *is a model of* $(\mathrm{pr}_1^* \omega_{V_1}^{-1}) \otimes (\mathrm{pr}_2^* \omega_{V_2}^{-1})$ *and*

$$\tau_{(\mathrm{pr}_1^* \mathscr{L}_1)\otimes(\mathrm{pr}_2^* \mathscr{L}_2)}(\mathscr{V}_1 \times_{\mathscr{C}} \mathscr{V}_2) = \tau_{\mathscr{L}_1}(\mathscr{V}_1)\tau_{\mathscr{L}_2}(\mathscr{V}_2).$$

Proof. In order to apply Proposition 2.17, we have to check that, for all closed points $p \in \mathscr{C}$,

$$\mu^*_{(\mathrm{pr}_1^* \mathscr{L}_1)\otimes(\mathrm{pr}_2^* \mathscr{L}_2)|(\mathscr{V}_1\times_{\mathscr{C}}\mathscr{V}_2)_{R_p}}(\mathrm{Gr}((\mathscr{V}_1 \times_{\mathscr{C}} \mathscr{V}_2)^{\circ}_{R_p})) = \mu^*_{\mathscr{L}_1|(\mathscr{V}_1)_{R_p}}(\mathrm{Gr}(\mathscr{V}^{\circ}_{1 R_p}))\mu^*_{\mathscr{L}_2|(\mathscr{V}_2)_{R_p}}(\mathrm{Gr}(\mathscr{V}^{\circ}_{2 R_p})).$$

Going back to Definition 1.21, and by the functoriality of Greenberg schemes, it is enough to check that on $\mathrm{Gr}((\mathscr{V}_1 \times_{\mathscr{C}} \mathscr{V}_2)^{\circ}_{R_p})$ one has

$$\varepsilon_{(\mathrm{pr}_1^* \mathscr{L}_1)\otimes(\mathrm{pr}_2^* \mathscr{L}_2)-(\Lambda^{n_1+n_2}\Omega^1_{\mathscr{V}_1\times\mathscr{V}_2/R_p})^{\vee}} = \varepsilon_{\mathscr{L}_1-(\Lambda^{n_1}\Omega^1_{\mathscr{V}_1/R_p})^{\vee}} + \varepsilon_{\mathscr{L}_2-(\Lambda^{n_2}\Omega^1_{\mathscr{V}_2/R_p})^{\vee}}. \tag{3.4.5}$$

We can assume that $\mathscr{V}_1$ and $\mathscr{V}_2$ are R_p-smooth. Let R'_p be an unramified extension of R_p, $\tilde{x} = (\tilde{x}_1, \tilde{x}_2) \in (\mathscr{V}_1 \times_{R_p} \mathscr{V}_2)(R'_p) \simeq \mathscr{V}_1(R'_p) \times_{\kappa(p)'} \mathscr{V}_2(R'_p)$ and take y_1, y_2, ω_1 and ω_2 to be generators respectively of $\tilde{x}_1^* \mathscr{L}_1$, $\tilde{x}_2^* \mathscr{L}_2$, $\tilde{x}_1^*(\Lambda^{n_1}\Omega^1_{\mathscr{V}_1/R_p})^{\vee}$ and $\tilde{x}_2^*(\Lambda^{n_2}\Omega^1_{\mathscr{V}_2/R_p})^{\vee}$. Then $y_1 y_2$ is a generator of $\tilde{x}^*(\mathrm{pr}_1^* \mathscr{L}_1)\otimes(\mathrm{pr}_2^* \mathscr{L}_2)$ and $\omega_1\omega_2$ is a generator of $\tilde{x}^*(\Lambda^{n_1+n_2}\Omega^1_{\mathscr{V}_1\times\mathscr{V}_2/R_p})^{\vee}$. Now (3.4.5) applied to $\tilde{x}$ is the identity $v_{R'_p}(\omega_1\omega_2/(y_1 y_2)) = v_{R'_p}(\omega_1/y_1) + v_{R'_p}(\omega_2/y_2)$. □

4. Equidistribution of curves

The goals of this section are

- to introduce and provide a definition of the equidistribution principle, which will be done with Definition 4.3,

- and then to prove Theorem C, which will be restated as Theorem 4.6, indicating that this principle does not depend on the choice of models me made in Setting 1.4.

The intuition behind this result is that the equidistribution hypothesis encodes (among many other things) the information one needs to switch from a multidegree coming from a given model to another one. Indeed, while the Batyrev–Manin–Peyre principle, Question 2, describes the expected asymptotic behaviour of the motivic measure of a certain moduli space of sections, the equidistribution principle describes the asymptotic behaviour of the sequence of motivic measures itself. In particular, it measures the motivic distribution of sections for which two different models give two different multidegrees.

In this section we assume that

- $\mathscr{V} \to \mathscr{C}$ is a proper model over $\mathscr{C}$ of a Fano-like variety V together with a model $\underline{\mathscr{L}} = (\mathscr{L}_i)$ of a family of invertible sheaves (L_i) on V whose classes form a $\mathbb{Z}$-basis of $\mathrm{Pic}(V)$ (see Definition 1 and Setting 1.4);
- U is a dense open subset of V;
- the motivic Tamagawa number $\tau_{\mathscr{L}_{\mathscr{V}}}(\mathscr{V})$, see Definition 3.2 and (3.3.4), is well-defined in either $\widehat{\mathscr{M}_k}^{\dim}$ or $\widehat{\mathscr{M}_k}^{w}$. The following discussion will not depend on the choice of the filtration.

4.1. *First approach.* Let $\mathscr{S}$ be a zero-dimensional subscheme of the smooth projective curve $\mathscr{C}$, $|\mathscr{S}|$ its set of closed points and $\mathscr{C}'$ the complement of $|\mathscr{S}|$. This subscheme $\mathscr{S}$ is given by a disjoint union of spectra of the form

$$\mathrm{Spec}(\mathscr{O}_{\mathscr{C},p}/(\mathfrak{m}_p^{m_p+1})) \simeq \mathrm{Spec}(\kappa(p)[\![t]\!]/t^{m_p+1})$$

for $p \in |\mathscr{S}|$. Its length is

$$\ell(\mathscr{S}) = \sum_{p\in|\mathscr{S}|} (m_p + 1)[\kappa(p) : k].$$

Then for every $\mathscr{C}$-morphism $\varphi : \mathscr{S} \to \mathscr{V}$ and every $\delta \in \mathrm{Pic}(V)^\vee$ we define

$$\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}}=\delta}(\mathscr{C}, \mathscr{V} \mid \varphi)_U$$

as being the schematic fibre above φ of the restriction morphism

$$\mathrm{res}^{\mathscr{V}}_{\mathscr{S}} : \mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}}=\delta}(\mathscr{C}, \mathscr{V})_U \to \mathrm{Hom}_{\mathscr{C}}(\mathscr{S}, \mathscr{V}).$$

We assume temporally that $\mathscr{L}_{\mathscr{V}}$ is isomorphic to $(\Lambda^n\Omega^1_{\mathscr{V}/\mathscr{C}})^\vee$ and that $\mathscr{V} \to \mathscr{C}$ is smooth above an open subset containing the closed points of $\mathscr{S}$. Then we say that there is weak equidistribution for $\mathscr{S}$ if, for every $\mathscr{C}$-morphism $\varphi : \mathscr{S} \to \mathscr{V}$, the normalised class

$$[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}}=\delta}(\mathscr{C}, \mathscr{V} \mid \varphi)_U]\, \mathbb{L}_k^{-\delta\cdot\omega_V^{-1}} \in \mathscr{M}_k$$

converges to

$$\tau(\mathscr{V})_{|\mathscr{C}'} \times \prod_{p\in|\mathscr{S}|} \mathbb{L}_p^{-(m_p+1)\dim(V)} \in \widehat{\mathscr{M}_k}$$

when the multidegree δ tends to infinity — again, by this we will always mean $\delta \in \mathrm{Eff}(V)^{\vee}_{\mathbb{Z}}$ and $d(\delta, \partial\,\mathrm{Eff}(V)^{\vee}) \to \infty$. This definition may be seen as a first extension of Peyre's definition [53, 5.8] to nonconstant families $\mathscr{V} \to \mathscr{C}$.

Remark 4.1. $\mathrm{Hom}_{\mathscr{S}}(\mathscr{S}, \mathscr{V}_{\mathscr{S}})$ can be interpreted as the product of spaces of jets

$$\prod_{p \in |\mathscr{S}|} \mathrm{Gr}_{m_p}(\mathscr{V}_{R_p}).$$

Since

$$\mathrm{Gr}_{m_i}(\mathscr{V}_{R_p}) \to \mathrm{Gr}_0(\mathscr{V}_{R_p}) \simeq \mathscr{V}_p$$

is a Zariski-locally trivial fibration over $\mathscr{V}_p$ with fibre an affine space of dimension $m_p \dim(V)$, the class of the space of m_p-jets of $\mathscr{V}_{R_p}$ in $K_0\mathbf{Var}_{\mathscr{V}_p}$ is $\mathbb{L}_p^{m_p \dim(V)}[\mathscr{V}_p]$. Finally the class

$$[\mathrm{Hom}_{\mathscr{C}}(\mathscr{S}, \mathscr{V})] \in K_0\mathbf{Var}_{\prod_{p \in |\mathscr{S}|} \mathscr{V}_p}$$

is sent to the finite product

$$\prod_{p \in |\mathscr{S}|} \frac{[\mathscr{V}_p]}{\mathbb{L}_p^{\dim(V)}} \mathbb{L}_p^{(m_p+1)\dim(V)} \in K_0\mathbf{Var}_k.$$

Thus weak equidistribution for $\mathscr{S}$ implies that

$$\mathbb{L}_k^{-\delta \cdot \omega_V^{-1}} [\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}} = \delta}(\mathscr{C}, \mathscr{V} \mid \varphi)_U][\mathrm{Hom}_{\mathscr{C}}(\mathscr{S}, \mathscr{V})]$$

tends to $\tau(\mathscr{V})$ when $\delta \to \infty$.

4.2. ***Equidistribution and arcs.*** Actually, the equidistribution hypothesis can be reformulated in terms of constructible sets of arcs. This reformulation is natural since we already interpreted the local factors of the motivic Tamagawa number as motivic densities of spaces of arcs. In this subsection S is any finite set of closed points of $\mathscr{C}$. We drop as well the previous assumption on $\mathscr{L}_{\mathscr{V}}$.

The restriction to $\mathrm{Spec}(\widehat{\mathscr{O}}_{\mathscr{C},p})$ provides a morphism

$$\mathrm{res}_{\mathsf{S}}^{\mathscr{V}} : \mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}} = \delta}(\mathscr{C}, \mathscr{V}) \to \prod_{p \in \mathsf{S}} \mathrm{Gr}_{\infty}(\mathscr{V}_{R_p})$$

for every multidegree $\delta \in \mathrm{Eff}(V)^{\vee}_{\mathbb{Z}}$. If $\varphi = (\varphi_p)_{p \in \mathsf{S}}$ is a finite collection of jets such that $\varphi_p \in \mathrm{Gr}_{m_p}(\mathscr{V}_{R_p})$ for every p in S, the schematic fibre of

$$\prod_{p \in \mathsf{S}} \theta_{m_p}^{\infty} \circ \mathrm{res}_{\mathsf{S}}^{\mathscr{V}}$$

above φ is written

$$\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}} = \delta}(\mathscr{C}, \mathscr{V} \mid \varphi)_U.$$

Definition 4.2. We say that there is weak equidistribution above S at level $(m_p)_{p \in \mathsf{S}}$ if, for every collection $\varphi = (\varphi_p)_{p \in \mathsf{S}} \in \prod_{p \in \mathsf{S}} \mathrm{Gr}_{m_p}(\mathscr{V}_{R_p})$ of jets above S, the class

$$[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}} = \delta}(\mathscr{C}, \mathscr{V} \mid \varphi)_U]\, \mathbb{L}_k^{-\delta \cdot \omega_V^{-1}}$$

tends to the nonzero effective element

$$\tau_{\mathscr{L}_{\mathscr{V}}}(\mathscr{V} \mid \varphi) = \tau_{\mathscr{L}_{\mathscr{V}}}(\mathscr{V})_{|\mathscr{C}\setminus \mathsf{S}} \times \prod_{p\in \mathsf{S}} \mu^*_{\mathscr{L}_{|\mathscr{V}_{R_p}}}((\theta^{\infty}_{m_p})^{-1}(\varphi_p) \cap \mathrm{Gr}(\mathscr{V}^{\circ}_{R_p}))$$

of $\widehat{\mathscr{M}}_k$, when δ becomes arbitrarily large.

This definition is consistent with the previous one since we have the factorisation

$$\mathrm{res}^{\mathscr{V}}_{\mathscr{S}} : \mathrm{Hom}^{\boldsymbol{d}}_{\mathscr{C}}(\mathscr{C}, \mathscr{V}) \xrightarrow{\mathrm{res}^{\mathscr{V}}_{\mathsf{S}}} \prod_{p\in \mathsf{S}} \mathrm{Gr}_{\infty}(\mathscr{V}_{R_p}) \longrightarrow \prod_{p\in \mathsf{S}} \mathrm{Gr}_{m_p}(\mathscr{V}_{R_p}) \simeq \mathrm{Hom}_{\mathscr{C}}(\mathscr{S}, \mathscr{V})$$

for every S-tuple $(m_p) \in \mathbb{N}^{\mathsf{S}}$ and corresponding zero-dimensional subscheme $\mathscr{S} \subset \mathscr{C}$ with support $|\mathscr{S}| = \mathsf{S}$.

More generally, if W is a product $\prod_{p\in\mathsf{S}} W_p$ of constructible subsets W_p of $\mathrm{Gr}_{\infty}(\mathscr{V}_{R_p})$,

$$\mathrm{Hom}^{\mathbf{deg}_{\underline{\mathscr{L}}} = \delta}_{\mathscr{C}}(\mathscr{C}, \mathscr{V} \mid W)_U$$

is defined as the schematic fibre of $\mathrm{res}^{\mathscr{V}}_{\mathsf{S}}$ over W. Recall that each constructible set W_p of arcs is nothing else but the preimage by a projection morphism of a certain constructible subset of jets.

Definition 4.3. We will say that there is *equidistribution with respect to* $W = \prod_{p\in\mathsf{S}} W_p$ *and the multidegree* $\mathbf{deg}_{\underline{\mathscr{L}}}$, where each W_p is a constructible subset of arcs, if

$$[\mathrm{Hom}^{\mathbf{deg}_{\underline{\mathscr{L}}} = \delta}_{\mathscr{C}}(\mathscr{C}, \mathscr{V} \mid W)_U]\, \mathbb{L}_k^{-\delta \cdot \omega_V^{-1}}$$

tends to

$$\tau_{\mathscr{L}_{\mathscr{V}}}(\mathscr{V} \mid W) = \tau_{\mathscr{L}_{\mathscr{V}}}(\mathscr{V})_{|\mathscr{C}\setminus S} \times \prod_{p\in \mathsf{S}} \mu^*_{\mathscr{L}_{|\mathscr{V}_{R_p}}}(W_p \cap \mathrm{Gr}(\mathscr{V}^{\circ}_{R_p}))$$

when the multidegree becomes arbitrarily large.

We will say that there is *equidistribution of curves*, *with respect to the multidegree* $\mathbf{deg}_{\underline{\mathscr{L}}}$ if the previous statement holds for every such W.

Remark 4.4. Note that the notion of equidistribution of curves is stronger that the motivic Batyrev–Manin–Peyre principle for curves we formulate in Question 2.

Remark 4.5. In Definition 4.3 one may ask if it would be possible to replace *constructible* by *measurable* to get a more general notion of equidistribution, or consider constructible subsets which are not products over S of constructible sets, as in Theorem 5.6, but this higher level of generality would be mostly useless in the present work.

4.3. *Checking equidistribution pointwise.* Let $\mathscr{S}$ be a zero-dimensional subscheme of $\mathscr{C}$. Assume that, for every $\delta \in \mathrm{Pic}(V)^{\vee}$, there exists a k-scheme F_δ (which depends on $\mathscr{S}$) such that

$$\mathrm{Hom}^{\mathbf{deg}_{\underline{\mathscr{L}}} = \delta}_{\mathscr{C}}(\mathscr{C}, \mathscr{V} \mid \varphi)_U \simeq (F_\delta \otimes \kappa(x))_{\mathrm{red}}$$

for every point $x \in \mathrm{Hom}_{\mathscr{C}}(\mathscr{S}, \mathscr{V})$ corresponding to a $\mathscr{C}$-morphism $\varphi : \mathscr{S} \to \mathscr{V}$. Then by Proposition 1.31, the reduction map

$$\mathrm{Hom}^{\mathbf{deg}_{\underline{\mathscr{L}}} = \delta}_{\mathscr{C}}(\mathscr{C}, \mathscr{V} \mid \varphi)_U \to \mathrm{Hom}_{\mathscr{C}}(\mathscr{S}, \mathscr{V})$$

is a piecewise trivial fibration with fibre F_δ and by Proposition 1.30, for every constructible subset W of $\mathrm{Hom}_{\mathscr{C}}(\mathscr{S},\mathscr{V})$,

$$[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}}=\delta}(\mathscr{C},\mathscr{V}\mid W)_U]=[F_\delta][W]$$

in $K_0\mathbf{Var}_k$. Hence, if one wishes to show that there is equidistribution of curves on $\mathscr{V}$ above $\mathscr{S}$, a strategy is to prove the existence of such an F_δ and then study the convergence of the normalised class $[F_\delta]\,\mathbb{L}_k^{-\delta\cdot\omega_V^{-1}}$. In general the situation is not as simple, but we use a similar argument in Section 5.5 in order to prove Theorem B.

4.4. *Equidistribution and models.* Our goal for the end of this section is to prove the following main result, which does not depend on the choice of the filtration (dimensional or by the weight) on $\mathscr{M}_{\mathscr{C}}$.

Theorem 4.6 (change of model). *Let $\mathscr{V}$ and $\mathscr{V}'$ be two proper models over $\mathscr{C}$ of the same Fano-like F-variety V, together with models $\underline{\mathscr{L}}=(\mathscr{L}_i)$ and $\underline{\mathscr{L}}'=(\mathscr{L}_i')$, respectively on $\mathscr{V}$ and $\mathscr{V}'$, of a family (L_i) of invertible sheaves forming a $\mathbb{Z}$-basis of* $\mathrm{Pic}(V)$, *as in Setting 1.4.*

Then there is equidistribution of curves for $(\mathscr{V},\underline{\mathscr{L}})$, in the sense of Definition 4.3, if and only if there is equidistribution of curves for $(\mathscr{V}',\underline{\mathscr{L}}')$.

The remainder of this section is devoted to the proof of Theorem 4.6. We take $\mathscr{V}$, $\underline{\mathscr{L}}$, $\mathscr{V}'$ and $\underline{\mathscr{L}}'$ as in Setting 1.4. As before, we know the existence of a nonempty open subset $\mathscr{C}'\subset\mathscr{C}$ above which we have an isomorphism of $\mathscr{C}'$-schemes. By Corollary 1.28, we can find a proper model $\widetilde{\mathscr{V}}\to\mathscr{C}$ of V whose $\mathscr{C}$-smooth locus is a Néron smoothening of both $\mathscr{V}'$ and $\mathscr{V}$. Above $\mathscr{C}'$, the three models are isomorphic:

$$\begin{tikzcd} & \widetilde{\mathscr{V}} \arrow[dl, "f"'] \arrow[dd, "\tilde{\pi}"] \arrow[dr, "f'"] & \\ \mathscr{V} \arrow[dr, "\pi"'] & & \mathscr{V}' \arrow[dl, "\pi'"] \\ & \mathscr{C} & \end{tikzcd}$$

This diagram induces morphisms

$$\begin{tikzcd} & \mathrm{Hom}_{\mathscr{C}}(\mathscr{C},\widetilde{\mathscr{V}})_U \arrow[dl, "f_*"'] \arrow[dr, "f'_*"] & \\ \mathrm{Hom}_{\mathscr{C}}(\mathscr{C},\mathscr{V})_U & & \mathrm{Hom}_{\mathscr{C}}(\mathscr{C},\mathscr{V}')_U \end{tikzcd}$$

between moduli spaces of sections.

Let $\widetilde{\mathscr{L}}_i$ and $\widetilde{\mathscr{L}}_i'$ be respectively the pull-backs of the sheaves $\mathscr{L}_i$ and $\mathscr{L}_i'$ to $\widetilde{\mathscr{V}}$ for all i. Then both $\widetilde{\mathscr{L}}_i$ and $\widetilde{\mathscr{L}}_i'$ are models of L_i on $\widetilde{\mathscr{V}}$. Up to shrinking $\mathscr{C}'$, we can assume that they are isomorphic above $\mathscr{C}'$. If $\tilde{\sigma}$ is a section of $\widetilde{\mathscr{V}}$ and $\sigma=f\circ\tilde{\sigma}$, one has the relation

$$\deg((\tilde{\sigma})^*\widetilde{\mathscr{L}}_i)=\deg((\tilde{\sigma})^*f^*\mathscr{L}_i)=\deg((f\circ\tilde{\sigma})^*\mathscr{L}_i)=\deg(\sigma^*\mathscr{L}_i)$$

for all $i\in\{1,\dots,r\}$, so that f_* bijectively sends points of

$$\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\widetilde{\mathscr{L}}}}=\delta}(\mathscr{C},\widetilde{\mathscr{V}})_U$$

to points of

$$\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}}=\delta}(\mathscr{C},\mathscr{V})_U,$$

and similarly for f'_* when considering the multidegrees given by $\underline{\widetilde{\mathscr{L}}}'$ and $\underline{\mathscr{L}}'$. By Proposition 1.31 this implies equality of the corresponding classes in $K_0\mathbf{Var}_k$.

We are going to compare the multidegrees $\mathbf{deg}_{\underline{\widetilde{\mathscr{L}}}}$ and $\mathbf{deg}_{\underline{\widetilde{\mathscr{L}}}'}$.

4.4.1. *Lifting equidistribution.* As an application of the change-of-variable formula Proposition 1.12, we show that equidistribution of curves holds for $(\mathscr{V},\underline{\mathscr{L}})$ if and only if it holds for $(\widetilde{\mathscr{V}},\underline{\widetilde{\mathscr{L}}})$.

Let S be the complement of $\mathscr{C}'$ in $\mathscr{C}$.

Lemma 4.7. *Let $\widetilde{W}$ be a finite product of constructible subsets $\widetilde{W}_p\subset\mathrm{Gr}(\widetilde{\mathscr{V}}_{R_p})$ for $p\in\mathrm{S}$, and let W be its image by f. Then*

$$\tau_{\widetilde{\mathscr{L}}_{\mathscr{V}}}(\widetilde{\mathscr{V}}\mid\widetilde{W})=\tau_{\mathscr{L}_{\mathscr{V}}}(\mathscr{V}\mid W)$$

and

$$[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\widetilde{\mathscr{L}}}}=\delta}(\mathscr{C},\widetilde{\mathscr{V}}\mid\widetilde{W})_U]=[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}}=\delta}(\mathscr{C},\mathscr{V}\mid W)_U]$$

for every $\delta\in\mathrm{Pic}(V)^\vee$.

In particular, for every $m\in\mathbb{Z}$,

$$\tau_{\widetilde{\mathscr{L}}_{\mathscr{V}}}(\widetilde{\mathscr{V}}\mid\widetilde{W})-[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\widetilde{\mathscr{L}}}}=\delta}(\mathscr{C},\widetilde{\mathscr{V}}\mid\widetilde{W})_U]\,\mathbb{L}^{-\delta\cdot\omega_V^{-1}}\in\mathcal{F}^m\mathscr{M}_k$$

if and only if

$$\tau_{\mathscr{L}_{\mathscr{V}}}(\mathscr{V}\mid W)-[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}}=\delta}(\mathscr{C},\mathscr{V}\mid W)_U]\,\mathbb{L}^{-\delta\cdot\omega_V^{-1}}\in\mathcal{F}^m\mathscr{M}_k.$$

Proof. Up to shrinking $\mathscr{C}'$ and adding trivial conditions, one can assume that S is contained in the complement of $\mathscr{C}'$. By Theorem 3.2.2 of [19, Chapter 5], the image of $\widetilde{W}_p$ in $\mathrm{Gr}(\mathscr{V}_{R_p})$ is a constructible subset W_p. Then f_* bijectively sends points of $\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\widetilde{\mathscr{L}}}}=\delta}(\mathscr{C},\widetilde{\mathscr{V}}\mid\widetilde{W})_U$ to points of $\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}}=\delta}(\mathscr{C},\mathscr{V}\mid W)_U$ and by Proposition 1.31,

$$[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\widetilde{\mathscr{L}}}}=\delta}(\mathscr{C},\widetilde{\mathscr{V}}\mid\widetilde{W})_U]=[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}}=\delta}(\mathscr{C},\mathscr{V}\mid W)_U]$$

so that the only thing to show is the equality of the motivic Tamagawa numbers.

Up to shrinking $\mathscr{C}'$ again, we only have to show the equality of local factors

$$\mu^*_{\mathscr{L}_{|\mathscr{V}_{R_p}}}(W_p\cap\mathrm{Gr}(\mathscr{V}^\circ_{R_p}))=\mu^*_{\widetilde{\mathscr{L}}_{|\widetilde{\mathscr{V}}_{R_p}}}(\widetilde{W}_p\cap\mathrm{Gr}(\widetilde{\mathscr{V}}^\circ_{R_p}))$$

above closed points $p\in\mathrm{S}$. By assumption V is smooth and both $\widetilde{\mathscr{V}}$ and $\mathscr{V}$ are models of V; thus by Corollary 3.2.4 of [19, Chapter 5] $\mathrm{ordjac}_{f_{R_p}}$ only takes a finite number of values. By the change of variable formula, Proposition 1.12, applied to the constructible function

$$\varepsilon_{\mathscr{L}_{\mathscr{V}}-(\Lambda^n\Omega^1_{\mathscr{V}/R_p})^\vee}\qquad\text{(see Definition 1.21)}$$

one has the following relation between local factors:

$$\begin{aligned}\mu^*_{\mathscr{L}|\mathscr{V}_{R_p}}(W_p\cap\mathrm{Gr}(\mathscr{V}^\circ_{R_p})) &= \int_{W_p\cap\mathrm{Gr}(\mathscr{V}^\circ_{R_p})}\mathbb{L}^{-\varepsilon_{\mathscr{L}_{\mathscr{V}}-(\Lambda^n\Omega^1_{\mathscr{V}/R_p})^\vee}}\,\mathrm{d}\mu_{\mathscr{V}_{R_p}}\\
&= \int_{W_p\cap\mathrm{Gr}(\mathscr{V}^\circ_{R_p})}\mathbb{L}^{-\operatorname{ord}_{\mathscr{L}_{\mathscr{V}}}+\operatorname{ord}_{(\Lambda^n\Omega^1_{\mathscr{V}/R_p})^\vee}}\,\mathrm{d}\mu_{\mathscr{V}_{R_p}}\\
&= \int_{\widetilde{W}_p\cap\mathrm{Gr}(\widetilde{\mathscr{V}}^\circ_{R_p})}\mathbb{L}^{-f^*\operatorname{ord}_{\mathscr{L}_{\mathscr{V}}}+f^*\operatorname{ord}_{(\Lambda^n\Omega^1_{\mathscr{V}/R_p})^\vee}-\operatorname{ordjac}_f}\,\mathrm{d}\mu_{\widetilde{\mathscr{V}}_{R_p}}\\
&= \int_{\widetilde{W}_p\cap\mathrm{Gr}(\widetilde{\mathscr{V}}^\circ_{R_p})}\mathbb{L}^{-\operatorname{ord}_{\widetilde{\mathscr{L}}_{\mathscr{V}}}+\operatorname{ord}_{(\Lambda^n\Omega^1_{\widetilde{\mathscr{V}}/R_p})^\vee}}\,\mathrm{d}\mu_{\widetilde{\mathscr{V}}_{R_p}} = \mu^*_{\widetilde{\mathscr{L}}|\widetilde{\mathscr{V}}_{R_p}}(\widetilde{W}_p\cap\mathrm{Gr}(\widetilde{\mathscr{V}}^\circ_{R_p}))\end{aligned}$$

in $\mathscr{M}_{\mathscr{V}_{R_p}}$, where we used the relations

$$\operatorname{ord}_{\widetilde{\mathscr{L}}_{\mathscr{V}}}-f^*\operatorname{ord}_{\mathscr{L}_{\mathscr{V}}}=0$$

and

$$f^*\operatorname{ord}_{(\Lambda^n\Omega^1_{\mathscr{V}/R_p})^\vee}-\operatorname{ord}_{(\Lambda^n\Omega^1_{\widetilde{\mathscr{V}}/R_p})^\vee}=\operatorname{ordjac}_f \qquad \text{(by Proposition 1.26)}$$

above the smooth R_p-locus. Taking the product over S, one gets

$$\tau_{\mathscr{L}_{\mathscr{V}}}(\mathscr{V}\mid W)=\tau_{\widetilde{\mathscr{L}}_{\mathscr{V}}}(\widetilde{\mathscr{V}}\mid\widetilde{W}),$$

and hence the lemma. □

4.4.2. *Switching the degree.* The difference of degrees on $\mathrm{Gr}(\widetilde{\mathscr{V}}_{R_p})$ is given by the map

$$\varepsilon_{\underline{\widetilde{\mathscr{L}}'}-\underline{\widetilde{\mathscr{L}}}}:\mathrm{Gr}(\widetilde{\mathscr{V}}_{R_p})\to\operatorname{Pic}(V)^\vee,\quad x\mapsto\left(\bigotimes_i L_i^{\otimes d_i}\mapsto\sum_{i=1}^r d_i\varepsilon_{\widetilde{\mathscr{L}}'_i-\widetilde{\mathscr{L}}_i}(x)\right),$$

which is trivial for all $p\notin\mathrm{S}$. For any $\varepsilon_p\in\operatorname{Pic}(V)^\vee$, let

$$\widetilde{\mathscr{W}}_p(\varepsilon_p)=\varepsilon^{-1}_{\underline{\widetilde{\mathscr{L}}'}-\underline{\widetilde{\mathscr{L}}}}(\{\varepsilon_p\}).$$

As a direct consequence of Lemma 1.19, we have the following.

Lemma 4.8. *The map $\varepsilon_{\underline{\widetilde{\mathscr{L}}'}-\underline{\widetilde{\mathscr{L}}}}$ is constructible and there is only a finite number of values of $\varepsilon_p\in\operatorname{Pic}(V)^\vee$ for which $\widetilde{\mathscr{W}}_p(\varepsilon_p)$ is nonempty.*

Now, for every $\varepsilon=(\varepsilon_s)\in(\operatorname{Pic}(V)^\vee)^{\mathrm{S}}$, let

$$\widetilde{\mathscr{W}}(\varepsilon)=\prod_{s\in\mathrm{S}}\widetilde{\mathscr{W}}_s(\varepsilon_s)\subset\prod_{s\in\mathrm{S}}\mathrm{Gr}_\infty(\widetilde{\mathscr{V}}_{R_s})$$

and let $\widetilde{W}$ be any finite product $\prod_{s\in\mathrm{S}}\widetilde{W}_s$ of constructible subsets $\widetilde{W}_s\subset\mathrm{Gr}(\widetilde{\mathscr{V}}_{R_s})$. Let W, W', W_s and W'_s be the corresponding images by f and f'. By the previous lifting lemma, Lemma 4.7,

$$\left[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\widetilde{\mathscr{L}}}=\delta}(\mathscr{C},\widetilde{\mathscr{V}}\mid\widetilde{W}\cap\widetilde{\mathscr{W}}(\varepsilon))_U\right]\mathbb{L}^{-\delta\cdot\omega_V^{-1}}\to\tau_{\widetilde{\mathscr{L}}_{\mathscr{V}}}(\widetilde{\mathscr{V}}\mid\widetilde{W}\cap\widetilde{\mathscr{W}}(\varepsilon))$$

when $\delta\in\operatorname{Eff}(V)^\vee_{\mathbb{Z}}$ becomes arbitrarily large.

Let $\mathscr{W}'(\varepsilon)$ be the image of $\widetilde{\mathscr{W}}(\varepsilon)$ in $\prod_{s\in S}\mathrm{Gr}(\mathscr{V}'_{R_s})$. We decompose our classes as follows:

$$\begin{aligned}\big[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}'}=\delta'}(\mathscr{C},\mathscr{V}'\mid W')\big] &= \sum_{\varepsilon\in(\mathrm{Pic}(V)^\vee)^S}\big[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}'}=\delta'}(\mathscr{C},\mathscr{V}'\mid W'\cap\mathscr{W}'(\varepsilon))\big]\\ &= \sum_{\varepsilon\in(\mathrm{Pic}(V)^\vee)^S}\big[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\widetilde{\mathscr{L}}}'}=\delta'}(\mathscr{C},\widetilde{\mathscr{V}}\mid \widetilde{W}\cap\widetilde{\mathscr{W}}(\varepsilon))\big];\end{aligned}$$

these sums are finite by Lemma 4.8. Normalising, we get

$$\begin{aligned}&[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}'}=\delta'}(\mathscr{C},\mathscr{V}'\mid W')]\,\mathbb{L}^{-\delta'\cdot\omega_V^{-1}}\\ &\qquad= \sum_{\varepsilon\in(\mathrm{Pic}(V)^\vee)^S}\big[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\widetilde{\mathscr{L}}}'}=\delta'}(\mathscr{C},\widetilde{\mathscr{V}}\mid \widetilde{W}\cap\widetilde{\mathscr{W}}(\varepsilon))\big]\,\mathbb{L}^{-\delta'\cdot\omega_V^{-1}}\\ &\qquad= \sum_{\varepsilon\in(\mathrm{Pic}(V)^\vee)^S}\big[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\widetilde{\mathscr{L}}}}=\delta'-|\varepsilon|}(\mathscr{C},\widetilde{\mathscr{V}}\mid \widetilde{W}\cap\widetilde{\mathscr{W}}(\varepsilon))\big]\,\mathbb{L}^{-(\delta'-|\varepsilon|)\cdot\omega_V^{-1}}\mathbb{L}^{-|\varepsilon|\cdot\omega_V^{-1}},\end{aligned}$$

where $|\varepsilon|$ stands for $\sum_{s\in S}\varepsilon_s\in\mathrm{Pic}(V)^\vee$. Then

$$\begin{aligned}&\big[\mathrm{Hom}_{\mathscr{C}}^{\mathbf{deg}_{\underline{\mathscr{L}}'}=\delta'}(\mathscr{C},\mathscr{V}'\mid W')\big]\,\mathbb{L}^{-\delta'\cdot\omega_V^{-1}}\\ &\qquad\xrightarrow[d(\delta',\partial\,\mathrm{Eff}(V)^\vee)\to\infty]{}\sum_{\varepsilon\in(\mathrm{Pic}(V)^\vee)^S}\tau_{\widetilde{\mathscr{L}}_{\mathscr{V}}}(\widetilde{\mathscr{V}}\mid\widetilde{W}\cap\widetilde{\mathscr{W}}(\varepsilon))\mathbb{L}^{-|\varepsilon|\cdot\omega_V^{-1}}=\tau_{\widetilde{\mathscr{L}}'_{\mathscr{V}}}(\widetilde{\mathscr{V}}\mid\widetilde{W})=\tau_{\mathscr{L}'_{\mathscr{V}}}(\mathscr{V}'\mid W')\end{aligned}$$

and Theorem 4.6 is proved.

5. Rational curves on smooth split projective toric varieties

In this section, we prove equidistribution of rational curves on smooth split projective toric varieties over any base field.

As a warm-up, we start with proving that the motivic Batyrev–Manin–Peyre principle holds for rational curves on this class of varieties, in line with the works of Bourqui [11; 12], Bilu [3] and Bilu–Das–Howe [6]; see Theorem 5.4.

Then we generalise this result, by proving equidistribution of rational curves on smooth split projective toric varieties; see Theorem 5.6.

5.1. ***Geometric setting.*** General references for toric varieties are [21; 33; 48]. Let U be a split torus of dimension n over k. Let

$$\mathcal{X}^*(U)=\mathrm{Hom}(U,\boldsymbol{G}_m)$$

be its group of characters and $\mathcal{X}_*(U)=\mathrm{Hom}_{\mathbb{Z}}(\mathcal{X}^*(U),\mathbb{Z})$ its dual as a $\mathbb{Z}$-module. Let Σ be a complete and regular fan of $\mathcal{X}_*(U)$, which defines a smooth projective toric variety V_Σ over k, with open orbit isomorphic to U. Let

$$r=\mathrm{rk}(\mathrm{Pic}(V_\Sigma))$$

be its Picard number, $\Sigma(1)$ the set of rays of the fan Σ and $(D_\alpha)_{\alpha\in\Sigma(1)}$ the set of its U-invariant divisors. Each ray $\alpha\in\Sigma(1)$ admits a minimal generator $\rho_\alpha\in\mathcal{X}_*(U)$ and the map sending a character $\chi\in\mathcal{X}^*(U)$

to the divisor

$$\sum_{\alpha\in\Sigma(1)} \langle \chi, \rho_\alpha\rangle D_\alpha$$

is part of the exact sequence [21, Theorem 4.1.3]

$$0 \to \mathcal{X}^*(U) \to \bigoplus_{\alpha\in\Sigma(1)} \mathbb{Z}D_\alpha \to \mathrm{Pic}(V_\Sigma) \to 0, \tag{5.1.6}$$

which provides, in particular, the equality

$$|\Sigma(1)| = n + r.$$

If σ is an element of the fan Σ, let $\sigma(1) \subset \Sigma(1)$ be the subset of rays which are faces of σ.

5.2. *Möbius functions.* Let $B_\Sigma \subset \{0, 1\}^{\Sigma(1)}$ be the complement of the image of

$$\Sigma \to \{0, 1\}^{\Sigma(1)}, \quad \sigma \mapsto (\mathbf{1}_{\sigma(1)}(\alpha))_{\alpha\in\Sigma(1)}.$$

In [12, Section 3.5], this set B_Σ is described explicitly as

$$B_\Sigma = \{\boldsymbol{n} \in \{0, 1\}^{\Sigma(1)} \mid \forall\sigma \in \Sigma,\ \exists\alpha \in \Sigma(1),\ \alpha \notin \sigma(1),\ \text{and } n_\alpha = 1\}.$$

It has a geometric interpretation in terms of the effective divisors D_α: it corresponds to the subsets $I \subset \Sigma(1)$ such that

$$\bigcap_{\alpha\in I} D_\alpha = \varnothing.$$

Then, the universal torsor of V_Σ admits an explicit description which goes back to Salberger [59]:

$$\mathcal{T}_\Sigma = \mathbb{A}^{\Sigma(1)} \setminus \Bigg(\bigcup_{J\in B_\Sigma} \bigcap_{\alpha\in J} \{x_\alpha = 0\}\Bigg).$$

5.2.1. *Local Möbius function.* Bourqui inductively defines a local Möbius function

$$\mu^0_{B_\Sigma} : \{0, 1\}^{\Sigma(1)} \to \mathbb{Z}$$

through the relation

$$\mathbf{1}_{\{0,1\}^{\Sigma(1)}\setminus B_\Sigma}(\boldsymbol{n}) = \sum_{0\leqslant \boldsymbol{n}'\leqslant \boldsymbol{n}} \mu^0_{B_\Sigma}(\boldsymbol{n}')$$

for every $\boldsymbol{n} \in \{0, 1\}^{\Sigma(1)}$. It comes with a generating polynomial

$$P_{B_\Sigma}(\boldsymbol{t}) = \sum_{\boldsymbol{n}\in\{0,1\}^{\Sigma(1)}} \mu^0_{B_\Sigma}(\boldsymbol{n})\boldsymbol{t}^{\boldsymbol{n}}$$

and a series

$$Q_{B_\Sigma}(\boldsymbol{t}) = \frac{P_{B_\Sigma}(\boldsymbol{t})}{\prod_{\alpha\in\Sigma(1)}(1 - t_\alpha)}.$$

Let

$$A(B_\Sigma) \subset \mathbb{N}^{\Sigma(1)}$$

be the set of tuples $\boldsymbol{n} \in \mathbb{N}^{\Sigma(1)}$ such that there is no $\boldsymbol{n}' \in B_\Sigma$ with $\boldsymbol{n} \geqslant \boldsymbol{n}'$. In particular, $\mathbf{0} \in A(B_\Sigma)$. It is the set of elements of $\mathbb{N}^{\Sigma(1)}$ *not lying above* B_Σ in the sense of [6, Section 4.4]. Let

$$\mu_{B_\Sigma} : \mathbb{N}^{\Sigma(1)} \to \mathbb{Z}$$

be the local Möbius function defined by the relation

$$\mathbf{1}_{A(B_\Sigma)}(\boldsymbol{n}) = \sum_{0 \leqslant \boldsymbol{n}' \leqslant \boldsymbol{n}} \mu_{B_\Sigma}(\boldsymbol{n}'). \tag{5.2.7}$$

As Bilu, Das and Howe [6, Section 5.2] pointed out, μ_{B_Σ} coincides with $\mu^0_{B_\Sigma}$ on $\{0,1\}^{\Sigma(1)}$ and is zero outside of this set. Hence

$$Q_{B_\Sigma}(\boldsymbol{t}) = \sum_{\boldsymbol{n} \in A(B_\Sigma)} \boldsymbol{t}^{\boldsymbol{n}}.$$

5.2.2. *Global motivic Möbius function.* For any $\boldsymbol{e} \in \mathbb{N}^{\Sigma(1)}$, let $(\mathbb{P}^1_k)^{\boldsymbol{e}}_{B_\Sigma}$ be the open subset of

$$\mathrm{Sym}^{\boldsymbol{e}}_{/k}(\mathbb{P}^1_k)$$

parametrizing $\Sigma(1)$-tuples of effective zero-cycles of degree e_α having disjoint supports with respect to B_Σ. More precisely,

$$(\mathbb{P}^1_k)^{\boldsymbol{e}}_{B_\Sigma} = \left\{ (C_\alpha) \in \mathrm{Sym}^{\boldsymbol{e}}_{/k}(\mathbb{P}^1_k) \;\middle|\; \bigcap_{\alpha \in J} \mathrm{Supp}(C_\alpha) = \varnothing \text{ for all } J \in B_\Sigma \right\}.$$

Up to a tuple of multiplicative factors, this set corresponds to $\Sigma(1)$-tuples of homogeneous polynomials $P(T_0, T_1)$ of degree e_α with coefficients in k such that for all $J \in B_\Sigma$ the polynomials $(P_\alpha)_{\alpha \in J}$ have no common root in any finite extension of k; see [12, Lemme 5.10].

Then, applying the definition of the motivic Euler product in Bilu's sense [3], we get

$$\prod_{p \in \mathbb{P}^1_k} Q_{B_\Sigma}(\boldsymbol{t}) = \sum_{\boldsymbol{d} \in \mathbb{N}^{\Sigma(1)}} [(\mathbb{P}^1_k)^{\boldsymbol{d}}_{B_\Sigma}]\, \boldsymbol{t}^{\boldsymbol{d}}.$$

The formalism of pattern-avoiding zero cycles allowed Bilu, Das and Howe to work with Bilu's motivic Euler product and to give a positive answer to a technical question of Bourqui [12, Question 5], which in turn provides a lift of Bourqui's main theorem [12, Théorème 1.1] from the localised Grothendieck ring of Chow motives $\mathscr{M}^\chi_k$ to the localised Grothendieck ring of varieties $\mathscr{M}_k$; see [6, Lemma 4.5.4, Remark 4.5.7]. Indeed, since

$$Q_{B_\Sigma}(\boldsymbol{t}) = P_{B_\Sigma}(\boldsymbol{t}) \prod_{\alpha \in \Sigma(1)} (1 - t_\alpha)^{-1},$$

one obtains, by taking motivic Euler products (in Bilu's sense)

$$\sum_{\boldsymbol{d} \in \mathbb{N}^{\Sigma(1)}} [(\mathbb{P}^1_k)^{\boldsymbol{d}}_{B_\Sigma}]\, \boldsymbol{t}^{\boldsymbol{d}} = \prod_{p \in \mathbb{P}^1_k} Q_{B_\Sigma}(\boldsymbol{t}) = \prod_{p \in \mathbb{P}^1_k} P_{B_\Sigma}(\boldsymbol{t}) \times \prod_{\alpha \in \Sigma(1)} Z_{\mathbb{P}^1_k}(t_\alpha), \tag{5.2.8}$$

where $Z_{\mathbb{P}^1_k}(t)$ is Kapranov's zeta function of the projective line

$$Z_{\mathbb{P}^1_k}(t) = \sum_{e \geqslant 0} [\mathrm{Sym}^e_{/k}(\mathbb{P}^1_k)]\, t^e.$$

Bourqui's construction [12, Section 3.3], applied to the projective line over k and the set B_Σ, provides a motivic global Möbius function

$$\mu_\Sigma : \mathbb{N}^{\Sigma(1)} \to \mathscr{M}_k$$

given by the relation

$$[(\mathbb{P}^1_k)^{\boldsymbol{e}}_{B_\Sigma}] = \sum_{\substack{\boldsymbol{e}\in\mathbb{N}^{\Sigma(1)}\\ \boldsymbol{e}'\leqslant\boldsymbol{e}}} \mu_\Sigma(\boldsymbol{e}')[\mathrm{Sym}^{\boldsymbol{e}-\boldsymbol{e}'}_{/k}(\mathbb{P}^1_k)]$$

for all $\boldsymbol{e} \in \mathbb{N}^{\Sigma(1)}1$, which is nothing else than what one obtains by considering the coefficient of multidegree $\boldsymbol{e}$ in expression (5.2.8).

It follows from the definitions that the motivic global Möbius function is linked to the local one by the relation

$$\prod_{p\in\mathbb{P}^1_k}\Bigg(\sum_{\boldsymbol{m}\in\mathbb{N}^{\Sigma(1)}} \mu_{B_\Sigma}(\boldsymbol{m})\boldsymbol{t}^{\boldsymbol{m}}\Bigg) = \sum_{\boldsymbol{e}\in\mathbb{N}^{\Sigma(1)}} \mu_\Sigma(\boldsymbol{e})\boldsymbol{t}^{\boldsymbol{e}}.$$

5.3. ***Motivic Tamagawa number.*** By the following proposition and remark, the constant $\tau(V_\Sigma)$ is well-defined in $\widehat{\mathscr{M}_k}^{\dim}$.

Proposition 5.1. *The motivic Euler product*

$$\Bigg(\prod_{p\in\mathbb{P}^1_k} P_{B_\Sigma}(\boldsymbol{t})\Bigg)(\mathbb{L}_k^{-1}) = \prod_{p\in\mathbb{P}^1_k}\Bigg(\sum_{\boldsymbol{m}\in\mathbb{N}^{\Sigma(1)}} \mu_{B_\Sigma}(\boldsymbol{m})\mathbb{L}_p^{-|\boldsymbol{m}|}\Bigg) = \sum_{\boldsymbol{e}\in\mathbb{N}^{\Sigma(1)}} \mu_\Sigma(\boldsymbol{e})\mathbb{L}_k^{-|\boldsymbol{e}|}$$

is well-defined in $\widehat{\mathscr{M}_k}^{\dim}$.

Proof. By [12, Lemme 3.8], the valuation of $P_{B_\Sigma}(T) - 1$ is at least equal to 2. Thus by [6, Lemma 4.2.5] the formal motivic Euler product $\prod_{p\in\mathbb{P}^1_k} P_{B_\Sigma}(\boldsymbol{t})$ converges at $\boldsymbol{t} = \mathbb{L}^{-1}$ for the dimensional filtration. □

Remark 5.2. The local factor of the motivic Euler product above is actually

$$(P_{B_\Sigma}(\boldsymbol{t}))_{|t_\alpha=\mathbb{L}_p^{-1}} = \sum_{\boldsymbol{m}\in\mathbb{N}^{\Sigma(1)}} \mu_{B_\Sigma}(\boldsymbol{m})\mathbb{L}_p^{-|\boldsymbol{m}|} = \frac{[V_\Sigma\otimes\kappa(p)]}{\mathbb{L}_p^{\dim(V_\Sigma)}}(1-\mathbb{L}_p^{-1})^{\mathrm{rk}(\mathrm{Pic}(V_\Sigma))} = \frac{[\mathcal{T}_\Sigma\otimes\kappa(p)]}{\mathbb{L}_p^{|\Sigma(1)|}}.$$

Indeed, we can interpret $[\mathcal{T}_\Sigma\otimes\kappa(p)]\,\mathbb{L}_p^{-|\Sigma(1)|}$ as the motivic density of $\kappa(p)$-arcs of $\mathbb{A}_k^{\Sigma(1)}$ with origin in $\mathcal{T}_\Sigma$, and $\mathbb{L}_p^{-|\boldsymbol{m}|}$ as the motivic density of the subspace $V_{\boldsymbol{m}}$ of $\kappa(p)$-arcs with $\Sigma(1)$-tuple of valuations greater than $\boldsymbol{m}$:

$$V_{\boldsymbol{m}} = \Big\{x\in\mathbb{A}_k^{\Sigma(1)}(\kappa(p)[\![t]\!]) \mid x_\alpha\in t^{m_\alpha}\kappa(p)[\![t]\!] \text{ for all } \alpha\in\Sigma(1)\Big\}.$$

We consider as well the subspace of arcs with given valuation:

$$\begin{aligned} V^\circ_{\boldsymbol{m}} &= \Big\{x\in\mathbb{A}_k^{\Sigma(1)}(\kappa(p)[\![t]\!]) \mid x_\alpha\in t^{m_\alpha}\kappa(p)[\![t]\!] \text{ and } x_\alpha\notin t^{m_\alpha+1}\kappa(p)[\![t]\!] \text{ for all } \alpha\in\Sigma(1)\Big\} \\ &= V_{\boldsymbol{m}} \setminus \bigcup_{\alpha\in\Sigma(1)} V_{\boldsymbol{m}+\boldsymbol{1}_\alpha}. \end{aligned}$$

The arc-space of $\mathcal{T}_\Sigma$ is the space of arcs whose $\Sigma(1)$-tuple of valuations does not lie above B_Σ:

$$\mathrm{Gr}_\infty(\mathcal{T}_\Sigma \otimes \kappa(p)) = \bigsqcup_{\boldsymbol{m}\in A(B_\Sigma)} V_{\boldsymbol{m}}^\circ = \bigsqcup_{\boldsymbol{m}\in A(B_\Sigma)} \Bigl(V_{\boldsymbol{m}} \setminus \bigcup_{\alpha\in\Sigma(1)} V_{\boldsymbol{m}+\boldsymbol{1}_\alpha} \Bigr)$$

and thus

$$\begin{aligned}
[\mathcal{T}_\Sigma \otimes \kappa(p)]\,\mathbb{L}_p^{-|\Sigma(1)|} &= \sum_{\boldsymbol{m}\in A(B_\Sigma)} \mu_V\Bigl(V_{\boldsymbol{m}} \setminus \bigcup_{\alpha\in\Sigma(1)} V_{\boldsymbol{m}+\boldsymbol{1}_\alpha} \Bigr)\\
&= \sum_{\boldsymbol{m}\in A(B_\Sigma)} \sum_{J\subset\Sigma(1)} (-1)^{|J|}\mu_V\Bigl(\bigcap_{\alpha\in J} V_{\boldsymbol{m}+\boldsymbol{1}_\alpha} \Bigr)\\
&= \sum_{\boldsymbol{m}\in A(B_\Sigma)} \mathbb{L}_p^{-|\boldsymbol{m}|} \prod_{\alpha\in\Sigma(1)} (1-\mathbb{L}_p^{-1})\\
&= \Bigl((Q_{B_\Sigma}(\boldsymbol{t})) \prod_{\alpha\in\Sigma(1)} (1-t_\alpha) \Bigr)_{|t_\alpha=\mathbb{L}_p^{-1}} = (P_{B_\Sigma}(\boldsymbol{t}))_{|t_\alpha=\mathbb{L}_p^{-1}}
\end{aligned}$$

as expected.

By compatibility of formal motivic Euler products with changes of variables of the form $t'_\alpha = \mathbb{L}_k^a t_\alpha$ with a an integer [3, Section 3.6.4], together with the compatibility with partial specialisation [5, Lemma 6.5.1], what we get by taking the corresponding motivic Euler product is exactly the motivic Tamagawa number of V_Σ given by Definition 3.2 and Notation 2.15:

$$\Bigl(\prod_{p\in\mathbb{P}^1_k} P_{B_\Sigma}(\boldsymbol{t}) \Bigr)_{|t_\alpha=\mathbb{L}_k^{-1}} = \Bigl(\prod_{p\in\mathbb{P}^1_k} \Bigl(1 + \Bigl(\frac{[\mathcal{T}_\Sigma\otimes\kappa(p)]}{\mathbb{L}_p^{|\Sigma(1)|}} - 1 \Bigr) t \Bigr) \Bigr)_{|t=1} = \tau(V_\Sigma).$$

5.4. *Nonconstrained rational curves.* Let

$$\mathrm{Hom}_k^\delta(\mathbb{P}^1_k, V_\Sigma)_U$$

be the quasiprojective scheme parametrizing morphisms $\mathbb{P}^1_k \to V_\Sigma$ of multidegree $\delta \in \mathrm{Pic}(X)^\vee$ intersecting the dense open subset $U \subset V_\Sigma$ (see Definition 1.5 and Lemma 1.6). It is empty whenever $\delta \notin \mathrm{Eff}(V_\Sigma)^\vee_{\mathbb{Z}}$ (see the remark after Notation 5.4 in [12]), so we will always assume that $\delta \in \mathrm{Eff}(V_\Sigma)^\vee_{\mathbb{Z}}$ in the remaining of this section.

Through the injection $\mathrm{Pic}(V_\Sigma)^\vee \hookrightarrow \mathbb{Z}^{\Sigma(1)}$ given by the exact sequence (5.1.6), $\mathrm{Eff}(V_\Sigma)^\vee_{\mathbb{Z}}$ can be see as the submonoid of tuples $(d_\alpha)_{\alpha\in\Sigma(1)} \in \mathbb{N}^{\Sigma(1)}$ such that

$$\sum_{\alpha\in\Sigma(1)} d_\alpha \langle \chi, \rho_\alpha\rangle = 0$$

for all $\chi \in \mathcal{X}^*(U)$. Note that this submonoid is denoted by $\mathbb{N}^{\Sigma(1)}_{(*)}$ in Bourqui's work [12, Notation 5.3].

For every $\boldsymbol{d} \in \mathrm{Eff}(V_\Sigma)^\vee_{\mathbb{Z}}$, let

$$\widetilde{(\mathbb{P}^1_k)^{\boldsymbol{d}}_{B_\Sigma}}$$

be the inverse image of the open subset

$$(\mathbb{P}^1_k)^{\boldsymbol{d}}_{B_\Sigma} \subset \mathrm{Sym}^{\boldsymbol{d}}_{/k}(\mathbb{P}^1_k) \simeq \prod_{\alpha\in\Sigma(1)} \mathbb{P}^{d_\alpha}_k$$

through the $\boldsymbol{G}_m^{\Sigma(1)}$-torsor

$$\prod_{\alpha\in\Sigma(1)} (\mathbb{A}_k^{d_\alpha+1}\setminus\{0\}) \to \prod_{\alpha\in\Sigma(1)} \mathbb{P}_k^{d_\alpha}.$$

One of Bourqui's key results is the following proposition.

Proposition 5.3 [12, Proposition 5.14]. *For every $\boldsymbol{d}\in \mathrm{Eff}(V_\Sigma)^\vee_{\mathbb{Z}}$,*

$$\widetilde{(\mathbb{P}^1_k)^{\boldsymbol{d}}_{B_\Sigma}}/T_{\mathrm{NS}}$$

represents the functor $\mathbf{Hom}_k^{\boldsymbol{d}}(\mathbb{P}^1, V_\Sigma)_U$.

Theorem 5.4. *The normalised class*

$$[\mathrm{Hom}_k^{\delta}(\mathbb{P}^1_k, V_\Sigma)_U]\,\mathbb{L}_k^{-\delta\cdot\omega^{-1}_{V_\Sigma}}$$

tends to the nonzero effective element

$$\tau(V_\Sigma) = \frac{\mathbb{L}_k^{\dim(V_\Sigma)}}{(1-\mathbb{L}_k^{-1})^{\mathrm{rk}(\mathrm{Pic}(V_\Sigma))}} \prod_{p\in\mathbb{P}^1_k} \frac{[V_\Sigma\otimes_k \kappa(p)]}{\mathbb{L}_p^{\dim(V_\Sigma)}}(1-\mathbb{L}_p^{-1})^{\mathrm{rk}(\mathrm{Pic}(V_\Sigma))} \in \widehat{\mathscr{M}}_k^{\dim}$$

when $\delta\in\mathrm{Eff}(V_\Sigma)^\vee_{\mathbb{Z}}$ goes arbitrarily far away from the boundary of the dual of the effective cone of V_Σ.

Moreover the error term

$$\tau(V_\Sigma) - [\mathrm{Hom}_k^{\delta}(\mathbb{P}^1_k, V_\Sigma)_U]\,\mathbb{L}_k^{-\delta\cdot\omega^{-1}_{V_\Sigma}}$$

has virtual dimension at most

$$-\tfrac{1}{4}\min_{\alpha\in\Sigma(1)}(\delta_\alpha) + \dim(V_\Sigma).$$

Proof. First note that since $\sum_{\alpha\in\Sigma(1)} D_\alpha$ is an anticanonical divisor of V_Σ, the anticanonical degree of a curve of multidegree $\boldsymbol{d}\in\mathrm{Eff}(V_\Sigma)^\vee_{\mathbb{Z}}$ is $|\boldsymbol{d}| = \sum_{\alpha\in\Sigma(1)} d_\alpha$. By Proposition 5.3, we have the relation

$$[\mathrm{Hom}_k^{\boldsymbol{d}}(\mathbb{P}^1_k, V_\Sigma)_U] = (\mathbb{L}_k - 1)^{\dim(V_\Sigma)}[(\mathbb{P}^1_k)^{\boldsymbol{d}}_{B_\Sigma}]$$

for every $\boldsymbol{d}\in\mathrm{Eff}(V_\Sigma)^\vee_{\mathbb{Z}}$. Therefore studying the asymptotic behaviour of $[\mathrm{Hom}_k^{\boldsymbol{d}}(\mathbb{P}^1_k, V_\Sigma)_U]\,\mathbb{L}_k^{-|\boldsymbol{d}|}$ when $\min_\alpha(d_\alpha)\to\infty$ goes back to studying the one of $[(\mathbb{P}^1_k)^{\boldsymbol{d}}_{B_\Sigma}]\,\mathbb{L}_k^{-|\boldsymbol{d}|}$. Moreover it is convenient to drop the assumption $\boldsymbol{d}\in\mathrm{Eff}(V_\Sigma)^\vee_{\mathbb{Z}}$.

Then (5.2.8) gives

$$\sum_{\boldsymbol{d}\in\mathbb{N}^{\Sigma(1)}} [(\mathbb{P}^1_k)^{\boldsymbol{d}}_{B_\Sigma}]\,\boldsymbol{t}^{\boldsymbol{d}} = \prod_{p\in\mathbb{P}^1_k} P_{B_\Sigma}(\boldsymbol{t}) \times \prod_{\alpha\in\Sigma(1)} Z^{\mathrm{Kapr}}_{\mathbb{P}^1_k}(t_\alpha)$$

and we proceed as in [31, Section 4.1]. First, recall that

$$Z^{\mathrm{Kapr}}_{\mathbb{P}^1_k}(t) = (1-t)^{-1}(1-\mathbb{L}_k t)^{-1}.$$

For any $A\subset\Sigma(1)$, set

$$Z_A(\boldsymbol{t}) = \prod_{\alpha\in A}(1-t_\alpha)^{-1}\prod_{\alpha\notin A}(1-\mathbb{L}_k t_\alpha)^{-1}$$

so that

$$\prod_{\alpha\in\Sigma(1)} Z^{\mathrm{Kapr}}_{\mathbb{P}^1_k}(t_\alpha) = \prod_{\alpha\in\Sigma(1)} \frac{1}{1-\mathbb{L}_k}\left(\frac{1}{1-t_\alpha} - \frac{\mathbb{L}_k}{1-\mathbb{L}_k t_\alpha}\right) = \sum_{A\subset\Sigma(1)} \frac{(-\mathbb{L}_k)^{|\Sigma(1)|-|A|}}{(1-\mathbb{L}_k)^{|\Sigma(1)|}} Z_A(\boldsymbol{t}). \tag{5.4.9}$$

The coefficient of order $\boldsymbol{d}\in\mathbb{N}^{\Sigma(1)}$ of

$$Z_A(\boldsymbol{t}) \times \prod_{p\in\mathbb{P}^1_k} P_{B_\Sigma}(\boldsymbol{t})$$

for a given $A\subset\Sigma(1)$ is the finite sum

$$\sum_{\substack{\boldsymbol{e}\in\mathbb{N}^{\Sigma(1)}\\ \boldsymbol{e}\leqslant\boldsymbol{d}}} \mu_\Sigma(\boldsymbol{e})\mathbb{L}_k^{\sum_{\alpha\in\Sigma(1)\setminus A} d_\alpha - e_\alpha} = \mathbb{L}_k^{|\boldsymbol{d}_{\Sigma(1)\setminus A}|} \sum_{\substack{\boldsymbol{e}\in\mathbb{N}^{\Sigma(1)}\\ \boldsymbol{e}\leqslant\delta}} \mu_\Sigma(\boldsymbol{e})\mathbb{L}_k^{-|\boldsymbol{e}_{\Sigma(1)\setminus A}|},$$

where we use again the notation of Lemma 2.21 for the restriction of $\boldsymbol{e}\in\mathbb{N}^{\Sigma(1)}$ to a subset of $\Sigma(1)$. Normalizing by $\mathbb{L}_k^{|\boldsymbol{d}|}$ and writing $\boldsymbol{e}_{\Sigma(1)\setminus A} = \boldsymbol{e} - \boldsymbol{e}_A$ one gets the sum

$$\sum_{\substack{\boldsymbol{e}\in\mathbb{N}^{\Sigma(1)}\\ \boldsymbol{e}\leqslant\boldsymbol{d}}} \mu_\Sigma(\boldsymbol{e})\mathbb{L}_k^{-|\boldsymbol{e}|}\mathbb{L}_k^{|\boldsymbol{e}_A|-|\boldsymbol{d}_A|}. \tag{5.4.10}$$

If $A=\varnothing$, this is exactly the $\boldsymbol{d}$-th partial sum

$$\sum_{\substack{\boldsymbol{e}\in\mathbb{N}^{\Sigma(1)}\\ \boldsymbol{e}\leqslant\boldsymbol{d}}} \mu_\Sigma(\boldsymbol{e})\mathbb{L}_k^{-|\boldsymbol{e}|}$$

and when $\min_{\alpha\in\Sigma(1)} d_\alpha$ goes to infinity, we know by Proposition 5.1 that this sum converges to

$$\sum_{\boldsymbol{e}\in\mathbb{N}^{\Sigma(1)}} \mu_\Sigma(\boldsymbol{e})\mathbb{L}_k^{-|\boldsymbol{e}|} = \prod_{p\in\mathbb{P}^1_k} \frac{[V_\Sigma\otimes\kappa(p)]}{\mathbb{L}_p^n}(1-\mathbb{L}_p^{-1})^r \qquad \text{(by Remark 5.2)}$$

in $\widehat{\mathscr{M}_k}^{\dim}$. By the proof of [6, Lemma 4.2.5] we have $\dim(\mu_\Sigma(\boldsymbol{e})\mathbb{L}_k^{-|\boldsymbol{e}|}) \leqslant -\frac{1}{2}|\boldsymbol{e}|$ for any $\boldsymbol{e}\in\mathbb{N}^{\Sigma(1)}$. Thus the error term

$$\sum_{\substack{\boldsymbol{e}\in\mathbb{N}^{\Sigma(1)}\\ \boldsymbol{e}\nleqslant\boldsymbol{d}}} \mu_\Sigma(\boldsymbol{e})\mathbb{L}_k^{-|\boldsymbol{e}|}$$

has virtual dimension at most $-\frac{1}{2}\min_{\alpha\in\Sigma(1)}(d_\alpha+1)$.

If $A\neq\varnothing$, then by Lemma 2.21 (taking $\boldsymbol{m}=\boldsymbol{e}$, $\mathfrak{c}_{\boldsymbol{m}} = \mu_\Sigma(\boldsymbol{e})\mathbb{L}_k^{-\boldsymbol{e}}$, $a=\frac{1}{2}$ and $b=0$), the sum (5.4.10) has virtual dimension at most

$$-\tfrac{1}{4}\min_{\alpha\in A}(d_\alpha);$$

hence it becomes negligible in comparison with the term given by $A=\varnothing$ as $\min(d_\alpha)\to\infty$.

Finally, putting everything together, one concludes that the normalised class

$$[\mathrm{Hom}_k^\delta(\mathbb{P}^1_k, V_\Sigma)_U]\,\mathbb{L}_k^{-\delta\cdot\omega^{-1}_{V_\Sigma}}$$

tends to

$$\frac{\mathbb{L}_k^{\dim(V_\Sigma)}}{(1-\mathbb{L}_k^{-1})^{\mathrm{rk}(\mathrm{Pic}(V_\Sigma))}} \prod_{p\in\mathbb{P}^1_k} \frac{[V_\Sigma\otimes\kappa(p)]}{\mathbb{L}_p^{\dim(V_\Sigma)}}(1-\mathbb{L}_p^{-1})^{\mathrm{rk}(\mathrm{Pic}(V_\Sigma))}$$

in $\widehat{\mathscr{M}}_k^{\dim}$ when $\delta \in \operatorname{Eff}(V_\Sigma)^\vee_{\mathbb{Z}}$ goes arbitrarily far away from the boundary $\partial \operatorname{Eff}(V_\Sigma)^\vee$, with error term of virtual dimension bounded by $-\frac{1}{4}\min_{\alpha\in\Sigma(1)}(\delta_\alpha)+\dim(V_\Sigma)$. ☐

Corollary 5.5. *Let*

$$\mathscr{F}(\boldsymbol{t}) = \sum_{\delta\in\operatorname{Eff}(V_\Sigma)^\vee_{\mathbb{Z}}} [\operatorname{Hom}^\delta_k(\mathbb{P}^1_k, V_\Sigma)_U]\, \boldsymbol{t}^\delta \prod_{\alpha\in\Sigma(1)} (1-\mathbb{L}_k t_\alpha).$$

Then $\mathscr{F}(\boldsymbol{t})$ converges at $t_\alpha = \mathbb{L}_k^{-1}$ to $\tau_{\mathbb{P}^1_k}(V_\Sigma)$.

Proof. Let $\mathfrak{b}_{\boldsymbol{d}}$ be the coefficient of multidegree $\boldsymbol{d}$ of $\mathscr{F}(\boldsymbol{t})$. Since

$$\mathscr{F}(\boldsymbol{t}) \prod_{\alpha\in\Sigma(1)} (1-\mathbb{L}_k t_\alpha)^{-1} = \mathscr{F}(\boldsymbol{t}) \sum_{\boldsymbol{d}\in\mathbb{N}^{\Sigma(1)}} \mathbb{L}_k^{|\boldsymbol{d}|}\boldsymbol{t}^{\boldsymbol{d}},$$

we have the relation

$$[\operatorname{Hom}^\delta_k(\mathbb{P}^1_k, V_\Sigma)_U] = \sum_{\boldsymbol{d}+\boldsymbol{d}'=\delta} \mathfrak{b}_{\boldsymbol{d}}\mathbb{L}_k^{|\boldsymbol{d}'|}$$

for every $\delta \in \operatorname{Eff}(V_\Sigma)^\vee_{\mathbb{Z}}$, which becomes after normalisation

$$[\operatorname{Hom}^\delta_k(\mathbb{P}^1_k, V_\Sigma)_U]\, \mathbb{L}_k^{-\delta\cdot\omega^{-1}_{V_\Sigma}} = \sum_{\boldsymbol{e}\leqslant\delta} \mathfrak{b}_{\boldsymbol{e}}\mathbb{L}_k^{-|\boldsymbol{e}|}.$$

This is exactly the δ-th partial sum of the series $\mathscr{F}(\mathbb{L}_k^{-1})$. Since $[\operatorname{Hom}^\delta_k(\mathbb{P}^1_k, V_\Sigma)_U]\,\mathbb{L}_k^{-\delta\cdot\omega^{-1}_{V_\Sigma}}$ converges to $\tau_{\mathbb{P}^1_k}(V_\Sigma)$ when $\min(\delta_\alpha)$ tends to infinity, the claim follows. ☐

5.5. *Equidistribution.* In the remainder of this section, we prove equidistribution of rational curves on smooth split projective toric varieties.

Theorem 5.6. *Let*

$$\mathscr{S} = \coprod_{p\in|\mathscr{S}|} \mathscr{S}_p$$

be a zero-dimensional subscheme of $\mathbb{P}^1_k$, $(m_p)_{p\in|\mathscr{S}|}$ nonnegative integers such that

$$\ell(\mathscr{S}_p) = (m_p+1)[\kappa(p):k]$$

for all $p\in|\mathscr{S}|$, and W a constructible subset of $\operatorname{Hom}_k(\mathscr{S}, V_\Sigma) \simeq \prod_{p\in|\mathscr{S}|}\operatorname{Gr}_{m_p}(V_\Sigma\otimes\kappa(p))$.

Then, when $\delta \in \operatorname{Eff}(V_\Sigma)^\vee_{\mathbb{Z}}$ goes arbitrarily far away from the boundary of the dual of the effective cone, the normalised class

$$[\operatorname{Hom}^\delta_k(\mathbb{P}^1_k, V_\Sigma \mid W)_U]\,\mathbb{L}_k^{-\delta\cdot\omega^{-1}_{V_\Sigma}} \in \mathscr{M}_k$$

tends to the nonzero effective element

$$\tau(V_\Sigma \mid W) = \frac{\mathbb{L}_k^{\dim(V_\Sigma)}}{(1-\mathbb{L}_k^{-1})^{\operatorname{rk}(\operatorname{Pic}(V_\Sigma))}} \times \prod_{p\notin|\mathscr{S}|}(1-\mathbb{L}_p^{-1})^{\operatorname{rk}(\operatorname{Pic}(V_\Sigma))}\frac{[V_\Sigma\otimes\kappa(p)]}{\mathbb{L}_p^{\dim(V_\Sigma)}}[W]\prod_{p\in|\mathscr{S}|}(1-\mathbb{L}_p^{-1})^{\operatorname{rk}(\operatorname{Pic}(V_\Sigma))}\mathbb{L}_p^{-(m_p+1)\dim(V_\Sigma)}$$

in the completion $\widehat{\mathscr{M}}_k^{\dim}$.

Moreover, the error term

$$\tau(V_\Sigma \mid W) - [\mathrm{Hom}_k^\delta(\mathbb{P}_k^1, V_\Sigma \mid W)_U]\,\mathbb{L}_k^{-\delta\cdot\omega_{V_\Sigma}^{-1}} \in \widehat{\mathscr{M}}_k^{\dim}$$

has virtual dimension smaller than

$$-\tfrac{1}{4}\min_{\alpha\in\Sigma(1)}(\delta_\alpha) + \ell(\mathscr{S}) + (1-\ell(\mathscr{S}))(\dim(V_\Sigma)-1) + \dim(W)$$

for all $\delta \in \mathrm{Eff}(V_\Sigma)_{\mathbb{Z}}^\vee$.

Corollary 5.7. *For any nonzero multidegree* $\delta \in \mathrm{Eff}(V_\Sigma)_{\mathbb{Z}}^\vee$ *such that*

$$\min_{\alpha\in\Sigma(1)}(\delta_\alpha) \geqslant 8\ell(\mathscr{S}) - 4,$$

the moduli space $\mathrm{Hom}_k^\delta(\mathbb{P}_k^1, V_\Sigma \mid W)_U$ *has dimension*

$$\delta\cdot\omega_{V_\Sigma}^{-1} + \dim(V_\Sigma)(1-\ell(\mathscr{S})) + \dim(W)$$

as expected.

Remark 5.8. The upper bound on the dimension of the error term we give can be made uniform in the set W of conditions, since the dimension of W is bounded by $\ell(\mathscr{S})\dim(V_\Sigma)$.

The remainder of this section is devoted to the proof of Theorem 5.6. We see $\mathbb{A}_k^2 \setminus \{0\}$ as the universal $\boldsymbol{G}_m$-torsor

$$\mathbb{A}_k^2 \setminus \{0\} \to \mathbb{P}_k^1.$$

Given a cocharacter $\chi : \boldsymbol{G}_m \to \boldsymbol{G}_m^{\Sigma(1)}$, or equivalently a tuple $\boldsymbol{d} = (d_\alpha) \in \mathbb{Z}^{\Sigma(1)}$ (we will switch freely between both notations), we consider the functor from k-schemes to sets

$$\mathbf{Hom}^\chi(\mathbb{A}_k^2 \setminus \{0\}, \mathbb{A}_k^{\Sigma(1)}) : S \rightsquigarrow \mathrm{Hom}_S^\chi(\mathbb{A}_S^2 \setminus \{0\}, \mathbb{A}_S^{\Sigma(1)})$$

of χ-equivariant morphisms, as well as its restriction

$$\mathbf{Hom}^\chi(\mathbb{A}_k^2 \setminus \{0\}, \mathbb{A}_k^{\Sigma(1)})^* : S \rightsquigarrow \mathrm{Hom}_S^\chi(\mathbb{A}_S^2 \setminus \{0\}, \mathbb{A}_S^{\Sigma(1)})^*$$

to χ-equivariant morphisms *with no trivial coordinate* and its second restriction

$$\mathbf{Hom}^\chi(\mathbb{A}_k^2 \setminus \{0\}, \mathcal{T}_\Sigma)^* : S \rightsquigarrow \mathrm{Hom}_S^\chi(\mathbb{A}_S^2 \setminus \{0\}, \mathcal{T}_\Sigma \times_k S)^*$$

to *nondegenerate* χ-equivariant morphisms with no trivial coordinate. These functors are represented respectively by the product

$$\prod_{\alpha\in\Sigma(1)} \mathbb{A}_k^{d_\alpha+1},$$

its restriction

$$\prod_{\alpha\in\Sigma(1)} (\mathbb{A}_k^{d_\alpha+1} \setminus \{0\}),$$

and the open subset

$$\widetilde{(\mathbb{P}^1_k)^{\boldsymbol{d}}_{B_\Sigma}} \subset \prod_{\alpha\in\Sigma(1)} (\mathbb{A}^{d_\alpha+1}_k \setminus \{0\})$$

(defined on page 930 just before Proposition 5.3).

If χ lies in $\mathrm{Eff}(V_\Sigma)^\vee_{\mathbb{Z}}$, composition by $\pi : \mathcal{T}_\Sigma \to V_\Sigma$ provides a map of functors

$$\pi_* : \mathbf{Hom}^\chi(\mathbb{A}^2_k \setminus \{0\}, \mathcal{T}_\Sigma)^* \to \mathbf{Hom}^{\boldsymbol{d}}_k(\mathbb{P}^1_k, V_\Sigma)$$

and we recover the T_{NS}-torsor

$$\widetilde{(\mathbb{P}^1_k)^{\boldsymbol{d}}_{B_\Sigma}} \to \mathrm{Hom}^{\boldsymbol{d}}_k(\mathbb{P}^1_k, V_\Sigma)_U$$

of Proposition 5.3.

5.5.1. *Restricting to $\mathscr{S}$.* Let $\iota : \mathscr{S} \hookrightarrow \mathbb{P}^1_k$ be a zero-dimensional subscheme of $\mathbb{P}^1_k$. In what follows, we will work with the restriction to $\mathscr{S}$ of the universal torsor $\mathbb{A}^2 \setminus \{0\} \to \mathbb{P}^1$, defined over any base scheme S by the following Cartesian square:

$$\begin{tikzcd}
(\mathbb{A}^2_S \setminus \{0\})_{|\mathscr{S}} \arrow[r] \arrow[d, "\mathrm{pr}_{\mathscr{S}}"] \arrow[dr, phantom, "\ulcorner", very near start] & \mathbb{A}^2_S \setminus \{0\} \arrow[d] \\
\mathscr{S} \times_k S \arrow[r, hook, "\iota_S"] & \mathbb{P}^1_S
\end{tikzcd}$$

For any cocharacter $\chi \in \mathcal{X}_*(\boldsymbol{G}_m^{\Sigma(1)})$, we consider the set of χ-equivariant S-morphisms

$$\mathrm{Hom}^\chi_S((\mathbb{A}^2_S \setminus \{0\})_{|\mathscr{S}}, \mathbb{A}^{\Sigma(1)}_S),$$

as well as its subset of morphisms landing in the universal torsor $\mathcal{T}_\Sigma \subset \mathbb{A}^{\Sigma(1)}_k$

$$\mathrm{Hom}^\chi_S((\mathbb{A}^2_S \setminus \{0\})_{|\mathscr{S}}, \mathcal{T}_{\Sigma,S}).$$

The groups $\boldsymbol{G}_m^{\Sigma(1)}(S)$ and $T_{\mathrm{NS}}(S)$ act on these sets via their action on the target.

Lemma 5.9. *For all $\chi \in \mathcal{X}_*(\boldsymbol{G}_m^{\Sigma(1)})$, the functors*

$$S \rightsquigarrow \mathrm{Hom}^\chi_S((\mathbb{A}^2_S \setminus \{0\})_{|\mathscr{S}}, \mathbb{A}^{\Sigma(1)}_S)$$

and

$$S \rightsquigarrow \mathrm{Hom}^\chi_S((\mathbb{A}^2_S \setminus \{0\})_{|\mathscr{S}}, \mathcal{T}_{\Sigma,S})$$

are respectively represented by the finite products

$$\prod_{p\in|\mathscr{S}|} \mathrm{Gr}_{m_p}(\mathbb{A}^{\Sigma(1)}_{\kappa(p)})$$

and

$$\prod_{p\in|\mathscr{S}|} \mathrm{Gr}_{m_p}(\mathcal{T}_\Sigma \times_k \kappa(p))$$

of jet schemes.

Proof. Since the restriction of $\mathbb{A}^2_k \setminus \{0\} \to \mathbb{P}^1_k$ to $\mathscr{S}$ is a trivial bundle, we may fix a section $s : \mathscr{S} \to (\mathbb{A}^2_k \setminus \{0\})_{|\mathscr{S}}$. Then composition by s induces a map

$$\mathrm{Hom}^{\chi}_S((\mathbb{A}^2_S \setminus \{0\})_{|\mathscr{S}}, \mathbb{A}^{\Sigma(1)}_S) \to \mathbb{A}^{\Sigma(1)}_k(\mathscr{S} \times_k S), \quad f \mapsto f \circ (s, \mathrm{id}_S),$$

which is functorial in S.

Now remark that an element of $\mathrm{Hom}^{\chi}_S((\mathbb{A}^2_S \setminus \{0\})_{|\mathscr{S}}, \mathbb{A}^{\Sigma(1)}_S)$ is entirely determined by its restriction to the image of s: indeed, for all $y \in (\mathbb{A}^2_S \setminus \{0\})_{|\mathscr{S}}(S)$, one has the relation

$$f(y) = \chi\big(y \cdot (s \circ \mathrm{pr}_{\mathscr{S}}(y))^{-1}\big) f(s \circ \mathrm{pr}_{\mathscr{S}}(y)),$$

where $y \cdot (s \circ \mathrm{pr}_{\mathscr{S}}(y))^{-1} \in \boldsymbol{G}_{m,\mathscr{S}}(S)$ is given by the $\boldsymbol{G}_{m,\mathscr{S}}$-torsor structure. An $\mathscr{S} \times_k S$-point of $\mathbb{A}^{\Sigma(1)}_S$ is the datum of such a restriction; hence it provides a unique χ-equivariant morphism. By the definition of Greenberg schemes, the conclusion follows. □

Composition by s and $\pi : \mathcal{T}_\Sigma \to V_\Sigma$ provides a map (functorial in S)

$$\mathrm{Hom}^{\chi}_S((\mathbb{A}^2_S \setminus \{0\})_{|\mathscr{S}}, \mathcal{T}_{\Sigma,S}) \to V_\Sigma(\mathscr{S} \times_k S), \quad f \mapsto (\pi, \mathrm{id}_S) \circ f \circ (s, \mathrm{id}_S).$$

Two χ-equivariant morphisms $\tilde{\varphi}, \tilde{\varphi}' : (\mathbb{A}^2_S \setminus \{0\})_{|\mathscr{S}} \to \mathbb{A}^{\Sigma(1)}_S$ induce the same $(\mathscr{S} \times_k S)$-point of V_Σ if and only if there is an element $a \in T_{\mathrm{NS}}(\mathscr{S} \times_k S)$ such that $\tilde{\varphi} = a \cdot \tilde{\varphi}'$. This map defines a $T_{\mathrm{NS},\mathscr{S}}$-torsor over $\mathrm{Hom}(\mathscr{S}, V_\Sigma)$.

Definition 5.10. For any constructible subset $\widetilde{W} \subset \mathrm{Hom}^{\chi}_S((\mathbb{A}^2_S \setminus \{0\})_{|\mathscr{S}}, \mathbb{A}^{\Sigma(1)}_S)$, we denote by

$$\mathrm{Hom}^{\chi}_S(\mathbb{A}^2_S \setminus \{0\}, \mathbb{A}^{\Sigma(1)}_S \mid \widetilde{W})^{(*)}$$

the subset of $\mathrm{Hom}^{\chi}_S(\mathbb{A}^2_S \setminus \{0\}, \mathbb{A}^{\Sigma(1)}_S)^{(*)}$ of morphisms whose restriction to $(\mathbb{A}^2_S \setminus \{0\})_{|\mathscr{S}}$ belongs to $\widetilde{W}$ (in the sequel the exponent $^{(*)}$ will be a convenient notation to say that one can restrict to morphisms having no trivial coordinate).

We will say that a χ-equivariant S-morphism *is nondegenerate* above $\mathscr{S}$ if its pull-back to $(\mathbb{A}^2_S \setminus \{0\})_{|\mathscr{S}}$ has image in $\mathcal{T}_{\Sigma,S} \subset \mathbb{A}^{\Sigma(1)}_S$.

This defines subfunctors of $\mathbf{Hom}^{\chi}(\mathbb{A}^2_k \setminus \{0\}, \mathbb{A}^{\Sigma(1)}_k)$.

5.5.2. *Euclidean division.* Fixing coordinates on $\mathbb{A}^2_k$, we can see χ-equivariant morphisms $\mathbb{A}^2_k \setminus \{0\} \to \mathbb{A}^{\Sigma(1)}_k$ as $\Sigma(1)$-tuples of homogeneous polynomials in two indeterminates t_0 and t_1. Let us temporarily choose a generator ϖ of the ideal defining $\mathscr{S}$ in $\mathbb{P}^1_k$, that is to say, a nontrivial homogeneous polynomial of degree $\ell(\mathscr{S})$ in two indeterminates. Up to changing coordinates on $\mathbb{P}^1_k$ we may assume furthermore that $[0:1]$ does not belong to $\mathscr{S}$ (that is to say, t_0 does not divide ϖ).

Then, the Euclidean division of a polynomial $P(t)$ of degree at most d by $\varpi(t) = \varpi(1,t)$ is the unique decomposition of the form

$$P(t) = Q(t)\varpi(t) + R(t),$$

where $Q(t)$ is of degree at most $d-\ell(\mathscr{S})$ and R of degree strictly smaller than $\ell(\mathscr{S})$. This provides a Euclidean division of $P(t_0,t_1)=t_0^dP(t_1/t_0)$ of the form

$$P(t_0,t_1)=t_0^dQ(t_1/t_0)\varpi(t_1/t_0)+t_0^dR(t_1/t_0)=Q(t_0,t_1)\varpi(t_0,t_1)+R(t_0,t_1),$$

where

$$\begin{aligned}Q(t_0,t_1)&=t_0^{d-\ell(\mathscr{S})}Q(t_1/t_0),\\ \varpi(t_0,t_1)&=t_0^{\ell(\mathscr{S})}\omega(t_1/t_0),\\ R(t_0,t_1)&=t_0^dR(t_1/t_0).\end{aligned}$$

Note that $Q(t_0,t_1)$, $\varpi(t_0,t_1)$ and $R(t_0,t_1)$ are homogeneous polynomials of degree d and that they do not depend on the choice of ϖ. The first one uniquely defines an element of

$$\mathrm{Hom}^d(\mathbb{A}_k^2\setminus\{0\},\mathbb{A}_k^1\mid \mathrm{res}_{\mathscr{S}}=0),$$

while the second one uniquely defines an element of

$$\mathrm{Hom}^d((\mathbb{A}_k^2\setminus\{0\})_{|\mathscr{S}},\mathbb{A}_k^1),$$

since in that case the k-vector space

$$k[t]/(\varpi(1,t))\simeq\prod_{p\in|\mathscr{S}|}\mathbb{A}_{\kappa(p)}^{\Sigma(1)}(\kappa(p)[t]/(t^{m_p+1}))\simeq\prod_{p\in|\mathscr{S}|}\mathrm{Gr}_{m_p}(\mathbb{A}_{\kappa(p)}^{\Sigma(1)})(\kappa(p))$$

provides a concrete incarnation of such a space of morphisms. Remember as well that taking the restriction to $\mathscr{S}$ is a linear operation.

One can perform this Euclidean division simultaneously for all the coordinates of an element of $\mathrm{Hom}^\chi(\mathbb{A}_k^2\setminus\{0\},\mathbb{A}_k^{\Sigma(1)})$. Recall that we fixed a section $s:\mathscr{S}\to(\mathbb{A}^2\setminus\{0\})_{|\mathscr{S}}$ in Lemma 5.9 so that

$$\prod_{p\in|\mathscr{S}|}\mathrm{Gr}_{m_p}(\mathbb{A}_{\kappa(p)}^{\Sigma(1)})$$

represents the functor $S\rightsquigarrow\mathrm{Hom}_S^\chi((\mathbb{A}_S^2\setminus\{0\})_{|\mathscr{S}},\mathbb{A}_S^{\Sigma(1)})$. We can see elements of this product of arc spaces as tuples $(r_\alpha(t))_{\alpha\in\Sigma(1)}$ of polynomials of degree at most $\ell(\mathscr{S})-1$. From these remarks, we deduce the following lemma.

Lemma 5.11. *For every $\chi\in\mathbb{N}^{\Sigma(1)}\subset\mathcal{X}_*(\boldsymbol{G}_m^{\Sigma(1)})\simeq\mathbb{Z}^{\Sigma(1)}$, Euclidean decomposition corresponds to the exact sequence of vector spaces over k*

$$\begin{tikzcd}
0 \arrow[r] & \ker(\mathrm{res}_{\mathscr{S}}) \arrow[r] & \mathrm{Hom}^\chi(\mathbb{A}_k^2\setminus\{0\},\mathbb{A}_k^{\Sigma(1)}) \arrow[dl, bend left, "\mathrm{res}_{\mathscr{S}}"'] \\
& \mathrm{Hom}^\chi((\mathbb{A}_k^2\setminus\{0\})_{|\mathscr{S}},\mathbb{A}_k^{\Sigma(1)}) \arrow[r] & 0
\end{tikzcd}$$

and $\mathrm{res}_{\mathscr{S}}$ *is a piecewise trivial fibration. Moreover the α-th coordinate of* $\mathrm{res}_{\mathscr{S}}$ *is surjective if $\chi_\alpha\geqslant\ell(\mathscr{S})-1$, injective if $\chi_\alpha\leqslant\ell(\mathscr{S})-1$, and nonempty fibres of* $\mathrm{res}_{\mathscr{S}}$ *have dimension*

$$\sum_{\alpha\in\Sigma(1)}\min(0,\chi_\alpha-\ell(\mathscr{S})+1).$$

Hence for any constructible subset $\widetilde{W} \subset \prod_{p\in|\mathscr{S}|} \mathrm{Gr}_{m_p}(\mathbb{A}^{\Sigma(1)}_{\kappa(p)})$ *we have the dimensional upper bound*

$$\dim_k\big(\mathrm{Hom}^\chi(\mathbb{A}^2_k \setminus \{0\}, \mathbb{A}^{\Sigma(1)}_k \mid \widetilde{W})\big) \leqslant \dim(\widetilde{W}) + \sum_{\alpha\in\Sigma(1)} \min(0, \chi_\alpha - \ell(\mathscr{S}) + 1). \tag{5.5.11}$$

Assume $\chi \geqslant \ell(\mathscr{S}) - 1$. *Then for any* $g \in \boldsymbol{G}_m^{\Sigma(1)}(\mathscr{S})$ *and constructible subset* $\widetilde{W} \subset \prod_{p\in|\mathscr{S}|} \mathrm{Gr}_{m_p}(\mathbb{A}^{\Sigma(1)}_{\kappa(p)})$ *there is a commutative diagram*

$$\begin{array}{ccc}
\mathrm{Hom}^\chi\big(\mathbb{A}^2_k \setminus \{0\}, \mathbb{A}^{\Sigma(1)}_k \mid \widetilde{W}\big)^{(*)} & \xrightarrow{\mathrm{res}_{\mathscr{S}}} & \mathrm{Hom}^\chi\big((\mathbb{A}^2_k \setminus \{0\})_{|\mathscr{S}}, \mathbb{A}^{\Sigma(1)}_k\big) \\
{\scriptstyle \tau_g}\big\downarrow & & \big\downarrow{\scriptstyle g\,\cdot} \\
\mathrm{Hom}^\chi\big(\mathbb{A}^2_k \setminus \{0\}, \mathbb{A}^{\Sigma(1)}_k \mid g\cdot\widetilde{W}\big)^{(*)} & \xrightarrow{\mathrm{res}_{\mathscr{S}}} & \mathrm{Hom}^\chi\big((\mathbb{A}^2_k \setminus \{0\})_{|\mathscr{S}}, \mathbb{A}^{\Sigma(1)}_k\big)
\end{array}$$

in which the vertical arrows are isomorphisms. The first one, τ_g, *sends a morphism of Euclidean decomposition*

$$(q_\alpha, r_\alpha)_{\alpha\in\Sigma(1)}$$

to

$$(q_\alpha, g_\alpha \cdot r_\alpha)_{\alpha\in\Sigma(1)}.$$

Up to a multiplicative constant, rational curves of degree $d \in \mathbb{N}$ in $\mathbb{P}^n_k$ are given by $(n+1)$-tuples of degree-d homogeneous polynomials with no common factor. Conversely, the parameter space of $(n+1)$-tuples of degree-d homogeneous polynomials admits a decomposition into disjoint subspaces corresponding to the degree of the common factor. The Möbius inversion we performed for nonconstrained curves generalises this remark.

Definition 5.12. We will say that a zero-cycle *avoids* $\mathscr{S}$ if it has support outside $|\mathscr{S}|$. This terminology naturally extends to χ-equivariant morphisms by considering their image through the $\boldsymbol{G}_m^{\Sigma(1)}$-torsor

$$\mathrm{Hom}^\chi(\mathbb{A}^2_k \setminus \{0\}, \mathbb{A}^{\Sigma(1)})^* \to \prod_{\alpha\in\Sigma(1)} \mathbb{P}^{\chi_\alpha}_k \simeq \mathrm{Sym}^\chi_{/k}(\mathbb{P}^1_k).$$

5.5.3. *The motivic Möbius inversion in details.* Equivariant morphisms with image contained in $\mathcal{T}_\Sigma$ are the morphisms $\mathbb{A}^2_k \setminus \{0\} \to \mathbb{A}^{\Sigma(1)}_k$ with no forbidden zeros, which we also call having no degeneracies. Our goal now is to adapt the Möbius inversion technique to the context of constrained curves. More precisely, we provide a relation between the classes of equivariant morphisms and the ones obtained by adding degeneracies to nondegenerate morphisms. This relation relies heavily on the following piecewise identification. Then we specialise this relation to morphisms with constraints. Finally, we approximate it and conclude.

Identification 5.13. Let $G = \boldsymbol{G}_m^{\Sigma(1)}$. We stratify $\mathrm{Hom}^\chi(\mathbb{A}^2 \setminus \{0\}, \mathbb{A}^{\Sigma(1)})^*$ with respect to the vanishing order at ∞. Each stratum can be viewed as the subspace of tuples of homogeneous polynomials of the form

$$P_\alpha(T_0, T_1) = a_\alpha T_1^{v_\infty(P_\alpha)} Q_\alpha(T_0, T_1),$$

where $a_\alpha \in k^\times$, $v_\infty(P_\alpha)$ is the vanishing order of P_α at ∞, and the coefficient of $T_1^{\chi_\alpha - v_\infty(P_\alpha)}$ in Q_α is 1; hence Q_α can be identified with a zero-cycle avoiding ∞. In this decomposition, a_α is the leading coefficient of $P_\alpha(1,T)$. Then, each stratum can be identified with $G \times \mathrm{Sym}^{\chi-v_\infty}_{/k}(\mathbb{P}^1_k \setminus \{\infty\})$ by sending (P_α) to $((a_\alpha),(Q_\alpha))$. This piecewise correspondence identifies

$$\mathrm{Hom}^\chi(\mathbb{A}^2_k \setminus \{0\}, \mathbb{A}^{\Sigma(1)}_k)^*$$

with

$$G \times_k \mathrm{Sym}^\chi_{/k}(\mathbb{P}^1_k) \simeq \mathrm{Sym}^\chi_{/G}(\mathbb{P}^1_G),$$

and

$$\mathrm{Hom}^\chi(\mathbb{A}^2_k \setminus \{0\}, \mathcal{T}_\Sigma)$$

with

$$G \times_k \mathrm{Sym}^\chi_{\mathbb{P}^1_k/k}(\mathbf{1}_{A(B_\Sigma)}\mathbb{P}^1_k) \simeq \mathrm{Sym}^\chi_{\mathbb{P}^1_G/G}(\mathbf{1}_{A(B_\Sigma)}\mathbb{P}^1_G)$$

(recall the definition of $A(B_\Sigma)$ given on page 926).

In particular, tuples such that $a_\alpha = 1$ for every $\alpha \in \Sigma(1)$ deserve to be called *unitary* and are identified with their tuple of zero-divisors living in

$$\mathrm{Sym}^\chi_{\mathbb{P}^1_k/k}(\mathbb{P}^1_k) \simeq \{1_G\} \times \mathrm{Sym}^\chi_{\mathbb{P}^1_k/k}(\mathbb{P}^1_k) \simeq \mathrm{Sym}^\chi_{\mathbb{P}^1_G/G}(\mathbb{P}^1_{\{1_G\}}).$$

The proof of the following lemma is left to the reader.

Lemma 5.14. *Let S be a scheme, and X, Y be two S-varieties. Assume that there exists a piecewise isomorphism $f = (f_j : X_j \to Y_j)$ between X and Y, that is to say, a finite number of pairwise disjoint locally closed subsets X_j and Y_j, respectively of X and Y, such that $X = \bigsqcup_j X_j$ and $Y = \bigsqcup_j Y_j$, together with isomorphisms $f_j : X_j \to Y_j$.*

Then

$$[Z \to Y] \mapsto [f^*(Z \to Y)] = \sum_j [f_j^*(Z \times_Y Y_j \to Y_j)]$$

defines a ring isomorphism $K_0\mathbf{Var}_Y \simeq K_0\mathbf{Var}_X$.

Notation 5.15. Let W be a constructible subset of $\mathrm{Hom}(\mathscr{S}, V_\Sigma)$. Its preimage through the map

$$\mathrm{Hom}^\chi((\mathbb{A}^2_S \setminus \{0\})_{|\mathscr{S}}, \mathcal{T}_{\Sigma,S}) \to \mathrm{Hom}(\mathscr{S}, V_\Sigma)$$

will be written $\widetilde{W}$. It is a Zariski-locally trivial $T_{\mathrm{NS},\mathscr{S}}$-torsor above W.

For every $d \in \mathbb{N}$, we fix a section of

$$\mathrm{Hom}^d(\mathbb{A}^2_k \setminus \{0\}, \mathbb{A}^1_k) \xrightarrow{\mathrm{res}_\mathscr{S}} \mathrm{Im}(\mathrm{res}_\mathscr{S}) \subset \mathrm{Hom}^d((\mathbb{A}^2_k \setminus \{0\})_{|\mathscr{S}}, \mathbb{A}^1_k)$$

so that we are able to see reduction modulo $\mathscr{S}$ as morphisms in $\mathrm{Hom}^d(\mathbb{A}^2_k \setminus \{0\}, \mathbb{A}^1_k)$.

Remark 5.16. Up to replacing $\mathscr{S}$ by $\mathscr{S} \cup \{[1:0]\}$ and W by $W \times V_\Sigma$, we can always assume that $[1:0] = \infty$ is a closed point of $\mathscr{S}$.

Notation 5.17. We will freely use the convenient notation

$$\bar{g}^{-1} = (\bar{g}_\alpha^{-1})_{\alpha\in\Sigma(1)}$$

for the inverse of the restriction to $\mathscr{S}$ of any χ-equivariant morphism $g : \mathbb{A}_k^2 \setminus \{0\} \to \mathbb{A}_k^{\Sigma(1)}$ avoiding $|\mathscr{S}|$.

Definition 5.18. For any $\chi, \chi' \in \mathbb{N}^{\Sigma(1)}$ such that $\chi' \leqslant \chi$, let $\Phi^\chi_{\chi'}$ the morphism given by the coordinatewise multiplication

$$\Phi^\chi_{\chi'} : \mathrm{Hom}^{\chi'}(\mathbb{A}_k^2 \setminus \{0\}, \mathbb{A}_k^{\Sigma(1)}) \times \mathrm{Hom}^{\chi-\chi'}(\mathbb{A}_k^2 \setminus \{0\}, \mathbb{A}_k^{\Sigma(1)}) \to \mathrm{Hom}^{\chi}(\mathbb{A}_k^2 \setminus \{0\}, \mathbb{A}_k^{\Sigma(1)}),$$
$$((f_\alpha)_{\alpha\in\Sigma(1)}, (g_\alpha)_{\alpha\in\Sigma(1)}) \mapsto (f_\alpha g_\alpha)_{\alpha\in\Sigma(1)}.$$

For any $(\chi - \chi')$-equivariant morphism g, consider the induced map

$$\Phi^\chi_g : \mathrm{Hom}^{\chi'}(\mathbb{A}_k^2 \setminus \{0\}, \mathbb{A}_k^{\Sigma(1)}) \otimes \kappa(g) \to \mathrm{Hom}^{\chi}(\mathbb{A}_k^2 \setminus \{0\}, \mathbb{A}_k^{\Sigma(1)}) \otimes \kappa(g),$$
$$(f_\alpha)_{\alpha\in\Sigma(1)} \mapsto (f_\alpha g_\alpha)_{\alpha\in\Sigma(1)}.$$

Our goal is to give an interpretation of the motivic Möbius inversion in terms of the $\Phi^\chi_{\chi'}$, in a way compatible with the stratification and piecewise identification of $\mathrm{Hom}^\chi(\mathbb{A}^2 \setminus \{0\}, \mathbb{A}^{\Sigma(1)})$ from Identification 5.13.

As a first step, instead of working over k, we are going to work with zero-cycles on $\mathbb{P}^1_G$ relative to $G = \boldsymbol{G}_m^{\Sigma(1)}$. In what follows, we are going to exploit the details of the proof of the multiplicative property of motivic Euler products as it is done in [3, Section 3.9]. We take $I_0 = \mathbb{N}^{\Sigma(1)}$ and $I = I_0 \setminus \{\boldsymbol{0}\}$, but in general one can take I to be any abelian semigroup and $I_0 = I \cup \{0\}$; see [3, Section 3.9.3].

Let X be a variety above a certain base scheme S and take $\boldsymbol{n}, \boldsymbol{n}', \boldsymbol{n}'' \in \mathbb{N}^{\Sigma(1)}$ such that

$$\boldsymbol{n} = \boldsymbol{n}' + \boldsymbol{n}''.$$

Let κ' and κ'' be partitions respectively of $\boldsymbol{n}'$ and $\boldsymbol{n}''$. The previous relation becomes

$$\sum_{\boldsymbol{i}\in I} \boldsymbol{i}\kappa'_{\boldsymbol{i}} + \sum_{\boldsymbol{i}\in I} \boldsymbol{i}\kappa''_{\boldsymbol{i}} = \boldsymbol{n}.$$

Let $\gamma = (n_{\boldsymbol{p},\boldsymbol{q}})_{(\boldsymbol{p},\boldsymbol{q})\in I_0^2\setminus\{0\}}$ be a collection of integers such that, for all $\boldsymbol{p}, \boldsymbol{q} \in I$,

$$\sum_{\boldsymbol{q}\in I_0} n_{\boldsymbol{p},\boldsymbol{q}} = \kappa'_{\boldsymbol{p}}, \qquad \sum_{\boldsymbol{p}\in I_0} n_{\boldsymbol{p},\boldsymbol{q}} = \kappa''_{\boldsymbol{q}}.$$

Let $\kappa = \kappa(\gamma)$ be the "overlap partition" of $\boldsymbol{n}$ given by

$$\kappa_{\boldsymbol{i}} = \sum_{\boldsymbol{p}+\boldsymbol{q}=\boldsymbol{i}} n_{\boldsymbol{p},\boldsymbol{q}}$$

for all $\boldsymbol{i} \in I$. It is important to note that κ, κ' and κ'' are entirely determined by γ. Let

$$\mathrm{Sym}^{\kappa'}_{/S}(X)_* \times_\gamma \mathrm{Sym}^{\kappa''}_{/S}(X)_*$$

be the locally closed subset of

$$\mathrm{Sym}^{\kappa'}_{/S}(X)_* \times \mathrm{Sym}^{\kappa''}_{/S}(X)_*$$

given by points whose $\mathrm{Sym}^{\kappa'_{\boldsymbol{p}}}_{/S}(X)$-component and $\mathrm{Sym}^{\kappa''_{\boldsymbol{q}}}_{/S}(X)$-component overlap exactly above an effective zero-cycle of degree $n_{\boldsymbol{p},\boldsymbol{q}}$ [3, Section 3.9.6]. One can show by induction [3, Section 3.9.7.3] that there is a canonical isomorphism

$$\mathrm{Sym}^{\kappa'}_{/S}(X)_* \times_\gamma \mathrm{Sym}^{\kappa''}_{/S}(X)_* \simeq \Bigg(\prod_{\boldsymbol{i}\in I} \prod_{\substack{(\boldsymbol{p},\boldsymbol{q})\in I_0^2\setminus\{0\}\\ \boldsymbol{p}+\boldsymbol{q}=\boldsymbol{i}}} \mathrm{Sym}^{n_{\boldsymbol{p},\boldsymbol{q}}}_{/S}(X)\Bigg)_*.$$

The right-hand side will be denoted by $\mathrm{Sym}^{\gamma}_{/S}(X)_*$. Then, there is a canonical morphism

$$\Phi^\gamma : \mathrm{Sym}^{\kappa'}_{/S}(X)_* \times_\gamma \mathrm{Sym}^{\kappa''}_{/S}(X)_* \simeq \mathrm{Sym}^{\gamma}_{/S}(X)_* \longrightarrow \mathrm{Sym}^{\kappa(\gamma)}_{/S}(X)_* \tag{5.5.12}$$

induced by the morphisms

$$\prod_{\boldsymbol{p}+\boldsymbol{q}=\boldsymbol{i}} \mathrm{Sym}^{n_{\boldsymbol{p},\boldsymbol{q}}}_{/S}(X) \to \mathrm{Sym}^{\kappa_{\boldsymbol{i}}(\gamma)}_{/S}(X), \quad \boldsymbol{i}\in I.$$

If $\mathscr{A} = (A_{\boldsymbol{p}})_{\boldsymbol{p}\in I}$ and $\mathscr{B} = (B_{\boldsymbol{q}})_{\boldsymbol{q}\in I}$ are two families of X-varieties, then

$$\mathrm{Sym}^{\kappa'(\gamma)}_{X/S}(\mathscr{A}) \times_\gamma \mathrm{Sym}^{\kappa''(\gamma)}_{X/S}(\mathscr{B})$$

is the class above $\mathrm{Sym}^{\kappa'}_{/S}(X)_* \times_\gamma \mathrm{Sym}^{\kappa''}_{/S}(X)_*$ obtained from

$$\mathrm{Sym}^{\kappa'(\gamma)}_{X/S}(\mathscr{A}) \boxtimes \mathrm{Sym}^{\kappa''(\gamma)}_{X/S}(\mathscr{B})$$

by pull-back, while $\mathrm{Sym}^{\gamma}_{/S}(\mathscr{A}\boxtimes_X \mathscr{B})_*$ is defined as

$$\Bigg(\prod_{\boldsymbol{i}\in I} \prod_{\boldsymbol{p}+\boldsymbol{q}=\boldsymbol{i}} \mathrm{Sym}^{n_{\boldsymbol{p},\boldsymbol{q}}}_{X/S}(A_{\boldsymbol{p}} \boxtimes_X B_{\boldsymbol{q}})\Bigg)_*.$$

Example 5.19. Taking $S = G$ and $X = \mathbb{P}^1_G$,

$$\mathrm{Sym}^{\kappa'}_{\mathbb{P}^1_G/G}(\mathbb{P}^1_G)_* \times_\gamma \mathrm{Sym}^{\kappa''}_{\mathbb{P}^1_G/G}(\mathbb{P}^1_G)_*,$$

the canonical morphism Φ^γ

$$\mathrm{Sym}^{\kappa'}_{/G}(\mathbb{P}^1_G)_* \times_\gamma \mathrm{Sym}^{\kappa''}_{/G}(\mathbb{P}^1_G)_* \simeq \Bigg(\prod_{(\boldsymbol{p},\boldsymbol{q})\in I_0\setminus\{0\}} \mathrm{Sym}^{n_{\boldsymbol{p},\boldsymbol{q}}}_{/G}(\mathbb{P}^1_G)\Bigg)_* \xrightarrow{\Phi^\gamma} \mathrm{Sym}^{\kappa(\gamma)}_{/G}(\mathbb{P}^1_G)_*$$

sends pairs of tuples of zero-cycles to their coordinatewise sum. This is the zero-cycle version of the map $\Phi^{\chi}_{\chi'}$ we previously defined.

Proposition 5.20 (multiplicativity of motivic Euler products: refined version). *Let X be a variety above a base scheme S. Let $\mathscr{A}$ and $\mathscr{B}$ be families of varieties above X indexed by I. Let $\gamma = (n_{\boldsymbol{p},\boldsymbol{q}})_{(\boldsymbol{p},\boldsymbol{q})\in I_0^2\setminus\{0\}}$ be a collection of integers as above. Then*

$$\mathrm{Sym}^{\gamma}_{/S}(\mathscr{A}\boxtimes_X \mathscr{B})_* = \mathrm{Sym}^{\kappa'(\gamma)}_{X/S}(\mathscr{A})_* \times_\gamma \mathrm{Sym}^{\kappa''(\gamma)}_{X/S}(\mathscr{B})_*$$

in $K_0\mathbf{Var}_{\mathrm{Sym}^{\kappa(\gamma)}_{/S}(X)}$.

Proof. See [3, Section 3.9.7]. $\square$

In the following remarks, the use of the subscript $_{(*)}$ means that the claims remain valid when one takes the restriction of the symmetric products to the complement of the diagonal.

Remark 5.21. Let $\mathfrak{a}$ be a class in the Grothendieck ring of varieties over a certain S-variety X. Then, for any $k \in \mathbb{N}^*$,

$$\mathrm{Sym}^k_{X/S}(2\mathfrak{a})_{(*)} = \sum_{k_1+k_2=k} \mathrm{Sym}^{k_1,k_2}(\mathfrak{a}, \mathfrak{a})_{(*)}$$

in $K_0\mathbf{Var}_{\mathrm{Sym}^k_{/S}(X)_{(*)}}$, and more generally, for any $k, \ell \in \mathbb{N}^*$,

$$\mathrm{Sym}^k_{X/S}(\ell\mathfrak{a})_{(*)} = \sum_{k_1+\cdots+k_\ell=k} \mathrm{Sym}^{k_1,\ldots,k_\ell}_{X/S}(\mathfrak{a}, \ldots, \mathfrak{a})_{(*)}.$$

It is important to recall that if $\mathfrak{a} = [Y \to X]$ is an effective class, and $Y_1, \ldots, Y_\ell$ are ℓ copies of Y, these identities come from the canonical decomposition of

$$\mathrm{Sym}^k_{X/S}(Y_1 \amalg \cdots \amalg Y_\ell)_{(*)}$$

into the $\mathrm{Sym}^{k_1,\ldots,k_\ell}_{X/S}(Y_1, \ldots, Y_\ell)_{(*)}$ relative to $\mathrm{Sym}^k_{/S}(X)_{(*)}$.

Remark 5.22. Denoting by $\mathcal{Q} \subset \mathbb{N}^{(\mathbb{N}^*)}$ the set of partitions of integers (in the usual sense) without holes, for any $k \in \mathbb{N}^*$ we have the relation

$$\mathrm{Sym}^k_{X/S}(-\mathfrak{a})_{(*)} = \sum_{\substack{\kappa=(k_i)_{i\in\mathbb{N}}\in\mathcal{Q} \\ \sum_i k_i=k}} (-1)^{|\{i\in\mathbb{N} \mid k_i>0\}|}\, \mathrm{Sym}^\kappa_{X/S}(\mathfrak{a})_{(*)}$$

above $\mathrm{Sym}^k_{/S}(X)_{(*)}$ [5, Example 6.1.4]. Again, it is important to remember where this relation comes from.

If $\mathfrak{a} = [Y \to X]$ is an effective class in $K_0\mathbf{Var}_X$, then $\mathrm{Sym}^k_{X/S}(-\mathfrak{a})$ is *by definition* the degree-k part of the inverse of (the class of)

$$\mathrm{Sym}^\bullet_{X/S}(Y) = (1, Y, \mathrm{Sym}^2_{X/S}(Y), \ldots)$$

viewed above

$$\mathrm{Sym}^\bullet_{/S}(X) = \prod_{\ell\in\mathbb{N}} \mathrm{Sym}^\ell_{/S}(X).$$

Indeed, $K_0\mathbf{Var}_{\mathrm{Sym}^\bullet_{/S}(X)}$ admits a natural structure of graded $K_0\mathbf{Var}_X$-algebra for which the product law is induced by the natural maps

$$\mathrm{Sym}^i_{/S}(X) \times \mathrm{Sym}^{k-i}_{/S}(X) \to \mathrm{Sym}^k_{/S}(X);$$

see [5, Section 6.1.1]. Then, one writes

$$\frac{1}{\mathrm{Sym}^\bullet_{X/S}(Y)} = \frac{1}{1 + (\mathrm{Sym}^\bullet_{X/S}(Y) - 1)} = \sum_{k=0}^{\infty} (-1)^k (0, Y, \mathrm{Sym}^2_{X/S}(Y), \ldots)^k$$

and takes the degree-k part. This provides an explicit definition of $\mathrm{Sym}^k_{X/S}(-[Y])$ in terms of the classes of the $\mathrm{Sym}^\kappa_{X/S}(Y)$, for $\kappa \in \mathcal{Q}$, partition of k and above $\mathrm{Sym}^k_{/S}(X)$. In particular, the arrows are explicit: they are the natural ones.

Now, starting from the relation

$$Q_{B_\Sigma}(\boldsymbol{t}) = \frac{P_{B_\Sigma}(\boldsymbol{t})}{\prod_{\alpha\in\Sigma(1)}(1-t_\alpha)}$$

in $\mathbb{Z}[\![\boldsymbol{t}]\!]$, that is to say,

$$\sum_{\boldsymbol{n}\in\mathbb{N}^{\Sigma(1)}} \mathbf{1}_{A(B_\Sigma)}(\boldsymbol{n})\boldsymbol{t}^{\boldsymbol{n}} = \Big(\sum_{\boldsymbol{n}\in\mathbb{N}^{\Sigma(1)}} \boldsymbol{t}^{\boldsymbol{n}}\Big)\Big(\sum_{\boldsymbol{n}\in\mathbb{N}^{\Sigma(1)}} \mu_{B_\Sigma}(\boldsymbol{n})\boldsymbol{t}^{\boldsymbol{n}}\Big)$$

(the definition of $A(B_\Sigma)$ was given on page 926), we take the motivic Euler products associated to the corresponding $\mathbb{P}^1_G$-families

$$(\mathbf{1}_{A(B_\Sigma)}(\boldsymbol{n})[\mathbb{P}^1_G]), \quad (\mathbb{P}^1_G), \quad (\mu_{B_\Sigma}(\boldsymbol{n})[\mathbb{P}^1_{\{1_G\}}]),$$

all three of them being indexed by $\boldsymbol{n}\in\mathbb{N}^{\Sigma(1)}\setminus\{0\}$ (an index we will drop in the following computations). More precisely, we apply Proposition 5.20 on page 940 to $\mathscr{A} = (\mathbb{P}^1_G)$ and $\mathscr{B} = (\mu_{B_\Sigma}(\boldsymbol{n})[\mathbb{P}^1_{\{1_G\}}])$. If ϖ is any generalised partition of a certain nonzero tuple $\boldsymbol{n}\in\mathbb{N}^{\Sigma(1)}$, then one gets the relation in $K_0\mathbf{Var}_{\mathrm{Sym}^{\varpi}_{/G}(\mathbb{P}^1_G)}$

$$\begin{aligned}\mathrm{Sym}^{\varpi}_{\mathbb{P}^1_G/G}(\mathbf{1}_{A(B_\Sigma)}[\mathbb{P}^1_G])_* &= \sum_{\substack{\gamma=(n_{\boldsymbol{p},\boldsymbol{q}})\\ \kappa(\gamma)=\varpi}} \mathrm{Sym}^{\gamma}_{\mathbb{P}^1_G/G}(\mathbb{P}^1_G \boxtimes_{\mathbb{P}^1_G} \mu_{B_\Sigma}[\mathbb{P}^1_{\{1_G\}}])\\ &= \sum_{\substack{\gamma=(n_{\boldsymbol{p},\boldsymbol{q}})\\ \kappa(\gamma)=\varpi}} \mathrm{Sym}^{\kappa'(\gamma)}_{\mathbb{P}^1_G/G}(\mathbb{P}^1_G)_* \times_\gamma \mathrm{Sym}^{\kappa''(\gamma)}_{/G}(\mu_{B_\Sigma}[\mathbb{P}^1_{\{1_G\}}])_*.\end{aligned}$$

Each

$$\mathrm{Sym}^{\kappa'(\gamma)}_{\mathbb{P}^1_G/G}(\mathbb{P}^1_G)_* \times_\gamma \mathrm{Sym}^{\kappa''(\gamma)}_{/G}(\mu_{B_\Sigma}[\mathbb{P}^1_{\{1_G\}}])_*$$

can be explicitly decomposed above

$$\mathrm{Sym}^{\kappa'(\gamma)}_{/G}(\mathbb{P}^1_G)_* \times_\gamma \mathrm{Sym}^{\kappa''(\gamma)}_{/G}(\mathbb{P}^1_{\{1_G\}})_*$$

as a linear combination of effective classes. Indeed, using the previous two remarks, we get that for all $\boldsymbol{p}\in\mathbb{N}^{\Sigma(1)}\setminus\{0\}$ the class

$$\mathrm{Sym}^{\kappa''_{\boldsymbol{p}}(\gamma)}_{\mathbb{P}^1_G/G}(\mu_{B_\Sigma}(\boldsymbol{p})[\mathbb{P}^1_{\{1_G\}}])_*$$

(which is zero if $\boldsymbol{p}\notin B_\Sigma$) is

$$\sum_{k_1+\cdots+k_{|\mu_{B_\Sigma}(\boldsymbol{p})|}=\kappa''_{\boldsymbol{p}}(\gamma)} \mathrm{Sym}^{k_1,\dots,k_{|\mu_{B_\Sigma}(\boldsymbol{p})|}}_{\mathbb{P}^1_G/G}(\mathrm{sign}(\mu_{B_\Sigma}(\boldsymbol{p}))[\mathbb{P}^1_{\{1_G\}}])$$

above $\mathrm{Sym}^{\kappa''_{\boldsymbol{p}}(\gamma)}_{/G}(\mathbb{P}^1_G)$. If $\mu_{B_\Sigma}(\boldsymbol{p})$ is negative, we replace

$$\mathrm{Sym}^{\kappa''_{\boldsymbol{p}}(\gamma)}_{\mathbb{P}^1_G/G}(-[\mathbb{P}^1_{\{1_G\}}])$$

by its definition

$$\sum_{\substack{\lambda=(\lambda_\iota)_{\iota\in\mathbb{N}^*}\in\mathcal{Q}\\ \sum_\iota \lambda_\iota=\kappa''_{\boldsymbol{p}}(\gamma)}} (-1)^{|\{\iota\in\mathbb{N}^*\mid\lambda_\iota>0\}|}[\mathrm{Sym}^{\lambda}_{/G}(\mathbb{P}^1_{\{1_G\}})]$$

in the expression above and pull it back to $\mathrm{Sym}^{k_1,\dots,k_{|\mu_{B_\Sigma}(\boldsymbol{p})|}}_{\mathbb{P}^1_G/G}(\mathbb{P}^1_{\{1_G\}})$. Finally, as always, one restricts to the complement of the diagonal. This shows explicitly that

$$\mathrm{Sym}^{\kappa'(\gamma)}_{\mathbb{P}^1_G/G}(\mathbb{P}^1_G)_* \times_\gamma \mathrm{Sym}^{\kappa''(\gamma)}_{/G}(\mu_{B_\Sigma}[\mathbb{P}^1_{\{1_G\}}])_*$$

is a linear combination with integer coefficients of restrictions of

$$\mathrm{Sym}^{\kappa'(\gamma)}_{/G}(\mathbb{P}^1_G)_* \times_\gamma \mathrm{Sym}^{\kappa''(\gamma)}_{\mathbb{P}^1_G/G}(\mathbb{P}^1_{\{1_G\}})_* \xrightarrow{\Phi^\gamma} \mathrm{Sym}^{\kappa(\gamma)}_{/G}(\mathbb{P}^1_G)_*$$

to constructible subsets of the form

$$\mathrm{Sym}^{\kappa'(\gamma)}_{/G}(\mathbb{P}^1_G)_* \times_\gamma \left(\prod_{\boldsymbol{p}}\prod_{\iota\geqslant 1} \mathrm{Sym}^{\lambda_{\boldsymbol{p},\iota,1},\dots,\lambda_{\boldsymbol{p},\iota,|\mu_{B_\Sigma}(\boldsymbol{p})|}}_{/G}(\mathbb{P}^1_{\{1_G\}})\right)_*,$$

with

$$\sum_\iota(\lambda_{\boldsymbol{p},\iota,1}+\cdots+\lambda_{\boldsymbol{p},\iota,|\mu_{B_\Sigma}(\boldsymbol{p})|}) = \kappa''_{\boldsymbol{p}}(\gamma)$$

for all $\boldsymbol{p}\in I = \mathbb{N}^{\Sigma(1)}\setminus\{0\}$ and

$$(\lambda_{\boldsymbol{p},\iota,1}+\cdots+\lambda_{\boldsymbol{p},\iota,|\mu_{B_\Sigma}(\boldsymbol{p})|})_{\iota\in\mathbb{N}^*}\in\mathcal{Q}.$$

When $\mu_{B_\Sigma}(\boldsymbol{p})$ is positive, as a convention, we will always take

$$\lambda_{\boldsymbol{p}} = (\lambda_{\boldsymbol{p},\iota,1}+\cdots+\lambda_{\boldsymbol{p},\iota,|\mu_{B_\Sigma}(\boldsymbol{p})|})_{\iota\in\mathbb{N}^*}\in\mathcal{Q}$$

to be the trivial partition $\lambda_{\boldsymbol{p}} = (\kappa''_{\boldsymbol{p}}(\gamma), 0, \dots)$ and we will only have to perform a sum over all possible partitions (in the usual sense) of $\kappa''_{\boldsymbol{p}}(\gamma)$ of length $\mu_{B_\Sigma}(\boldsymbol{p})$.

For all χ, we apply Lemma 5.14 to the G-equivariant piecewise isomorphism between

$$\mathrm{Hom}^\chi(\mathbb{A}^2\setminus\{0\}, \mathbb{A}^{\Sigma(1)})^*$$

and

$$G\times \mathrm{Sym}^\chi_{/k}(\mathbb{P}^1_k)\simeq \mathrm{Sym}^\chi_{/G}(\mathbb{P}^1_G)$$

from Identification 5.13 on page 937. In particular, in

$$K_0\mathbf{Var}_{\mathrm{Hom}^\chi(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}_k^{\Sigma(1)})^*}\simeq K_0\mathbf{Var}_{\mathrm{Sym}^\chi_{/G}(\mathbb{P}^1_G)}$$

we identify the class of the space of unitary χ-equivariant morphisms with the one of

$$\mathrm{Sym}^\chi_{/G}(\mathbb{P}^1_{\{1_G\}})\simeq \mathrm{Sym}^\chi_{/k}(\mathbb{P}^1_k).$$

Recall that this induces a piecewise identification between $\mathrm{Hom}^\chi(\mathbb{A}^2\setminus\{0\},\mathcal{T}_\Sigma)$ and $\mathrm{Sym}^\chi_{\mathbb{P}^1_G/G}(\mathbf{1}_{A(B_\Sigma)}\mathbb{P}^1_G)$. These piecewise isomorphisms commute with addition of cycles (the Φ^γ of (5.5.12) on page 940) and multiplication of the corresponding polynomials (the $\Phi^\chi_{\chi'}$ of Definition 5.18 on page 939). Putting all this together, we get

$$
\begin{aligned}
&[\mathrm{Hom}^{\chi}(\mathbb{A}^2_k\setminus\{0\},\mathcal{T}_\Sigma)]\\
&\quad=\sum_{\substack{\varpi\text{ partition of }\chi\\ \gamma=(n_{q,p})\\ \kappa(\gamma)=\varpi}} \mathrm{Sym}^{\kappa'(\gamma)}_{\mathbb{P}^1_G/G}(\mathbb{P}^1_G)_*\times_\gamma \mathrm{Sym}^{\kappa''(\gamma)}_{/G}(\mu_{B_\Sigma}[\mathbb{P}^1_{\{1_G\}}])_*\\
&\quad=\sum_{\substack{\varpi\text{ partition of }\chi\\ \gamma=(n_{q,p})\\ \kappa(\gamma)=\varpi}}\ \sum_{\substack{((\lambda_{p,\iota})_{\iota\in\mathbb{N}^*})\in\mathcal{Q}\times\{p\in I\mid\mu_{B_\Sigma}(p)<0\}\\ \sum_\iota\lambda_{p,\iota}=\kappa''_p(\gamma)\\ \lambda_{p,\iota,1}+\cdots+\lambda_{p,\iota,|\mu_{B_\Sigma}(p)|}=\lambda_{p,\iota}}} (-1)^{\sum_{p\in I,\,\mu_{B_\Sigma}(p)<0}|\{\iota\in\mathbb{N}^*\mid\lambda_{p,\iota}>0\}|}\,\mathrm{Sym}^{\kappa'(\gamma)}_{/G}(\mathbb{P}^1_G)_*\\
&\qquad\qquad\times_\gamma\Big(\prod_{p\in I}\prod_{\iota\geqslant1}\mathrm{Sym}^{\lambda_{p,\iota,1},\dots,\lambda_{p,\iota,|\mu_{B_\Sigma}(p)|}}_{/G}(\mathbb{P}^1_{\{1_G\}})\Big)_* \qquad (5.5.13)
\end{aligned}
$$

in $K_0\mathbf{Var}_{\mathrm{Hom}^\chi(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k)^*}\simeq K_0\mathbf{Var}_{\mathrm{Sym}^\chi_{/G}(\mathbb{P}^1_G)}$, with structure morphisms given by the Φ^γ, seen as restrictions of the $\Phi^\chi_{\chi'}$.

Example 5.23. If $V=\mathbb{P}^n_k$, then $B_\Sigma=\{(1,\dots,1)\}=\{\mathbf{1}\}$ and

$$
\begin{aligned}
&\mu_{B_\Sigma}(\mathbf{0})=1,\\
&\mu_{B_\Sigma}(\mathbf{1})=-1,\\
&\mu_{B_\Sigma}(\boldsymbol{n})=0\quad\text{whenever }\boldsymbol{n}\notin\{\mathbf{0},\mathbf{1}\},
\end{aligned}
$$

so in this case (5.5.13) is the sum over all $\gamma=((n_{q,\mathbf{0}}),(n_{q,\mathbf{1}}),n_{\mathbf{0},\mathbf{1}})\in\mathbb{N}^{(I)}\times\mathbb{N}^{(I)}\times\mathbb{N}$ and all possible partitions $\lambda\in\mathcal{Q}$ of the number $\kappa''(\gamma)_{\mathbf{1}}=n_{\mathbf{0},\mathbf{1}}+\sum_{q\in I}n_{\mathbf{q},1}$ of the class

$$(-1)^{|\{\iota\in\mathbb{N}^*\mid\lambda_\iota>0\}|}\,\mathrm{Sym}^{\kappa'(\gamma)}_{/G}(\mathbb{P}^1_G)_*\times_\gamma\mathrm{Sym}^{\lambda}_{/G}(\mathbb{P}^1_{\{1_G\}})_*,$$

the overlap partition being $\kappa(\gamma)=(n_{q,\mathbf{0}})+(n_{q-\mathbf{1},\mathbf{1}})$. The relation one obtains corresponds to the removal of certain spaces of common divisors of the coordinates of the morphisms.

Example 5.24. Let V be the blow-up in one point of $\mathbb{P}^2_k$. Let L_1, L_2 and L_3 be strict transforms of three distinct lines such that the intersection of L_1 and L_3 is the point we blew up and the third one does not contain it. Let $E=L_0$ be the exceptional line. Since $L_2\cap L_0=\varnothing$ and $L_1\cap L_3=\varnothing$ are the only *empty* possible intersections between two of these four divisors, the minimal elements of B_Σ are $(1,0,1,0)$ and $(0,1,0,1)$. Then one checks that

$$
\begin{aligned}
&\mu_{B_\Sigma}(\mathbf{0})=1,\quad \mu_{B_\Sigma}((1,0,1,0))=\mu_{B_\Sigma}((0,1,0,1))=-1,\\
&\mu_{B_\Sigma}(\mathbf{1})=1,\qquad\quad \mu_{B_\Sigma}(\boldsymbol{n})=0\quad\text{otherwise},
\end{aligned}
$$

and hence

$$\sum_{\boldsymbol{n}\in\{0,1\}^4}\mu_{B_\Sigma}(\boldsymbol{n})\boldsymbol{t}^{\boldsymbol{n}}=1-(t_0t_2+t_1t_3)+t_0t_1t_2t_3.$$

Since $|\mu_{B_\Sigma}(\boldsymbol{n})|\leqslant1$ for all $\boldsymbol{n}$, the sets of partitions of the $\lambda_{p,\iota}$ are trivial in (5.5.13). The product over I becomes

$$\bigg(\bigg(\prod_{\iota\geqslant1}\Big(\mathrm{Sym}^{\lambda_{(1,0,1,0),\iota}}_{/G}(\mathbb{P}^1_{\{1_G\}})\times\mathrm{Sym}^{\lambda_{(0,1,0,1),\iota}}_{/G}(\mathbb{P}^1_{\{1_G\}})\Big)\bigg)\times\mathrm{Sym}^{\kappa''_{(1,1,1,1)}(\gamma)}_{/G}(\mathbb{P}^1_{\{1_G\}})\bigg)_*.$$

In general, the combinatorics involved in our computation quickly become complicated, as the following second example shows. In particular, $|\mu_{B_\Sigma}|$ can take values different from 0 or 1.

Example 5.25. Let V be the blow-up of $\mathbb{P}^2_k$ in three general points p_1, p_2 and p_3. This case (for which $n + r = 6$) was already considered in the arithmetic setting in an unpublished work of Peyre from 1993 [50].

Let L_1, L_2 and L_3 be the exceptional lines in V lying above the three general points, respectively p_1, p_2 and p_3, and let L_4, L_5 and L_6 be the strict transforms of the lines (p_2, p_3), (p_1, p_3) and (p_1, p_2).

Then μ_{B_Σ} can be more easily computed by considering the so-called graph $\mathscr{G}$ of *nonintersection* of these six exceptional lines, whose vertices are labelled by the L_i's, $i \in \{1, \dots, 6\} = \Sigma(1)$, and edges are (L_1, L_2), (L_2, L_3), (L_3, L_1), (L_4, L_5), (L_5, L_6), (L_6, L_4) and (L_1, L_4), (L_2, L_5), (L_3, L_6).

Indeed, the set B_Σ can be identified with the set of induced subgraphs of $\mathscr{G}$ by sending $\boldsymbol{n} \in B_\Sigma$ to the subgraph of $\mathscr{G}$ induced by $\{L_i \mid n_i = 1\}$. Actually it is enough to compute the values of μ_{B_Σ} for connected ones, μ_{B_Σ} being multiplicative for pairs of elements having disjoint supports. For the convenience of the reader, we include an exhaustive list of these connected subgraphs (for $|\boldsymbol{n}| \geqslant 2$), together with the corresponding values of μ_{B_Σ}, in Figure 1. In the end, the polynomial $P_{B_\Sigma}(\boldsymbol{t})$ equals

$$\begin{aligned}\sum_{\boldsymbol{n}\in\{0,1\}^6} \mu_{B_\Sigma}(\boldsymbol{n})\boldsymbol{t}^{\boldsymbol{n}} = 1 &- (t_1t_2 + t_2t_3 + t_3t_1 + t_4t_5 + t_5t_6 + t_6t_4 + t_1t_4 + t_2t_5 + t_3t_6) \\ &+ 2(t_1t_2t_3 + t_4t_5t_6) \\ &+ (t_2t_4t_5 + t_1t_4t_2 + t_1t_3t_4 + t_3t_4t_6 + t_2t_3t_5 + t_3t_5t_6) \\ &+ (t_1t_4t_5 + t_1t_2t_5 + t_1t_3t_6 + t_1t_4t_6 + t_2t_3t_6 + t_2t_5t_6) \\ &- (t_1t_2t_4t_5 + t_1t_3t_4t_6 + t_2t_3t_5t_6) \\ &- (t_1t_2t_3t_6 + t_3t_4t_5t_6 + t_1t_2t_3t_4 + t_1t_4t_5t_6 + t_1t_2t_3t_5 + t_2t_4t_5t_6) \\ &+ t_1t_2t_3t_4t_5t_6.\end{aligned}$$

In particular, the monomials $t_1t_2t_3$ and $t_4t_5t_6$ contribute twice (with a positive coefficient); hence we have to sum over partitions of $\kappa''_{(1,1,1,0,0,0)}(\gamma)$ and $\kappa''_{(0,0,0,1,1,1)}(\gamma)$ of length 2.

Taking symmetric products, one gets this sort of exclusion-inclusion relation (5.5.13) between our class of interest, $[\mathrm{Hom}^\chi(\mathbb{A}^2_k \setminus \{0\}, \mathcal{T}_\Sigma)]$, and classes of subspaces of $\mathrm{Hom}^\chi(\mathbb{A}^2_k \setminus \{0\}, \mathbb{A}^6_k)$ consisting of equivariant morphisms which may take values in some intersection of hyperplanes that is not allowed.

5.5.4. *Detwisting.* In what follows μ is any partition of $\chi - \chi'$ *whose support is contained in* B_Σ. We identify $\mathrm{Sym}^\mu_{/k}(\mathbb{P}^1_k)_*$ with the space of unitary $(\chi-\chi')$-equivariant morphisms whose zeros have multiplicities prescribed by μ. We are going to use the subscript notation

$$(\cdots)_{\widetilde{W}}$$

for the preimages of $\mathrm{Hom}^\chi(\mathbb{A}^2_k \setminus \{0\}, \mathbb{A}^{\Sigma(1)}_k \mid \widetilde{W})$ by the $\Phi^\chi_{\chi'}$, as well as the concise notation

$$\mathrm{S}^\mu_{\widehat{|\mathscr{S}|}*} \quad \text{and} \quad \mathrm{H}^\chi$$

respectively for $\mathrm{Sym}^\mu_{/k}(\mathbb{P}^1_k \setminus |\mathscr{S}|)_*$ and Hom^χ, when necessary.

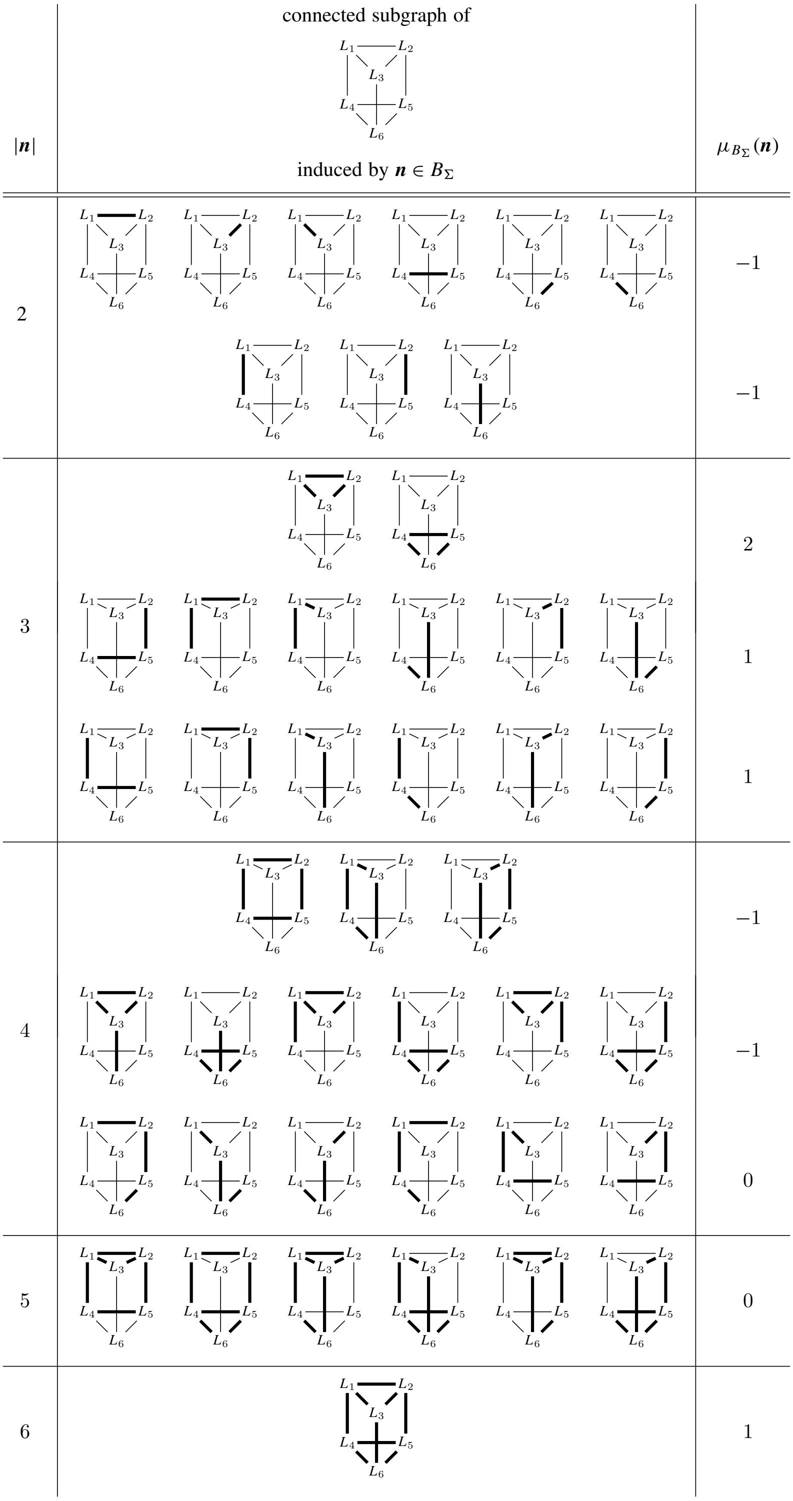

Figure 1. Values of μ_{B_Σ} for the blow-up of $\mathbb{P}^2_k$ in three general points.

Let

$$\begin{aligned}(\mathrm{Hom}^{\chi'}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k)^*\times \mathrm{Sym}^{\mu}_{/k}(\mathbb{P}^1_k)_*)_{\widetilde{W}} &= (\mathrm{Hom}^{\chi'}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k)^*\times \mathrm{Sym}^{\mu}_{/k}(\mathbb{P}^1_k\setminus|\mathscr{S}|)_*)_{\widetilde{W}}\\ &= (\mathrm{H}^{\chi'}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k)^*\times \mathrm{S}^{\mu}_{\widehat{|\mathscr{S}|}*})_{\widetilde{W}}\end{aligned}$$

be the preimage of $\mathrm{Hom}^{\chi}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k\mid\widetilde{W})^*$ by

$$\Phi^{\chi}_{\mu}:\mathrm{Hom}^{\chi'}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k)^*\times \mathrm{Sym}^{\mu}_{/k}(\mathbb{P}^1_k)_*\xrightarrow{\Phi^{\chi}_{\chi'}}\mathrm{Hom}^{\chi}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k)^*,$$

where the first equality comes from the fact that one cannot add common zeros above $\mathscr{S}$ since $\widetilde{W}$ is a constructible subset of $\mathrm{Hom}(\mathscr{S},\mathcal{T}_{\Sigma})$. The projection onto the second factor endows it with the structure of a $\mathrm{Sym}^{\mu}_{/k}(\mathbb{P}^1_k)_*$-variety. We are going to compare its class with the one of

$$\mathrm{Hom}^{\chi'}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k\mid\widetilde{W})^*\times \mathrm{Sym}^{\mu}_{/k}(\mathbb{P}^1_k\setminus|\mathscr{S}|)_*.$$

The relation between all the spaces involved is summarised by the following commutative diagram:

$$\begin{tikzcd}
& (\mathrm{H}^{\chi'}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k)^*\times\mathrm{S}^{\mu}_{\widehat{|\mathscr{S}|}*})_{\widetilde{W}} \arrow[rr, "\Phi^{\chi}_{\mu}"] \arrow[dl, hook] \arrow[dd, "(\mathrm{res}_{\mathscr{S}},\mathrm{pr}_2)"] & & \mathrm{H}^{\chi}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k\mid\widetilde{W})^* \arrow[dl, hook] \arrow[dd, "\mathrm{res}_{\mathscr{S}}"] \\
\mathrm{H}^{\chi'}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k)^*\times\mathrm{S}^{\mu}_{\widehat{|\mathscr{S}|}*} \arrow[rr, "\Phi^{\chi}_{\mu}"] \arrow[dd, "(\mathrm{res}_{\mathscr{S}},\mathrm{pr}_2)"'] & & \mathrm{H}^{\chi}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k)^* \arrow[dd] & \\
& (\mathrm{Hom}(\mathscr{S},\mathbb{A}^{\Sigma(1)}_k)\times\mathrm{S}^{\mu}_{\widehat{|\mathscr{S}|}*})_{\widetilde{W}} \arrow[rr, "(\varphi,D)\mapsto\varphi\bar{D}"] \arrow[dl] & & \widetilde{W} \arrow[dl, hook] \\
\mathrm{Hom}(\mathscr{S},\mathbb{A}^{\Sigma(1)}_k)\times\mathrm{S}^{\mu}_{\widehat{|\mathscr{S}|}*} \arrow[rr, "(\varphi,D)\mapsto\varphi\bar{D}"] & & \mathrm{Hom}(\mathscr{S},\mathbb{A}^{\Sigma(1)}_k) &
\end{tikzcd}$$

For any point $D\in\mathrm{Sym}^{\mu}_{/k}(\mathbb{P}^1_k\setminus|\mathscr{S}|)_*$, the preimage of $\mathrm{Hom}^{\chi}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k\mid\widetilde{W})^*$ by Φ^{χ}_{D} is the subspace

$$\mathrm{Hom}^{\chi'}(\mathbb{A}^2_{\kappa(D)}\setminus\{0\},\mathbb{A}^{\Sigma(1)}_{\kappa(D)}\mid\bar{D}^{-1}\widetilde{W})^*$$

of χ'-equivariant morphisms whose reduction modulo $\mathscr{S}$ lies in $\bar{D}^{-1}\widetilde{W}$. Moreover, when $\chi'\geqslant\ell(\mathscr{S})$, this preimage is isomorphic to

$$\mathrm{Hom}^{\chi'}(\mathbb{A}^2_{\kappa(D)}\setminus\{0\},\mathbb{A}^{\Sigma(1)}_{\kappa(D)}\mid\widetilde{W})^*,$$

the isomorphism being explicitly given in Lemma 5.11: it sends an element of Euclidean decomposition modulo ϖ

$$(q_{\alpha},\bar{D}^{-1}_{\alpha}w_{\alpha})_{\alpha\in\Sigma(1)},$$

with $(w_{\alpha})\in\widetilde{W}$, to

$$(q_{\alpha},w_{\alpha})_{\alpha\in\Sigma(1)}.$$

Now we can prove the following version of the motivic Möbius inversion.

Proposition 5.26. *For all $\chi \in \mathbb{N}^{\Sigma(1)}$, we have*

$$\big[\mathrm{Hom}^{\chi}(\mathbb{A}^2_k \setminus \{0\}, \mathcal{T}_\Sigma \mid \widetilde{W})^*\big] = \sum_{\chi',\,\mu} \big[\mathrm{Hom}^{\chi'}(\mathbb{A}^2_k \setminus \{0\}, \mathbb{A}_k^{\Sigma(1)} \mid \widetilde{W})^*\big]\,\mathrm{Sym}^{\mu}_{\mathbb{P}^1_k}(\mu_{B_\Sigma}\cdot[\mathbb{P}^1_k \setminus |\mathscr{S}|])_* + E^{\chi}$$

in $K_0\mathbf{Var}_k$, with the error term E^χ of bounded dimension

$$\dim_k(E^\chi) \leqslant -\min_{\alpha\in\Sigma(1)}(\chi_\alpha) + |\chi| + (1-|\Sigma(1)|)(\ell(\mathscr{S})-1) + \dim(\widetilde{W}).$$

Proof. First, note that the class $\mathrm{Sym}^{\mu}_{\mathbb{P}^1_k}(\mu_{B_\Sigma}\cdot[\mathbb{P}^1_k \setminus |\mathscr{S}|])_*$ is zero if the support of μ is not contained in B_Σ. Then, using the decomposition (5.5.13) on page 944 of the motivic Möbius inversion we made explicit in the previous pages (starting from on page 940 concerning the notation), and pulling it back to $\mathrm{Hom}^{\chi}(\mathbb{A}^2_k \setminus \{0\}, \mathbb{A}_k^{\Sigma(1)} \mid \widetilde{W})^*$, we get that $[\mathrm{Hom}^{\chi}(\mathbb{A}^2_k \setminus \{0\}, \mathcal{T}_\Sigma \mid \widetilde{W})^*]$ is a linear combination with integer coefficients of restrictions of the Φ^γ. More explicitly,

$$\begin{aligned}
&[\mathrm{Hom}^{\chi}(\mathbb{A}^2_k \setminus \{0\}, \mathcal{T}_\Sigma \mid \widetilde{W})^*] \\
&= \sum_{\substack{\varpi \text{ partition of } \chi \\ \gamma=(n_{\boldsymbol{q},\boldsymbol{p}}) \\ \kappa(\gamma)=\varpi}} \big(\mathrm{Sym}^{\kappa'(\gamma)}_{/G}(\mathbb{P}^1_G)_* \times_\gamma \mathrm{Sym}^{\kappa''(\gamma)}_{\mathbb{P}^1_G/G}(\mu_{B_\Sigma}[\mathbb{P}^1_{\{1_G\}}])_*\big)_{\widetilde{W}} \\
&= \sum_{\substack{\varpi \text{ partition of } \chi \\ \gamma=(n_{\boldsymbol{q},\boldsymbol{p}}) \\ \kappa(\gamma)=\varpi}} \sum_{\substack{((\lambda_{\boldsymbol{p},\iota})_{\iota\in\mathbb{N}^*})\in\mathcal{Q}\times\{\boldsymbol{p}\in I \mid \mu_{B_\Sigma}(\boldsymbol{p})<0\} \\ \sum_\iota \lambda_{\boldsymbol{p},\iota}=\kappa''_{\boldsymbol{p}}(\gamma) \\ \lambda_{\boldsymbol{p},\iota,1}+\cdots+\lambda_{\boldsymbol{p},\iota,|\mu_{B_\Sigma}(\boldsymbol{p})|}=\lambda_{\boldsymbol{p},\iota}}} (-1)^{\sum_{\boldsymbol{p}\in I,\ \mu_{B_\Sigma}(\boldsymbol{p})<0} |\{\iota\in\mathbb{N}\mid\lambda_{\boldsymbol{p},\iota}>0\}|} \\
&\qquad \times \underbrace{\Bigg(\mathrm{Sym}^{\kappa'(\gamma)}_{/G}(\mathbb{P}^1_G)_* \times_\gamma \Bigg(\prod_{\boldsymbol{p}\in I}\prod_{\iota\geqslant 1} \mathrm{Sym}^{\lambda_{\boldsymbol{p},\iota,1},\dots,\lambda_{\boldsymbol{p},\iota,|\mu_{B_\Sigma}(\boldsymbol{p})|}}_{/G}(\mathbb{P}^1_{\{1_G\}})\Bigg)_*\Bigg)_{\widetilde{W}}}_{=\left(\mathrm{Sym}^{\kappa'(\gamma)}_{/G}(\mathbb{P}^1_G)_*\times_\gamma\left(\prod_{\boldsymbol{p}\in I}\prod_{\iota\geqslant 1}\mathrm{Sym}^{\lambda_{\boldsymbol{p},\iota,1},\dots,\lambda_{\boldsymbol{p},\iota,|\mu_{B_\Sigma}(\boldsymbol{p})|}}_{/G}(\mathbb{P}^1_{\{1_G\}}\setminus|\mathscr{S}|)\right)_*\right)_{\widetilde{W}}}.
\end{aligned} \tag{5.5.14}$$

For every γ appearing in the first sum, we apply Identification 5.13 to the factors of the locally closed subsets

$$\Bigg(\mathrm{Sym}^{\kappa'(\gamma)}_{/G}(\mathbb{P}^1_G)_* \times_\gamma \Bigg(\prod_{\boldsymbol{p}\in I}\prod_{\iota\geqslant 1} \mathrm{Sym}^{\lambda_{\boldsymbol{p},\iota,1},\dots,\lambda_{\boldsymbol{p},\iota,|\mu_{B_\Sigma}(\boldsymbol{p})|}}_{/G}(\mathbb{P}^1_{\{1_G\}} \setminus |\mathscr{S}|)\Bigg)_*\Bigg)_{\widetilde{W}}$$

of

$$(\mathrm{Sym}^{\kappa'(\gamma)}_{/G}(\mathbb{P}^1_G)_* \times \mathrm{Sym}^{\kappa''(\gamma)}_{\mathbb{P}^1_G/G}(\mathbb{P}^1_{\{1_G\}})_*)_{\widetilde{W}}.$$

In particular, it is sufficient to approximate the class of

$$\big(\mathrm{Hom}^{\chi'}(\mathbb{A}^2_k \setminus \{0\}, \mathbb{A}_k^{\Sigma(1)})^* \times \mathrm{Sym}^{\kappa''(\gamma)}_{/k}(\mathbb{P}^1_k \setminus |\mathscr{S}|)_*\big)_{\widetilde{W}} \xrightarrow{\Phi^{\chi}_{\kappa''(\gamma)}} \mathrm{Hom}^{\chi}(\mathbb{A}^2_k \setminus \{0\}, \mathbb{A}_k^{\Sigma(1)} \mid \widetilde{W})^* \tag{5.5.15}$$

whenever $\kappa'(\gamma)$ is a partition of χ', since all the other classes involved are obtained from this one by pull-back and restriction. Moreover, since we are going to perform a motivic sum over $\mathrm{Hom}^{\chi}(\mathbb{A}^2 \setminus \{0\}, \mathbb{A}^{\Sigma(1)} \mid \widetilde{W})^*$, we can view (5.5.15) as a variety above $\mathrm{Sym}^{\kappa''(\gamma)}_{/k}(\mathbb{P}^1_k \setminus |\mathscr{S}|)_*$ and then take the motivic sum, using the commutativity of the following diagram:

$$\begin{tikzcd}
\left(\mathrm{Hom}^{\chi'}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k)^*\times \mathrm{Sym}^{\kappa''(\gamma)}_{/k}(\mathbb{P}^1_k\setminus|\mathscr{S}|)_*\right)_{\widetilde{W}} \arrow[r, "\mathrm{pr}_1"] \arrow[d, "\Phi^{\chi}_{\kappa''(\gamma)}"] & \mathrm{Sym}^{\kappa''(\gamma)}_{/k}(\mathbb{P}^1_k\setminus|\mathscr{S}|)_* \arrow[d] \\
\mathrm{Hom}^{\chi}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k\mid\widetilde{W})^* \arrow[r] & \mathrm{Spec}(k)
\end{tikzcd}$$

By [5, Lemma 2.5.5] it is enough to argue fibre by fibre, so that the previous diagram becomes

$$\begin{tikzcd}
\mathrm{Hom}^{\chi'}(\mathbb{A}^2_{\kappa(D)}\setminus\{0\},\mathbb{A}^{\Sigma(1)}_{\kappa(D)}\mid\overline{D}^{-1}\widetilde{W})^* \arrow[r] \arrow[d, "\Phi^{\chi}_{D}"] & \mathrm{Spec}(\kappa(D)) \arrow[d] \\
\mathrm{Hom}^{\chi}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k)^*\otimes_k\kappa(D) \arrow[r] & \mathrm{Spec}(k)
\end{tikzcd}$$

and our argument will be entirely compatible with restrictions to constructible subsets of $\mathrm{Sym}^{\kappa''(\gamma)}_{/k}(\mathbb{P}^1_k\setminus|\mathscr{S}|)_*$ such as $\prod_{\boldsymbol{p}\in I}\prod_{\iota\geqslant 1}\mathrm{Sym}^{\lambda_{\boldsymbol{p},\iota,1},\dots,\lambda_{\boldsymbol{p},\iota,|\mu_{B_\Sigma}(\boldsymbol{p})|}}_{/G}(\mathbb{P}^1_{\{1_G\}}\setminus|\mathscr{S}|)$.

We can apply the second part of Lemma 5.11 on page 936 only when $\chi'\geqslant\ell(\mathscr{S})-1$, which in that case gives

$$\mathrm{Hom}^{\chi'}(\mathbb{A}^2_{\kappa(D)}\setminus\{0\},\mathbb{A}^{\Sigma(1)}_{\kappa(D)}\mid\overline{D}^{-1}\widetilde{W})^*\xrightarrow[\tau_{\overline{D}}]{\sim}\mathrm{Hom}^{\chi'}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k\mid\widetilde{W})^*\otimes\kappa(D)$$

as $\kappa(D)$-schemes. In general, we consider the error term

$$\begin{aligned}E^{\chi'}_{\mu}=&\left[\left(\mathrm{Hom}^{\chi'}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k)^*\times\mathrm{Sym}^{\kappa''(\gamma)}_{/k}(\mathbb{P}^1_k\setminus|\mathscr{S}|)_*\right)_{\widetilde{W}}\right]\\
&-\left[\mathrm{Hom}^{\chi'}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}^{\Sigma(1)}_k\mid\widetilde{W})^*\times\mathrm{Sym}^{\kappa''(\gamma)}_{/k}(\mathbb{P}^1_k\setminus|\mathscr{S}|)_*\right]\in K_0\mathbf{Var}_{\mathrm{Sym}^{\kappa''(\gamma)}_{\mathbb{P}^1_k}(\mathbb{P}^1_k\setminus|\mathscr{S}|)_*},\end{aligned}$$

as well as its restrictions

$$\begin{aligned}E^{\gamma}_{\lambda}=&\left[\left(\mathrm{Sym}^{\kappa'(\gamma)}_{/G}(\mathbb{P}^1_G)_*\times_\gamma\left(\prod_{\boldsymbol{p}\in I}\prod_{\iota\geqslant 1}\mathrm{Sym}^{\lambda_{\boldsymbol{p},\iota,1},\dots,\lambda_{\boldsymbol{p},\iota,|\mu_{B_\Sigma}(\boldsymbol{p})|}}_{/G}(\mathbb{P}^1_{\{1_G\}}\setminus|\mathscr{S}|)\right)_*\right)_{\widetilde{W}}\right]\\
&-\left[(\mathrm{Sym}^{\kappa'(\gamma)}_{/G}(\mathbb{P}^1_G)_*)_{\widetilde{W}}\times_\gamma\left(\prod_{\boldsymbol{p}\in I}\prod_{\iota\geqslant 1}\mathrm{Sym}^{\lambda_{\boldsymbol{p},\iota,1},\dots,\lambda_{\boldsymbol{p},\iota,|\mu_{B_\Sigma}(\boldsymbol{p})|}}_{/G}(\mathbb{P}^1_{\{1_G\}}\setminus|\mathscr{S}|)\right)_*\right]\end{aligned}$$

for every $(\lambda_{\boldsymbol{p}})=((\lambda_{\boldsymbol{p},\iota})_{\iota\in\mathbb{N}^*})\in\mathscr{Q}\times I$ such that $\sum_\iota\lambda_{\boldsymbol{p},\iota}=\kappa''_{\boldsymbol{p}}(\gamma)$ and $\lambda_{\boldsymbol{p},\iota,1}+\dots+\lambda_{\boldsymbol{p},\iota,|\mu_{B_\Sigma}(\boldsymbol{p})|}=\lambda_{\boldsymbol{p},\iota}$ (still with the convention that we only consider the trivial partition of $\kappa''_{\boldsymbol{p}}(\gamma)$ if $\mu_{B_\Sigma}(\boldsymbol{p})>0$). The previous argument shows that $E^{\chi'}_{\mu}=0$ if $\chi'\geqslant\ell(\mathscr{S})-1$. By (5.5.11) of Lemma 5.11, the relative dimension of $E^{\chi'}_{\mu}$ (hence also of E^{γ}_{λ}) is bounded by

$$\dim(\widetilde{W})+\sum_{\alpha\in\Sigma(1)}\max(0,\chi'_\alpha-\ell(\mathscr{S})+1)$$

and if $\chi'\not\geqslant\ell(\mathscr{S})-1$, then there is at least one term of this sum which is equal to zero. Hence under this assumption it is bounded by

$$-\min_{\alpha\in\Sigma(1)}(\chi'_\alpha)+\ell(\mathscr{S})-1+|\chi'|+|\Sigma(1)|(1-\ell(\mathscr{S}))+\dim(\widetilde{W}).\tag{5.5.16}$$

Now we bound the total dimension of $E_\mu^{\chi'}$, that is to say,

$$\dim_k(E_\mu^{\chi'}) = \dim_{\mathrm{Sym}^\mu_{\mathbb{P}^1_k}(\mathbb{P}^1_k\setminus|\mathscr{S}|)_*}(E_\mu^{\chi'}) + \dim_k(\mathrm{Sym}^\mu_{\mathbb{P}^1_k}(\mathbb{P}^1_k\setminus|\mathscr{S}|)_*).$$

Since in practice we work with the family $\mu_{B_\Sigma}[\mathbb{P}^1_k]$, remembering that $\mu_{B_\Sigma}(\boldsymbol{n}) = 0$ if $\boldsymbol{n} \notin B_\Sigma$, we can assume that μ is a partition of the form

$$\mu = (\delta_J)_{J\in B_\Sigma} \in \mathbb{N}^{B_\Sigma}.$$

Let $\varphi(\underline{\delta}) \in \mathbb{N}^{\Sigma(1)} \subset \mathcal{X}_*(\boldsymbol{G}_m^{\Sigma(1)})$ be the cocharacter whose α-coordinate is

$$\varphi(\underline{\delta})_\alpha = \sum_{J\ni\alpha} \delta_J.$$

Then, by (5.5.16) $E_\mu^{\chi'}$ has dimension over k bounded by

$$\begin{aligned}
-\min_{\alpha\in\Sigma(1)}(\chi'_\alpha) + \ell(\mathscr{S}) - 1 + |\chi'| + |\Sigma(1)|(1-\ell(\mathscr{S})) + \dim(\widetilde{W}) + |\underline{\delta}| \\
&= -\min_{\alpha\in\Sigma(1)}(\chi_\alpha - \varphi(\underline{\delta})_\alpha) + |\chi| - |\varphi(\underline{\delta})| + |\underline{\delta}| + (|\Sigma(1)|-1)(1-\ell(\mathscr{S})) + \dim(\widetilde{W}) \\
&\leqslant -\min_{\alpha\in\Sigma(1)}(\chi_\alpha) + |\chi| + (|\Sigma(1)|-1)(1-\ell(\mathscr{S})) + \dim(\widetilde{W}),
\end{aligned}$$

where the first equality is given by

$$\chi = \chi' + \varphi(\underline{\delta})$$

and the last inequality comes from the expression

$$|\varphi(\underline{\delta})| = \sum_{J\in B_\Sigma} |J|\delta_J$$

together with the fact that $|J| \geqslant 2$ for all $J \in B_\Sigma$; hence

$$-\min_{\alpha\in\Sigma(1)}(\chi_\alpha - \varphi(\underline{\delta})_\alpha) - |\varphi(\underline{\delta})| \leqslant -\min_{\alpha\in\Sigma(1)}(\chi_\alpha) + \max_{\alpha\in\Sigma(1)}(\varphi(\underline{\delta})_\alpha) - |\varphi(\underline{\delta})| \leqslant -\min_{\alpha\in\Sigma(1)}(\chi_\alpha)$$

and the proposition is finally proved for $E^\chi = \sum_{\gamma,\lambda} E_\lambda^\gamma$ by replacing every

$$\left(\mathrm{Sym}_{/G}^{\kappa'(\gamma)}(\mathbb{P}^1_G)_* \times_\gamma \left(\prod_{p\in I}\prod_{\iota\geqslant 1}\mathrm{Sym}_{/G}^{\lambda_{p,\iota,1},\dots,\lambda_{p,\iota,|\mu_{B_\Sigma}(p)|}}(\mathbb{P}^1_{\{1_G\}}\setminus|\mathscr{S}|)\right)_*\right)_{\widetilde{W}}$$

with

$$(\mathrm{Sym}_{/G}^{\kappa'(\gamma)}(\mathbb{P}^1_G)_*)_{\widetilde{W}} \times_\gamma \left(\prod_{p\in I}\prod_{\iota\geqslant 1}\mathrm{Sym}_{/G}^{\lambda_{p,\iota,1},\dots,\lambda_{p,\iota,|\mu_{B_\Sigma}(p)|}}(\mathbb{P}^1_{\{1_G\}}\setminus|\mathscr{S}|)\right)_*$$

in (5.5.14) on page 948. □

Final computation. Let

$$E_W(\boldsymbol{t}) = \sum_{\chi\in\mathbb{N}^{\Sigma(1)}} E^\chi \boldsymbol{t}^\chi.$$

The previous proposition can be rewritten as

$$\sum_{\boldsymbol{d}\in\mathbb{N}^{\Sigma(1)}}[\mathrm{Hom}^{\boldsymbol{d}}(\mathbb{A}^2_k\backslash\{0\},\mathcal{T}_\Sigma\mid\widetilde{W})^*]\boldsymbol{t}^{\boldsymbol{d}}=\Bigg(\prod_{p\notin\mathscr{S}}P_{B_\Sigma}(\boldsymbol{t})\Bigg)\times\Bigg(\sum_{\boldsymbol{d}\in\mathbb{N}^{\Sigma(1)}}[\mathrm{Hom}^{\boldsymbol{d}}(\mathbb{A}^2_k\backslash\{0\},\mathbb{A}_k^{\Sigma(1)}\mid\widetilde{W})^*]\,\boldsymbol{t}^{\boldsymbol{d}}\Bigg)+E_W(\boldsymbol{t})$$

in $K_0\mathbf{Var}_k[\![\boldsymbol{t}]\!]$. We define $\mu_\Sigma^{|\mathscr{S}|}(\boldsymbol{e})$, $\boldsymbol{e}\in\mathbb{N}^{\Sigma(1)}$, to be the coefficients of the motivic Euler product

$$\prod_{p\notin|\mathscr{S}|}P_{B_\Sigma}(\boldsymbol{t}).$$

By the definition of $\widetilde{W}$, together with Proposition 5.3 and the equivalent description of the functor $S\rightsquigarrow\mathrm{Hom}^\chi_S(\mathbb{A}^2_S\setminus\{0\},\mathcal{T}_{\Sigma,S})^*$ we gave, we have the relation

$$(\mathbb{L}_k-1)^r[\mathrm{Hom}^{\boldsymbol{d}}_k(\mathbb{P}^1_k,V_\Sigma\mid W)_U]=[\mathrm{Hom}^{\boldsymbol{d}}_k(\mathbb{A}^2\setminus\{0\},\mathcal{T}_\Sigma\mid\widetilde{W})^*]$$

as soon as $\boldsymbol{d}\in\mathrm{Eff}(V)^\vee_{\mathbb{Z}}$, and by Lemma 5.11

$$[\mathrm{Hom}^{\boldsymbol{d}}_k(\mathbb{A}^2\setminus\{0\},\mathbb{A}^{\Sigma(1)}\mid\widetilde{W})^*]=[\widetilde{W}](\mathbb{L}-1)^{|\Sigma(1)|}\prod_{\alpha\in\Sigma(1)}[\mathbb{P}_k^{d_\alpha-\ell(\mathscr{S})}]$$

whenever $\boldsymbol{d}\geqslant\ell(\mathscr{S})$. Thus we decompose the following series into two parts:

$$\sum_{\boldsymbol{d}\in\mathbb{N}^{\Sigma(1)}}[\mathrm{Hom}^{\boldsymbol{d}}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}_k^{\Sigma(1)}\mid\widetilde{W})]\,\boldsymbol{t}^{\boldsymbol{d}}=[\widetilde{W}](\mathbb{L}-1)^{|\Sigma(1)|}\prod_{\alpha\in\Sigma(1)}t_\alpha^{\ell(\mathscr{S})}Z^{\mathrm{Kapr}}_{\mathbb{P}^1_k}(t_\alpha)+H_W(\boldsymbol{t}),$$

where

$$H_W(\boldsymbol{t})=\sum_{\substack{\boldsymbol{d}\in\mathbb{N}^{\Sigma(1)}\\ \boldsymbol{d}\ngeqslant\ell(\mathscr{S})}}[\mathrm{Hom}^{\boldsymbol{d}}(\mathbb{A}^2_k\setminus\{0\},\mathbb{A}_k^{\Sigma(1)}\mid\widetilde{W})^*]\,\boldsymbol{t}^{\boldsymbol{d}}.$$

Then, we use again the decomposition (5.4.9) given on page 931

$$\prod_{\alpha\in\Sigma(1)}Z^{\mathrm{Kapr}}_{\mathbb{P}^1_k}(t_\alpha)=\sum_{A\subset\Sigma(1)}\frac{(-\mathbb{L})^{|\Sigma(1)|-|A|}}{(1-\mathbb{L})^{|\Sigma(1)|}}Z_A(\boldsymbol{t})$$

of this product of Kapranov zeta functions, where for any $A\subset\Sigma(1)$

$$Z_A(\boldsymbol{t})=\prod_{\alpha\in A}(1-t_\alpha)^{-1}\prod_{\alpha\notin A}(1-\mathbb{L}\,t_\alpha)^{-1}.$$

By identification, the coefficient of order $\boldsymbol{d}$ of

$$\boldsymbol{t}^{\ell(\mathscr{S})}Z_A(\boldsymbol{t})\times\prod_{p\notin|\mathscr{S}|}P_{B_\Sigma}(\boldsymbol{t})$$

is the sum

$$\mathfrak{s}^A_{\boldsymbol{d}}=\sum_{\boldsymbol{e}\leqslant\boldsymbol{d}}\mu_\Sigma^{|\mathscr{S}|}(\boldsymbol{e})\mathbb{L}^{\sum_{\alpha\notin A}d_\alpha-\ell(\mathscr{S})-e_\alpha}$$

whenever $\boldsymbol{d}\geqslant\ell(\mathscr{S})$, and zero otherwise.

If $A=\varnothing$, then after dividing by $\mathbb{L}^{-|\boldsymbol{d}|}$ it becomes

$$\mathfrak{s}^A_{\boldsymbol{d}}\mathbb{L}^{-|\boldsymbol{d}|}=\mathbb{L}^{-|\Sigma(1)|\ell(\mathscr{S})}\sum_{\boldsymbol{e}\leqslant\boldsymbol{d}}\mu_\Sigma^{|\mathscr{S}|}(\boldsymbol{e})\mathbb{L}^{-|\boldsymbol{e}|}$$

which is, up to the factor $\mathbb{L}^{-|\Sigma(1)|\ell(\mathscr{S})}$, the $\boldsymbol{d}$-th partial sum of $\prod_{p\notin|\mathscr{S}|} P_{B_\Sigma}(\mathbb{L}^{-1})$. The corresponding error term

$$\mathbb{L}^{-|\Sigma(1)|\ell(\mathscr{S})} \sum_{\boldsymbol{e}\not\leqslant\boldsymbol{d}} \mu_\Sigma^{|\mathscr{S}|}(\boldsymbol{e})\mathbb{L}^{-|\boldsymbol{e}|}$$

has virtual dimension at most

$$-|\Sigma(1)|\ell(\mathscr{S}) - \tfrac{1}{2} \min_{\alpha\in\Sigma(1)} (d_\alpha + 1).$$

If $A \neq \varnothing$, then one gets instead

$$\mathbb{L}^{-(|\Sigma(1)|-|A|)\ell(\mathscr{S})} \sum_{\boldsymbol{e}\leqslant\boldsymbol{d}} \mu_\Sigma^{|\mathscr{S}|}(\boldsymbol{e})\mathbb{L}^{-|\boldsymbol{e}|}\mathbb{L}^{|\boldsymbol{d}_A-\boldsymbol{e}_A|}.$$

In that case, recalling that $\dim(\mu_\Sigma(\boldsymbol{e})\mathbb{L}_k^{-|\boldsymbol{e}|}) \leqslant -\frac{1}{2}|\boldsymbol{e}|$ for all $\boldsymbol{e} \in \mathbb{N}^{\Sigma(1)}$, Lemma 2.21 on page 913 gives

$$\dim\Biggl(\sum_{\boldsymbol{e}\leqslant\boldsymbol{d}} \mu_\Sigma^{|\mathscr{S}|}(\boldsymbol{e})\mathbb{L}^{-|\boldsymbol{e}|}\mathbb{L}^{|\boldsymbol{d}_A-\boldsymbol{e}_A|}\Biggr) \leqslant -\tfrac{1}{4}\min_{\alpha\in A}(d_\alpha).$$

Now we consider the terms coming from H_W. The coefficient of order $\boldsymbol{d}$ of

$$H_W(\boldsymbol{t}) \times \prod_{p\notin|\mathscr{S}|} P_{B_\Sigma}(\boldsymbol{t})$$

is

$$\mathfrak{h}_{\boldsymbol{d}} = \sum_{\substack{\boldsymbol{e}\leqslant\boldsymbol{d}\\ \boldsymbol{d}\ngeqslant\ell(\mathscr{S})+\boldsymbol{e}}} \mu_\Sigma^{|\mathscr{S}|}(\boldsymbol{e})\bigl[\mathrm{Hom}^{\boldsymbol{d}-\boldsymbol{e}}(\mathbb{A}_k^2\setminus\{0\}, \mathbb{A}_k^{\Sigma(1)} \mid \widetilde{W})^*\bigr].$$

Dividing by $\mathbb{L}^{|\boldsymbol{d}|}$, we get

$$\mathfrak{h}_{\boldsymbol{d}}\mathbb{L}^{-|\boldsymbol{d}|} = \sum_{\substack{\boldsymbol{e}\leqslant\boldsymbol{d}\\ \boldsymbol{d}\ngeqslant\ell(\mathscr{S})+\boldsymbol{e}}} \mu_\Sigma^{|\mathscr{S}|}(\boldsymbol{e})\mathbb{L}^{-|\boldsymbol{e}|}\bigl[\mathrm{Hom}^{\boldsymbol{d}-\boldsymbol{e}}(\mathbb{A}_k^2\setminus\{0\}, \mathbb{A}_k^{\Sigma(1)} \mid \widetilde{W})^*\bigr]\mathbb{L}^{-|\boldsymbol{d}-\boldsymbol{e}|}.$$

As for the coefficients of $E_W(\boldsymbol{t})$, we have the dimensional upper bound coming from (5.5.11) of Lemma 5.11

$$\dim\bigl(\mathrm{Hom}^{\boldsymbol{d}'}(\mathbb{A}_k^2\setminus\{0\}, \mathbb{A}_k^{\Sigma(1)} \mid \widetilde{W})^*\bigr) \leqslant \dim(\widetilde{W}) + \sum_{\alpha\in\Sigma(1)} \min(0, d'_\alpha - \ell(\mathscr{S}) + 1).$$

Given $\boldsymbol{d}' \in \mathbb{N}^{\Sigma(1)}$ such that $\boldsymbol{d}' \ngeqslant \ell(\mathscr{S})$, there exists at least one element $\alpha \in \Sigma(1)$ such that $d_\alpha < \ell(\mathscr{S})$, that is to say, such that $\min(0, d'_\alpha - \ell(\mathscr{S}) + 1) = 0$. Hence the sum

$$\sum_{\alpha\in\Sigma(1)} \min(0, d'_\alpha - \ell(\mathscr{S}) + 1)$$

is bounded by

$$|\boldsymbol{d}'| + |\Sigma(1)|(1 - \ell(\mathscr{S})) - \min_{\substack{\alpha\in\Sigma(1)\\ d'_\alpha<|\mathscr{S}|}} (d'_\alpha) + \ell(\mathscr{S}) - 1$$

and the bound on $\dim\bigl(\mathrm{Hom}^{\boldsymbol{d}'}(\mathbb{A}_k^2\setminus\{0\}, \mathbb{A}_k^{\Sigma(1)} \mid \widetilde{W})^*\bigr)$ becomes

$$\dim\bigl(\mathrm{Hom}^{\boldsymbol{d}'}(\mathbb{A}_k^2\setminus\{0\}, \mathbb{A}_k^{\Sigma(1)} \mid \widetilde{W})^*\bigr) \leqslant \dim(\widetilde{W}) + |\boldsymbol{d}'| + |\Sigma(1)|(1-\ell(\mathscr{S})) - \min_{\substack{\alpha\in\Sigma(1)\\ d'_\alpha<|\mathscr{S}|}} (d'_\alpha) + \ell(\mathscr{S}) - 1 \quad (5.5.17)$$

for all $\boldsymbol{d}' \in \mathbb{N}^{\Sigma(1)}$ such that $\boldsymbol{d}' \not\geqslant \ell(\mathscr{S})$. Thus the dimension of

$$\left[\mathrm{Hom}^{\boldsymbol{d}-\boldsymbol{e}}(\mathbb{A}^2_k \setminus \{0\}, \mathbb{A}_k^{\Sigma(1)} \mid \widetilde{W})\right] \mathbb{L}^{-|\boldsymbol{d}-\boldsymbol{e}|}$$

in the expression of $\mathfrak{h}_{\boldsymbol{d}}$ above is bounded. We can be more precise and argue as we did in the proof of Lemma 2.21. If $2\boldsymbol{e} \leqslant \boldsymbol{d}$ then $2(\boldsymbol{d}-\boldsymbol{e}) \geqslant \boldsymbol{d}$ and

$$\dim\left(\mu_{\Sigma}^{|\mathscr{S}|}(\boldsymbol{e})\mathbb{L}^{-|\boldsymbol{e}|}\left[\mathrm{Hom}^{\boldsymbol{d}-\boldsymbol{e}}(\mathbb{A}^2_k \setminus \{0\}, \mathbb{A}_k^{\Sigma(1)} \mid \widetilde{W})^*\right] \mathbb{L}^{-|\boldsymbol{d}-\boldsymbol{e}|}\right)$$

is at most

$$-\tfrac{1}{2} \min_{\alpha\in\Sigma(1)} (d_\alpha) + \dim(\widetilde{W}) + (1-\ell(\mathscr{S}))(|\Sigma(1)|-1),$$

while if $2\boldsymbol{e} \not\leqslant \boldsymbol{d}$, we use the coarse upper bound deduced from (5.5.17)

$$\dim\left(\left[\mathrm{Hom}^{\boldsymbol{d}-\boldsymbol{e}}(\mathbb{A}^2_k \setminus \{0\}, \mathbb{A}_k^{\Sigma(1)} \mid \widetilde{W})^*\right] \mathbb{L}^{-|\boldsymbol{d}-\boldsymbol{e}|}\right) \leqslant \dim(\widetilde{W}) + (1-\ell(\mathscr{S}))(|\Sigma(1)|-1)$$

together with

$$\dim(\mu_{\Sigma}^{|\mathscr{S}|}(\boldsymbol{e})\mathbb{L}^{-|\boldsymbol{e}|}) \leqslant -\tfrac{1}{2}|\boldsymbol{e}| < -\tfrac{1}{4} \min_{\alpha\in\Sigma(1)} (d_\alpha).$$

Therefore, for any $\boldsymbol{d}$ we have

$$\dim(\mathfrak{h}_{\boldsymbol{d}}\mathbb{L}^{-|\boldsymbol{d}|}) \leqslant -\tfrac{1}{4} \min_{\alpha\in\Sigma(1)} (d_\alpha) + \dim(\widetilde{W}) + (1-\ell(\mathscr{S}))(|\Sigma(1)|-1).$$

Remember from Proposition 5.26 that the $\boldsymbol{d}$-th term of $E_W(\boldsymbol{t})$ has dimension bounded by

$$-\min_{\alpha\in\Sigma(1)} (d_\alpha) + |\chi| + (\Sigma(1)-1)(1-\ell(\mathscr{S})) + \dim(\widetilde{W}).$$

Now we rewrite the motivic density of $\widetilde{W}$ as

$$[\widetilde{W}]\mathbb{L}^{-|\Sigma(1)|\ell(\mathscr{S})} = [W]\,\mathbb{L}^{-\ell(\mathscr{S})\dim(V_\Sigma)} \times [T_{\mathrm{NS},\mathscr{S}}]\,\mathbb{L}^{-r\ell(\mathscr{S})} = \frac{[W]}{\mathbb{L}^{\ell(\mathscr{S})\dim(V_\Sigma)}} \prod_{p\in|\mathscr{S}|} (1-\mathbb{L}_p^{-1})^r.$$

Putting everything together, we get

$$\begin{aligned}
&[\mathrm{Hom}_k^{\boldsymbol{d}}(\mathbb{P}^1_k, V_\Sigma \mid W)_U]\,\mathbb{L}^{-|\boldsymbol{d}|}\\
&\quad = (\mathbb{L}-1)^{-r}\left(\mathbb{L}^{|\Sigma(1)|}[\widetilde{W}] \sum_{A\subset\Sigma(1)} (-\mathbb{L})^{-|A|}\mathfrak{s}_{\boldsymbol{d}}^{A}\mathbb{L}^{-|\boldsymbol{d}|} + \mathfrak{h}_{\boldsymbol{d}}\mathbb{L}^{-|\boldsymbol{d}|} + \mathfrak{e}_{\boldsymbol{d}}\mathbb{L}^{-|\boldsymbol{d}|}\right)\\
&\quad = \frac{\mathbb{L}^{\dim(V_\Sigma)}}{(1-\mathbb{L}^{-1})^r}[W]\,\mathbb{L}^{-\ell(\mathscr{S})\dim(V_\Sigma)} \prod_{p\in|\mathscr{S}|} (1-\mathbb{L}_p^{-1})^r \prod_{p\notin|\mathscr{S}|} P_{B_\Sigma}(\mathbb{L}^{-1})\\
&\qquad + \text{an error term of dimension at most } -\tfrac{1}{4}\min_{\alpha\in\Sigma(1)} (d_\alpha) + (1-\ell(\mathscr{S}))(\dim(V_\Sigma)-1) + \dim(W)
\end{aligned}$$

for all $\boldsymbol{d} \in \mathrm{Eff}(V_\Sigma)^\vee_{\mathbb{Z}}$. This concludes the proof of Theorem 5.6. □

6. Twisted products of toric varieties

The goal of this section is to apply the notion of equidistribution of (rational) curves to the case of a certain kind of twisted product. It provides a going-up theorem answering the following question in a particular setting: given a fibration, if a Batyrev–Manin–Peyre principle holds for the base and for the fibres, does it hold for the entire fibration?

First, we recall the construction and geometric properties of such a twisted product, as is done in [17]. Then we study the moduli space of rational curves and apply the change of model Theorem 4.6 to this context.

6.1. *Generalities on twisted products.* In this section we adapt the framework of [17] and [63] to the study of rational curves. Concerning torsors, we will refer to [20].

In this paragraph S is a scheme, G is a linear flat group scheme over S, with connected fibres, and $g:\mathscr{B}\to S$ a flat scheme over S. Recall that a G-torsor over $\mathscr{B}$ is a scheme $\mathscr{T}\to\mathscr{B}$ over $\mathscr{B}$ which is faithfully flat and locally of finite presentation, endowed with a G-action $\tau : G\times_S\mathscr{T}\to\mathscr{T}$ over $\mathscr{B}$ such that the induced morphism

$$(\tau,\mathrm{pr}_2):G\times_S\mathscr{T}\to\mathscr{T}\times_{\mathscr{B}}\mathscr{T}$$

is an isomorphism. Moreover, in this article we will only consider torsors which are locally trivial for the Zariski topology.

6.1.1. *Twisted products and twisted invertible sheaves.* Following [17, Section 2], let $f:X\to S$ be a flat (quasicompact and quasiseparated) S-scheme endowed with an action of G/S. Let $\mathscr{T}\to\mathscr{B}$ be a G-torsor locally trivial for the Zariski topology. We construct a fibration $\pi:\mathscr{X}=\mathscr{T}\times^G X\to\mathscr{B}$ locally isomorphic to X over $\mathscr{B}$ in the following manner. Let $(U_i)_{i\in I}$ be a Zariski covering of $\mathscr{B}$ together with trivialisation $\phi_i : G\times_S U_i\to\mathscr{T}_{U_i}$. For all $i,j\in I$ there exists a unique section g_{ij} of G over $U_i\cap U_j$ such that $\phi_i=g_{ij}\phi_j$ on $U_i\cap U_j$. This data provides a cocycle whose class in $H^1(\mathscr{B}_{\mathrm{Zar}},G)$ represents the isomorphism class of $\mathscr{T}$ as a G-torsor. Then we set $\mathscr{X}_i=X\times_S U_i$. The action of G/S on X/S induces an action of g_{ij} over $X\times_S(U_i\cap U_j)$ and the later yields an isomorphism $\varphi_{ij}:\mathscr{X}_{j\,|U_i\cap U_j}\simeq\mathscr{X}_{i\,|U_i\cap U_j}$. Gluing via the φ_{ij} defines $\pi:\mathscr{X}\to\mathscr{B}$. Up to a unique isomorphism, this construction does not depend on the choice of the open sets (U_i).

There exists a functor ϑ from the category of G-linearised quasicoherent sheaves over X to the category of quasicoherent sheaves over $\mathscr{X}$ [17, Construction 2.1.7] which is compatible with the standard operations for sheaves (direct sum, tensor product, localisation). It sends a G-linearised quasicoherent sheaf over X to its twisted version over $\mathscr{X}$, the gluing isomorphisms being given by the $\varphi_{i,j}$. This functor induces a map on the isomorphism classes. In particular, such a map sends $\Omega^1_{X/S}$ to $\Omega^1_{\mathscr{X}/\mathscr{B}}$ [17, Proposition 2.1.8].

If $X=S$ then $\mathscr{X}=\mathscr{B}$ and this functor ϑ is written $\eta_{\mathscr{T}}$. It induces a group morphism $\mathcal{X}^*(G)\to\mathrm{Pic}(\mathscr{B})$, also written $\eta_{\mathscr{T}}$, sending χ to the (isomorphism class of the) line bundle on $\mathscr{B}$ obtained via the gluing morphisms

$$(u,t)\in(U_i\cap U_j)\times_S\mathbb{A}^1_S\mapsto(u,\chi(g_{ij})t)\in(U_j\cap U_i)\times_S\mathbb{A}^1_S,$$

where $(g_{ij})\in H^1(\mathscr{B}_{\mathrm{Zar}},G)$ is the cocycle defined above.

We define $\mathrm{Pic}^G(X)$ to be the group of isomorphism classes of G-linearised invertible sheaves on X. If X/S and $\mathscr{B}/S$ are smooth, the canonical sheaf over X/S is endowed with a canonical G-linearisation and

$$\omega_{\mathscr{X}/S}\simeq\vartheta(\omega_{X/S})\otimes\pi^*\omega_{\mathscr{B}/S}$$

by [17, Proposition 2.1.8]. The forgetful functor ϖ induces a forgetful morphism

$$\varpi : \mathrm{Pic}^G(X) \to \mathrm{Pic}(X).$$

Let

$$\iota : \mathcal{X}^*(G) \to \mathrm{Pic}^G(X)$$

be the group morphism sending χ to the (isomorphism class of the) trivial bundle

$$X \times_S \mathbb{A}^1_S,$$

together with the action of G given by

$$g \cdot (x, t) = (g \cdot x, \chi(g)t)$$

for all $(x, t) \in X \times_S \mathbb{A}^1_S$ and $g \in G$.

Putting ι, $\eta_{\mathscr{T}}$, ϑ and π^* together, we get morphisms

$$\mathcal{X}^*(G) \xrightarrow{(\iota, -\eta_{\mathscr{T}})} \mathrm{Pic}^G(X) \oplus \mathrm{Pic}(\mathscr{B})$$

and

$$\mathrm{Pic}^G(X) \oplus \mathrm{Pic}(\mathscr{B}) \xrightarrow{\vartheta \otimes \pi^*} \mathrm{Pic}(\mathscr{X}).$$

For every character χ, there is a canonical isomorphism of invertible sheaves on $\mathscr{X}$

$$\vartheta(\iota(\chi)) \simeq \pi^* \eta_{\mathscr{T}}(\chi) \tag{6.1.18}$$

by [17, Proposition 2.1.11].

6.1.2. *Twisted products over a field: an exact sequence.* Assume that S is the spectrum of a field k, that $\mathscr{B}$ is a smooth proper and geometrically integral variety over k and G is a multiplicative group. Then, there is an exact sequence [20, (2.0.2), Theorem 1.5.1]

$$0 \to H^1(k, G) \to H^1(\mathscr{B}, G) \to \mathrm{Hom}(\mathcal{X}^*(G), \mathrm{Pic}(\overline{\mathscr{B}})) \to H^2(k, G) \to H^2(\mathscr{B}, G).$$

Assume moreover that $\mathscr{B}$ admits an open subset U such that $\mathrm{Pic}(\overline{U}) = 0$. Then by [20, Remark 2.2.7, Proposition 2.2.8], in the previous exact sequence $H^2(k, G) \to H^2(\mathscr{B}, G)$ is injective and the resulting short exact sequence

$$0 \to H^1(k, G) \to H^1(\mathscr{B}, G) \to \mathrm{Hom}(\mathcal{X}^*(G), \mathrm{Pic}(\overline{\mathscr{B}})) \to 0 \tag{6.1.19}$$

splits. It is the case if the base $\mathscr{B}$ has a k-rational point, the splitting being given by the evaluation map $H^1(\mathscr{B}, G) \to H^1(k, G)$ at this point.

6.1.3. *H90 multiplicative groups.* We again take S to be the spectrum of a field k and G is a linear connected group over k.

Definition 6.1. We will say that G is an H90 multiplicative algebraic group if

- $H^1(k, G)$ is trivial;
- G is multiplicative and solvable over k.

If G acts on a projective k-variety V, we will always assume that every line bundle on V admits a G-linearisation.

Example 6.2. If k has cohomological dimension at most 1 and G is a linear connected group which is solvable over k, then by [61, Théorème 1′] the first cohomology group $H^1(k, G)$ is trivial.

Example 6.3. If V is a split smooth toric variety and G is its torus, then G is an H90 multiplicative algebraic group, by Hilbert 90.

6.2. *Twisted models of X over $\mathbb{P}^1_k$.* From now on we assume that X is Fano-like, that G is H90 multiplicative and acts on X, and that $\mathscr{B}(k)$ is Zariski dense in $\mathscr{B}$. Moreover, we assume that the Picard groups of $\mathscr{B}$ and X coincide respectively with their geometric Picard group: $\operatorname{Pic}(\overline{\mathscr{B}}) \simeq \operatorname{Pic}(\mathscr{B})$ and $\operatorname{Pic}(\overline{X}) \simeq \operatorname{Pic}(X)$.

Then the sequence

$$0 \longrightarrow \mathcal{X}^*(G) \xrightarrow{(\iota, -\eta_{\mathscr{T}})} \operatorname{Pic}^G(X) \oplus \operatorname{Pic}(\mathscr{B}) \xrightarrow{\vartheta \otimes \pi^*} \operatorname{Pic}(\mathscr{X}) \longrightarrow 0 \tag{6.2.20}$$

is exact by [17, Théorème 2.2.4]. As a corollary, we get exact sequences

$$0 \longrightarrow \mathcal{X}^*(G) \xrightarrow{\iota} \operatorname{Pic}^G(X) \xrightarrow{\varpi} \operatorname{Pic}(X) \longrightarrow 0$$

(by taking $\mathscr{B} = \operatorname{Spec}(k)$ in (6.2.20)) and

$$0 \longrightarrow \operatorname{Pic}(\mathscr{B}) \xrightarrow{\pi^*} \operatorname{Pic}(\mathscr{X}) \xrightarrow{\widetilde{\varpi}} \operatorname{Pic}(X) \longrightarrow 0. \tag{6.2.21}$$

The map $\widetilde{\varpi} : \operatorname{Pic}(\mathscr{X}) \to \operatorname{Pic}(X)$ above is the map sending the class of a line bundle of the form

$$\vartheta(L) \otimes \pi^*(\mathscr{L}),$$

with $\mathscr{L}$ a line bundle on $\mathscr{B}$ and L a G-linearised line bundle on X, to the one of $\varpi(L)$.

6.2.1. *Pulling-back.* Let $f : \mathbb{P}^1_k \to \mathscr{B}$ be a rational curve on $\mathscr{B}$. It induces a morphism $\mathbf{deg}\, f : \operatorname{Pic}(\mathscr{B}) \to \operatorname{Pic}(\mathbb{P}^1_k) \simeq \mathbb{Z}$. Since in our situation we assume G to be an H90 multiplicative group, type and class coincide by (6.1.19), so that $\eta_{\mathscr{T}}$ and the type $\alpha \in \operatorname{Hom}(\mathcal{X}^*(G), \operatorname{Pic}(\mathscr{B}))$ of the G-torsor $\mathscr{T} \to \mathscr{B}$ can be identified (we refer the interested reader to [20, Section 2] for the precise definition of type). The pulling-back operation

$$\begin{tikzcd} \mathscr{T}_f \arrow[r] \arrow[d] \arrow[dr, phantom, "\ulcorner"] & \mathscr{T} \arrow[d] \\ \mathbb{P}^1_k \arrow[r, "f"] & \mathscr{B} \end{tikzcd}$$

induces a G-torsor $\mathscr{T}_f$ whose type (or class) is given by $(\mathbf{deg}\, f) \circ \alpha \in \mathcal{X}_*(G)$, together with functors on quasicoherent sheaves $\vartheta_f = f^*_{\mathscr{X}} \circ \vartheta$ and $\eta_{\mathscr{T}_f} = f^* \circ \eta_{\mathscr{T}}$.

Then, remark that the pull-back

$$\begin{tikzcd} \mathscr{X}_f \arrow[r, "f_{\mathscr{X}}"] \arrow[d] \arrow[dr, phantom, "\ulcorner", very near start] & \mathscr{X} \arrow[d] \\ \mathbb{P}^1_k \arrow[r, "f"] & \mathscr{B} \end{tikzcd}$$

only depends on the multidegree of f since it is exactly the twisted product obtained by starting from the G-torsor $\mathscr{T}_f \to \mathbb{P}^1_k$ of class $f^* \circ \eta_{\mathscr{T}} = \mathbf{deg}(f) \circ \alpha$.

In order to compare degrees of line bundles on models of X above $\mathbb{P}^1_k$ coming from different f of the same multidegree $\delta_{\mathscr{B}}$, we need to find canonical isomorphisms between the Picard groups of these different models. So we take f and f' to be two rational curves $\mathbb{P}^1 \to \mathscr{B}$ of equal multidegree $\delta_{\mathscr{B}}$. They induce pull-backs $\mathscr{T}_f$, $\mathscr{T}_{f'}$ and $\mathscr{X}_f$, $\mathscr{X}_{f'}$. Since $\mathscr{T}_f$ and $\mathscr{T}_{f'}$ have equal types and classes, $\mathscr{X}_f$ and $\mathscr{X}_{f'}$ are isomorphic as G-varieties. We get a commutative diagram of exact sequences

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{X}^*(G) \arrow[r, "(\iota, -\eta_{\mathscr{T}})"'] \arrow[d, equal] & \operatorname{Pic}^G(X) \oplus \operatorname{Pic}(\mathscr{B}) \arrow[r, "\vartheta \otimes \pi^*"'] \arrow[d, "(\mathrm{id}, \delta_{\mathscr{B}})"'] & \operatorname{Pic}(\mathscr{X}) \arrow[r] \arrow[d, "f_{\mathscr{X}}^*"] \arrow[dd, bend left, "{f'_{\mathscr{X}}}^*"] & 0 \\ 0 \arrow[r] & \mathcal{X}^*(G) \arrow[r, "(\iota, -\eta_{\mathscr{T}_f})"'] \arrow[d, equal] & \operatorname{Pic}^G(X) \oplus \operatorname{Pic}(\mathbb{P}^1_k) \arrow[r, "\vartheta_f \otimes \pi_f^*"'] \arrow[d, equal] & \operatorname{Pic}(\mathscr{X}_f) \arrow[r] \arrow[d, dashed, "\exists ! \simeq"'] & 0 \\ 0 \arrow[r] & \mathcal{X}^*(G) \arrow[r, "(\iota, -\eta_{\mathscr{T}_{f'}})"'] & \operatorname{Pic}^G(X) \oplus \operatorname{Pic}(\mathbb{P}^1_k) \arrow[r, "\vartheta_{f'} \otimes \pi_{f'}^*"'] & \operatorname{Pic}(\mathscr{X}_{f'}) \arrow[r] & 0 \end{tikzcd}$$

providing a canonical isomorphism $\operatorname{Pic}(\mathscr{X}_f) \simeq \operatorname{Pic}(\mathscr{X}_{f'})$.

6.2.2. *Multidegrees of sections of $\mathscr{X}_f \to \mathbb{P}^1_k$.* Assume now that $f : \mathbb{P}^1_k \to \mathscr{B}$ comes from a morphism $g : \mathbb{P}^1_k \to \mathscr{X}$, that is to say, $f = \pi \circ g$. Then we obtain the Cartesian square

$$\begin{tikzcd} \mathscr{X}_f \arrow[r, "f_{\mathscr{X}}"] \arrow[d, "\pi_f"'] & \mathscr{X} \arrow[d, "\pi"] \\ \mathbb{P}^1_k \arrow[r, "f"'] \arrow[u, dashed, bend right, "\sigma"'] \arrow[ur, "g"] & \mathscr{B} \end{tikzcd}$$

in which g induces a unique section $\sigma : \mathbb{P}^1_k \to \mathscr{X}_f$ such that $g = f_{\mathscr{X}} \circ \sigma$. We deduce from this square the relations on degree maps

$$\begin{aligned} \mathbf{deg}(g) &= \mathbf{deg}(\sigma) \circ f_{\mathscr{X}}^*, \\ \mathbf{deg}(f) &= \mathbf{deg}(g) \circ \pi^* = \mathbf{deg}(\sigma) \circ f_{\mathscr{X}}^* \circ \pi^*, \\ \mathrm{id}_{\operatorname{Pic}(\mathbb{P}^1_k)} &= \mathbf{deg}(\sigma) \circ \pi_f^*. \end{aligned}$$

Setting 6.4. Let $L_1, \dots, L_{r_X}$ be a family of line bundles on X whose classes form a $\mathbb{Z}$-basis of $\operatorname{Pic}(X)$. We fix a section $s : \operatorname{Pic}(X) \to \operatorname{Pic}^G(X)$ by choosing a G-linearisation on each L_i.

From (6.2.20) and (6.2.21) one deduces the commutative diagram of exact sequences

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Pic}(\mathscr{B}) \arrow[r, "\pi^*"] \arrow[d, "\mathbf{deg}(f)"] & \mathrm{Pic}(\mathscr{X}) \arrow[r, "\widetilde{\varpi}"] \arrow[d, "f_{\mathscr{X}}^*"] & \mathrm{Pic}^G(X)/\iota(\mathcal{X}^*(G)) \simeq \mathrm{Pic}(X) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathrm{Pic}(\mathbb{P}^1_k) \arrow[r, "\pi_f^*"] & \mathrm{Pic}(\mathscr{X}_f) \arrow[r, "\widetilde{\varpi}_f"] & \mathrm{Pic}^G(X)/\iota(\mathcal{X}^*(G)) \simeq \mathrm{Pic}(X) \arrow[r] & 0
\end{tikzcd}$$

where the arrow $\widetilde{\varpi}_f : \mathrm{Pic}(\mathscr{X}_f) \to \mathrm{Pic}(X) \simeq \mathbb{Z}$ is obtained from $\widetilde{\varpi}$ by replacing ϑ by ϑ_f and π by π_f.

Furthermore $\mathbf{deg}(\sigma) : \mathrm{Pic}(\mathscr{X}_f) \to \mathrm{Pic}(\mathbb{P}^1_k)$ induces by composition with $s : \mathrm{Pic}(X) \to \mathrm{Pic}^G(X)$ and $\vartheta_f : \mathrm{Pic}^G(X) \to \mathrm{Pic}(\mathscr{X}_f)$ a multidegree

$$\delta_X(\sigma) : \mathrm{Pic}(X) \to \mathrm{Pic}(\mathbb{P}^1_k) \simeq \mathbb{Z}$$

sending the class of a line bundle L on X to

$$\mathbf{deg}(\sigma) \cdot (\vartheta_f \circ s)([L]) = \mathbf{deg}(g) \cdot (\vartheta \circ s)([L]).$$

If σ' is another section obtained in this way, that is to say, from another g' and another f' such that $\pi \circ g' = f'$ and $\mathbf{deg}(g) = \mathbf{deg}(g')$, then $\mathbf{deg}(f) = \mathbf{deg}(f') = \delta_{\mathscr{B}}$, and $\mathscr{X}_f \simeq \mathscr{X}_{f'}$. The following commutative diagram summarises the situation and shows that $\delta_X(\sigma) = \delta_X(\sigma') = \mathbf{deg}(g) \circ \vartheta \circ s$, which is an element of $\mathrm{Pic}(X)^\vee$ and will be denoted by $\delta_X(g)$:

$$\begin{tikzcd}
 & 0 \arrow[r] & \mathrm{Pic}(\mathscr{B}) \arrow[r, "\pi^*"] \arrow[d, "\delta_{\mathscr{B}}"'] & \mathrm{Pic}(\mathscr{X}) \arrow[r] \arrow[dl, "\mathbf{deg}(g)"'] \arrow[d, "f_{\mathscr{X}}^*"] \arrow[dd, bend left, "{f'_{\mathscr{X}}}^*"] & \mathrm{Pic}(X) \arrow[r] \arrow[d, equal] \arrow[l, bend right, "\vartheta \circ s"'] \arrow[dl, "\upsilon_f \circ s"] & 0 \\
s & 0 \arrow[r] & \mathrm{Pic}(\mathbb{P}^1_k) \arrow[r, "\pi_f^*"] \arrow[d, equal] & \mathrm{Pic}(\mathscr{X}_f) \arrow[r, dashed] \arrow[d, "\simeq"] \arrow[l, bend left, "\mathbf{deg}(\sigma)"] & \mathrm{Pic}(X) \arrow[r] \arrow[d, equal] & 0 \\
 & 0 \arrow[r] & \mathrm{Pic}(\mathbb{P}^1_k) \arrow[r, "\pi_{f'}^*"] & \mathrm{Pic}(\mathscr{X}_{f'}) \arrow[r] \arrow[l, bend left, "\mathbf{deg}(\sigma')"] & \mathrm{Pic}(X) \arrow[r] & 0
\end{tikzcd}$$

By duality, from (6.2.20) we get an exact sequence

$$0 \longrightarrow \mathrm{Pic}(\mathscr{X})^\vee \xrightarrow{(\vartheta^\vee, \pi_*)} \mathrm{Pic}^G(X)^\vee \oplus \mathrm{Pic}(\mathscr{B})^\vee \longrightarrow \mathcal{X}_*(G) \longrightarrow 0,$$

which allows us to decompose a multidegree on $\mathscr{X}$.

Lemma 6.5. *Let* $\mathbf{deg}(g) = (\delta_X^G(g), \delta_{\mathscr{B}}(g))$ *viewed in* $\mathrm{Pic}^G(X)^\vee \oplus \mathrm{Pic}(\mathscr{B})^\vee$. *Then the morphism*

$$[L] \in \mathrm{Pic}^G(X) \longmapsto \delta_X^G(g) \cdot [L] - \delta_X(g) \cdot [\varpi(L)] \in \mathrm{Pic}(\mathbb{P}^1_k) \simeq \mathbb{Z}$$

defines a cocharacter of G *given by*

$$\chi \in \mathcal{X}^*(G) \mapsto \delta_{\mathscr{B}}(g) \cdot (\eta_{\mathscr{T}} \circ \iota)(\chi).$$

Proof. We use again our favourite exact sequences to get the diagram

$$
\begin{tikzcd}
& & 0 \arrow[d] & 0 \arrow[d] & \\
& & \mathcal{X}^*(G) \arrow[r, equal] \arrow[d, "{(\iota,-\eta_{\mathscr{T}})}"] & \mathcal{X}^*(G) \arrow[d, "\iota"] & \\
& & \mathrm{Pic}^G(X)\oplus\mathrm{Pic}(\mathscr{B}) \arrow[r] \arrow[dl] \arrow[d, "\vartheta\otimes\pi^*"'] & \mathrm{Pic}^G(X) \arrow[dl, "\vartheta"'] \arrow[d, shift left, "\varpi"] \arrow[ddll, "\delta_X^G(g)"] & \\
0 \arrow[r] & \mathrm{Pic}(\mathscr{B}) \arrow[r, "\pi^*"] \arrow[d, "\delta_{\mathscr{B}}(g)"'] & \mathrm{Pic}(\mathscr{X}) \arrow[r] \arrow[dl, "\mathbf{deg}(g)"] \arrow[d, dashed] & \mathrm{Pic}(X) \arrow[r] \arrow[u, bend left, "s"] \arrow[d] \arrow[dll, bend left, "\delta_X(g)"] & 0 \\
0 \arrow[r] & \mathrm{Pic}(\mathbb{P}^1_k) & 0 & 0 &
\end{tikzcd}
$$

from which one reads $\delta_X(g) = \delta_X^G(g)\circ s$ and $\delta_X^G(g) = \mathbf{deg}(g)\circ\vartheta$.

Let L be a G-linearised line bundle on X. Since s is a section of ϖ, there exists a unique character $\chi \in \mathcal{X}^*(G)$ such that

$$[L] = (s\circ\varpi)([L]) + \iota(\chi)$$

in $\mathrm{Pic}^G(X)$. Taking intersection degrees, we get

$$
\begin{aligned}
\delta_X^G(g)\cdot[L] &= \delta_X^G(g)\cdot(s\circ\varpi)([L]) + \delta_X^G(g)\cdot\iota(\chi)\\
&= \delta_X(g)\cdot\varpi([L]) + \mathbf{deg}(g)\cdot(\vartheta\circ\iota(\chi))\\
&= \delta_X(g)\cdot\varpi([L]) + \mathbf{deg}(g)\cdot(\pi^*\circ\eta_{\mathscr{T}}(\chi)) \quad \text{(by (6.1.18) on page 955)}\\
&= \delta_X(g)\cdot\varpi([L]) + \delta_{\mathscr{B}}(g)\cdot\eta_{\mathscr{T}}(\chi).
\end{aligned}
$$

Hence

$$(\delta_X^G(g)\cdot\vartheta - \delta_X(g)\cdot\varpi) : [L] \longmapsto \delta_{\mathscr{B}}\cdot\eta_{\mathscr{T}}([L] - s\circ\varpi[L])$$

lies in $\mathcal{X}_*(G)$. □

We reformulate these remarks in terms of moduli spaces of rational curves in the following section.

6.3. ***Moduli spaces of morphisms and sections.*** In what follows $\mathscr{U}$ is a dense open subset of $\mathscr{B}$, U is a dense open subset of X which is stable under the action of G, and $\widetilde{\mathscr{U}}$ is the intersection of the preimage of $\mathscr{U}$ with $\mathscr{T}\times^G U$ in $\mathscr{X}$.

Let k' be an extension of k and $f : \mathbb{P}^1_{k'} \to \mathscr{B}_{k'}$ be a k'-morphism given by a k'-point x of $\mathrm{Hom}(\mathbb{P}^1_k, \mathscr{B})_{\mathscr{U}}$. As before, the morphism f defines pull-backs $\mathscr{T}_f = \mathscr{T}\times_f \mathbb{P}^1_{k'}$ and $\mathscr{X}_f = \mathbb{P}^1_{k'}\times_f \mathscr{X}_{k'}$ over $\mathbb{P}^1_{k'}$. We fix once and for all a representative $\mathscr{T}_{\delta_{\mathscr{B}}}$ of the isomorphism class of $\mathscr{T}_f$, whenever $\delta_{\mathscr{B}} = \mathbf{deg}(f) : \mathrm{Pic}(\mathscr{B}_{k'}) \to \mathrm{Pic}(\mathbb{P}^1_{k'})$, as well as a corresponding twisted product $\mathscr{X}_{\delta_{\mathscr{B}}}$. We have canonical isomorphisms $\mathscr{T}_{\delta_{\mathscr{B}}} \simeq \mathscr{T}_f$, $\mathscr{X}_{\delta_{\mathscr{B}}} \simeq \mathscr{X}_f$ and $\mathrm{Pic}(\mathscr{X}_{\delta_{\mathscr{B}}}) \simeq \mathrm{Pic}(\mathscr{X}_f)$.

Lemma 6.6. *The schematic fibre M_x of*

$$\pi_* : \mathrm{Hom}(\mathbb{P}^1_k, \mathscr{X})_{\widetilde{\mathscr{U}}} \to \mathrm{Hom}(\mathbb{P}^1_k, \mathscr{B})_{\mathscr{U}}$$

over the k'-point x corresponding to f is canonically isomorphic to

$$\mathrm{Hom}_{\mathbb{P}^1_{k'}}(\mathbb{P}^1_{k'}, \mathscr{X}_f)_U \simeq \mathrm{Hom}_{\mathbb{P}^1_{k'}}(\mathbb{P}^1_{k'}, \mathscr{X}_{\delta_{\mathscr{B}}})_U.$$

Proof. On the one hand, if we consider T-points of $M_{k'}$, where T is a scheme over k', we get T-morphisms $g : T \times_{k'} \mathbb{P}^1_{k'} \to T \times_{k'} \mathscr{X}_{k'}$ and the following commutative diagram:

$$\begin{tikzcd} \mathscr{X}_T \times_{\mathscr{B}_T} \mathbb{P}^1_T \arrow[r, "\mathrm{pr}_{\mathscr{X}_T}"] \arrow[d, "\mathrm{pr}_{\mathbb{P}^1_T}"'] \arrow[dr, phantom, "\ulcorner", very near start] & \mathscr{X}_T \arrow[d, "\pi_T"] \\ \mathbb{P}^1_T \arrow[ur, "g"] \arrow[r, "(\mathrm{id}_T \times f)"] & \mathscr{B}_T \end{tikzcd}$$

The product $\mathscr{X}_T \times_{\mathscr{B}_T} \mathbb{P}^1_T$ is the extension of scalars of $\mathscr{X}_f$ to T, and the previous square is

$$\begin{tikzcd} T \times_{k'} \mathscr{X}_f \arrow[r] \arrow[d, shift right, "\mathrm{pr}_{\mathbb{P}^1_T}"'] \arrow[dr, phantom, "\ulcorner", very near start] & T \times_{k'} \mathscr{X}_{k'} \arrow[d, "(\mathrm{id} \times \pi_{k'})"] \\ T \times_{k'} \mathbb{P}^1_{k'} \arrow[u, dashed, shift right, "\exists!"'] \arrow[ur, "g"] \arrow[r, "(\mathrm{id}_T \times f)"] & T \times_{k'} \mathscr{B}_{k'} \end{tikzcd} \tag{6.3.22}$$

giving the existence of a unique T-section $\sigma : \mathbb{P}^1_T \to T \times_{k'} \mathscr{X}_f$. On the other hand, such a T-section defines a unique T-morphism $g : \mathbb{P}^1_T \to T \times \mathscr{X}_{k'}$ making the bottom right triangle commutative, that is, a unique T-point of $M_{k'}$. Thus the schematic fibre of π_* at the k'-point x corresponding to $f : \mathbb{P}^1_{k'} \to \mathscr{B}_{k'}$ is canonically isomorphic to $\mathrm{Hom}_{\mathbb{P}^1_{k'}}(\mathbb{P}^1_{k'}, \mathscr{X}_f)$ as a k'-scheme. □

In particular, the previous argument shows that for every k'-scheme T there is a map of sets

$$\Sigma_\delta(T) : \mathrm{Hom}^\delta_k(\mathbb{P}^1_k, \mathscr{X})(T) \to \mathrm{Hom}^{\delta^G_X \circ s}_{\mathbb{P}^1_k}(\mathbb{P}^1_k, \mathscr{X}_{\delta_{\mathscr{B}}})(T)$$

sending a T-point $g : \mathbb{P}^1_T \to \mathscr{X} \times_k T$ of multidegree $\delta \in \mathrm{Pic}(\mathscr{X})^\vee$ to the unique T-point σ of

$$\mathrm{Hom}_{\mathbb{P}^1_k}(\mathbb{P}^1_k, \mathscr{X}_f) \simeq \mathrm{Hom}_{\mathbb{P}^1_k}(\mathbb{P}^1_k, \mathscr{X}_{\delta_{\mathscr{B}}})$$

given by the dashed arrow in (6.3.22). Note that this construction is functorial in T, leading to a morphism of schemes

$$\Sigma_\delta : \mathrm{Hom}^\delta_k(\mathbb{P}^1_k, \mathscr{X}) \to \mathrm{Hom}^{\delta^G_X \circ s}_{\mathbb{P}^1_k}(\mathbb{P}^1_k, \mathscr{X}_{\delta_{\mathscr{B}}}).$$

From Proposition 1.30 on page 901 we deduce:

Proposition 6.7. *Let $s : \mathrm{Pic}(X) \to \mathrm{Pic}^G(X)$ be a section of the forgetful morphism ϖ. Then for any class $\delta = (\delta^G_X, \delta_{\mathscr{B}})$ we have*

$$[\mathrm{Hom}^{\delta_{\mathscr{X}}}_k(\mathbb{P}^1_k, \mathscr{X})_{\widetilde{\mathscr{U}}}] = [\mathrm{Hom}^{\delta_{\mathscr{B}}}_k(\mathbb{P}^1_k, \mathscr{B})_{\mathscr{U}}][\mathrm{Hom}^{\delta^G_X \circ s}_{\mathbb{P}^1_k}(\mathbb{P}^1_k, \mathscr{X}_{\delta_{\mathscr{B}}})_U]$$

in $K_0\mathbf{Var}_k$.

6.4. ***Asymptotic behaviour.*** We assume that the motivic constants $\tau_{\mathbb{P}^1_k}(X)$ and $\tau_{\mathbb{P}^1_k}(\mathscr{B})$ are well-defined in $\widehat{\mathscr{M}}_k = \widehat{\mathscr{M}}_k^{w}$ or $\widehat{\mathscr{M}}_k = \widehat{\mathscr{M}}_k^{\dim}$.

Lemma 6.8. *The symbol $\tau_{\mathbb{P}^1_k}(\mathscr{X})$ is well-defined and one has*

$$\tau_{\mathbb{P}^1_k}(\mathscr{X}) = \tau_{\mathbb{P}^1_k}(X)\tau_{\mathbb{P}^1_k}(\mathscr{B})$$

in $\widehat{\mathscr{M}}_k$.

Proof. As abstract series, the equality $\tau_{\mathbb{P}^1_k}(\mathscr{X}) = \tau_{\mathbb{P}^1_k}(X)\tau_{\mathbb{P}^1_k}(\mathscr{B})$ is a consequence of the multiplicative property of the motivic Euler product given by Proposition 2.12. Indeed, by local triviality of the fibration, one has the relation $[\mathscr{X} \times_k \mathbb{P}^1_k] = [X \times_k \mathbb{P}^1_k][\mathscr{B} \times_k \mathbb{P}^1_k]$ in $\mathscr{M}_{\mathbb{P}^1_k}$. Since $\tau_{\mathbb{P}^1_k}(X)$ and $\tau_{\mathbb{P}^1_k}(\mathscr{B})$ both converge in $\widehat{\mathscr{M}}_k$, so does $\tau_{\mathbb{P}^1_k}(\mathscr{X})$. □

Theorem 6.9. *Let X and $\mathscr{B}$ be two Fano-like varieties*[6] *defined over the base field k. Assume that G is an $H90$-multiplicative group*[7] *acting on X and that every line bundle on X admits a G-linearisation. Let U and $\mathscr{U}$ be dense open subsets respectively of X and $\mathscr{B}$, with U stable under the action of G.*

Let $\mathscr{T}$ be a G-torsor over $\mathscr{B}$ and

$$\mathscr{X} = \mathscr{T} \times^G X$$

the twisted product[8] *of X and $\mathscr{T}$ over $\mathscr{B}$. Let $\widetilde{\mathscr{U}}$ be the intersection of the preimage of $\mathscr{U}$ with $\mathscr{T} \times^G U$ in $\mathscr{X}$.*

Assume that the motivic Batyrev–Manin–Peyre principle for rational curves[9] *holds both for X and $\mathscr{B}$ for curves generically intersecting U and $\mathscr{U}$ respectively, which means that*

$$[\mathrm{Hom}_k^{\delta_X}(\mathbb{P}^1_k, X)_U]\,\mathbb{L}^{-\delta_X \cdot \omega_X^{-1}} \to \tau(X),$$
$$[\mathrm{Hom}_k^{\delta_{\mathscr{B}}}(\mathbb{P}^1_k, \mathscr{B})_{\mathscr{U}}]\,\mathbb{L}^{-\delta_{\mathscr{B}} \cdot \omega_{\mathscr{B}}^{-1}} \to \tau(\mathscr{B})$$

when $d(\delta_X, \partial\,\mathrm{Eff}(X)^\vee)$ and $d(\delta_{\mathscr{B}}, \partial\,\mathrm{Eff}(\mathscr{B})^\vee)$ both tend to infinity, in $\widehat{\mathscr{M}}_k = \widehat{\mathscr{M}}_k^{w}$ or $\widehat{\mathscr{M}}_k^{\dim}$.

Assume furthermore that equidistribution of rational curves[10] *holds for X.*

Then for $\delta \in \mathrm{Eff}(\mathscr{X})^\vee_{\mathbb{Z}}$ the normalised class

$$[\mathrm{Hom}_k^{\delta}(\mathbb{P}^1_k, \mathscr{X})_{\widetilde{\mathscr{U}}}]\,\mathbb{L}^{-\delta \cdot \omega_{\mathscr{X}}^{-1}}$$

tends to the nonzero effective element

$$\tau(\mathscr{X}) = \tau(X)\tau(\mathscr{B}) \in \widehat{\mathscr{M}}_k$$

when the distance $d(\delta, \partial\,\mathrm{Eff}(\mathscr{X})^\vee)$ goes to infinity.

Together with Theorem 5.6, we get the following.

---

[6] See Definition 1 on page 885.

[7] See Definition 6.1 on page 955. For example, take G to be a split torus.

[8] See Section 6.1 on page 954.

[9] See Question 1 on page 887, and more generally Question 2 on page 917.

[10] See Definition 4.3 on page 921.

Corollary 6.10. *Let X be a smooth projective split toric variety with open orbit $U \simeq \boldsymbol{G}_m^n$ and $\mathscr{T} \to \mathscr{B}$ a $\boldsymbol{G}_m^n$-torsor above a Fano-like variety $\mathscr{B}$. Assume that the Batyrev–Manin–Peyre principle holds for rational curves on $\mathscr{B}$. Then it holds as well for rational curves on the twisted product $\mathscr{X} = \mathscr{T} \times^G X$.*

Proof of Theorem 6.9. Let $\delta_{\mathscr{X}} = (\delta_X^G, \delta_{\mathscr{B}}) \in \operatorname{Pic}(\mathscr{X})^\vee$ viewed in $\operatorname{Pic}^G(X)^\vee \oplus \operatorname{Pic}(\mathscr{B})^\vee$. Fix a section

$$s : \operatorname{Pic}(X) \to \operatorname{Pic}^G(X)$$

of the forgetful morphism ϖ as in Setting 6.4. That is to say, fix line bundles $L_1, \dots, L_{r_X}$ forming a basis of $\operatorname{Pic}(X)$ together with a G-linearisation on each of them.

Given a curve $f : \mathbb{P}_k^1 \to \mathscr{B}$, we know from the previous sections that the isomorphism class (as a scheme over $\mathbb{P}_k^1$) of the pull-back $\mathscr{X}_f$ only depends on its multidegree $\delta_{\mathscr{B}}$ and that it is a twisted model of X over $\mathbb{P}_k^1$. In the beginning of Section 6.3, we chose once and for all a representative $\mathscr{X}_{\delta_{\mathscr{B}}}$ of its isomorphism class:

$$\begin{tikzcd} \mathscr{X}_{\delta_{\mathscr{B}}} \arrow[r] \arrow[d] \arrow[dr, phantom, "\ulcorner"] & \mathscr{X} \arrow[d, "\pi"] \\ \mathbb{P}_k^1 \arrow[r] & \mathscr{B} \end{tikzcd}$$

This model comes with functors $\vartheta_{\delta_{\mathscr{B}}}$ so that $\vartheta_{\delta_{\mathscr{B}}}(L_i)$ is a twisted model of L_i on $\mathscr{X}_{\delta_{\mathscr{B}}}$, and $\vartheta(s \circ \varpi(\omega_X^{-1}))$ a model of ω_X^{-1}. We fix $\delta_{\mathscr{B}}$ and consider sections σ of $\mathscr{X}_{\delta_{\mathscr{B}}}$ of corresponding multidegree

$$\delta_X^G \circ s : [L] \mapsto \delta_X^G \cdot s([L]) = \delta \cdot \vartheta_{\delta_{\mathscr{B}}}(s([L])).$$

By Theorem 4.6,

$$[\operatorname{Hom}_{\mathbb{P}_k^1}^{\delta_X^G \circ s}(\mathbb{P}_k^1, \mathscr{X}_{\delta_{\mathscr{B}}})_U]\, \mathbb{L}^{-(\delta_X^G \circ s)\cdot \omega_V^{-1}}$$

tends to $\tau_{\vartheta(s\circ\varpi(\omega_X^{-1}))}(\mathscr{X}_\delta)$ as $d(\delta_X^G \circ s, \partial \operatorname{Eff}(X)^\vee) \to \infty$. Note that doing this we obtain a motivic Tamagawa number with respect to the model $\vartheta(s \circ \varpi(\omega_X^{-1}))$ of ω_X^{-1} and that we can apply Lemma 6.5 to get the relation

$$\tau_{\vartheta(s\circ\varpi(\omega_X^{-1}))}(\mathscr{X}_{\delta_{\mathscr{B}}}) = \mathbb{L}_k^{\delta_{\mathscr{B}}\cdot \eta_{\mathscr{T}}([\omega_V^{-1}] - s\circ\varpi[\omega_V^{-1}])} \tau_{\vartheta(\omega_X^{-1})}(\mathscr{X}_{\delta_{\mathscr{B}}}) = \mathbb{L}_k^{\delta_{\mathscr{B}}\cdot \eta_{\mathscr{T}}([\omega_V^{-1}] - s\circ\varpi[\omega_V^{-1}])} \tau(X).$$

By Proposition 6.7 we have the equality of classes

$$[\operatorname{Hom}_k^{\delta}(\mathbb{P}_k^1, \mathscr{X})_{\widetilde{\mathscr{U}}}] = [\operatorname{Hom}_k^{\delta_{\mathscr{B}}}(\mathbb{P}_k^1, \mathscr{B})_{\mathscr{U}}]\, [\operatorname{Hom}_{\mathbb{P}_k^1}^{\delta_X^G \circ s}(\mathbb{P}_k^1, \mathscr{X}_{\delta_{\mathscr{B}}})_U].$$

Moreover, the expression

$$\omega_{\mathscr{X}} = \vartheta(\omega_X) \otimes \pi^*(\omega_{\mathscr{B}})$$

and the projection formula provide the decomposition of anticanonical degrees

$$\begin{aligned} \delta \cdot \omega_{\mathscr{X}}^{-1} &= \delta_X^G \cdot \omega_X^{-1} + \delta_{\mathscr{B}} \cdot \omega_{\mathscr{B}}^{-1} \\ &= (\delta_X^G \circ s) \cdot \varpi[\omega_V^{-1}] + \delta_{\mathscr{B}} \cdot \eta_{\mathscr{T}}([\omega_V^{-1}] - s \circ \varpi[\omega_V^{-1}]) + \delta_{\mathscr{B}} \cdot \omega_{\mathscr{B}}^{-1} \end{aligned}$$

so that the normalised class

$$[\operatorname{Hom}_k^{\delta}(\mathbb{P}_k^1, \mathscr{X})_{\widetilde{\mathscr{U}}}]\, \mathbb{L}^{-\delta\cdot\omega_{\mathscr{X}}^{-1}}$$

is the product

$$\big[\mathrm{Hom}_k^{\delta_{\mathscr{B}}}(\mathbb{P}^1_k, \mathscr{B})_{\mathscr{U}}\big]\,\mathbb{L}^{-\delta_{\mathscr{B}}\cdot\omega_{\mathscr{B}}^{-1}} \times \big[\mathrm{Hom}_{\mathbb{P}^1_k}^{\delta_X^G\circ s}(\mathbb{P}^1_k, \mathscr{X}_{\delta_{\mathscr{B}}})_U\big]\,\mathbb{L}^{-(\delta_X^G\circ s)\cdot\omega_V^{-1}}\mathbb{L}^{-\delta_{\mathscr{B}}\cdot\eta_{\mathscr{T}}([\omega_V^{-1}]-s\circ\varpi[\omega_V^{-1}])}$$

of well-normalised classes, as expected.

To conclude the proof, we use [17, Théorème 2.2.9] ensuring that under our assumptions we have

$$\mathrm{Eff}(\mathscr{X})^\vee_{\mathbb{Z}} = \vartheta(\mathrm{Eff}^G(X))^\vee_{\mathbb{Z}} \oplus \pi^*(\mathrm{Eff}(\mathscr{B}))^\vee_{\mathbb{Z}}$$

in $\mathrm{Pic}^G(X)^\vee \oplus \mathrm{Pic}(\mathscr{B})^\vee$. Hence the condition $d(\delta, \partial\,\mathrm{Eff}(\mathscr{X})^\vee) \to \infty$ means

$$d(\delta_X^G, \partial\,\mathrm{Eff}^G(X)^\vee) \to \infty \quad\text{and}\quad d(\delta_{\mathscr{B}}, \partial\,\mathrm{Eff}(X)^\vee) \to \infty,$$

the first of these two conditions implying $d(\delta_X^G\circ s, \partial\,\mathrm{Eff}(X)^\vee) \to \infty$ by Lemma 6.5 for $\delta_{\mathscr{B}}$ fixed. The result follows by continuity of the multiplication. □

Acknowledgements

I am very grateful to my Ph.D. advisor Emmanuel Peyre for all the remarks and suggestions he made during the writing of this article. I warmly thank Margaret Bilu and Tim Browning for some valuable comments they made on a preliminary version of this work. I would like to thank David Bourqui as well for several helpful conversations. Finally, I thank the anonymous referee for their very careful reading and their numerous comments and suggestions which helped me a lot in improving the exposition, besides fixing several typos, and Elizabeth Weaver for the final editing work.

During the revision process of this work, the author received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Grant Agreement No. 101034413.

References

[1] V. V. Batyrev and Y. I. Manin, "Sur le nombre des points rationnels de hauteur borné des variétés algébriques", *Math. Ann.* **286**:1-3 (1990), 27–43. MR Zbl

[2] V. V. Batyrev and Y. Tschinkel, "Tamagawa numbers of polarized algebraic varieties", pp. 299–340 in *Nombre et répartition de points de hauteur bornée* (Paris, 1996), edited by E. Peyre, Astérisque **251**, Soc. Math. France, Paris, 1998. MR Zbl

[3] M. Bilu, *Motivic Euler products and motivic height zeta functions*, Mem. Amer. Math. Soc. **1396**, Amer. Math. Soc., Providence, RI, 2023. MR Zbl

[4] M. Bilu and T. Browning, "A motivic circle method", preprint, 2023. arXiv 2304.09645

[5] M. Bilu and S. Howe, "Motivic Euler products in motivic statistics", *Algebra Number Theory* **15**:9 (2021), 2195–2259. MR Zbl

[6] M. Bilu, R. Das, and S. Howe, "Zeta statistics and Hadamard functions", *Adv. Math.* **407** (2022), art. id. 108556. MR Zbl

[7] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Math. (3) **21**, Springer, 1990. MR Zbl

[8] S. Boucksom, J.-P. Demailly, M. Păun, and T. Peternell, "The pseudo-effective cone of a compact Kähler manifold and varieties of negative Kodaira dimension", *J. Algebraic Geom.* **22**:2 (2013), 201–248. MR Zbl

[9] N. Bourbaki, *Algèbre, Chapitres 1 à 3*, Hermann, Paris, 1970. MR Zbl

[10] N. Bourbaki, *Algèbre commutative, Chapitres 8 et 9*, Masson, Paris, 1983. MR Zbl

[11] D. Bourqui, *Fonctions zêta des hauteurs des variétés toriques en caractéristique positive*, Ph.D. thesis, Université Joseph Fourier–Grenoble I, 2003, available at https://theses.hal.science/tel-00004008/.

[12] D. Bourqui, "Produit eulérien motivique et courbes rationnelles sur les variétés toriques", *Compos. Math.* **145**:6 (2009), 1360–1400. MR Zbl

[13] D. Bourqui, "Fonctions L d'Artin et nombre de Tamagawa motiviques", *New York J. Math.* **16** (2010), 179–233. MR Zbl

[14] D. Bourqui, "Asymptotic behaviour of rational curves", preprint, 2011. arXiv 1107.3824

[15] A. Chambert-Loir and F. Loeser, "Motivic height zeta functions", *Amer. J. Math.* **138**:1 (2016), 1–59. MR Zbl

[16] A. Chambert-Loir and Y. Tschinkel, "Fonctions zêta des hauteurs des espaces fibrés", pp. 71–115 in *Rational points on algebraic varieties*, edited by E. Peyre and Y. Tschinkel, Progr. Math. **199**, Birkhäuser, Basel, 2001. MR Zbl

[17] A. Chambert-Loir and Y. Tschinkel, "Torseurs arithmétiques et espaces fibrés", pp. 37–70 in *Rational points on algebraic varieties*, edited by E. Peyre and Y. Tschinkel, Progr. Math. **199**, Birkhäuser, Basel, 2001. MR Zbl

[18] A. Chambert-Loir and Y. Tschinkel, "Integral points of bounded height on partial equivariant compactifications of vector groups", *Duke Math. J.* **161**:15 (2012), 2799–2836. MR Zbl

[19] A. Chambert-Loir, J. Nicaise, and J. Sebag, *Motivic integration*, Progr. Math. **325**, Birkhäuser, New York, 2018. MR Zbl

[20] J.-L. Colliot-Thélène and J.-J. Sansuc, "La descente sur les variétés rationnelles, II", *Duke Math. J.* **54**:2 (1987), 375–492. MR Zbl

[21] D. A. Cox, J. B. Little, and H. K. Schenck, *Toric varieties*, Grad. Stud. Math. **124**, Amer. Math. Soc., Providence, RI, 2011. MR Zbl

[22] R. Darda and T. Yasuda, "The Batyrev–Manin conjecture for DM stacks", *J. Eur. Math. Soc.* (online publication July 2024).

[23] O. Debarre, *Higher-dimensional algebraic geometry*, Springer, 2001. MR Zbl

[24] P. Deligne, "Théorie de Hodge, II", *Inst. Hautes Études Sci. Publ. Math.* **40** (1971), 5–57. MR Zbl

[25] P. Deligne, "La conjecture de Weil, I", *Inst. Hautes Études Sci. Publ. Math.* **43** (1974), 273–307. MR Zbl

[26] J. Denef and F. Loeser, "Germs of arcs on singular algebraic varieties and motivic integration", *Invent. Math.* **135**:1 (1999), 201–232. MR Zbl

[27] A. Grothendieck, "Éléments de géométrie algébrique, III: Étude cohomologique des faisceaux cohérents, II", *Inst. Hautes Études Sci. Publ. Math.* **17** (1963), 5–91. MR Zbl

[28] A. Grothendieck, "Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, III", *Inst. Hautes Études Sci. Publ. Math.* **28** (1966), 5–255. MR Zbl

[29] J. S. Ellenberg, A. Venkatesh, and C. Westerland, "Homological stability for Hurwitz spaces and the Cohen–Lenstra conjecture over function fields", *Ann. of Math.* (2) **183**:3 (2016), 729–786. MR Zbl

[30] J. S. Ellenberg, M. Satriano, and D. Zureick-Brown, "Heights on stacks and a generalized Batyrev–Manin–Malle conjecture", *Forum Math. Sigma* **11** (2023), art. id. e14. MR Zbl

[31] L. Faisant, "Geometric Batyrev–Manin–Peyre for equivariant compactifications of additive groups", *Beitr. Algebra Geom.* **64**:3 (2023), 783–850. MR Zbl

[32] J. Franke, Y. I. Manin, and Y. Tschinkel, "Rational points of bounded height on Fano varieties", *Invent. Math.* **95**:2 (1989), 421–435. MR Zbl

[33] W. Fulton, *Introduction to toric varieties*, Ann. of Math. Stud. **131**, Princeton Univ. Press, 1993. MR Zbl

[34] A. Grothendieck, "Techniques de construction et théorèmes d'existence en géométrie algébrique, IV: Les schémas de Hilbert", exposé 221 in *Séminaire Bourbaki*, 1960/1961, Benjamin, Amsterdam, 1966. Reprinted as pp. 249–276 in *Séminaire Bourbaki* **6**, Soc. Math. France, Paris, 1995. Zbl

[35] A. Grothendieck, *Cohomologie l-adique et fonctions L* (Séminaire de Géométrie Algébrique du Bois Marie 1965–1966), Lecture Notes in Math. **589**, Springer, 1977. MR Zbl

[36] R. Hartshorne, *Algebraic geometry*, Grad. Texts in Math. **52**, Springer, 1977. MR Zbl

[37] S. Howe, "Motivic random variables and representation stability, II: Hypersurface sections", *Adv. Math.* **350** (2019), 1267–1313. MR Zbl

[38] S. L. Kleiman, "The Picard scheme", pp. 235–321 in *Fundamental algebraic geometry*: *Grothendieck's FGA explained*, Math. Surveys Monogr. **123**, Amer. Math. Soc., Providence, RI, 2005. MR Zbl

[39] A. Landesman, R. Vakil, and M. M. Wood, "Low-degree Hurwitz stacks in the Grothendieck ring", *Compos. Math.* **160**:8 (2024), 1784–1849. MR

[40] B. Lehmann and S. Tanimoto, "On the geometry of thin exceptional sets in Manin's conjecture", *Duke Math. J.* **166**:15 (2017), 2815–2869. MR Zbl

[41] B. Lehmann and S. Tanimoto, "Geometric Manin's conjecture and rational curves", *Compos. Math.* **155**:5 (2019), 833–862. MR Zbl

[42] B. Lehmann, S. Tanimoto, and Y. Tschinkel, "Balanced line bundles on Fano varieties", *J. Reine Angew. Math.* **743** (2018), 91–131. MR Zbl

[43] B. Lehmann, A. K. Sengupta, and S. Tanimoto, "Geometric consistency of Manin's conjecture", *Compos. Math.* **158**:6 (2022), 1375–1427. MR Zbl

[44] D. Litt, "Zeta functions of curves with no rational points", *Michigan Math. J.* **64**:2 (2015), 383–395. MR Zbl

[45] E. Looijenga, "Motivic measures", exposé 874, pp. 267–297 in *Séminaire Bourbaki*, 1999/2000, Astérisque **276**, Soc. Math. France, Paris, 2002. MR Zbl

[46] J. S. Milne, *Étale cohomology*, Princeton Math. Ser. **33**, Princeton Univ. Press, 1980. MR Zbl

[47] J. Nicaise and J. Sebag, "Motivic Serre invariants, ramification, and the analytic Milnor fiber", *Invent. Math.* **168**:1 (2007), 133–173. MR Zbl

[48] T. Oda, *Convex bodies and algebraic geometry: an introduction to the theory of toric varieties*, Ergebnisse der Math. (3) **15**, Springer, 1988. MR Zbl

[49] C. A. M. Peters and J. H. M. Steenbrink, *Mixed Hodge structures*, Ergebnisse der Math. (3) **52**, Springer, 2008. MR Zbl

[50] E. Peyre, "Points de hauteur bornée sur une surface de Del Pezzo", preprint, 1993, available at https://tinyurl.com/peyredelp.

[51] E. Peyre, "Hauteurs et mesures de Tamagawa sur les variétés de Fano", *Duke Math. J.* **79**:1 (1995), 101–218. MR Zbl

[52] E. Peyre, "Points de hauteur bornée sur les variétés de drapeaux en caractéristique finie", *Acta Arith.* **152**:2 (2012), 185–216. MR Zbl

[53] E. Peyre, "Beyond heights: slopes and distribution of rational points", pp. 215–279 in *Arakelov geometry and Diophantine applications*, edited by E. Peyre and G. Rémond, Lecture Notes in Math. **2276**, Springer, 2021. MR Zbl

[54] E. Peyre, "Distribution of rational curves", online lecture, Banff Int. Res. Station, 2021, available at http://www.birs.ca/events/2021/5-day-workshops/21w5051/videos/watch/202107150738-Peyre.html.

[55] M. Pieropan, A. Smeets, S. Tanimoto, and A. Várilly-Alvarado, "Campana points of bounded height on vector group compactifications", *Proc. Lond. Math. Soc.* (3) **123**:1 (2021), 57–101. MR Zbl

[56] M. Saito, "Modules de Hodge polarisables", *Publ. Res. Inst. Math. Sci.* **24**:6 (1988), 849–995. MR Zbl

[57] M. Saito, "Mixed Hodge modules", *Publ. Res. Inst. Math. Sci.* **26**:2 (1990), 221–333. MR Zbl

[58] M. Saito, "A young person's guide to mixed Hodge modules", pp. 517–553 in *Hodge theory and L^2-analysis*, edited by L. Ji, Adv. Lect. Math. **39**, Int. Press, Somerville, MA, 2017. MR Zbl

[59] P. Salberger, "Tamagawa measures on universal torsors and points of bounded height on Fano varieties", pp. 91–258 in *Nombre et répartition de points de hauteur bornée* (Paris, 1996), edited by E. Peyre, Astérisque **251**, Soc. Math. France, Paris, 1998. MR Zbl

[60] J. Sebag, "Intégration motivique sur les schémas formels", *Bull. Soc. Math. France* **132**:1 (2004), 1–54. MR Zbl

[61] J.-P. Serre, *Cohomologie galoisienne*, Lecture Notes in Math. **5**, Springer, 1964. Zbl

[62] "The Stacks project", electronic reference, 2005–, available at http://stacks.math.columbia.edu.

[63] M. Strauch and Y. Tschinkel, "Height zeta functions of toric bundles over flag varieties", *Selecta Math.* (*N.S.*) **5**:3 (1999), 325–396. MR Zbl

[64] R. Vakil and M. M. Wood, "Discriminants in the Grothendieck ring", *Duke Math. J.* **164**:6 (2015), 1139–1185. MR Zbl

Communicated by Jean-Louis Colliot-Thélène
Received 2023-03-31 Revised 2024-05-30 Accepted 2024-07-16

lois.faisant@polytechnique.org *Institute of Science and Technology Austria, Klosterneuburg, Austria*

mathematical sciences publishers msp

ALGEBRA AND NUMBER THEORY 19:5 (2025)
https://doi.org/10.2140/ant.2025.19.967

Smooth cuboids in group theory

Joshua Maglione and Mima Stanojkovski

A smooth cuboid can be identified with a 3×3 matrix of linear forms in three variables, with coefficients in a field K, whose determinant describes a smooth cubic in the projective plane. To each such matrix one can associate a group scheme over K. We produce isomorphism invariants of these groups in terms of their *adjoint algebras*, which also give information on the number of their maximal abelian subgroups. Moreover, when K is finite, we give a characterization of the isomorphism types of the groups in terms of isomorphisms of elliptic curves and also describe their automorphism groups. We conclude by applying our results to the determination of the automorphism groups and isomorphism testing of finite p-groups of class 2 and exponent p arising in this way.

1. Introduction

The Baer correspondence is a classical way of associating an alternating bilinear map with a nilpotent group or a nilpotent Lie algebra over some field K. In the case of groups of prime-power order, this is also referred to as the Lazard correspondence and allows one to study groups in the (often easier) context of Lie algebras. As K-bilinear maps can be represented as matrices of linear forms, the study of groups arising from the Baer correspondence, moreover, affords an additional geometric point of view. In this paper, our focus is on a systematic study of the groups, which we call *E-groups*, obtained by inputting matrices of linear forms, whose determinant defines an elliptic curve in $\mathbb{P}^2_K$. This work also expands on both the results and techniques of [Stanojkovski and Voll 2021].

1.1. ***Notation.*** Throughout p denotes an odd prime number, and G a p-group. Moreover, K denotes an arbitrary field and F a finite field of characteristic p and cardinality q. Let n and d be positive integers.

MSC2020: primary 20D15, 14M12; secondary 68Q25, 11G20, 15A69, 20D45.
Keywords: finite p-groups, isomorphism testing, automorphism groups, Baer correspondence, Pfaffians, determinantal representations of cubics, elliptic curves.

For a vector $\boldsymbol{y} = (y_1, \ldots, y_d)$, we denote by $K[\boldsymbol{y}]_1$ the vector space of linear homogeneous polynomials with coefficients in K. We write $\mathrm{Mat}_n(K[\boldsymbol{y}]_1)$ for the $n \times n$ matrices of linear forms in $y_1, \ldots, y_d$ with coefficients in K.

1.2. ***Baer correspondence and Pfaffians.*** Given a skew-symmetric matrix of linear forms $\mathrm{B} \in \mathrm{Mat}_{2n}(F[\boldsymbol{y}]_1)$, the Baer correspondence associates B with a p-group $G = \mathrm{G}_{\mathrm{B}}(F)$ of exponent p and class at most 2 with underlying set F^{2n+d}. A *nondegenerate* matrix B completely prescribes the commutator relations on G and ensures that the bilinear map

$$t_G : G/\mathrm{Z}(G) \times G/\mathrm{Z}(G) \longrightarrow G' = [G, G] \tag{1-1}$$

induced by the commutator map on G is F-bilinear (so not just $\mathbb{F}_p$-bilinear). On the other hand, as we explain below, F and B can also be recovered from G.

Given a finite p-group G of class 2 and exponent p, one can construct a skew-symmetric matrix of linear forms B_G over $\mathbb{F}_p$ from the commutator map of G, for example, in terms of a minimal generating set of G. Moreover, if F is an extension of $\mathbb{F}_p$ over which the map in (1-1) is F-bilinear, then we can express B_G as a matrix $\mathrm{B} = \mathrm{B}_F$ of linear forms with coefficients in F. If B has an odd number of rows and columns, then $\det(\mathrm{B}) = 0$; otherwise, there exists a homogeneous polynomial $\mathrm{Pf}(\mathrm{B}) \in F[y_1, \ldots, y_d]$ of degree n, called the *Pfaffian*, such that $\det(\mathrm{B}) = \mathrm{Pf}(\mathrm{B})^2$. The equation $\mathrm{Pf}(\mathrm{B}) = 0$ defines a projective, degree-n hypersurface in $\mathbb{P}_F^{d-1}$, also called a *linear determinantal hypersurface*. There are now many examples in the literature, see [Stanojkovski and Voll 2021, Section 1.5.4], describing how the intrinsic geometry of B strongly influences many invariants of $\mathrm{G}_{\mathrm{B}}(F)$, like the number of conjugacy classes [Boston and Isaacs 2004; O'Brien and Voll 2015; Rossmann 2020; 2025; Rossmann and Voll 2024], faithful dimensions [Bardestani et al. 2019], automorphism group sizes [du Sautoy and Vaughan-Lee 2012; Stanojkovski and Voll 2021; Vaughan-Lee 2018], and the number of immediate descendants [du Sautoy and Vaughan-Lee 2012; Lee 2016]. We look at the Baer correspondence in more detail in Section 2.4.

1.3. ***Elliptic groups.*** The focus of this paper is, in the language of Section 1.2, to study groups $\mathrm{G}_{\mathrm{B}}(F)$ with $d = n = 3$ and $\mathrm{Pf}(\mathrm{B}) = 0$ defining an elliptic curve. Moreover, we are concerned with isomorphisms and automorphisms of abstract groups.

Definition 1.1. An *elliptic group* (abbreviated to *E-group*) is a group G that is isomorphic to $\mathrm{G}_{\mathrm{B}}(K)$, where B is a skew-symmetric matrix of linear forms over a field K such that $\mathrm{Pf}(\mathrm{B}) = 0$ defines an elliptic curve in $\mathbb{P}_K^2$. If K is finite of characteristic p, the group G is called an *elliptic p-group*.

From Definition 1.1 it follows that, if $G \cong \mathrm{G}_{\mathrm{B}}(F)$ is an E-group, then the matrix B belongs to $\mathrm{Mat}_6(F[y_1, y_2, y_3]_1)$ and $|G| = q^9$.

1.4. ***Elliptic groups and variations over the primes.*** In the study of p-groups, the groups arising from the Baer correspondence are sometimes specializations $\mathrm{G}_{\mathrm{B}}(\mathfrak{O}_k/\mathfrak{p})$ to a quotient ring or field of global unipotent group schemes G_{B} over the ring of integers $\mathfrak{O}_k$ of some number field k. In this respect, it is natural to study how the properties of the group $\mathrm{G}_{\mathrm{B}}(\mathfrak{O}_k/\mathfrak{p})$ vary with $\mathfrak{p}$. Significant concepts in this regard are those of quasipolynomiality (also called *polynomiality on residue classes*, PORC) [Higman 1960a] and *polynomiality on Frobenius sets* (i.e., polynomiality on finite Boolean combinations of sets of primes defined by the solvability of polynomial congruences; see [Stanojkovski and Voll 2021, Section 1.5.2]). Of particular relevance is Higman's PORC conjecture [1960b] about the function $\{p \in \mathbb{Z} \mid p \text{ prime}\} \to \mathbb{Z}$ enumerating the isomorphism classes of groups of order p^n for fixed n.

We recall that a function $f : \{p \in \mathbb{Z} \mid p \text{ prime}\} \to \mathbb{Z}$ is *quasipolynomial* if there exists a positive integer N and polynomials $f_0, \dots, f_{N-1} \in \mathbb{Z}[x]$ such that

$$f(p) = f_i(p) \quad \text{whenever } p \equiv i \bmod N.$$

In the context of quasipolynomiality, elliptic groups are for instance employed in [du Sautoy and Vaughan-Lee 2012] to construct a family of p-groups where the number of isomorphism classes is not a quasipolynomial in p. More specifically, the elliptic group scheme G is defined over $\mathbb{Z}$, and the family arises as a collection of central extensions of $\mathrm{G}(\mathbb{F}_p)$. In earlier work, du Sautoy [2001] showed that the number of subgroups, resp. normal subgroups, of index p^3 of $\mathrm{G}(\mathbb{Z})$, for almost all primes p, depends on the number of $\mathbb{F}_p$-points on E, written $|E(\mathbb{F}_p)|$. Du Sautoy [2002] extended this to show that, for a parametrized family $(E_D)_D$ of elliptic curves given in short Weierstrass form, (infinitely many terms of) the subgroup zeta functions of a resulting parametrized family $(\mathrm{G}_D)_D$ of E-groups depend on $|E_D(\mathbb{F}_p)|$. In the normal subgroup case, these zeta functions were made explicit by Voll [2004] as an application of more general results on smooth curves in the plane, which was further generalized in [Voll 2005] to smooth projective hypersurfaces with no lines. Recently Voll and the second author [Stanojkovski and Voll 2021] showed that the automorphism group sizes of a class of elliptic p-groups are multiples of the number of 3-torsion points of the corresponding curves. For more context, not only involving elliptic groups, we refer to [Stanojkovski and Voll 2021, Section 1.5.2].

1.5. ***Groups from points on curves.*** As we explain in Section 4, there is a straightforward way to construct examples of elliptic groups from triples (K, E, P), where K is a field, E is an elliptic curve given by a short Weierstrass equation

$$y^2 = x^3 + ax + b, \quad \text{with } a, b \in K, \tag{1-2}$$

and $P = (\lambda, \mu)$ is a point in $E(K)$. In this case, the matrix is defined as

$$\mathrm{B}_{E,P} = \begin{pmatrix} 0 & J_{E,P} \\ -J_{E,P}^{\mathrm{t}} & 0 \end{pmatrix}, \quad \text{where } J_{E,P} = \begin{pmatrix} y_1 - \lambda y_3 & y_2 - \mu y_3 & 0 \\ y_2 + \mu y_3 & \lambda y_1 + (a + \lambda^2) y_3 & y_1 \\ 0 & y_1 & -y_3 \end{pmatrix}. \tag{1-3}$$

The matrix $J_{E,P}$ is a particular instance of a *smooth cuboid*: indeed this 3×3 matrix of linear forms in three variables can be interpreted as a $(3, 3, 3)$ *cuboid* as in [Ng 1995], and it is not difficult to see that by homogenizing the *smooth* curve (1-2), one recovers precisely $\mathrm{Pf}(\mathrm{B}_{E,P}) = 0$. For simplicity, we denote the group $\mathrm{G}_{\mathrm{B}_{E,P}}(K)$ by $\mathrm{G}_{E,P}(K)$.

1.6. ***The contributions of this paper.*** The main results of this paper are Theorems A, B, D, and E. The first three results are proven in Section 5, while the fourth is given in Section 6 together with the necessary computational conventions.

If E is an elliptic curve, we indicate by $\mathcal{O}$ its identity element. If E is given by a Weierstrass equation as in (1-2), then, in projective coordinates, one has $\mathcal{O} = (0:1:0)$. If E and E' are elliptic curves in the plane with identity elements $\mathcal{O}$ and $\mathcal{O}'$ respectively, then an isomorphism $E \to E'$ is an isomorphism of projective varieties mapping $\mathcal{O}$ to $\mathcal{O}'$. The automorphism group of the elliptic curve E is denoted by $\mathrm{Aut}_{\mathcal{O}}(E)$, and its isomorphism type depends only on the j-invariant $j(E)$ of E. Moreover, if P is a point on E, then we write $\mathrm{Aut}_{\mathcal{O}}(E) \cdot P$ for the orbit of P under the action of $\mathrm{Aut}_{\mathcal{O}}(E)$ on E. For a positive integer n, the n-torsion subgroup of E is denoted by $E[n]$. If $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$ and E is an elliptic curve defined by $f = 0$ over F, then $\sigma(E)$ is defined by the polynomial $\sigma(f)$, where σ acts on the coefficients of f. Moreover, if $P = (a:b:c) \in E(F)$ then $\sigma(P) \in \sigma(E)(F)$ is defined by $\sigma(P) = (\sigma(a):\sigma(b):\sigma(c))$.

The following two theorems greatly generalize Theorem 1.1 from [Stanojkovski and Voll 2021].

Theorem A. *Let F be a finite field with $\mathrm{char}(F) = p \geqslant 5$. Let, moreover, E and E' be elliptic curves in $\mathbb{P}^2_F$ given by Weierstrass equations, and let $P \in E(F) \setminus \{\mathcal{O}\}$ and $P' \in E'(F) \setminus \{\mathcal{O}'\}$. Then the following are equivalent*:

(1) *The groups $\mathrm{G}_{E,P}(F)$ and $\mathrm{G}_{E',P'}(F)$ are isomorphic.*

(2) *There exist $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$ and an isomorphism $\varphi : E' \to \sigma(E)$ of elliptic curves such that $\varphi(P') = \sigma(P)$.*

Theorem B. *Let F be a field with $\mathrm{char}(F) = p \geqslant 5$ and cardinality p^e. Let, moreover, E be an elliptic curve in $\mathbb{P}^2_F$ given by a short Weierstrass equation, and let $P \in E(F) \setminus \{\mathcal{O}\}$. Then there exists a subgroup S of $\mathrm{Gal}(F/\mathbb{F}_p)$ such that*

$$\frac{|\mathrm{Aut}(\mathrm{G}_{E,P}(F))|}{p^{18e^2}} = |S| \cdot |E[3](F)| \cdot \frac{|\mathrm{Aut}_{\mathcal{O}}(E)|}{|\mathrm{Aut}_{\mathcal{O}}(E) \cdot P|} \cdot \begin{cases} |\mathrm{GL}_2(F)| & \textit{if } P \in E[2](F), \\ 2(p^e - 1)^2 & \textit{otherwise.} \end{cases}$$

For the precise definition of the subgroup S from Theorem B we refer the reader to (2-5); see also Theorem 2.15 and, for an example, Remark 5.11. For the groups $\mathrm{G}_{E,P}(F)$, a generator of the subgroup S can be computed efficiently. This is not necessarily the case for groups $\mathrm{G}_{\mathrm{B}}(F)$, where B is arbitrary.

Combining Theorem B with [Weinstein 2016, Theorem 2.2.1] and the classification from [Bandini and Paladino 2012], one obtains that, although the function in (1-4) counting the number of automorphisms of the family $(\mathrm{G}_{E,P}(\mathbb{F}_p))_p$ is polynomial on Frobenius sets, it is almost never quasipolynomial; see Corollary C and Remark 1.2 for some more detail.

Corollary C. *Let E be an elliptic curve given by the Weierstrass equation*

$$y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{Q},$$

and $P \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$. Over the set of primes for which E has good reduction, the function

$$p \longmapsto |\mathrm{Aut}(\mathrm{G}_{E,P}(\mathbb{F}_p))| \tag{1-4}$$

is polynomial on Frobenius sets and is quasipolynomial precisely in the following cases:

(1) $a = 0$ *and there exists* $\beta \in \mathbb{Q}^\times$ *such that* $b = 2\beta^3$.

(2) $b \neq 0$ *and there exist* $h, \ell \in \mathbb{Q}^\times$ *such that*

$$h^3 = -16(4a^3 + 27b^2) \quad \textit{and} \quad \ell^2 = \tfrac{1}{3}(-h - 4a)$$

and one of the following holds:

(a) *There exist* $\alpha, \beta, m \in \mathbb{Q}$ *with* $\beta \neq 0$ *that satisfy*

$$m^2 = \alpha^2 + 3\beta^2, \quad a = -3m^2 + 6\beta m, \quad b = 2\alpha^3 + 12\alpha\beta^2 - 6\alpha\beta m.$$

(b) *For* $\gamma = -\ell^2 - 4a - 8b/\ell$, *the element* $-\ell^3 - 8a\ell - 16b + (-\ell^2 + 4b/\ell)\sqrt{\gamma}$ *is a square in the splitting field of* $(x^2 - \gamma)(x^3 - 1)$.

Remark 1.2. The case distinction in Corollary C comes from the explicit description, given in [Bandini and Paladino 2012], of curves E in short Weierstrass form for which the Galois group of

$$\mathbb{Q}(E[3]) = \mathbb{Q}(\{x, y \mid (x, y) \in E[3](\mathbb{Q}^{\mathrm{sep}})\})$$

is abelian. Thanks to [Weinstein 2016, Theorem 2.2.1], i.e., the abelian polynomial theorem from [Wyman 1972], $\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})$ is abelian if and only if the function $p \mapsto |E[3](\mathbb{F}_p)|$ is quasipolynomial. With one of the classical definitions of heights for elliptic curves (defined for short Weierstrass equations as $\mathrm{ht}(E) = \max\{|a|^3, |b|^2\}$), Theorem 1 from [Duke 1997] implies that the density of isomorphism classes of rational elliptic curves for which $\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})$ is abelian is 0. In particular, this tells us that examples of groups $\mathrm{G}_{E,P}$ as in Corollary C for which $p \mapsto |\mathrm{Aut}(\mathrm{G}_{E,P}(\mathbb{F}_p))|$ is quasipolynomial are very rare.

Theorems A and B and Corollary C concern the groups from Section 1.5, which might not appear to be representative of the class of E-groups. However, up to equivalence, which we define in Section 4, these groups seem to occur with probability $\frac{1}{2}$ in the precise sense explained in Section 6.4.

One of the main tools we use to extract the core geometric properties of the groups $\mathrm{G}_{E,P}(F)$ is the adjoint algebra, which has recently been used to understand the structure of p-groups [Brooksbank et al. 2019; Brooksbank and Wilson 2012]. We define adjoint algebras in Section 2.2, but remark that their isomorphism types are polynomial-time computable isomorphism invariants of p-groups since they are constructed by solving linear systems. With the notation from Section 2.2, Theorem D follows from combining the more general Theorem 3.13 with Proposition 5.1. The relevance of $\mathcal{O}$ being a flex point is explained in Remark 4.9. In Theorem D, we use the fact that a smooth cubic in the projective plane with a marked rational point has the structure of an elliptic curve.

Theorem D. *Let* K *be a field with* $6K = K$. *Let, moreover,* $\mathrm{B} \in \mathrm{Mat}_6(K[y_1, y_2, y_3]_1)$ *be skew-symmetric with* $\mathrm{Pf}(\mathrm{B}) = 0$ *defining a smooth cubic* E *in* $\mathbb{P}^2_K$ *with a flex point* $\mathcal{O} \in E(K)$, *and set* $G = \mathrm{G}_{\mathrm{B}}(K)$. *Then the following hold*:

(1) *There is* $P \in E(K) \setminus E[2](K)$ *with* $G \cong \mathrm{G}_{E,P}(K)$ *if and only if* $\mathrm{Adj}(\mathrm{B}) \cong \boldsymbol{X}_1(K)$.

(2) *There is* $P \in E[2](K) \setminus \{\mathcal{O}\}$ *with* $G \cong \mathrm{G}_{E,P}(K)$ *if and only if* $\mathrm{Adj}(\mathrm{B}) \cong \boldsymbol{S}_2(K)$.

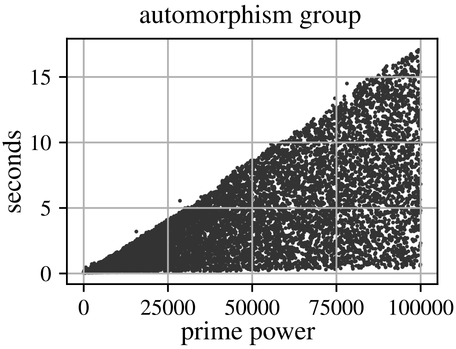

Figure 1. The runtimes of a Magma implementation of Theorem E on the prime powers p^e, for $p \notin \{2, 3\}$, up to 10^5.

Our next main theorem allows us to constructively recognize elliptic p-groups and to decide whether two such groups are isomorphic. Deciding whether two groups of order n are isomorphic uses, in the worst case, $n^{O(\log n)}$ operations [Miller 1978], which is just a brute-force search, and the same timing prevails for constructing generators of the automorphism group. General purpose algorithms, like [Cannon and Holt 2003; Eick et al. 2002], use induction by constructing known characteristic subgroups, which are subgroups fixed by the automorphism group. Even with recent tools to uncover more characteristic subgroups [Brooksbank et al. 2019; Maglione 2017; 2021; Wilson 2013], elliptic p-groups evade capture. Prior to this work, it seems that the best general purpose algorithm [Ivanyos and Qiao 2019], together with the reduction from Theorem 2.15, would construct generators for their automorphism group using $O(|G|^{8/9} \log |G|)$ operations (without Theorem 2.15 the number of operations is $|G|^{O(\log |G|)}$). We significantly improve upon this timing.

Theorem E. *There are algorithms that, given groups G_1 and G_2 of order p^{9m}, with $p \geqslant 5$,*

(i) *decide if, for each $i \in \{1, 2\}$ and field F of cardinality p^m, there exist*
   - *an elliptic curve E_i given by a short Weierstrass equation with F-coefficients,*
   - *a point $P_i \in E_i(F) \setminus \{(0 : 1 : 0)\}$*

   such that G_i is isomorphic to $\mathrm{G}_{E_i,P_i}(F)$, and if so

(ii) *return the possibly empty coset of isomorphisms $G_1 \to G_2$.*

The algorithm for (i) is of Las Vegas type and uses $O(m^7 + m \log p)$ field operations. The algorithm for (ii) uses $O(p^m)$ field operations.

Some of the algorithms we use are of *Las Vegas* type. These are randomized algorithms that only return correct answers and for some probability, determined by a user-prescribed upper bound, terminate without an answer.

In Theorem E(ii), if the groups are isomorphic, the algorithm returns an isomorphism $G_1 \to G_2$ together with a generating set for $\mathrm{Aut}(G_1)$. In order to demonstrate the efficacy of Theorem E, we have constructed generators for the automorphism groups of several instances of $\mathrm{G}_{E,P}(F)$, built uniformly at random as explained in Section 6.4.

Remark 1.3. As the careful reader has noticed, in our main theorems p is at least 5. The prime 2 is excluded to begin with because there does not exist a group of class 2 and exponent 2. Moreover, if $p \in \{2, 3\}$, elliptic curves need not admit a short Weierstrass form and, in this case, their 3×3 determinantal representations might not be equivalent to any $J_{E,P}$; see Sections 1.5 and 4.2.

2. Tensors and unipotent group schemes

Fix finite-dimensional K-vector spaces U, W, V, V', and T. By a 3-*tensor* (or simply *tensor*, throughout), we mean a K-bilinear map $t : V \times V' \to T$, that is, for all $u, v \in V$, all $u', v' \in V'$, and all $\lambda, \mu \in K$, the following holds:

$$t(u+\lambda v, u'+\mu v') = t(u, u') + \lambda t(v, u') + \mu t(u, v') + \lambda\mu t(v, v').$$

A tensor $t : V \times V \to T$ is *alternating* if, for all $v \in V$, one has $t(v, v) = 0$.

Definition 2.1. Let $t : V \times V \to T$ be a tensor. A subspace $U \leqslant V$ is *totally isotropic* with respect to t if, for every $u, u' \in U$, one has $t(u, u') = 0$, in other words if the restriction of t to $U \times U$ is the zero map.

Note that, if $t : V \times V \to T$ is alternating, every line in V is totally isotropic.

Definition 2.2. An alternating tensor $t : V \times V \to T$ is *isotropically decomposable* if there exist totally isotropic subspaces $U, W \leqslant V$ such that $V = U \oplus W$.

By choosing bases for U, W, and T, we may write $t : U \times W \to T$ as a matrix of linear forms or as a system of forms, that is, a sequence of matrices over K. Let $\{e_1, \dots, e_m\}$, $\{f_1, \dots, f_n\}$, and $\{g_1, \dots, g_d\}$ be bases for U, W, and T, respectively. For $i \in [m]$, $j \in [n]$, and $k \in [d]$, define $b_{ij}^{(k)} \in K$ such that

$$t(e_i, f_j) = \sum_{k=1}^{d} b_{ij}^{(k)} g_k.$$

The matrix of linear forms $\mathrm{B} = (b_{ij}) \in \mathrm{Mat}_{m\times n}(K[\boldsymbol{y}]_1)$ corresponding to t is given by

$$b_{ij} = \sum_{k=1}^{d} b_{ij}^{(k)} y_k.$$

In the sequel we will always assume that a tensor $t : U \times W \to T$ is given together with a choice of bases for U, W, T. If $t : V \times V \to T$ is an alternating tensor, we take the same basis on the first and second copies of V and, if V is given by an isotropic decomposition $U \oplus W$, we assume that the basis on V is the composite of a basis of U and a basis of W.

Remark 2.3. Since every 3-tensor t is, with respect to a choice of bases, given by a matrix B of linear forms, throughout the paper everything that is defined for tensors will also apply to matrices of linear forms.

If $t : V \times V \to T$ is an alternating tensor, just as matrices of linear forms associated with t vary as the bases for V and T vary, so does the corresponding Pfaffian. We will say that $\mathrm{Pf}(t) \in K[\boldsymbol{y}]$ is a Pfaffian for t if there exists some choice of bases for V and T whose associated matrix of linear forms B satisfies $\mathrm{Pf}(t) = \mathrm{Pf}(\mathrm{B})$.

Definition 2.4. A tensor $t : U \times W \to T$ is *nondegenerate* if the following are satisfied:

(i) $t(u, W) = 0$ implies $u = 0$.

(ii) $t(U, w) = 0$ implies $w = 0$.

We say that t is *full* if $t(U, W) = T$. A tensor t is *fully nondegenerate* if t is both nondegenerate and full.

2.1. ***Maps between 3-tensors.*** In this section we present various types of maps between tensors that we will exploit in later sections for the determination of isomorphisms between groups and Lie algebras. Many of these definitions can be found in [Brooksbank et al. 2019].

Definition 2.5. Two K-tensors $s : U \times W \to T$ and $t : U' \times W' \to T'$ are *equivalent* if $T = T'$ and there exist K-linear isomorphisms $\alpha : U \to U'$ and $\beta : W \to W'$ such that for all $u \in U$ and all $w \in W$, one has $t(\alpha(u), \beta(w)) = s(u, w)$; equivalently, the following diagram commutes:

$$\begin{array}{ccc} U \times W & \xrightarrow{\quad s \quad} & T \\ {\scriptstyle\alpha}\downarrow \quad \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle \mathrm{id}} \\ U' \times W' & \xrightarrow{\quad t \quad} & T' \end{array}$$

In the case $U = W$, $U' = W'$, and $\alpha = \beta$, we say the two tensors are *isometric*.

Relevant to our context is a different form of equivalence from Definition 2.5, namely, *pseudoisometry*. Isomorphisms of groups induce this weaker equivalence, which is considered in more detail in the next section.

Definition 2.6. Let $L \subset K$ be a subfield and let $s : V \times V \to T$ and $t : V' \times V' \to T'$ be K-tensors. An *L-pseudoisometry* from s to t is a pair (α, β) such that $\alpha : V \to V'$ and $\beta : T \to T'$ are L-linear isomorphisms and, for all $u, v \in V$, the equality $t(\alpha(u), \alpha(v)) = \beta(s(u, v))$ holds; equivalently the following diagram commutes:

$$\begin{array}{ccc} V \times V & \xrightarrow{\quad s \quad} & T \\ {\scriptstyle\alpha}\downarrow \quad \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle \beta} \\ V' \times V' & \xrightarrow{\quad t \quad} & T' \end{array}$$

The set of L-pseudoisometries from s to t is denoted by $\Psi\mathrm{Isom}_L(s, t)$ and, if $\Psi\mathrm{Isom}_L(s, t)$ is nonempty, s and t are called *L-pseudoisometric*. If $s = t$, then the group of L-pseudoisometries of t is denoted by $\Psi\mathrm{Isom}_L(t)$ instead of $\Psi\mathrm{Isom}_L(t, t)$.

Remark 2.7. We emphasize that $\Psi\mathrm{Isom}_L(s, t)$ has more structure than an arbitrary set. Indeed, identifying V with V' and T with T', we can view $\Psi\mathrm{Isom}_L(s, t)$ both as a left $\Psi\mathrm{Isom}_L(t)$-coset and a right $\Psi\mathrm{Isom}_L(s)$-coset of $\mathrm{GL}_L(V) \times \mathrm{GL}_L(T)$. That is, if $(\alpha, \beta) \in \Psi\mathrm{Isom}_L(s, t)$, while $(\gamma, \delta) \in \Psi\mathrm{Isom}_L(t)$ and $(\varepsilon, \zeta) \in \Psi\mathrm{Isom}_L(s)$, then

$$(\gamma\alpha, \delta\beta), (\alpha\varepsilon, \beta\zeta) \in \Psi\mathrm{Isom}_L(s, t).$$

Because $\Psi\mathrm{Isom}_L(t) \cdot (\alpha, \beta) = (\alpha, \beta) \cdot \Psi\mathrm{Isom}_L(s) = \Psi\mathrm{Isom}_L(s, t)$, we will just refer to $\Psi\mathrm{Isom}_L(s, t)$ as a coset.

Remark 2.8. If G is a p-group with central elementary abelian derived subgroup, then its commutator determines a fully nondegenerate $\mathbb{F}_p$-tensor $t_G : G/\mathrm{Z}(G) \times G/\mathrm{Z}(G) \to G'$ given by $(g\,\mathrm{Z}(G), h\,\mathrm{Z}(G)) \mapsto [g, h]$. If G and H are two such p-groups whose tensors t_G and t_H are $\mathbb{F}_p$-pseudoisometric, then G and H are *isoclinic*; see [Hall 1940]. If, in addition, both G and H have exponent p, then G and H are isomorphic.

Definition 2.9. Let $L \subset K$ be a subfield and let $s : U \times W \to T$ and $t : U' \times W' \to T'$ be K-tensors. An *L-isotopism* from s to t is a triple (α, β, γ) such that $\alpha : U \to U'$, $\beta : W \to W'$, and $\gamma : T \to T'$ are L-linear isomorphisms and, for all $(u, w) \in U \times W$, the equality $t(\alpha(u), \beta(w)) = \gamma(s(u, w))$ holds; equivalently the following diagram commutes:

$$\begin{array}{ccc} U \times W & \xrightarrow{\quad s \quad} & T \\ {\scriptstyle\alpha}\downarrow \quad \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} \\ U' \times W' & \xrightarrow{\quad t \quad} & T' \end{array}$$

If $s = t$, then the triple (α, β, γ) is called an *L-autotopism* of t and the group of L-autotopisms of t is denoted by $\mathrm{Auto}_L(t)$.

Remark 2.10. Assume $\mathrm{M} \in \mathrm{Mat}_n(F[y_1, \dots, y_d]_1)$ realizes the tensor $\tilde{t} : U \times W \to T$. Then the autotopism group of M can be described as

$$\mathrm{Auto}_F(\mathrm{M}) = \{(X, Y, Z) \in \mathrm{GL}_n(F) \times \mathrm{GL}_n(F) \times \mathrm{GL}_d(F) \mid X^{\mathrm{t}}\,\mathrm{M}(\boldsymbol{y})Y = \mathrm{M}(Z\boldsymbol{y})\}.$$

In particular, if $U \oplus W = V$ is an isotropic decomposition for the tensor $t : V \times V \to T$ inducing $\tilde{t}$ and with associated matrix B, then every triple $(X, Y, Z) \in \mathrm{Auto}_F(\tilde{t})$ yields an element of $\Psi\mathrm{Isom}_F(t)$ via

$$\begin{aligned} \begin{pmatrix} X^{\mathrm{t}} & 0 \\ 0 & Y^{\mathrm{t}} \end{pmatrix} \mathrm{B} \begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix} &= \begin{pmatrix} X^{\mathrm{t}} & 0 \\ 0 & Y^{\mathrm{t}} \end{pmatrix} \begin{pmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & 0 \end{pmatrix} \begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix} \\ &= \begin{pmatrix} 0 & X^{\mathrm{t}}\mathrm{M}(\boldsymbol{y})Y \\ -Y^{\mathrm{t}}\mathrm{M}(\boldsymbol{y})^{\mathrm{t}}X & 0 \end{pmatrix} = \begin{pmatrix} 0 & \mathrm{M}(Z\boldsymbol{y}) \\ -\mathrm{M}(Z\boldsymbol{y})^{\mathrm{t}} & 0 \end{pmatrix} = \mathrm{B}(Z\boldsymbol{y}). \end{aligned}$$

2.2. *Algebras associated to 3-tensors.* Throughout this subsection, we use tensors rather than matrices of linear forms, but the content applies to both. These algebras are also found in [Brooksbank et al. 2019].

Let $t : U \times W \to T$ be a K-tensor. The *centroid* of t is the K-subalgebra of

$$\mathcal{E} = \mathrm{End}_K(U) \times \mathrm{End}_K(W) \times \mathrm{End}_K(T)$$

defined by

$$\mathrm{Cent}(t) = \{(\alpha, \beta, \gamma) \in \mathcal{E} \mid \forall u \in U,\ \forall w \in W,\ t(\alpha(u), w) = t(u, \beta(w)) = \gamma(t(u, w))\}. \tag{2-1}$$

Let $c = (\alpha, \beta, \gamma) \in \mathrm{Cent}(t)$, and suppose $\mathrm{Cent}(t)$ acts on U, W, and T by respectively applying α, β, and γ. Then, for each pair $(u, w) \in U \times W$, we have

$$c \cdot t(u, w) = t(c \cdot u, w) = t(u, c \cdot w).$$

Thus, t is $\mathrm{Cent}(t)$-bilinear. Additionally, the centroid satisfies the following universal property. If t is also A-bilinear for some K-algebra A, then there is a unique ring homomorphism $A \to \mathrm{Cent}(t)$ such that the action of A on U, W, and T is that of $\mathrm{Cent}(t)$; see [Wilson 2012, Lemma 6.8(ii)].

Lemma 2.11. *If t is fully nondegenerate, then* $\mathrm{Cent}(t)$ *is commutative.*

Proof. Take $(\alpha, \beta, \gamma), (\alpha', \beta', \gamma') \in \mathrm{Cent}(t)$; then, for all $u \in U$ and all $w \in W$,

$$t(\alpha\alpha'(u), w) = t(\alpha'(u), \beta(w)) = \gamma'(t(u, \beta(w))) = \gamma'(t(\alpha(u), w)) = t(\alpha'\alpha(u), w).$$

This implies that $t((\alpha\alpha' - \alpha'\alpha)(u), w) = 0$, and since t is fully nondegenerate, it follows that $\alpha\alpha' = \alpha'\alpha$. Similar arguments hold for the other coordinates as well. □

For a ring R, we denote by R^{op} the *opposite ring* of R, with opposite product given by $x \cdot_{\mathrm{op}} y = yx$ for all $x, y \in R$. The *adjoint algebra* of t is the K-algebra

$$\mathrm{Adj}(t) = \{(\alpha, \beta) \in \mathrm{End}(U) \times \mathrm{End}(W)^{\mathrm{op}} \mid \forall u \in U,\ \forall w \in W,\ t(\alpha(u), w) = t(u, \beta(w))\}. \tag{2-2}$$

If $t : V \times V \to T$ is alternating, then the natural anti-isomorphism $* : \mathrm{Adj}(t) \to \mathrm{Adj}(t)^{\mathrm{op}}$, given by $(\alpha, \beta) \mapsto (\beta, \alpha)$, makes $\mathrm{Adj}(t)$ a $*$-*algebra*; see Section 2.3. To see this, let $(\alpha, \beta) \in \mathrm{Adj}(t)$. Then, for all $u, v \in V$, one has

$$t(\beta(u), v) = -t(v, \beta(u)) = -t(\alpha(v), u) = t(u, \alpha(v)),$$

from which it follows that $(\beta, \alpha) \in \mathrm{Adj}(t)^{\mathrm{op}}$.

We define a module version of the adjoint algebra. For this, let $t : U \times W \to T$ and $s : U' \times W' \to T'$ be K-tensors. Identifying T with T', the *adjoint module* of s and t is

$$\mathrm{Adj}(s, t) = \{(\alpha, \beta) \in \mathrm{Hom}(U', U) \times \mathrm{Hom}(W, W') \mid \forall u' \in U',\ \forall w \in W,\ t(\alpha(u'), w) = s(u', \beta(w))\}. \tag{2-3}$$

We remark that $\mathrm{Adj}(s, t)$ is a left $\mathrm{Adj}(t)$-module and a right $\mathrm{Adj}(s)$-module via defining

$$(\gamma, \delta) \cdot (\alpha, \beta) = (\gamma\alpha, \beta\delta) \quad \text{and} \quad (\alpha, \beta) \cdot (\varepsilon, \zeta) = (\alpha\varepsilon, \zeta\beta)$$

for all $(\alpha, \beta) \in \mathrm{Adj}(s, t)$, all $(\gamma, \delta) \in \mathrm{Adj}(t)$, and all $(\varepsilon, \zeta) \in \mathrm{Adj}(s)$.

The key computational advantage to the vector spaces in (2-1), (2-2), and (2-3) is that they are simple to compute, since they are given by a system of linear equations, and carry useful structural information. Although they are computed by solving a linear system, this is the computational bottleneck for Theorem E(i).

2.3. ***Structure of Artinian $*$-rings.*** We will need specific structural information about $*$-rings. We follow the treatment given in [Brooksbank and Wilson 2012, Section 2] and, only in Section 2.3, use right action in accordance to the existing literature on $*$-algebras.

A $*$-*ring* is a pair $(A, *)$, where A is an Artinian ring and $* : A \to A^{\mathrm{op}}$ is a ring homomorphism such that, for all $a \in A$, the equality $(a^*)^* = a$ holds. A $*$-*homomorphism* $\varphi : (A, *_A) \to (B, *_B)$ is a ring homomorphism $A \to B$ such that $\varphi(a^{*_A}) = \varphi(a)^{*_B}$. A $*$-*ideal* is an ideal I of A such that $I^* = I$. A $*$-ring A is *simple* if its only $*$-ideals are 0 and A. Moreover, from [loc. cit., Theorem 2.1], the Jacobson radical of a $*$-ring is a $*$-ideal, and the quotient by the Jacobson radical R decomposes into a direct sum of simple $*$-rings. If A is a $*$-ring with Jacobson radical R such that $S = A/R$, then we write $A \cong R \rtimes S$.

For finite fields of odd characteristic, we can completely describe the simple $*$-rings. Using the notation from [loc. cit.], we have the following classification.

Theorem 2.12 [Brooksbank and Wilson 2012, Theorem 2.2]. *Let $(A, *)$ be a simple $*$-algebra over F. Then there is a positive integer n such that $(A, *)$ is $*$-isomorphic to one of the following*:

(i) $\boldsymbol{O}_n^{\varepsilon}(F) = (\mathrm{Mat}_n(F), X \mapsto DX^{\mathrm{t}}D^{-1})$, *where D is one of the diagonal matrices in $\{I_n, I_{n-1} \oplus \omega\}$ for a nonsquare $\omega \in F$, and $\varepsilon \in \{+, -, \circ\}$ according to whether the form $(u, v) \mapsto u^{\mathrm{t}}Dv$ induces an orthogonal geometry of type ε.*

(ii) $\boldsymbol{U}_n(L) = (\mathrm{Mat}_n(L), X \mapsto \overline{X}^{\mathrm{t}})$, *where $\alpha \mapsto \bar{\alpha}$ is the nontrivial Galois automorphism of the degree-2 extension L/F.*

(iii) $\boldsymbol{S}_{2n}(F) = (\mathrm{Mat}_{2n}(F), X \mapsto JX^{\mathrm{t}}J^{-1})$, *where J is the n-fold direct sum of $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.*

(iv) $\boldsymbol{X}_n(F) = (\mathrm{Mat}_n(F) \oplus \mathrm{Mat}_n(F), (X, Y) \mapsto (Y^{\mathrm{t}}, X^{\mathrm{t}}))$.

We stress that in this paper we are mostly concerned with (iii) and (iv) from the last classification. We mention (i) primarily for Theorem 3.13 for the values $n = 1$ and $\varepsilon = \circ$, in which case $\boldsymbol{O}_n^{\varepsilon}(K) = \boldsymbol{O}_1^{\varepsilon}(K)$ is a field isomorphic to K.

2.4. ***Unipotent group schemes and nilpotent Lie algebras from 3-tensors.*** Let $t : V \times V \to T$ be an alternating K-tensor and assume that $K = 2K$. Then the set $V \oplus T$, with multiplication given by

$$(v, w) \cdot (v', w') = \left(v + v', w + w' + \tfrac{1}{2}t(v, v')\right),$$

is a nilpotent group (of class at most 2), called the *Baer group associated with t*. The commutator map of $\mathrm{G}_t(K) = (V \oplus T, \cdot)$ is given by

$$((v, w), (v', w')) \longmapsto [(v, w), (v', w')] = (0, t(v, v')).$$

Interpreting the last commutator map as a Lie bracket, the Lie algebra $\mathfrak{g}_t(K)$ associated to t is precisely $V \oplus T$ together with this Lie product. We note that this construction is the same as in [Stanojkovski and Voll 2021], where t is assumed to be isotropically decomposable (and the associated half-matrix B to be symmetric).

The (Baer) group scheme G_t associated to t is determined in the following way — without requiring $K = 2K$; see [Rossmann and Voll 2024, Section 2.4]. Fix bases $(v_1, \dots, v_n)$ and $(w_1, \dots, w_d)$ of V and T respectively. Let L be an associative commutative unital K-algebra, and identify $\mathrm{G}_t(L)$ with the set $(V \otimes_K L) \oplus (T \otimes_K L)$. For $\ell \in L$, we abbreviate $v_i \otimes \ell$ and $w_j \otimes \ell$ to ℓv_i and ℓw_j in $V \otimes_K L$ and $T \otimes_K L$ respectively.

We define the multiplication $\bullet$ on $\mathrm{G}_t(L)$ as follows. For $v = a_1v_1 + \dots + a_nv_n$ and $v' = b_1v_1 + \dots + b_nv_n$ with $a_1, \dots, a_n, b_1, \dots, b_n \in L$, we set

$$v \bullet v' = v + v' - \sum_{1 \leqslant i < j \leqslant n} a_j b_i \cdot t(v_i, v_j).$$

Additionally, for all $x \in \mathrm{G}_t(L)$ and $w \in T \otimes_K L$, define $x \bullet w = x + w = w \bullet x$. This determines the group structure and is independent of the chosen bases: shall the tensors be given in terms of a matrix B of linear forms, we will write $\mathrm{G}_{\mathrm{B}}(L)$ for the resulting group. The last construction defines a representable functor from the category of K-algebras (associative, commutative, and unital) to groups; namely, via $L \mapsto ((V \otimes_K L) \oplus (T \otimes_K L), \bullet)$. Concretely, if $K = 2K$, then $\mathrm{G}_t(K)$ is isomorphic to the Baer group associated with t since the two groups yield pseudoisometric commutator tensors. One approaches Lie algebras in a similar fashion.

Our main source of unipotent group schemes comes from linear determinantal representations of elliptic curves, but this change of perspective from determinantal representations to nilpotent groups comes with a few subtleties. For example, the specific Pfaffian hypersurface associated to the linear Pfaffian representation is an invariant in the equivalence class as given in Definition 3.4. However, for nilpotent groups of class 2, the Pfaffian hypersurface is not an invariant of the group — the next theorem, essentially due to Baer [1938], illustrates this point.

Theorem 2.13. *Let $s : V \times V \to T$ and $t : V' \times V' \to T'$ be alternating, full K-tensors, where* $\mathrm{char}(K) = p > 2$. *Then the following hold*:

(1) *The K-Lie algebras $\mathfrak{g}_s(K)$ and $\mathfrak{g}_t(K)$ are isomorphic if and only if s and t are K-pseudoisometric.*

(2) *The groups $\mathrm{G}_s(K)$ and $\mathrm{G}_t(K)$ are isomorphic if and only if s and t are $\mathbb{F}_p$-pseudoisometric.*

Proof. We prove the claim for groups as the Lie algebras statement is similar. Since s and t are full, the commutator subgroups of $\mathrm{G}_s(K)$ and $\mathrm{G}_t(K)$ are equal to $0 \oplus T$ and $0 \oplus T'$, respectively. An isomorphism from $\mathrm{G}_s(K)$ to $\mathrm{G}_t(K)$ induces an isomorphism of their commutator subgroups and their abelianizations. These yield $\mathbb{F}_p$-linear isomorphisms $V \to V'$ and $T \to T'$, so s and t are $\mathbb{F}_p$-pseudoisometric.

Conversely if $\alpha : V \to V'$ and $\beta : T \to T'$ are $\mathbb{F}_p$-linear isomorphisms with $(\alpha, \beta) \in \Psi\mathrm{Isom}_{\mathbb{F}_p}(s, t)$, then, for all $v, v' \in V$ and all $w, w' \in T$, the following holds:

$$\begin{aligned}(\alpha(v), \beta(w)) \cdot (\alpha(v'), \beta(w')) &= \big(\alpha(v + v'), \beta(w + w') + \tfrac{1}{2} t(\alpha(v), \alpha(v'))\big) \\ &= \big(\alpha(v + v'), \beta\big(w + w' + \tfrac{1}{2} s(v, v')\big)\big).\end{aligned}$$

In other words, $\mathrm{diag}(\alpha, \beta)$ yields an isomorphism of groups. □

For an F-vector space V with a fixed basis $\mathcal{B}$, we extend the action of $\mathrm{Gal}(F/\mathbb{F}_p)$ from F to V in the following way:

$$\mathrm{Gal}(F/\mathbb{F}_p) \longrightarrow \mathrm{Aut}_{\mathbb{F}_p}(V), \quad \sigma \longmapsto \Big(u = \sum_{b \in \mathcal{B}} c_b b \longmapsto \sigma(u) = \sum_{b \in \mathcal{B}} \sigma(c_b) b\Big).$$

Definition 2.14. Let $t : V \times V \to T$ be an F-tensor and let $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$. For a fixed choice of bases for V and T, the tensor ${}^{\sigma}t : V \times V \to T$ is defined by

$${}^{\sigma}t(u, v) = \sigma t(\sigma^{-1}(u), \sigma^{-1}(v)).$$

On the level of matrices of linear forms, if $t(u, v) = u^{\mathrm{t}}\,\mathrm{B}\,v$, then ${}^{\sigma}t(u, v) = u^{\mathrm{t}}(\sigma(\mathrm{B}))v$, where the action of σ on B is entrywise, so $\sigma(\mathrm{B}) = (\sigma(b_{ij}))$.

The action of $\mathrm{Gal}(F/\mathbb{F}_p)$ on an F-tensor $t : V \times V \to T$ depends on the choice of F-bases for V and T, and different choices of bases may yield different F-pseudoisometry classes. This shall not concern us because this does not happen on the level of $\mathbb{F}_p$-pseudoisometries — our primary focus when working with $\mathrm{Gal}(F/\mathbb{F}_p)$ — as σ is $\mathbb{F}_p$-linear.

The next theorem has many appearances in different guises [Brooksbank et al. 2017; Stanojkovski and Voll 2021; Wilson 2017], and it describes the group $\Psi\mathrm{Isom}_{\mathbb{F}_p}(t)$ as a subgroup of a direct product of F-semilinear groups. The *F-semilinear group* of V is $\mathrm{GL}_F(V)\rtimes\mathrm{Gal}(F/\mathbb{F}_p)$, and, for a fixed basis of V, it acts on V by mapping v to $(X,\sigma)v = X\sigma(v)$. For $(X,\sigma),(Y,\tau)\in\mathrm{GL}_F(V)\rtimes\mathrm{Gal}(F/\mathbb{F}_p)$, we compute that $(X,\sigma)\cdot(Y,\tau) = (X\sigma Y\sigma^{-1},\sigma\tau)$, and we extend this operation to the larger $(\mathrm{GL}_F(V)\times\mathrm{GL}_F(T))\rtimes\mathrm{Gal}(F/\mathbb{F}_p)$ by setting

$$(\alpha,\beta,\sigma)\cdot(\gamma,\delta,\tau) = (\alpha\sigma\gamma\sigma^{-1},\beta\sigma\delta\sigma^{-1},\sigma\tau). \tag{2-4}$$

Then the *F-semilinear pseudoisometry group* of t is

$$\mathrm{S\Psi I}_{F/\mathbb{F}_p}(t) = \{(\alpha,\beta,\sigma)\in(\mathrm{GL}_F(V)\times\mathrm{GL}_F(T))\rtimes\mathrm{Gal}(F/\mathbb{F}_p) \mid (\alpha,\beta)\in\Psi\mathrm{Isom}_F({}^{\sigma}t,t)\}$$

with the induced multiplication. Note that, though the definition of $\mathrm{S\Psi I}_{F/\mathbb{F}_p}(t)$ we gave clearly depends on a choice of bases of V and T, its isomorphism type does not. We will write

$$\mathrm{Gal}_t(F/\mathbb{F}_p) = \{\sigma\in\mathrm{Gal}(F/\mathbb{F}_p) \mid \Psi\mathrm{Isom}_F({}^{\sigma}t,t)\neq\varnothing\}. \tag{2-5}$$

By using the operation from (2-4), a calculation shows that $\mathrm{Gal}_t(F/\mathbb{F}_p)$ is a subgroup of $\mathrm{Gal}(F/\mathbb{F}_p)$.

Theorem 2.15. *Let $t : V\times V\to T$ be an alternating, fully nondegenerate F-tensor. If $\mathrm{Cent}(t)\cong F$, then the following hold*:

(1) $\mathrm{Aut}(\mathrm{G}_t(F))\cong\mathrm{Hom}_{\mathbb{F}_p}(V,T)\rtimes\mathrm{S\Psi I}_{F/\mathbb{F}_p}(t)$.

(2) $|\mathrm{S\Psi I}_{F/\mathbb{F}_p}(t)| = |\Psi\mathrm{Isom}_F(t)|\cdot|\mathrm{Gal}_t(F/\mathbb{F}_p)|$.

Proof. Let $\mathfrak{g}=\mathfrak{g}_t(F)$ be the Lie algebra associated to $G=\mathrm{G}_t(F)$. Since G is of class 2 with exponent $p>2$, the Baer correspondence guarantees that $\mathrm{Aut}(G)\cong\mathrm{Aut}_{\mathbb{F}_p}(\mathfrak{g})$. Since t is full, $T=[\mathfrak{g},\mathfrak{g}]$, so every endomorphism of $\mathfrak{g}=V\oplus T$ maps T into T. Thus, we have a split exact sequence of groups

$$1\longrightarrow\mathrm{Hom}_{\mathbb{F}_p}(V,T)\longrightarrow\mathrm{Aut}_{\mathbb{F}_p}(\mathfrak{g})\longrightarrow\Psi\mathrm{Isom}_{\mathbb{F}_p}(t)\longrightarrow 1,$$

where the penultimate map is given by $\alpha\mapsto(\alpha_V,\alpha_T)$ with $\alpha_V : V\to V$ given by $v+T\mapsto\alpha(v)+T$ and $\alpha_T=\alpha|_T$ is the restriction of α to T.

The group $\Psi\mathrm{Isom}_{\mathbb{F}_p}(t)$ acts on $\mathrm{Cent}(t)$ via conjugation. If $(X,Y,Z)\in\mathrm{Cent}(t)$ and $(\alpha,\beta)\in\Psi\mathrm{Isom}_{\mathbb{F}_p}(t)$, then $(\alpha X\alpha^{-1},\alpha Y\alpha^{-1},\beta Z\beta^{-1})$ belongs to $\mathrm{Cent}(t)$. This defines a homomorphism $\gamma : \Psi\mathrm{Isom}_{\mathbb{F}_p}(t)\to\mathrm{Aut}(\mathrm{Cent}(t))$, where $\mathrm{Aut}(\mathrm{Cent}(t))$ denotes the automorphism group of $\mathrm{Cent}(t)$ as a unital $\mathbb{F}_p$-algebra. Since $\mathrm{Cent}(t)\cong F$, the kernel of this map is $\Psi\mathrm{Isom}_F(t)$. The choice of an isomorphism $\varphi:\mathrm{Aut}(\mathrm{Cent}(t))\to\mathrm{Gal}(F/\mathbb{F}_p)$ yields the exact sequence of groups

$$1\longrightarrow\Psi\mathrm{Isom}_F(t)\longrightarrow\Psi\mathrm{Isom}_{\mathbb{F}_p}(t)\longrightarrow\mathrm{Gal}(F/\mathbb{F}_p).$$

We show that $\mathrm{im}(\varphi\circ\gamma)=\mathrm{Gal}_t(F/\mathbb{F}_p)$. Given $\sigma\in\mathrm{Gal}_t(F/\mathbb{F}_p)$, we have that $\sigma\in\mathrm{im}(\varphi\circ\gamma)$ if and only if there exists $(X,Y)\in\mathrm{GL}_F(V)\times\mathrm{GL}_F(T)$ such that $(\alpha,\beta)=(X\sigma,Y\sigma)\in\Psi\mathrm{Isom}_{\mathbb{F}_p}(t)$. This condition is equivalent to the equation

$$t(X\sigma(u), X\sigma(v)) = t(\alpha(u), \alpha(v)) = \beta t(u, v) = Y\sigma t(u, v) = Y({}^{\sigma}t(\sigma(u), \sigma(v))) \tag{2-6}$$

being satisfied for all $u, v \in V$. However, since σ induces an automorphism of V, the outer equality of (2-6) is equivalent to having $(X, Y) \in \Psi\mathrm{Isom}_F({}^{\sigma}t, t)$, meaning that $\sigma \in \mathrm{Gal}_t(F/\mathbb{F}_p)$. As a result, the following is a short exact sequence:

$$1 \longrightarrow \Psi\mathrm{Isom}_F(t) \longrightarrow \Psi\mathrm{Isom}_{\mathbb{F}_p}(t) \longrightarrow \mathrm{Gal}_t(F/\mathbb{F}_p) \longrightarrow 1.$$

In particular, the size of $\Psi\mathrm{Isom}_{\mathbb{F}_p}(t)$ is equal to $|\,\Psi\mathrm{Isom}_F(t)| \cdot |\,\mathrm{Gal}_t(F/\mathbb{F}_p)|$.

We conclude by showing that $\Psi\mathrm{Isom}_{\mathbb{F}_p}(t)$ and $\mathrm{S}\Psi\mathrm{I}_{F/\mathbb{F}_p}(t)$ are isomorphic. For this, note that, if $(\alpha, \beta) \in \Psi\mathrm{Isom}_{\mathbb{F}_p}(t)$ is such that $\varphi\gamma((\alpha, \beta)) = \sigma$, then $(\alpha\sigma^{-1}, \beta\sigma^{-1})$ belongs to $\Psi\mathrm{Isom}_F({}^{\sigma}t, t)$. Therefore, the map

$$\mathrm{S}\Psi\mathrm{I}_{F/\mathbb{F}_p}(t) \longrightarrow \Psi\mathrm{Isom}_{\mathbb{F}_p}(t) \quad \text{given by} \quad (\alpha, \beta, \sigma) \longmapsto (\alpha\sigma, \beta\sigma)$$

defines an isomorphism. Putting everything together, the theorem follows. □

Following [Grunewald and Segal 1984, Section 4], we say two homogeneous polynomials $f, g \in F[y_1, \dots, y_d]$ are *projectively semiequivalent* if there exist $M = (m_{ij}) \in \mathrm{GL}_d(F)$, $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$, and $\lambda \in F^{\times}$ such that

$$(\sigma(f))(m_{11}y_1 + \cdots + m_{1d}y_d, \dots, m_{d1}y_1 + \cdots + m_{dd}y_d) = \lambda g(\boldsymbol{y}), \tag{2-7}$$

where $(\sigma(f))(\boldsymbol{y})$ is the polynomial obtained by applying σ to the coefficients of f. If $\sigma = 1$, then we just say that f and g are *projectively equivalent*. Projective equivalence yields an isomorphism of the varieties of f and g, but the converse is not true in general. Moreover projective semiequivalence need not induce an isomorphism of varieties of f and g but of $\sigma(f)$ and g instead. The following corollary collects some direct geometric implications of Theorem 2.13; some more will be presented in Section 3.

Corollary 2.16. *Assume that $s : V \times V \to T$ and $t : V' \times V' \to T'$ are fully nondegenerate, that* $\mathrm{Cent}(t) \cong \mathrm{Cent}(s) \cong F$, *and that* $\mathrm{G}_s(F) \cong \mathrm{G}_t(F)$. *Let* $\mathrm{Pf}(s)$ *and* $\mathrm{Pf}(t)$ *be Pfaffians over F of s and t, respectively. Then the following hold*:

1. *The polynomials* $\mathrm{Pf}(s)$ *and* $\mathrm{Pf}(t)$ *are projectively semiequivalent.*
2. *The F-points of the singular loci of* $\mathrm{Pf}(s)$ *and* $\mathrm{Pf}(t)$ *are in bijection.*
3. *The polynomials* $\mathrm{Pf}(s)$ *and* $\mathrm{Pf}(t)$ *have the same splitting behavior, i.e., the degrees of their irreducible factors, counted with multiplicities, are the same.*

Proof. Thanks to Theorem 2.13(2), there exist $\mathbb{F}_p$-linear isomorphisms $\alpha : V \to V'$ and $\beta : T \to T'$ such that, for all $u, v \in V$,

$$t(\alpha(u), \alpha(v)) = \beta(s(u, v)). \tag{2-8}$$

Then the following map $\mathrm{Cent}(s) \to \mathrm{Cent}(t)$ is an isomorphism of $\mathbb{F}_p$-algebra:

$$(X, Y, Z) \longmapsto (\kappa_\alpha(X), \kappa_\alpha(Y), \kappa_\beta(Z)) := (\alpha X\alpha^{-1}, \alpha Y\alpha^{-1}, \beta Z\beta^{-1}).$$

Let $\varphi_s : F \to \mathrm{Cent}(s)$ and $\varphi_t : F \to \mathrm{Cent}(t)$ be field isomorphisms, so s and t are F-bilinear via φ_s and φ_t, respectively. Since s and t are fully nondegenerate, the maps $\pi_s : \mathrm{Cent}(s) \to \mathrm{End}_{\mathbb{F}_p}(T)$ and $\pi_t : \mathrm{Cent}(t) \to \mathrm{End}_{\mathbb{F}_p}(T')$ given by

$$(X, Y, Z) \longmapsto Z \quad \text{and} \quad (X', Y', Z') \longmapsto Z',$$

respectively, are injective, so $\mathrm{im}(\pi_s) \cong \mathrm{im}(\pi_t) \cong F$. Set $\psi_s = \pi_s\varphi_s$ and $\psi_t = \pi_t\varphi_t$, so $\sigma = \psi_t^{-1}\kappa_\beta\psi_s \in \mathrm{Gal}(F/\mathbb{F}_p)$. Thus, β is F-semilinear: for all $u, v \in T$ and all $\lambda \in F$,

$$\beta(u + \lambda v) = \beta(u + \psi_s(\lambda)v) = \beta(u) + \kappa_\beta\psi_s(\lambda)\beta(v) = \beta(u) + \sigma(\lambda)\beta(v).$$

By a similar argument, α is also F-semilinear for some $\sigma' \in \mathrm{Gal}(F/F_p)$.

Choose F-bases for V, V', T, and T'. Since both α and β are F-semilinear, there exist F-matrices M and N such that α is given by (N, σ') and β by (M, σ) relative to our choice of bases. If $u, v \in V$ are basis vectors, then (2-8) implies

$$t(Nu, Nv) = t(\alpha(u), \alpha(v)) = \beta(s(u, v)) = M\sigma(s(u, v)). \tag{2-9}$$

With $\lambda = \det(N)^2 \in F^\times$, the equality in (2-9) implies (2-7) for the Pfaffians of s and t over F. Hence, (1) holds. The other statements (2) and (3) easily follow from (1). □

3. Tensors and irreducible Pfaffians

In the study of elliptic p-groups $\mathrm{G}_t(F)$, the number of the maximal totally isotropic subspaces of V is a fundamental invariant. We will show in this section that there are four possible situations for the isotropic subspaces, distinguished by the adjoint algebra of t. These four possibilities fit into two larger frameworks: B is either isotropically decomposable or isotropically indecomposable. As a matter of fact, we prove this within the much larger framework of groups for which $\mathrm{Pf}(t)$ is an irreducible variety. We eventually make an additional "genericity" assumption, which is satisfied by all tensors coming from E-groups.

3.1. ***Pfaffians and isotropic subspaces.*** In this section we present a number of results on isotropic subspaces with respect to an alternating tensor with irreducible Pfaffian.

Lemma 3.1. *Let $t : V \times V \to T$ be an alternating K-tensor. If $\mathrm{Pf}(t) \neq 0$ and $U \leqslant V$ is totally isotropic, then $2\dim_K U \leqslant \dim_K V$.*

Proof. From $\mathrm{Pf}(t) \neq 0$ it follows that $\dim_K V = 2n$ for some $n \geqslant 1$. For a contradiction, let U be a totally isotropic subspace of V with $\dim_K U \geqslant n + 1$. Extend a basis of U to a basis of V, and with this basis represent t as the matrix of linear forms

$$\mathrm{B} = \begin{pmatrix} 0 & \mathrm{M}_1 \\ -\mathrm{M}_1^{\mathrm{t}} & \mathrm{M}_2 \end{pmatrix}, \quad \text{with } \mathrm{M}_1, \mathrm{M}_2 \in \mathrm{Mat}_n(K[y_1, \dots, y_d]_1),\ \mathrm{M}_2^{\mathrm{t}} = -\mathrm{M}_2 .$$

Note that M_1 contains a zero column since $\dim_K U \geqslant n + 1$, and so, for some $u \in K^\times$, the equality $\mathrm{Pf}(t) = u\det(\mathrm{M}_1) = 0$ holds, which is a contradiction. □

Definition 3.2. Let $t : V \times V \to T$ be an alternating K-tensor. The set of totally isotropic subspaces of V of dimension $\frac{1}{2}\dim_K V$ is denoted by $\mathcal{T}(t)$.

Lemma 3.3. *Let $t : V \times V \to T$ be an alternating K-tensor such that* $\mathrm{Pf}(t)$ *is irreducible over K. If $U, W \in \mathcal{T}(t)$, then either $U = W$ or $U \cap W = 0$.*

Proof. Fix $U, W \in \mathcal{T}(t)$. Suppose $U \cap W \neq 0$ and $U \neq W$. Let $\mathcal{B}_{U\cap W}$ be a basis of $U \cap W$, and extend it to bases of U and W, denoted by $\mathcal{B}_U$ and $\mathcal{B}_W$, respectively. Extend $\mathcal{B}_U \cup \mathcal{B}_W$ to a basis $\mathcal{B}$ of V. Let B be a matrix of linear forms associated to t via this choice of basis for V. Since $\mathrm{Pf}(t) \neq 0$, we know that $\dim_K V = 2n$ for some $n \geqslant 1$. It follows that there exist $n \times n$ matrices M_1 and M_2 of linear forms, with M_2 skew-symmetric, such that

$$\mathrm{B} = \begin{pmatrix} 0 & \mathrm{M}_1 \\ -\mathrm{M}_1^{\mathrm{t}} & \mathrm{M}_2 \end{pmatrix}.$$

By construction, there are two overlapping $n \times n$ blocks of zeros (corresponding to U and W) along the diagonal of B. In particular M_1 is block-upper triangular, and therefore $\det(M_1)$ is not irreducible in $K[y_1, \dots, y_d]$. Since $\mathrm{Pf}(t)/\det(\mathrm{M}_1)$ is a nonzero scalar, we have reached a contradiction. □

We remark that the proof of Lemma 3.3 may be further generalized to describe the intersection of $U, W \in \mathcal{T}(t)$ for Pfaffians that split into a product of irreducible polynomials.

Definition 3.4. Let $\mathcal{V}$ be a hypersurface in $\mathbb{P}_K^{d-1}$ of degree n and let $I(\mathcal{V}) \subseteq K[\boldsymbol{y}]$ be the ideal of $\mathcal{V}$. The following notions are defined as follows:

(1) If $\mathrm{M}, \mathrm{M}' \in \mathrm{Mat}_n(K[\boldsymbol{y}]_1)$ are such that $\det \mathrm{M}, \det \mathrm{M}' \in I(\mathcal{V})$, then

$$\mathrm{M} \sim \mathrm{M}' \quad \Longleftrightarrow \quad \text{there exist } X, Y \in \mathrm{GL}_n(K) \text{ with } \mathrm{M}' = X\,\mathrm{M}\,Y.$$

(2) If $\mathrm{M} \in \mathrm{Mat}_n(K[\boldsymbol{y}]_1)$ is such that $\det \mathrm{M} \in I(\mathcal{V})$, then

$$[\mathrm{M}] = \{\mathrm{M}' \in \mathrm{Mat}_n(K[\boldsymbol{y}]_1) \mid \mathrm{M} \sim \mathrm{M}'\}.$$

(3) $\mathcal{L}_{\mathcal{V}}$ is the set of all $[\mathrm{M}]$, where M is as in (2).

(4) $\mathcal{L}_{\mathcal{V}}^{\mathrm{sym}}$ is the subset of $\mathcal{L}_{\mathcal{V}}$ consisting of all $[\mathrm{M}]$ with a symmetric representative.

We remark that the relation $\sim$ defined above is the standard equivalence relation considered in the study of determinantal varieties; see Definition 2.5. Moreover, it is clear that, for any two equivalent elements M, M', there exists $u \in K^{\times}$ such that $\det \mathrm{M} = u \det \mathrm{M}'$. When $n = d$, we refer to M as a *cuboid*, which is *smooth*, if $\det \mathrm{M}$ is a smooth polynomial in $K[\boldsymbol{y}]$. The name "smooth cuboids" is borrowed from [Ng 1995, Section 2]; see Remark 5.7.

Proposition 3.5. *Let $t : V \times V \to T$ be an alternating K-bilinear map with an irreducible Pfaffian and associated matrix* $\mathrm{B} \in \mathrm{Mat}_{2n}(K[y_1, \dots, y_d]_1)$. *If $|\mathcal{T}(t)| \geqslant 2$, then there exists* $\mathrm{M} \in \mathrm{Mat}_n(K[\boldsymbol{y}]_1)$ *such that* B *is pseudoisometric to*

$$\begin{pmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & 0 \end{pmatrix}$$

and exactly one of the following holds:

(1) $|\mathcal{T}(t)| > 2$ *and* $[\mathrm{M}] \in \mathcal{L}_{\mathcal{V}}^{\mathrm{sym}}$.

(2) $|\mathcal{T}(t)| = 2$ *and* $[\mathrm{M}] \in \mathcal{L}_{\mathcal{V}} \setminus \mathcal{L}_{\mathcal{V}}^{\mathrm{sym}}$.

Proof. Suppose $|\mathcal{T}(t)| \geqslant 2$, and take $U, W \in \mathcal{T}(t)$ to be distinct. Then Lemma 3.3 yields $U \cap W = 0$, so there exists $\mathrm{M} \in \mathrm{Mat}_n(K[\boldsymbol{y}]_1)$ and a choice of basis for V such that

$$\mathrm{B} = \begin{pmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & 0 \end{pmatrix}.$$

Since t has nonzero Pfaffian, t is nondegenerate, so M defines a nondegenerate tensor $\tilde{t} : U \times W \to T$. Fix bases of U and W, and let $W \to U$ be the linear map identifying the chosen bases, written as $w \mapsto \bar{w}$.

Let $X \in \mathcal{T}(t)$, and assume without loss of generality that $X \cap U = 0$. Then both W and X are complements of U in V, so there is $D \in \mathrm{Mat}_n(K)$ such that $X = \{w + D\bar{w} \mid w \in W\}$. Fix such a D. Now X is totally isotropic if and only if, for all $w, w' \in W$, the element $t(w + D\bar{w}, w' + D\bar{w}')$ is trivial. This happens if and only if, for all $w, w' \in W$, one has

$$0 = \begin{pmatrix} \bar{w}^{\mathrm{t}} D^{\mathrm{t}} & w^{\mathrm{t}} \end{pmatrix} \begin{pmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & 0 \end{pmatrix} \begin{pmatrix} D\bar{w}' \\ w' \end{pmatrix} = -\bar{w}^{\mathrm{t}} \mathrm{M}^{\mathrm{t}} D w' + \bar{w}^{\mathrm{t}} D^{\mathrm{t}} \mathrm{M}\, w'. \tag{3-1}$$

We conclude from (3-1) that X is totally isotropic if and only if $D^{\mathrm{t}}\mathrm{M} = \mathrm{M}^{\mathrm{t}} D = (D^{\mathrm{t}}\mathrm{M})^{\mathrm{t}}$, equivalently

$$\begin{pmatrix} D^{\mathrm{t}} & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & 0 \end{pmatrix} \begin{pmatrix} D & 0 \\ 0 & I \end{pmatrix} = \begin{pmatrix} 0 & D^{\mathrm{t}}\mathrm{M} \\ -D^{\mathrm{t}}\mathrm{M} & 0 \end{pmatrix}. \tag{3-2}$$

Call B' the matrix on the right-hand side of (3-2). If D is invertible, then $X \neq W$ and B and B' are K-pseudoisometric. This proves (1). If D is not invertible, then let $w \in W \setminus \{0\}$ be such that $D\bar{w} = 0$. It follows that

$$w = w + D\bar{w} \in X \cap W,$$

and so Lemma 3.3 yields $X = W$, which proves (2) and completes the proof. □

Corollary 3.6. *Let $t : V \times V \to T$ be an alternating F-tensor such that* $\mathrm{Pf}(t)$ *describes an elliptic curve in $\mathbb{P}^2_F$. Then* $\dim V = 2 \dim T = 6$ *and* $|\mathcal{T}(t)|$ *takes values in* $\{0, 1, 2, q+1\}$.

Proof. An elliptic curve in $\mathbb{P}^2_F$ is defined by a homogeneous cubic polynomial in three variables and therefore the dimensions of V and T are respectively 6 and 3. Moreover, if $|\mathcal{T}(t)| > 2$, then Proposition 3.5 yields that t can be represented by a symmetric matrix of linear forms. The claim follows from [Stanojkovski and Voll 2021, Proposition 4.10]. □

3.2. ***Adjoint algebras of half-generic tensors.*** Before dealing directly with the specific situation where $n = 3$ and $\mathrm{M} = J_{E,P}$, we turn to the more general case of half-generic tensors (see Definition 3.8), for which $|\mathcal{T}(t)| \geqslant 1$. In this case, indeed, we have some more characteristic information given by the existence of maximal totally isotropic subspaces. As we will see, the adjoint algebra can tell exactly how many such subspaces are present and whether the equivalence class of B satisfies some additional symmetry constraints. As supported by computational evidence, when $|\mathcal{T}(t)| = 0$, we expect to find that $\mathrm{Adj}(t) \cong K$. The adjoint algebras for half-generic tensors in the case when $|\mathcal{T}(t)| \geqslant 2$ are, thanks to Proposition 3.5, already determined without much additional work. We analyze the case where $|\mathcal{T}(t)| = 1$ in Lemmas 3.10 and 3.11.

Lemma 3.7. *Let* $\mathrm{M} \in \mathrm{Mat}_n(K[\boldsymbol{y}]_1)$ *and write*

$$\mathrm{B} = \begin{pmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & 0 \end{pmatrix}.$$

Then

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}, \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} \right) \;\middle|\; \begin{array}{c} (A_{11}, B_{22}), (B_{11}, A_{22}) \in \mathrm{Adj}(\mathrm{M}), \\ (A_{21}, -B_{21}) \in \mathrm{Adj}(\mathrm{M}, \mathrm{M}^{\mathrm{t}}),\ (A_{12}, -B_{12}) \in \mathrm{Adj}(\mathrm{M}^{\mathrm{t}}, \mathrm{M}) \end{array} \right\}.$$

Proof. For $i, j \in [2]$, let $A_{ij}, B_{ij} \in \mathrm{Mat}_n(K)$. Then

$$\begin{pmatrix} A_{11}^{\mathrm{t}} & A_{21}^{\mathrm{t}} \\ A_{12}^{\mathrm{t}} & A_{22}^{\mathrm{t}} \end{pmatrix} \begin{pmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & 0 \end{pmatrix} = \begin{pmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & 0 \end{pmatrix} \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$$

implies that the following equations hold:

$$-A_{21}^{\mathrm{t}}\,\mathrm{M}^{\mathrm{t}} = \mathrm{M}\,B_{21}, \quad A_{11}^{\mathrm{t}}\,\mathrm{M} = \mathrm{M}\,B_{22}, \quad -A_{22}^{\mathrm{t}}\,\mathrm{M}^{\mathrm{t}} = -\mathrm{M}^{\mathrm{t}}\,B_{11}, \quad A_{12}^{\mathrm{t}}\,\mathrm{M} = -\mathrm{M}^{\mathrm{t}}\,B_{12}. \qquad \square$$

Definition 3.8. A skew-symmetric matrix $\mathrm{B} \in \mathrm{Mat}_{2n}(K[\boldsymbol{y}]_1)$ is *half-generic* if B is pseudoisometric to

$$\begin{pmatrix} 0 & \mathrm{M} \\ -\mathrm{M}^{\mathrm{t}} & \mathrm{S} \end{pmatrix},$$

where $\mathrm{M}, \mathrm{S} \in \mathrm{Mat}_n(K[\boldsymbol{y}]_1)$ satisfy

$$\mathrm{Adj}(\mathrm{M}) \cong K \quad \text{and} \quad \mathrm{Adj}(\mathrm{M}, \mathrm{M}^{\mathrm{t}}) = \mathrm{Adj}(\mathrm{M}^{\mathrm{t}}, \mathrm{M}) = \begin{cases} \mathrm{Adj}(\mathrm{M}) & \text{if } \mathrm{M}^{\mathrm{t}} = \mathrm{M}, \\ 0 & \text{otherwise.} \end{cases}$$

If M can be chosen to satisfy $\mathrm{M}^{\mathrm{t}} = \mathrm{M}$, then B is *symmetrically half-generic* and *asymmetrically half-generic* if no such M exists.

Remark 3.9. In the situation described in Definition 3.8, both $\mathrm{Adj}(\mathrm{M})$ and $\mathrm{Adj}(\mathrm{M}^{\mathrm{t}}, \mathrm{M})$ are as small as possible. This is what we expect in general for "most" linear determinantal representations, motivating the name "half-generic". Indeed, if $\mathrm{M} = \mathrm{M}_1\, y_1 + \cdots + \mathrm{M}_d\, y_d$ with $\mathrm{M}_1, \ldots, \mathrm{M}_d \in \mathrm{Mat}_n(K)$, then

$$\mathrm{Adj}(\mathrm{M}) = \bigcap_{i=1}^{d} \mathrm{Adj}(\mathrm{M}_i), \qquad \mathrm{Adj}(\mathrm{M}, \mathrm{M}^{\mathrm{t}}) = \bigcap_{i=1}^{d} \mathrm{Adj}(\mathrm{M}_i, \mathrm{M}_i^{\mathrm{t}}).$$

Generically, both $\mathrm{Adj}(\mathrm{M}_i)$ and $\mathrm{Adj}(\mathrm{M}_i, \mathrm{M}_i^{\mathrm{t}})$ define a codimension n^2 subspace of K^{2n^2}, so for sufficiently large d, generically $\mathrm{Adj}(\mathrm{M})$ and $\mathrm{Adj}(\mathrm{M}, \mathrm{M}^{\mathrm{t}})$ are given as in Definition 3.8.

Because half-genericity is defined for pseudoisometry classes, it makes sense to extend Definition 3.8 to tensors, via the choice of a basis. Alternating tensors $t : V \times V \to T$ with $|\mathcal{T}(t)| \geqslant 1$ and whose Pfaffian defines an elliptic curve are half-generic; see Remark 5.2.

Lemma 3.10. *Let $t : V \times V \to T$ be an asymmetrically half-generic K-tensor such that $|\mathcal{T}(t)| = 1$. Then $\mathrm{Adj}(t)$ is $*$-isomorphic to $\boldsymbol{O}_1(K)$.*

Proof. Let $\mathrm{B} \in \mathrm{Mat}_{2n}(K[\boldsymbol{y}])$ be associated with t and in the form given in Definition 3.8. Since t is asymmetrically half-generic, $\mathrm{Adj}(\mathrm{M}, \mathrm{M}^{\mathrm{t}}) = \mathrm{Adj}(\mathrm{M}^{\mathrm{t}}, \mathrm{M}) = 0$, and hence by a computation similar to that carried out in the proof of Lemma 3.7, we have

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} aI_n & \Gamma \\ 0 & (a-k)I_n \end{pmatrix}, \begin{pmatrix} (a-k)I_n & \Phi \\ 0 & aI_n \end{pmatrix} \right) \;\middle|\; \begin{array}{c} a, k \in K,\ \Gamma, \Phi \in \mathrm{Mat}_n(K), \\ \Gamma^{\mathrm{t}}\mathrm{M} + \mathrm{M}^{\mathrm{t}}\Phi = k\mathrm{S} \end{array} \right\}. \tag{3-3}$$

Now we consider the K-vector space

$$L = \{(\Gamma, \Phi, k) \in \mathrm{Mat}_n(K)^2 \oplus K \mid \Gamma^{\mathrm{t}}\mathrm{M} + \mathrm{M}^{\mathrm{t}}\Phi = k\mathrm{S}\},$$

which we will show to be trivial. First, we show that $\dim_K L \leqslant 1$. For this note that, if $(\Gamma, \Phi, 0) \in L$, then $(\Gamma, -\Phi) \in \mathrm{Adj}(\mathrm{M}^{\mathrm{t}}, \mathrm{M}) = 0$. Now, if $(\Gamma, \Phi, k), (\Gamma', \Phi', k') \in L$ with $k \neq 0$, then there exists $\lambda \in K$ such that $\lambda k = k'$. It follows that $(\lambda\Gamma - \Gamma', \lambda\Phi - \Phi', 0) \in L$ and therefore $(\lambda\Gamma, \lambda\Phi, \lambda k) = (\Gamma', \Phi', k')$. This proves the claim.

Suppose now, for a contradiction, that $\dim_K L = 1$, and let $(X, Y, 1) \in L$. Since S is skew-symmetric, also $(Y, X, -1)$ belongs to L. It follows that $(X+Y, -(X+Y)) \in \mathrm{Adj}(\mathrm{M}^{\mathrm{t}}, \mathrm{M})$, equivalently $Y = -X$. Hence, $\dim_K \mathrm{Adj}(t) = 2$, and

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} aI_n & kX \\ 0 & (a-k)I_n \end{pmatrix}, \begin{pmatrix} (a-k)I_n & -kX \\ 0 & aI_n \end{pmatrix} \right) \;\middle|\; \begin{array}{c} a, k \in K,\ X \in \mathrm{Mat}_n(K), \\ X^{\mathrm{t}}\mathrm{M} - \mathrm{M}^{\mathrm{t}}X = \mathrm{S} \end{array} \right\}.$$

In particular, $\mathrm{Adj}(\mathrm{B})$ contains

$$(\alpha, \alpha^*) = \left(\begin{pmatrix} 0 & -X \\ 0 & I_n \end{pmatrix}, \begin{pmatrix} I_n & X \\ 0 & 0 \end{pmatrix} \right).$$

It follows that $\alpha\alpha^* = \alpha^*\alpha = 0$. Hence, for all $u, v \in V$, we compute

$$t(\alpha(u), \alpha(v)) = t(u, \alpha^*\alpha(v)) = 0 = t(\alpha\alpha^*(u), v) = t(\alpha^*(u), \alpha^*(v)).$$

It follows that $\alpha(V)$ and $\alpha^*(V)$ are two distinct n-dimensional, totally isotropic subspaces, which contradicts $|\mathcal{T}(t)| = 1$. We have proven that $\dim_K L = 0$, from which we derive that $\mathrm{Adj}(\mathrm{B}) \cong K \cong \boldsymbol{O}_1(K)$. $\square$

Recall from Section 2.3 that the notation $A \cong R \rtimes S$ indicates that R is the Jacobson radical of the $*$-ring A and that $A/R \cong S$.

Lemma 3.11. *Let $t : V \times V \to T$ be a symmetrically half-generic K-tensor such that $|\mathcal{T}(t)| = 1$. Assume that* $\mathrm{char}(K) \neq 2$. *Then* $\mathrm{Adj}(t)$ *is $*$-isomorphic to $K \rtimes \boldsymbol{O}_1(K)$ and, if $(\alpha, \beta) \neq (0, 0)$ is in the Jacobson radical of* $\mathrm{Adj}(t)$, *then* $\mathcal{T}(t) = \{\alpha(V)\}$.

Proof. Suppose, without loss of generality, that the matrix B associated with t is given in the form from Definition 3.8 with $\mathrm{M}^{\mathrm{t}} = \mathrm{M}$. It follows from the assumptions that $\mathrm{Adj}(\mathrm{M}^{\mathrm{t}}, \mathrm{M}) = \mathrm{Adj}(\mathrm{M}) \cong K$ and in the same way as in Lemma 3.10 we derive

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} \Gamma_{11} & \Gamma_{12} \\ kI_n & \Gamma_{22} \end{pmatrix}, \begin{pmatrix} \Phi_{11} & \Phi_{12} \\ -kI_n & \Phi_{22} \end{pmatrix} \right) \;\middle|\; \begin{array}{c} k \in K,\ \Gamma_{ij}, \Phi_{ij} \in \mathrm{Mat}_n(K), \\ \Gamma_{11}^{\mathrm{t}}\mathrm{M} - \mathrm{M}\Phi_{22} = -k\mathrm{S},\ \Gamma_{22}^{\mathrm{t}}\mathrm{M} - \mathrm{M}\Phi_{11} = k\mathrm{S}, \\ \Gamma_{12}^{\mathrm{t}}\mathrm{M} + \mathrm{M}\Phi_{12} = \mathrm{S}\Phi_{22} - \Gamma_{22}^{\mathrm{t}}\mathrm{S} \end{array} \right\}.$$

Since $\mathrm{Adj}(\mathrm{M}) \cong K$, the K-vector space

$$P = \{(\Gamma, \Phi, k) \in \mathrm{Mat}_n(K)^2 \oplus K \mid \Gamma^{\mathrm{t}}\mathrm{M} - \mathrm{M}\,\Phi = k\mathrm{S}\}$$

has dimension 1 or 2. Indeed $(\Gamma, \Phi, 0) \in P$ is equivalent to $(\Gamma, \Phi) \in \mathrm{Adj}(\mathrm{M})$: the forward implication implies that $\dim_K P \leqslant 2$, while the reverse one ensures $\dim_K P \geqslant 1$.

We claim that $\dim_K P = 1$ and we prove so working by contradiction. To this end, assume that $\dim_K P = 2$ and let $\{(I_n, I_n, 0), (X, Y, 1)\}$ be a basis of P. Since S is skew-symmetric, $(Y, X, 1)$ also belongs to P, so $(X - Y, Y - X) \in \mathrm{Adj}(\mathrm{M})$. Hence, there exists $\rho \in K$ such that $X - Y = \rho I_n = Y - X$. This implies $2(X - Y) = 0$, and since $\mathrm{char}(K) \neq 2$, we derive $X = Y$. Define now $\mathrm{S}' = \mathrm{S}X + X^{\mathrm{t}}\mathrm{S}$. With this, we have

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} aI_n - kX & C \\ kI_n & bI_n + kX \end{pmatrix}, \begin{pmatrix} bI_n + kX & D \\ -kI_n & aI_n - kX \end{pmatrix} \right) \;\middle|\; \begin{array}{c} a, b, k \in K,\ C, D \in \mathrm{Mat}_n(K), \\ C^{\mathrm{t}}\mathrm{M} + \mathrm{M}\,D = (a-b)\mathrm{S} - k\mathrm{S}', \\ X^{\mathrm{t}}\mathrm{M} - \mathrm{M}\,X = \mathrm{S} \end{array} \right\}.$$

Now we consider the vector space

$$P' = \{(C, D, c, d) \in \mathrm{Mat}_n(K)^2 \oplus K^2 \mid C^{\mathrm{t}}\mathrm{M} + \mathrm{M}\,D = c\mathrm{S} - d\mathrm{S}'\}.$$

Note that whenever $(C, D, c, 0) \in P'$ the element $(C, -D, c)$ belongs to P. It then follows from $\dim_K P = 2$ that $\dim_K P' \in \{2, 3\}$. If $\dim_K P' = 2$, then a basis for P' is $\{(I_n, -I_n, 0, 0), (X, -X, 1, 0)\}$ and

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} aI_n & cI_n + (a-b)X \\ 0 & bI_n \end{pmatrix}, \begin{pmatrix} bI_n & -cI_n + (b-a)X \\ 0 & aI_n \end{pmatrix} \right) \;\middle|\; \begin{array}{c} a, b, c \in K, \\ X^{\mathrm{t}}\mathrm{M} - \mathrm{M}\,X = \mathrm{S} \end{array} \right\}.$$

In particular, $\mathrm{Adj}(\mathrm{B})$ contains the element

$$(\alpha, \alpha^*) = \left(\begin{pmatrix} 0 & -X \\ 0 & I_n \end{pmatrix}, \begin{pmatrix} I_n & X \\ 0 & 0 \end{pmatrix} \right). \tag{3-4}$$

It follows that $\alpha(V)$ and $\alpha^*(V)$ are two distinct n-dimensional, totally isotropic subspaces, which contradicts $|\mathcal{T}(t)| = 1$. This proves that $\dim_K P' \neq 2$, so $\dim_K P' = 3$.

Let now $\{(I_n, -I_n, 0, 0), (X, -X, 1, 0), (Y, Z, \ell, 1)\}$ be a basis of P'. Since both S and S$'$ are skew-symmetric, we have $(Z, Y, -\ell, -1) \in P'$, so $(Y + Z, Y + Z, 0, 0) \in P'$. The characteristic of K being different from 2, this implies that $Z = -Y$. Thus, if $C, D \in \mathrm{Mat}_n(K)$ and $a, b, k \in K$ are such that

$$C^{\mathrm{t}}\mathrm{M} + \mathrm{M}\,D = (a-b)\mathrm{S} - k\mathrm{S}',$$

then the following holds: for some $c \in K$,

$$C = cI_n + (a - b - k\ell)X + kY = -D.$$

Thus, taking $b = 1$ and $a = c = k = 0$, we see that the element in (3-4) is also contained in $\mathrm{Adj}(\mathrm{B})$, which is a contradiction. In particular $\dim_K P' \neq 3$, which yields that $\dim_K P \neq 2$ and, consequently, that $\dim_K P = 1$.

We conclude by observing that $\mathrm{Adj}(t) \cong K \rtimes \boldsymbol{O}_1(K)$ because

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} aI_n & bI_n \\ 0 & aI_n \end{pmatrix}, \begin{pmatrix} aI_n & -bI_n \\ 0 & aI_n \end{pmatrix} \right) \;\middle|\; a, b \in K \right\}. \tag{3-5}$$

We also see from (3-5) that if $0 \neq (\alpha, -\alpha)$ is in the radical of $\mathrm{Adj}(\mathrm{B})$, then $\alpha(V) \in \mathcal{T}(t)$. □

Proposition 3.12. *Let $t : V \times V \to T$ be a K-tensor with irreducible Pfaffian. If* $\mathrm{Adj}(t)$ *is $*$-isomorphic to either $\boldsymbol{X}_1(K)$ or $\boldsymbol{S}_2(K)$, then $|\mathcal{T}(t)| = 2$ or $|\mathcal{T}(t)| > 2$, respectively.*

Proof. Let $\varphi : \mathrm{Adj}(t) \to A$ be a $*$-isomorphism, where A is either $\boldsymbol{X}_1(K)$ or $\boldsymbol{S}_2(K)$.

If $A = \boldsymbol{X}_1(K)$ and $(X, Y) = \varphi^{-1}((1, 0))$, then Theorem 2.12 yields that $XY = 0 = YX$ and $X + Y = I_{2n}$. Then $U = XV$ and $W = YV$ are totally isotropic subspaces and satisfy $U + W = V$. In particular, $|\mathcal{T}(t)| \geqslant 2$. To show that equality holds, we assume for a contradiction that $U' \in \mathcal{T}(t) \setminus \{U, W\}$. Then thanks to Lemma 3.3, we write $V = U \oplus U'$. Taking $\alpha : V \to U$ and $\beta : V \to U'$ to be projections such that $\alpha_{|U} = \mathrm{id}_U$ and $\beta_{|U'} = \mathrm{id}_{U'}$, it follows that $(\alpha, \beta) \in \mathrm{Adj}(t)$ and so the dimensions of A and $\mathrm{Adj}(t)$ do not coincide.

Assume now that $A = \boldsymbol{S}_2(K)$ and define

$$(X_1, Y_1) = \varphi^{-1}\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right) \quad \text{and} \quad (X_2, Y_2) = \varphi^{-1}\left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right).$$

Theorem 2.12 yields that $X_1Y_1 = Y_1X_1 = 0 = X_2Y_2 = Y_2X_2$. Therefore X_1V, X_2V, and Y_1V are totally isotropic subspaces. Moreover, as $X_1 + Y_1$, $X_1 + X_2$, and $X_2 + Y_1$ are invertible, Lemma 3.3 ensures that they are distinct. In particular $|\mathcal{T}(t)| > 2$. □

In the following, all isomorphisms concerning adjoint algebras are taken as $*$-algebras.

Theorem 3.13. *Let $t : V \times V \to T$ be a full, half-generic K-tensor with irreducible Pfaffian. Then* $\mathrm{Cent}(t) \cong K$, *and the following hold*:

(1) $|\mathcal{T}(t)| = 1$ *and t asymmetrically half-generic imply* $\mathrm{Adj}(t) \cong \boldsymbol{O}_1(K)$.

(2) $|\mathcal{T}(t)| = 1$, *t symmetrically half-generic, and $2K = K$ imply* $\mathrm{Adj}(t) \cong K \rtimes \boldsymbol{O}_1(K)$.

(3) $|\mathcal{T}(t)| = 2$ *if and only if* $\mathrm{Adj}(t) \cong \boldsymbol{X}_1(K)$.

(4) $|\mathcal{T}(t)| > 2$ *if and only if* $\mathrm{Adj}(t) \cong \boldsymbol{S}_2(K)$.

Proof. Let $\mathrm{B} \in \mathrm{Mat}_{2n}(K[\boldsymbol{y}]_1)$ be the matrix associated with t. Since the Pfaffian is nonzero, we write $\dim_K V = 2n$. If $|\mathcal{T}(t)| = 1$, then Lemmas 3.10 and 3.11 settle (1)–(2). If $|\mathcal{T}(t)| = 2$, we know from Proposition 3.5 that B is asymmetrically half-generic. In this case Lemma 3.7 yields

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} aI_n & 0 \\ 0 & bI_n \end{pmatrix}, \begin{pmatrix} bI_n & 0 \\ 0 & aI_n \end{pmatrix} \right) \;\middle|\; a, b \in K \right\} \cong \boldsymbol{X}_1(K). \tag{3-6}$$

This proves the forward direction of (3). If, on the other hand, $|\mathcal{T}(t)| > 2$, then B is symmetrically half-generic by Proposition 3.5. By Lemma 3.7, we have

$$\mathrm{Adj}(\mathrm{B}) = \left\{ \left(\begin{pmatrix} aI_n & bI_n \\ cI_n & dI_n \end{pmatrix}, \begin{pmatrix} dI_n & -bI_n \\ -cI_n & aI_n \end{pmatrix} \right) \;\middle|\; a, b, c, d \in K \right\} \cong \boldsymbol{S}_2(K). \tag{3-7}$$

Thus, the forward direction of (4) follows from (3-7). The reverse directions for (3) and (4) follow from Proposition 3.12.

We conclude by showing that $\mathrm{Cent}(t) \cong K$. Because $\mathrm{Pf}(t)$ is irreducible and t is full, t is fully nondegenerate. Thus, Lemma 2.11 ensures that $\mathrm{Cent}(t)$ is commutative. Moreover, from [Brooksbank et al. 2020, Theorem A], we know that $\mathrm{Cent}(t)$ embeds into the center of $\mathrm{Adj}(t)$ which is, in the four cases of this theorem, always isomorphic to K. □

4. Determinantal representations of cubics

Let E be an elliptic curve in $\mathbb{P}^2_K$ with identity element $\mathcal{O}$. Let $E(K)$ denote the K-rational points of E and $\oplus$ the addition on E. If $P \in E(K)$ and m is a positive integer, we write $\ominus P$ for the opposite of P, $[m]P \in E(K)$ for the sum of m copies of P, and $E[m]$ for the m-torsion subgroup of E. We write $\mathrm{Aut}(E)$ for the group of automorphisms of E as a projective curve, and $\mathrm{Aut}_{\mathcal{O}}(E)$ for the automorphism group of the elliptic curve E. In particular, $\mathrm{Aut}_{\mathcal{O}}(E)$ comprises the elements of $\mathrm{Aut}(E)$ that fix $\mathcal{O}$. We let $\mathrm{Div}(E)$ be the Weil divisor group of E and $\mathrm{Div}^0(E)$ the degree-0 part of the divisor group of E. We denote the class of D in the Picard group $\mathrm{Pic}(E)$ by $[D]$ and write $\mathrm{Pic}^0(E)$ for the degree-0 part of $\mathrm{Pic}(E)$. If $D \in \mathrm{Div}(E)$, denote by $\mathcal{L}(D)$ the sheaf of D, which is also commonly denoted by $\mathcal{O}_E(D)$. Our notation is mostly adherent to the one from [Silverman 2009, Chapter II] and we refer the reader to [Hartshorne 1977; Silverman 2009] for the geometric background of Sections 4 and 5.

4.1. *Divisors on elliptic curves.* In this section, we recall some basic facts on divisors.

Lemma 4.1 [Hartshorne 1977, Proposition II.6.13]. *Let $D, D' \in \mathrm{Div}(E)$. Then the following are equivalent*:

(1) $[D] = [D']$.

(2) *$\mathcal{L}(D)$ and $\mathcal{L}(D')$ are isomorphic.*

Let $\mathcal{L}_0$ denote the collection of isomorphism classes of noneffective degree-0 line bundles on E. As a consequence of Lemma 4.1 one can easily derive that the map

$$\mathrm{Pic}^0(E) \setminus \{0\} \longrightarrow \mathcal{L}_0, \quad [D] \longmapsto \mathcal{L}(D), \tag{4-1}$$

is a well-defined bijection. Moreover, [Silverman 2009, Proposition III.3.4] ensures that the following map is a well-defined bijection:

$$E \setminus \{\mathcal{O}\} \longrightarrow \mathrm{Pic}^0(E) \setminus \{0\}, \quad P \longmapsto [P - \mathcal{O}]. \tag{4-2}$$

Lemma 4.2 (Abel's theorem, see [Silverman 2009, Corollary III.3.5]). *Let $D = \sum_{P \in E(K)} n_P P \in \mathrm{Div}(E)$. Then $[D] = 0$ if and only if $\sum_{P \in E(K)} n_P = 0$ and $\bigoplus_{P \in E(K)} [n_P]P = 0$.*

4.2. *Linear representations and noneffective line bundles.* This short section collects a few results on equivalence classes of determinantal representations of cubics from [Ishitsuka 2017], which build upon the seminal paper [Beauville 2000].

Lemma 4.3 [Ishitsuka 2017, Theorem 5.2]. *Let C be a smooth genus-1 curve in $\mathbb{P}^2_K$. Then there is a natural bijection between*

(1) *the set $\mathcal{L}_C$ as given in Definition 3.4(3), and*

(2) *the set of isomorphism classes of noneffective line bundles of degree-0 on C.*

Definition 4.4. Let $\mathcal{C}$ denote the collection of smooth genus-1 curves in $\mathbb{P}^2_K$ and write

$$\mathcal{L}_{\mathcal{C}} = \bigcup_{C \in \mathcal{C}} \mathcal{L}_C.$$

For each choice of $\mathrm{M} \in \mathcal{L}_{\mathcal{C}}$, the notation $[\![\mathrm{M}]\!]$ is used for the orbit of M with respect to the action of $\Gamma = \mathrm{GL}_3(K) \times \mathrm{GL}_3(K) \times \mathrm{GL}_3(K)$ on $\mathcal{L}_{\mathcal{C}}$ that is defined by

$$\Gamma \times \mathcal{L}_{\mathcal{C}} \longrightarrow \mathcal{L}_{\mathcal{C}}, \quad ((X, Y, Z), \mathrm{M}(\boldsymbol{y})) \longmapsto X^{\mathrm{t}}\mathrm{M}(Z\boldsymbol{y})Y.$$

Moreover, $\mathcal{M}_{\mathcal{C}}$ denotes the collection of all $[\![\mathrm{M}]\!]$ where $\mathrm{M} \in \mathcal{L}_{\mathcal{C}}$.

Proposition 4.5. *Let $\mathcal{C}$ denote the collection of smooth genus-1 curves in $\mathbb{P}^2_K$. Let* $[\mathrm{M}], [\mathrm{M}'] \in \mathcal{L}_{\mathcal{C}}$ *and write C and C' for the curves defined by* $\det \mathrm{M} = 0$ *and* $\det \mathrm{M}' = 0$, *respectively. Let, moreover, $\mathcal{L}$ and $\mathcal{L}'$ be degree-0 noneffective line bundles on C resp. C' associated to* M *and* M′ *as in Lemma 4.3. Then the following are equivalent:*

(1) $[\![\mathrm{M}]\!] = [\![\mathrm{M}']\!]$,

(2) *There exists a linear isomorphism $\gamma : C \to C'$ such that $\gamma^*\mathcal{L}' = \mathcal{L}$.*

Proof. Rephrasing Definition 4.4, one has that $[\![\mathrm{M}]\!] = [\![\mathrm{M}']\!]$ if and only if there exists $Z \in \mathrm{GL}_3(K)$ such that $[\mathrm{M}'(\boldsymbol{y})] = [\mathrm{M}(Z\boldsymbol{y})]$. By calling γ the map $C \to C'$ that is induced by Z, it follows from Lemma 4.3 that $[\![\mathrm{M}]\!] = [\![\mathrm{M}']\!]$ if and only if $\gamma^*\mathcal{L}' = \mathcal{L}$. □

4.3. *Explicit Weierstrass representations.* Until the end of the present section, let $a, b \in K$ with $4a^3 + 27b^2 \neq 0$ and let E denote the elliptic curve

$$E : y^2 z = x^3 + axz^2 + bz^3. \tag{4-3}$$

In this paper, when talking of a *Weierstrass equation* of a curve E we will mean an equation of the form (4-3), commonly referred to as a short Weierstrass equation of E. In the following definition, the matrix $J_{E,P}$ is equivalent, in the sense of Definition 3.4, to the matrix M_P from [Ishitsuka 2017, Example 7.6].

Definition 4.6. Let $P = (\lambda, \mu, 1) \in E(K)$. Then $J_{E,P} \in \mathrm{Mat}_3(K[x, y, z])$ is defined by

$$J_{E,P} = J_{E,P}(x, y, z) = \begin{pmatrix} x - \lambda z & y - \mu z & 0 \\ y + \mu z & \lambda x + (a + \lambda^2)z & x \\ 0 & x & -z \end{pmatrix}.$$

Moreover, the matrix $\mathrm{B}_{E,P} = \mathrm{B}_{E,P}(x, y, z) \in \mathrm{Mat}_6(K[x, y, z])$ is defined as

$$\mathrm{B}_{E,P} = \begin{pmatrix} 0 & J_{E,P} \\ -J_{E,P}^{\mathrm{t}} & 0 \end{pmatrix}$$

and the group $\mathrm{G}_{\mathrm{B}_{E,P}}(K)$ is denoted by $\mathrm{G}_{E,P}(K)$.

Note that all (projective) points in $E(K)\setminus\{\mathcal{O}\}$ are of the form $(\lambda,\mu,1)$ as in Definition 4.6. The following result is the combination of Theorem 5.2, i.e., this paper's Lemma 4.3, and Proposition 7.1 from [Ishitsuka 2017]; see also Example 7.6 of that work. For an alternative reference, see for instance [Ravindra and Tripathi 2014, Theorem 1].

Proposition 4.7. *Assume $6K = K$. Then the following hold*:

(1) *The following map is a well-defined bijection*:

$$E(K)\setminus\{\mathcal{O}\}\longrightarrow\mathcal{L}_E,\qquad P\longmapsto[J_{E,P}].$$

(2) *For $P\in E(K)\setminus\{\mathcal{O}\}$, one has*

$$[J_{E,P}]\in\mathcal{L}_E^{\mathrm{sym}}\quad\iff\quad P\in E[2](K).$$

Remark 4.8. Let $P=(\lambda,\mu,1)\in E(K)$. Then the following hold:

(1) $J_{E,P}^{\mathrm{t}}=J_{E,\ominus P}$.

(2) $J_{E,P}$ is symmetric if and only if $\mu=0$, equivalently P has order 2 in $E(K)$.

(3) If $\mu=0$, then $J_{E,P}$ is equivalent to the "Hessian matrix"

$$\mathrm{H}_{E,P}=\begin{pmatrix}3\lambda x+az & y & a\lambda z+ax+3bz\\ y & x-\lambda z & -\lambda y\\ a\lambda z+ax+3bz & -\lambda y & a\lambda x+3\lambda bz+3bx-a^2z\end{pmatrix}.$$

This matrix corresponds to one of the three solutions to Hesse's system for E [1844] and, with direct connection to this paper's work, [Stanojkovski and Voll 2021, equation (1.6)].

Remark 4.9 (flex points for linearity). An elliptic curve $\widetilde{E}$ in $\mathbb{P}_K^2$ is defined by a smooth cubic in $K[y_1,y_2,y_3]$ which, however, need not be in short Weierstrass form. For a K-linear change of coordinates to exist in order to express $\widetilde{E}$ by a short Weierstrass equation, a sufficient condition is for $\widetilde{E}$ to have a flex point over K. This is explicitly explained in [Cremona 2003, Section 4.4] and accounts of this transformation can also be found in [Silverman 2009, Proposition III.3.1] and [Silverman and Tate 2015, Section 1.3]. Via this change of coordinates, the flex point is mapped to the point at infinity $\mathcal{O}=(0:1:0)$, given in projective coordinates, which is also taken to be the identity for the group law on $\widetilde{E}$. Once this identification is made, it is a classical result that the collection of flex points in $\widetilde{E}(K)$ coincides with $\widetilde{E}[3](K)$ where the unique element of order 1 is precisely $\mathcal{O}$; see [Fulton 1969, Problem 5.37].

5. Proofs of Theorems A, B, and D

Relying on a number of techniques including the employment of Lie algebras (via the Baer correspondence) and results on the realization of elliptic curves as zero sets of determinants of 3×3 matrices of linear forms, in Sections 5.1, 5.2, and 5.3 we prove Theorems D, A, and B in the forms of Corollary 5.3, Theorem 5.6, and Corollary 5.10, respectively. To this end, we let E denote the elliptic curve

$$E: y^2z=x^3+axz^2+bz^3,\quad a,b\in K,\ \text{ with } 4a^3+27b^2\neq 0.$$

5.1. ***Adjoint algebras for E-groups and the proof of Theorem D.*** We are now ready to describe the structure of the adjoint algebras of E-groups coming from an isotropically decomposable B with upper-right corner $\mathrm{M} = J_{E,P}$.

Proposition 5.1. *Assume $K = 2K$, and let $P = (\lambda, \mu, 1) \in E(K)$. Then one has*

$$(EP) = \{(kI_3, kI_3) \mid k \in K\} \quad \text{and} \quad \mathrm{Adj}(J_{E,P}, J_{E,P}^{\mathrm{t}}) = \begin{cases} \mathrm{Adj}(J_{E,P}) & \text{if } \mu = 0, \\ 0 & \text{otherwise}. \end{cases}$$

Proof. Let $z = (z_1, z_2, z_3)$ be variables. The adjoint algebra $\mathrm{Adj}(J_{E,P})$ is determined by a linear system of 27 equations in 18 variables. We describe an $M(z) \in \mathrm{Mat}_{18\times 27}(K[z])$ such that the left kernel of $M(\lambda, \mu, a+\lambda^2)$ is in bijection with $\mathrm{Adj}(J_{E,P})$. Write $J_{E,P} = Ax + By + Cz$ for $A, B, C \in \mathrm{Mat}_3(K)$ computable from Definition 4.6, and define

$$M(z) = \begin{bmatrix} -A & 0 & 0 & -B & 0 & 0 & -C & 0 & 0 \\ 0 & -A & 0 & 0 & -B & 0 & 0 & -C & 0 \\ 0 & 0 & -A & 0 & 0 & -B & 0 & 0 & -C \\ E_{11} & z_1E_{21}+E_{31} & E_{21} & E_{21} & E_{11} & 0 & -z_1E_{11}-z_2E_{21} & z_2E_{11}+z_3E_{21} & -E_{31} \\ E_{12} & z_1E_{22}+E_{32} & E_{22} & E_{22} & E_{12} & 0 & -z_1E_{12}-z_2E_{22} & z_2E_{12}+z_3E_{22} & -E_{32} \\ E_{13} & z_1E_{23}+E_{33} & E_{23} & E_{23} & E_{13} & 0 & -z_1E_{13}-z_2E_{23} & z_2E_{13}+z_3E_{23} & -E_{33} \end{bmatrix}, \tag{5-1}$$

where E_{ij} is the 3×3 matrix with 1 in the (i, j)-entry and 0 elsewhere.

By performing Gaussian elimination over $K[z]$ on the columns of $M(z)$, one can conclude that the left kernel of $M(z)$ is 1-dimensional, regardless of the values of λ, μ, or a. The computations have been carried out in SageMath [2019] and Magma [Bosma et al. 1997]. Now, since the adjoint algebra is unital, the left kernel of $M(z)$ being 1-dimensional implies that $\mathrm{Adj}(J_{E,P}) \cong K$.

For $\mathrm{Adj}(J_{E,P}, J_{E,P}^{\mathrm{t}})$, Remark 4.8(2) ensures that, if $\mu = 0$, then $\mathrm{Adj}(J_{E,P}, J_{E,P}^{\mathrm{t}}) = \mathrm{Adj}(J_{E,P})$. Now assume that $\mu \neq 0$. A matrix $M'(z)$ whose left kernel defines a basis for $\mathrm{Adj}(J_{E,P}, J_{E,P}^{\mathrm{t}})$, at $z = (\lambda, \mu, a+\lambda^2)$, is obtained from $M(z)$ by replacing the three blocks $-C$ with $-C^{\mathrm{t}}$. By performing Gaussian elimination over $K[z]$ one can show that $M'(z)$ has full rank, implying $\mathrm{Adj}(J_{E,P}, J_{E,P}^{\mathrm{t}}) = 0$. These computations have also been carried out in SageMath and Magma. ☐

Remark 5.2. The consequence of Proposition 5.1, combined with Remark 4.8, is that for all skew-symmetric matrices $\mathrm{S} \in \mathrm{Mat}_3(K)$, the matrix

$$\mathrm{B} = \begin{pmatrix} 0 & J_{E,P} \\ -J_{E,P}^{\mathrm{t}} & \mathrm{S} \end{pmatrix}$$

is half-generic.

Corollary 5.3. *Let $t : V \times V \to T$ be a fully nondegenerate alternating K-tensor whose Pfaffian defines a smooth cubic E in $\mathbb{P}^2_K$ with a flex point $\mathcal{O} \in E(K)$. Assume $6K = K$. Then the following hold*:

(1) $|\mathcal{T}(t)| = 2$ *if and only if* $\mathrm{Adj}(t) \cong \boldsymbol{X}_1(K)$.

(2) $|\mathcal{T}(t)| > 2$ *if and only if* $\mathrm{Adj}(t) \cong \boldsymbol{S}_2(K)$.

Proof. Since t is fully nondegenerate with a Pfaffian defining a smooth cubic in $\mathbb{P}^2_K$, one has $\dim_K V = 6$ and $\dim_K T = 3$. Let $\mathrm{B} \in \mathrm{Mat}_6(K[y_1, y_2, y_3]_1)$ be associated with t.

First we assume $|\mathcal{T}(t)| \geqslant 2$. Without loss of generality, assume B is isotropically decomposed with top right 3×3 block equal to M. Since $\mathrm{char}(K) \notin \{2, 3\}$ and $\mathrm{Pf}(\mathrm{B})$ has a K-rational flex, Remark 4.9 together with Proposition 4.5 ensure the existence of a pair (E, P) such that $[\![\mathrm{M}]\!] = [\![J_{E,P}]\!]$. Therefore, $\mathrm{Adj}(\mathrm{M}) \cong \mathrm{Adj}(J_{E,P})$, and by Proposition 5.1, the tensor t is half-generic. The forward directions for both (1) and (2) follow from Theorem 3.13. The reverse directions for both follow from Proposition 3.12. $\square$

Proof of Theorem D. If t is the tensor associated to the matrix B from Theorem D, then by Corollary 5.3 the following equivalences hold:

$$|\mathcal{T}(t)| = 2 \iff \mathrm{Adj}(t) \cong \boldsymbol{X}_1(K), \qquad |\mathcal{T}(t)| > 2 \iff \mathrm{Adj}(t) \cong \boldsymbol{S}_2(K).$$

Relying on B being (a)symmetrically half-generic, as is done in the proof Theorem 3.13, combining Proposition 5.1 with Remark 4.8 we deduce that

$$|\mathcal{T}(t)| = 2 \iff P \in E(K) \setminus E[2](K), \qquad |\mathcal{T}(t)| > 2 \iff P \in E[2](K) \setminus \{\mathcal{O}\}. \qquad \square$$

5.2. *Isomorphism testing via isogenies and the proof of Theorem A.* In this section, we give necessary and sufficient conditions for two groups of the form $\mathrm{G}_{E,P}(F)$ and $\mathrm{G}_{E',P'}(F)$ to be isomorphic.

Lemma 5.4. *Define the following matrices in* $\mathrm{GL}_3(K)$:

$$X_0 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \textit{and} \quad Z_0 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

For every elliptic curve E in short Weierstrass form over K and every $P \in E(K) \setminus \{\mathcal{O}\}$, the following holds:

$$\begin{pmatrix} 0 & X_0 \\ X_0 & 0 \end{pmatrix} \mathrm{B}_{E,P}(Z_0 \boldsymbol{y}) \begin{pmatrix} 0 & X_0 \\ X_0 & 0 \end{pmatrix} = \mathrm{B}_{E,P}(\boldsymbol{y}).$$

For the next result, recall that a group G acts *k-transitively* on a set X if its induced action $g\cdot(x_1, \dots, x_k) = (g(x_1), \dots, g(x_k))$ on the subset of X^k of all elements with pairwise distinct entries is transitive. The next result is an easy consequence of [Stanojkovski and Voll 2021, Proposition 4.10].

Lemma 5.5. *Let E be an elliptic curve in short Weierstrass form over the field K and let $P \in E[2](K) \setminus \{\mathcal{O}\}$. Define, moreover, $\psi : \mathrm{GL}_2(K) \to \mathrm{GL}_6(K)$ by*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} aI_3 & bI_3 \\ cI_3 & dI_3 \end{pmatrix}.$$

Then $\psi(\mathrm{GL}_2(K))$ acts 2-transitively on $\mathcal{T}(\mathrm{B}_{E,P})$.

Theorem 5.6. *Let E and E' be elliptic curves in $\mathbb{P}^2_F$ given by Weierstrass equations, and let $P \in E(F) \setminus \{\mathcal{O}\}$ and $P' \in E'(F) \setminus \{\mathcal{O}'\}$. Assume $\mathrm{char}(F) = p \geqslant 5$. Then the following are equivalent*:

(1) *The F-Lie algebras $\mathfrak{g}_{E,P}(F)$ and $\mathfrak{g}_{E',P'}(F)$ are isomorphic.*

(2) *The set* $\Psi\mathrm{Isom}_F(\mathrm{B}_{E,P}, \mathrm{B}_{E',P'})$ *is nonempty.*

(3) *There exists an isomorphism* $\varphi : E \to E'$ *of elliptic curves such that* $\varphi(P) = P'$.

Proof. Let $t : U \times W \to T$ and $t' : U' \times W' \to T'$ be the F-tensors defined by $J_{E,P}$ and $J_{E',P'}$, respectively. Up to postcomposing with the automorphisms from Lemma 5.4 or Lemma 5.5, the Lie algebras $\mathfrak{g}_{E,P}(F)$ and $\mathfrak{g}_{E',P'}(F)$ are isomorphic if and only if there exists an isomorphism $\mathfrak{g}_{E,P}(F) \to \mathfrak{g}_{E',P'}(F)$ mapping U to U' and W to W', which is equivalent to saying there are matrices $X, Y, Z \in \mathrm{GL}_3(F)$ such that (X, Y, Z) is an F-isotopism $t \to t'$. In particular, $\mathfrak{g}_{E,P}(F)$ and $\mathfrak{g}_{E',P'}(F)$ are isomorphic if and only if $[\![J_{E',P'}]\!] = [\![J_{E,P}]\!]$; see Definition 4.4.

Now let $\mathcal{L}$ and $\mathcal{L}'$ be line bundles on $C = E$ and $C' = E'$ and let $\gamma : E \to E'$ be linear as given by Proposition 4.5. Without loss of generality, we take $\mathcal{L} = \mathcal{L}(P - \mathcal{O})$ and $\mathcal{L}' = \mathcal{L}(P' - \mathcal{O}')$; see (4-1) and (4-2). Moreover, note that the line bundles $\mathcal{M} = \mathcal{L}(3\mathcal{O})$ and $\mathcal{M}' = \mathcal{L}(3\mathcal{O}')$ define the given embeddings of $E \to \mathbb{P}^2_F$ and $E' \to \mathbb{P}^2_F$; see also [Silverman 2009, Proposition III.3.1]. In particular, the condition on the map γ can be replaced with the existence of a (not necessarily linear) isomorphism $\delta : E \to E'$ such that

$$\delta^*\mathcal{L}' = \mathcal{L} \quad \text{and} \quad \delta^*\mathcal{M}' = \mathcal{M}. \tag{5-2}$$

We now show that the existence of δ satisfying (5-2) is equivalent to the existence of an isomorphism of elliptic curves $\varphi : E \to E'$ with the property that $\varphi(P) = P'$. By using the symbol δ also for the map $\mathrm{Div}(E) \to \mathrm{Div}(E')$ that is induced by δ, we rewrite (5-2) as

$$\delta^*\mathcal{L}' = \mathcal{L} \quad \text{and} \quad \mathcal{L}(3\delta^{-1}(\mathcal{O}')) = \delta^*\mathcal{L}(3\mathcal{O}') = \delta^*\mathcal{M}' = \mathcal{M} = \mathcal{L}(3\mathcal{O}).$$

We derive from Lemma 4.1 that $[3\delta^{-1}(\mathcal{O}')] = [3\mathcal{O}]$, in other words $[3(\delta^{-1}(\mathcal{O}') - 3\mathcal{O})] = 0$. It now follows from Abel's theorem, i.e., Lemma 4.2, that $[3](\delta^{-1}(\mathcal{O}') \ominus \mathcal{O}) = \mathcal{O}$ and so $\delta^{-1}(\mathcal{O}')$ belongs to $E[3](F)$. Let τ denote translation by $\delta^{-1}(\mathcal{O}')$ on E. We then get that $\delta \circ \tau : E \to E'$ is an isomorphism of elliptic curves. Set $\varphi = \delta \circ \tau$. To conclude the proof, we show that $\varphi(P) = P'$. For this, note that $\varphi^*\mathcal{L} = \varphi^*\mathcal{L}(P - \mathcal{O}) = \mathcal{L}(\varphi^{-1}(P) - \varphi^{-1}(\mathcal{O}))$. As a consequence, (5-2) and Lemma 4.1 yield

$$[\varphi^{-1}(P') - \mathcal{O}] = [\varphi^{-1}(P') - \varphi^{-1}(\mathcal{O}')] = [P - \mathcal{O}].$$

Abel's theorem implies now that $\varphi^{-1}(P') = P$, equivalently that $\varphi(P) = P'$. □

Proof of Theorem A. Let $t : U \times W \to T$ and $t' : U' \times W' \to T'$ be the F-tensors defined by $J_{E,P}$ and $J_{E',P'}$, respectively. By Theorem 2.13, the groups $\mathrm{G}_{E,P}(F)$ and $\mathrm{G}_{E',P'}(F)$ are isomorphic if and only if there exists an $\mathbb{F}_p$-pseudoisometry between t and t'. From Corollary 5.3, we know that $\mathrm{Cent}(t) \cong \mathrm{Cent}(t') \cong F$. Thus, arguing as in the proof of Theorem 2.15, we get that $\Psi\mathrm{Isom}_{\mathbb{F}_p}(t, t')$ can be considered as contained in the set $\Psi\mathrm{Isom}_F(t, t') \times \mathrm{Gal}(F/\mathbb{F}_p)$. Therefore, t and t' are $\mathbb{F}_p$-pseudoisometric if and only if there exists $\sigma \in \mathrm{Gal}(F/\mathbb{F}_p)$ such that ${}^{\sigma}t$ and t' are F-pseudoisometric. The matrix of linear forms associated to ${}^{\sigma}t$ is $\mathrm{B}_{\sigma(E),\sigma(P)}$. Again by Theorem 2.13, the tensors ${}^{\sigma}t$ and t' are F-pseudoisometric if and only if $\mathfrak{g}_{\sigma(E),\sigma(P)}(F)$ and $\mathfrak{g}_{E',P'}(F)$ are isomorphic F-Lie algebras. To conclude apply Theorem 5.6. □

Remark 5.7 (the work of Ng). For a nice overview of the geometry of the Γ-orbits of $\mathcal{L}_{\mathcal{C}}$ we refer to [Ng 1995, Section 2]. Theorem 5.6 is a specialized variation of Theorem 1 of [loc. cit.], which classifies the complex Γ-orbits in terms of triples (E, L_1, L_2) where L_1 and L_2 are particularly chosen line bundles on E; see (5-2). The study in [loc. cit.] goes beyond the smooth case classifying also singular cuboids up to Γ-equivalence. In future work, we hope to come back to the investigation of the class of groups arising from this last family.

5.3. ***Automorphisms of elliptic groups and the proof of Theorem B.*** In this section we compute the size of the automorphism group of a group arising from a tensor satisfying $\mathcal{T}(t) \geqslant 2$ and whose Pfaffian class defines a cubic with a flex point over F. Indeed, using pseudoisometries, any such curve can be put in short Weierstrass equation, and thus the group in question will be isomorphic to a group of the form $\mathrm{G}_{E,P}(F)$.

Theorem 5.8. *Let E be an elliptic curve in $\mathbb{P}^2_F$ given by a Weierstrass equation, and let $P \in E(F) \setminus \{\mathcal{O}\}$. Assume that* $\mathrm{char}(F) = p \geqslant 5$. *Then*

$$|\,\Psi\mathrm{Isom}_F(\mathrm{B}_{E,P})| = \frac{|\mathrm{Aut}_{\mathcal{O}}(E)|}{|\mathrm{Aut}_{\mathcal{O}}(E)\cdot P|}\cdot|E[3](F)|\cdot\begin{cases}|\,\mathrm{GL}_2(F)| & \text{if } P \in E[2](F),\\ 2(q-1)^2 & \text{otherwise}.\end{cases}$$

Proof. Let $t : V \times V \to T$ be the tensor defined by $\mathrm{B}_{E,P} \in \mathrm{Mat}_6(F[y_1, y_2, y_3])$ and let $\mathfrak{g} = \mathfrak{g}_t(F)$ be the Lie algebra of $\mathrm{G}_t(F)$ via the Baer correspondence. We compute the order of $\Psi\mathrm{Isom}_F(t)$. Following the strategy in [Stanojkovski and Voll 2021], we work with the automorphism group $\mathrm{Aut}(\mathfrak{g}) = \mathrm{Aut}_F(\mathfrak{g})$ of the F-algebra $\mathfrak{g}$. For this, let U, W be distinct elements of $\mathcal{T}(t)$ corresponding to the base choice yielding $\mathrm{B}_{E,P}$ and note that $V = U \oplus W$. We define the following subgroups of $\mathrm{Aut}(\mathfrak{g})$:

- $\mathrm{Aut}_V(\mathfrak{g}) = \{\alpha \in \mathrm{Aut}(\mathfrak{g}) \mid \alpha(V) = V\}$.
- $\mathrm{Aut}_V^f(\mathfrak{g}) = \{\alpha \in \mathrm{Aut}(\mathfrak{g}) \mid \alpha(U) = U,\ \alpha(W) = W\}$.

Since t is full, if $(\alpha, \beta) \in \Psi\mathrm{Isom}_F(t)$, then α uniquely determines β. In particular, we have that $\Psi\mathrm{Isom}_F(t) \cong \mathrm{Aut}_V(\mathfrak{g})$. We now look at the action of $\mathrm{Aut}_V(\mathfrak{g})$ on $\mathcal{T}(t)$. Using Lemmas 5.4 and 5.5, we derive that this action is 2-transitive. It follows that the stabilizer of the pair (U, W) is equal to $\mathrm{Aut}_V^f(\mathfrak{g})$ and has index $|\mathcal{T}(t)|(|\mathcal{T}(t)| - 1)$ in $\mathrm{Aut}_V(\mathfrak{g})$. By Corollary 3.6, it thus holds that

$$|\,\Psi\mathrm{Isom}_F(\mathrm{B}_{E,P})| = |\mathrm{Aut}_V(\mathfrak{g})| = |\mathrm{Aut}_V^f(\mathfrak{g})|\cdot\begin{cases}q(q+1) & \text{if } P \in E[2](F),\\ 2 & \text{otherwise}.\end{cases} \tag{5-3}$$

To determine $|\mathrm{Aut}_V^f(\mathfrak{g})|$ we note that, via Remark 2.10, an element

$$\mathrm{diag}(X, Y, Z) = \begin{pmatrix} X & 0 & 0\\ 0 & Y & 0\\ 0 & 0 & Z\end{pmatrix} \in \mathrm{GL}_9(F), \quad \text{with } X, Y, Z \in \mathrm{GL}_3(F),$$

belongs to $\mathrm{Aut}_V^f(\mathfrak{g})$ if and only if $X^{\mathrm{t}} J_{E,P}(Z\boldsymbol{y})Y = J_{E,P}(\boldsymbol{y})$. Since the change of coordinates given by Z maps E to itself, the following map is well-defined:

$$\varphi : \mathrm{Aut}_V^f(\mathfrak{g}) \longrightarrow \mathrm{Aut}(E), \quad \mathrm{diag}(X, Y, Z) \longmapsto Z.$$

Thus, φ maps into the linear part of $\mathrm{Aut}(E)$, namely those automorphisms of E that extend to linear transformations of $\mathbb{P}^2_F$. From the proof of Theorem 5.6, we know that

$$|\operatorname{im}\varphi| = |E[3](F)| \cdot \big|\{\varphi \in \mathrm{Aut}_{\mathcal{O}}(E) \mid \varphi(P) = P\}\big| = |E[3](F)| \cdot \frac{|\mathrm{Aut}_{\mathcal{O}}(E)|}{|\mathrm{Aut}_{\mathcal{O}}(E) \cdot P|}.$$

We claim that $|\ker\varphi| = (q-1)^2$. To prove this, we start by observing that

$$\ker\varphi = \{\mathrm{diag}(X, Y, cI_3) \mid X, Y \in \mathrm{GL}_3(F),\ c \in F^\times,\ X^{\mathrm{t}} J_{E,P}(c\mathbf{y})Y = J_{E,P}(\mathbf{y})\}.$$

The last equality in the definition of $\ker\varphi$ can be rewritten as $(cX^{\mathrm{t}})J_{E,P}Y = J_{E,P}$, so since Y is invertible, we get a map

$$\ker\varphi \longrightarrow \mathrm{Adj}(J_{E,P}), \quad \mathrm{diag}(X, Y, cI_3) \longmapsto (cX, Y^{-1}).$$

All elements of the form $(aI_3, bI_3, (ab)^{-1}I_3)$ with $a, b \in F^\times$ are elements of $\ker\varphi$, and as a consequence of Proposition 5.1, the converse is also true. Indeed, if $\mathrm{diag}(X, Y, cI_3)$ belongs to $\ker\varphi$, then (cX, Y^{-1}) is an element of $\mathrm{Adj}(J_{E,P}) = \{(kI_3, kI_3) \mid k \in F\}$. In particular, there exists $k \in F^\times$ such that $cX = kI_3 = Y^{-1}$. It then follows that $X = c^{-1}kI_3$ and $Y = k^{-1}I_3$. Thus, $\ker\varphi = \{(aI_3, bI_3, (ab)^{-1}I_3) \mid a, b \in F^\times\}$, and we conclude that $|\ker\varphi| = |F^\times|^2 = (q-1)^2$. Since $|\mathrm{GL}_2(F)| = q(q+1)(q-1)^2$, the proof is complete. □

For an elliptic curve E in $\mathbb{P}^2_F$ given by a short Weierstrass equation and $P \in E(F) \setminus \{\mathcal{O}\}$, we write

$$\mathrm{Gal}_{E,P}(F/\mathbb{F}_p) = \{\sigma \in \mathrm{Gal}(F/\mathbb{F}_p) : \Psi\mathrm{Isom}(\mathrm{B}_{E,P}, \mathrm{B}_{\sigma(E),\sigma(P)}) \neq \varnothing\}.$$

The following two corollaries follow in a straightforward way from Theorems 2.15 and 5.8. Note that the denominators on the left side are $|\mathrm{Hom}_F(V, T)|$ and $|\mathrm{Hom}_{\mathbb{F}_p}(V, T)|$, respectively.

Corollary 5.9. *Let E be an elliptic curve in $\mathbb{P}^2_F$ given by a Weierstrass equation. Moreover, let $P \in E(F) \setminus \{\mathcal{O}\}$. Assume that* $\mathrm{char}(F) = p \geqslant 5$. *Then*

$$\frac{|\mathrm{Aut}_F(\mathfrak{g}_{E,P}(F))|}{q^{18}} = |E[3](F)| \cdot \frac{|\mathrm{Aut}_{\mathcal{O}}(E)|}{|\mathrm{Aut}_{\mathcal{O}}(E) \cdot P|} \cdot \begin{cases} |\mathrm{GL}_2(F)| & \text{if } P \in E[2](F), \\ 2(q-1)^2 & \text{otherwise.} \end{cases}$$

Corollary 5.10. *Let E be an elliptic curve in $\mathbb{P}^2_F$ given by a Weierstrass equation and $P \in E(F) \setminus \{\mathcal{O}\}$. Assume that* $\mathrm{char}(F) = p \geqslant 5$ *and $|F| = p^e$. Then*

$$\frac{|\mathrm{Aut}(\mathrm{G}_{E,P}(F))|}{p^{18e^2}} = |\mathrm{Gal}_{E,P}(F/\mathbb{F}_p)| \cdot |E[3](F)| \cdot \frac{|\mathrm{Aut}_{\mathcal{O}}(E)|}{|\mathrm{Aut}_{\mathcal{O}}(E) \cdot P|} \cdot \begin{cases} |\mathrm{GL}_2(F)| & \text{if } P \in E[2](F), \\ 2(p^e-1)^2 & \text{otherwise.} \end{cases}$$

Remark 5.11. Let E be an elliptic curve given by the Weierstrass equation (4-3) over F and let $P = (\lambda, \mu, 1) \in E(F)$. To compute the size of $\mathrm{Gal}_{E,P}(F/\mathbb{F}_p)$ one can rely on Theorem 5.6 in the following way. For σ to belong to $\mathrm{Gal}_{E,P}(F/\mathbb{F}_p)$ a necessary and sufficient condition is that $\Psi\mathrm{Isom}_F(\mathrm{B}_{E,P}, \mathrm{B}_{\sigma(E),\sigma(P)})$ be nonempty. Thanks to Theorem 5.6 the last condition is equivalent to the existence of an isomorphism of elliptic curves $\varphi : E \to \sigma(E)$ such that $\varphi(P) = \sigma(P)$. With the aid of, for instance, [Silverman 2009,

Table III.3.1, p. 45], one shows that such a φ is given by a map $(x, y) \mapsto (u^2x, u^3y)$, where $u \in F$ is chosen such that $(\sigma(\lambda), \sigma(\mu)) = (u^2\lambda, u^3\mu)$ and

$$(u^4, u^6) = \begin{cases} (u^4, \sigma(b)b^{-1}) & \text{if } a = 0 \quad (\text{equiv. } j(E) = 0), \\ (\sigma(a)a^{-1}, u^6) & \text{if } b = 0 \quad (\text{equiv. } j(E) = 1728), \\ (\sigma(a)a^{-1}, \sigma(b)b^{-1}) & \text{otherwise.} \end{cases}$$

Example 5.12. Let E be the elliptic curve defined over $\mathbb{F}_5$ by $y^2 = x^3 - 2x$ and note that $E[2](\mathbb{F}_5) = \{\mathcal{O}, (0, 0)\}$, while, setting $F = \mathbb{F}_5[\sqrt{2}]$, we get

$$E[2](F) = \{\mathcal{O}, (0, 0), (\sqrt{2}, 0), (-\sqrt{2}, 0)\}.$$

The matrices $J_{E,P}$ corresponding to $P \in E[2](F) \setminus \{\mathcal{O}\}$ are equivalent to the Hessian matrices given in [Stanojkovski and Voll 2021, Section 1.4], where δ is chosen to be 2. We show that for each choice of P, the group $\mathrm{Gal}_{E,P}(F/\mathbb{F}_p)$ coincides with $\mathrm{Gal}(F/\mathbb{F}_p)$. For this, we note that in this case $b = 0$, so we can identify $\mathrm{Aut}_{\mathcal{O}}(E)$ with $\mathbb{F}_5^{\times}$; see [Silverman 2009, Section III.10]. Following the notation from Remark 5.11, we fill the following table:

σ	u^4	$\sigma(0,0)$	$\sigma(\sqrt{2},0)$	$\sigma(-\sqrt{2},0)$
id	1	$(0,0)$	$(\sqrt{2},0)$	$(-\sqrt{2},0)$
$x \mapsto x^5$	1	$(0,0)$	$(-\sqrt{2},0)$	$(\sqrt{2},0)$

Taking $u = 1$ in the first row and $u = 2$ in the second yields the claim.

Example 5.13. Let $f(x) = x^2 - x + 2 \in \mathbb{F}_5[x]$, which is irreducible. Set $F = \mathbb{F}_5[x]/(f(x))$, and let $\alpha \in F$ be a root of f. Let E be the elliptic curve in $\mathbb{P}^2_F$ given by $y^2 = x^3 + \alpha x + \alpha$. The j-invariant of E is $\alpha - 1$. Let $\sigma \in \mathrm{Gal}(F/\mathbb{F}_5)$ be the map $x \mapsto x^5$ so that $\sigma(E)$ is defined by $y^2 = x^3 + \alpha^5 x + \alpha^5$. The j-invariant of $\sigma(E)$ is $\alpha^5 - 1 = -\alpha$, so the elliptic curves E and $\sigma(E)$ are not isomorphic. Let now $P = (\alpha^3, \alpha) \in E(F)$ and note that $\sigma(P) = (\alpha^{15}, \alpha^5) \in \sigma(E)(F)$. It follows that $\mathfrak{g} = \mathfrak{g}_{E,P}(F)$ and $\mathfrak{g}_\sigma = \mathfrak{g}_{\sigma(E),\sigma(P)}(F)$ are not isomorphic as F-Lie algebras — that is, there is no F-linear isomorphism $\mathfrak{g} \to \mathfrak{g}_\sigma$ since E and $\sigma(E)$ are not isomorphic. However, $(I_9, \sigma) \in \mathrm{GL}_9(F) \rtimes \mathrm{Gal}(F/\mathbb{F}_5)$ yields an F-semilinear isomorphism $\mathfrak{g} \to \mathfrak{g}_\sigma$. Thus, as $\mathbb{F}_5$-Lie algebras, $\mathfrak{g} \cong \mathfrak{g}_\sigma$ and, consequently, $\mathrm{G}_{E,P}(F) \cong \mathrm{G}_{\sigma(E),\sigma(P)}(F)$. To make this isomorphism explicit, observe that

$$J = J_{E,P} = \begin{pmatrix} x - \alpha^3 z & y - \alpha z & 0 \\ y + \alpha z & \alpha^3 x + (\alpha + \alpha^6) z & x \\ 0 & x & -z \end{pmatrix}. \tag{5-4}$$

Viewing F as a 2-dimensional vector space with basis $\{1, \alpha\}$ over $\mathbb{F}_5$, we rewrite J from (5-4) as an $\mathbb{F}_5$-tensor $\mathbb{F}_5^6 \times \mathbb{F}_5^6 \to \mathbb{F}_5^6$. The associated matrix of linear forms is

$$\bar{J} = \begin{pmatrix} x_1+2z_1+z_2 & x_2+3z_1+3z_2 & y_1-z_2 & y_2+2z_1-z_2 & 0 & 0 \\ x_2+3z_1+3z_2 & 3x_1+x_2-z_1+z_2 & y_2+2z_1-z_2 & 3y_1+y_2+2z_1+z_2 & 0 & 0 \\ y_1+z_2 & y_2+3z_1+z_2 & 3x_1-x_2+2z_1+z_2 & 2x_1+2x_2+3z_1+3z_2 & x_1 & x_2 \\ y_2+3z_1+z_2 & 3y_1+y_2+3z_1-z_2 & 2x_1+2x_2+3z_1+3z_2 & x_1-x_2-z_1+z_2 & x_2 & 3x_1+x_2 \\ 0 & 0 & x_1 & x_2 & -z_1 & -z_2 \\ 0 & 0 & x_2 & 3x_1+x_2 & -z_2 & 2z_1-z_2 \end{pmatrix}.$$

We do the same construction for the matrix $\sigma(J)$ associated to $\sigma(E)$ and $\sigma(P)$:

$$\overline{\sigma(J)} = \begin{pmatrix} x_1+3z_1-z_2 & x_2+2z_1+2z_2 & y_1-z_1+z_2 & y_2+3z_1 & 0 & 0 \\ x_2+2z_1+2z_2 & 3x_1+x_2+z_1-z_2 & y_2+3z_1 & 3y_1+y_2+3z_2 & 0 & 0 \\ y_1+z_1-z_2 & y_2+2z_1 & 2x_1+x_2+3z_1-z_2 & 3x_1+3x_2+2z_1+2z_2 & x_1 & x_2 \\ y_2+2z_1 & 3y_1+y_2+2z_2 & 3x_1+3x_2+2z_1+2z_2 & -x_1+x_2+z_1-z_2 & x_2 & 3x_1+x_2 \\ 0 & 0 & x_1 & x_2 & -z_1 & -z_2 \\ 0 & 0 & x_2 & 3x_1+x_2 & -z_2 & 2z_1-z_2 \end{pmatrix}.$$

To define the isomorphism corresponding to (I_9, σ), we define a 6×6 block diagonal matrix $D = \operatorname{diag}(X, X, X)$ by setting

$$X = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}.$$

Note that $X^{-1} = X$. One can check that $D^{\mathrm{t}} \bar{J}(D\boldsymbol{x}) D = \overline{\sigma(J)}$, implying that

$$\begin{pmatrix} D^{\mathrm{t}} & 0 \\ 0 & D^{\mathrm{t}} \end{pmatrix} \begin{pmatrix} 0 & \bar{J}(D\boldsymbol{x}) \\ -\bar{J}^{\mathrm{t}}(D\boldsymbol{x}) & 0 \end{pmatrix} \begin{pmatrix} D & 0 \\ 0 & D \end{pmatrix} = \begin{pmatrix} 0 & \overline{\sigma(J)} \\ -\overline{\sigma(J)}^{\mathrm{t}} & 0 \end{pmatrix}.$$

Thus, $(\operatorname{diag}(D, D), D)$ is an $\mathbb{F}_5$-pseudoisometry, and therefore, $\mathrm{G}_{E,P}(F) \cong \mathrm{G}_{\sigma(E),\sigma(P)}(F)$. This argument also shows that the Galois part of $\operatorname{Aut}(\mathrm{G}_{E,P}(F))$ must be trivial — otherwise one would for example get that E and $\sigma(E)$ are isomorphic. Theorem 2.15 yields

$$\operatorname{Aut}(\mathrm{G}_{E,P}(F)) \cong \operatorname{Hom}_{\mathbb{F}_5}(\mathbb{F}_5^{12}, \mathbb{F}_5^{6}) \rtimes \Psi\mathrm{Isom}_F(\mathrm{B}_{E,P}).$$

6. Isomorphism testing for E-groups

The main goal of this section is to prove Theorem E, which we do in Section 6.3. For this, we develop a number of algorithms to recognize when a p-group is (isomorphic to) an E-group. We even consider the more general situation computing an isotropic decomposition of alternating tensors with irreducible Pfaffian in Section 6.2. We end with a discussion in Section 6.4 about our implementation of Theorem E in Magma [Bosma et al. 1997], where we also provide some examples.

6.1. ***Computational models for finite groups.*** Common computational models for finite groups are given by (small) sets of generators in either (1) matrix groups over finite fields [Luks 1992] or (2) permutation groups [Seress 2003]. Although polycyclic and "power-commutator" presentations seem to work well in practice, it is not known whether multiplication with these presentations can be done in polynomial time [Leedham-Green and Soicher 1998].

Throughout, we work with the "permutation group quotient" model proposed in [Kantor and Luks 1990]. This avoids issues where the given p-group G can only be faithfully represented as a permutation group on a set whose size is approximately $|G|$; see the example in [Neumann 1986]. The following proposition ensures that we can efficiently go from groups to tensors using the permutation group quotient model. With appropriate bounds for the prime p, one can achieve this for the matrix group model as well [Luks 1992].

Proposition 6.1 [Kantor and Luks 1990, Section 4]. *Given a group G as a quotient of a permutation group, each of the following problems has an algorithm that runs in time polynomial in* $\log|G|$.

(1) *Compute* $|G|$.

(2) *Given $x, x_1, \dots, x_k \in G$ either write x as a word in $\{x_1, \dots, x_k\}$, or else prove $x \notin \langle x_1, \dots, x_k\rangle$.*

(3) *Find generators for* $\mathrm{Z}(G)$ *and for* $[G, G]$.

(4) *Decide if G is nilpotent of class* 2.

(5) *If G is nilpotent of class* 2, *construct the commutator tensor of G as a matrix of linear forms.*

6.2. ***Isotropic decompositions.*** We depart from the focused setting of E-groups, and we consider the more general setting of computing an isotropic decomposition for an alternating F-tensor $t : V \times V \to T$.

Theorem 6.2. *Let* $\mathrm{B} \in \mathrm{Mat}_{2n}(F[y_1, \dots, y_d]_1)$ *be skew-symmetric. Then there exist Las Vegas algorithms, using* $O(n^6 d + n^2 d^5)$ *and* $O(n^6 d)$ *operations in F respectively, to do the following*:

(1) *Write* B *over* $C = \mathrm{Cent}(\mathrm{B})$, *provided C is a field, call it* B_C.

(2) *Return* $X \in \mathrm{GL}_{2n}(F)$ *such that* $X^{\mathrm{t}}\,\mathrm{B}_C\,X$ *gives an isotropic decomposition whenever* B_C *is decomposable with irreducible Pfaffian.*

We prove Theorem 6.2 with the next two lemmas. Common to both algorithms, and also their bottleneck, is computing a basis of a large system of linear equations.

Lemma 6.3. *There exists a Las Vegas algorithm that, given* $\mathrm{B} \in \mathrm{Mat}_{m\times n}(F[y_1, \dots, y_d]_1)$, *decides whether its centroid is a field extension C/F and, if so, returns the matrix of linear forms* B_C *over C using* $O(mnd(m^2 + n^2 + d^2)^2)$ *operations in F.*

Proof. Algorithm. Compute a basis for the centroid $C = \mathrm{Cent}(\mathrm{B})$ by solving a system of linear equations. Use [Brooksbank and Wilson 2015, Theorem 1.3] to determine if C is a field or not, and if C is a field, then find a generator $X = (X_1, X_2, X_3)$ of C as a unital F-algebra. If C is not a field, then just return B, so we assume C is a field. Let $V_1 = F^m$, $V_2 = F^n$, and $V_3 = F^d$. Find a maximal set of nonzero vectors $\mathcal{B}_i$ in V_i which are all in different X_i orbits. For each $(u, v) \in \mathcal{B}_1 \times \mathcal{B}_2$, write $u^{\mathrm{t}}\,\mathrm{B}\,v$ as $\sum_{w\in\mathcal{B}_3} f^{(w)}_{u,v}(X)w$, where $f^{(w)}_{u,v}(z) \in F[z]$. Return the matrix $\mathrm{B}_C = (f^{(w)}_{u,v}(X))_{u,v,w}$, running through all $(u, v, w) \in \mathcal{B}_1 \times \mathcal{B}_2 \times \mathcal{B}_3$.

Correctness. We only ever proceed beyond the construction of a basis for C if C is a field. In this case, the V_i are C-vector spaces. The sets $\mathcal{B}_i$ are C-bases for the V_i.

Complexity. A basis for the centroid C is computed by solving a homogeneous system of mnd linear equations in $m^2 + n^2 + d^2$ variables over F. By [loc. cit., Theorem 1.3], determining whether or not C is a field is done constructively in polynomial time using a Las Vegas algorithm, but this complexity is dominated by the complexity to compute a basis for C. The complexity to find bases $\mathcal{B}_i$ and rewrite B over C is also dominated by the complexity for the centroid. □

Lemma 6.4. *There is an algorithm that, given* $\mathrm{B} \in \mathrm{Mat}_{2n}(F[y_1, \dots, y_d]_1)$ *skew-symmetric, returns* $X \in \mathrm{GL}_{2n}(F)$ *such that* $X^{\mathrm{t}}\,\mathrm{B}\,X$ *gives an isotropic decomposition whenever* B *is decomposable with irreducible Pfaffian, using* $O(n^6 d)$ *operations in F.*

Proof. Algorithm. Compute $A = \mathrm{Adj}(\mathrm{B})$. Determine if A is isomorphic to either $\boldsymbol{X}_1(F)$ or $\boldsymbol{S}_2(F)$. If not, report that B is not isotropically decomposable with an irreducible Pfaffian. Otherwise, construct an isomorphism of $*$-algebras $\varphi : A \to S$, where S is either $\boldsymbol{X}_1(F)$ or $\boldsymbol{S}_2(F)$. Set

$$\mathcal{E} = \begin{cases} \{E_{11}, E_{22}\} & \text{if } S = \boldsymbol{S}_2(F), \\ \{(1,0), (0,1)\} & \text{if } S = \boldsymbol{X}_1(F), \end{cases}$$

where E_{ij} is the matrix with 1 in the (i, j) entry and 0 elsewhere. For each $e \in \mathcal{E}$, set $(Y, Z) = \varphi^{-1}(e) \in A$ and let $U_e \leqslant F^n$ be the column span of Y. Let $\mathcal{B}$ a basis for F^{2n} containing bases for U_e for all $e \in \mathcal{E}$, and return the transition matrix $X \in \mathrm{GL}_{2n}(F)$.

Correctness. By Theorem 3.13, if B is isotropically decomposable with an irreducible Pfaffian, then A is isomorphic to either $\boldsymbol{X}_1(F)$ or $\boldsymbol{S}_2(F)$. In both cases, $\mathcal{E}$ is a set of elements in S whose images induce distinct, n-dimensional, totally isotropic subspaces; see the proof of Proposition 3.12. To show that U_e is totally isotropic, set $(Y, Z) = \varphi^{-1}(e)$. For each $u, v \in F^{2n}$ one has $u^{\mathrm{t}} Y^{\mathrm{t}}\, \mathrm{B}\, Y v = u^{\mathrm{t}}\, \mathrm{B}\, Z Y v = 0$, proving that U_e is totally isotropic.

Complexity. A basis for Adj(B) is constructed by solving $n^2 d$ (homogeneous) linear equations in $2n^2$ variables. By [Brooksbank and Wilson 2012, Theorem 4.1], the complexity for the constructive recognition of $*$-algebras is dominated by the cost of constructing a basis for Adj(B). □

Proof of Theorem 6.2. Use Lemma 6.3 for (1), and for (2), apply Lemma 6.4. □

6.3. *Isomorphism testing of E-groups and the proof of Theorem E.* Theorem 6.2 is almost enough to prove the first two statements of Theorem E. The next lemma fills the gap by providing an algorithm to find flex points on smooth cubics; see Remark 4.9.

Lemma 6.5. *Given a homogeneous cubic $f \in F[y_1, y_2, y_3]$, there exists an algorithm that decides if f is smooth and if so returns all $a \in F^3 \setminus \{(0,0,0)\}$ such that $f(a) = 0$ and a is a flex point of f, which uses $O(\log q)$ field operations.*

Proof. Algorithm. Compute a Gröbner basis $\mathcal{G}_1$ for the ideal

$$I_1 = \langle \partial f/\partial y_1, \partial f/\partial y_2, \partial f/\partial y_3, f \rangle \text{ of } F[y_1, y_2, y_3]$$

using the lexicographical monomial order. Let $g \in \mathcal{G}_1$ be homogeneous with at most two variables. Factor g using univariate algorithms [von zur Gathen and Gerhard 2013, Chapter 14], and use those solutions to find all the solutions to the polynomial system determined by $\mathcal{G}_1$. If a solution exists, declare f "singular," and return a singular point. Otherwise f is smooth.

Compute the determinant of the Hessian matrix of f, which yields a homogeneous cubic $H \in F[y_1, y_2, y_3]$. Construct a Gröbner basis $\mathcal{G}_2$ for the ideal $I_2 = \langle f, H \rangle$ using the lexicographical monomial order. Return the set of solutions to the polynomial system determined by $\mathcal{G}_2$ in the same fashion as above.

Correctness. The algorithm to decide whether f is smooth is correct by definition and the fact that $\langle \mathcal{G}_1 \rangle = I_1$. The existence of such a $g \in \mathcal{G}_1$ is the content of the elimination theorem [Cox et al. 2015, Section 3.1]. If the algorithm starts to compute the flexes, we know that f is, therefore, smooth. By Bézout's theorem the number of flex points is bounded above by 9. Thus, I_2 is 0-dimensional and the flexes are the solutions to the polynomial system determined by $\mathcal{G}_2$.

Complexity. Computing a Gröbner basis for a set of polynomials whose degree and number of variables are constant is done using $O(1)$ field operations. We can solve the polynomial systems determined by $\mathcal{G}_i$ by calling a constant number of univariate factoring algorithms. Since the degrees are bounded by some absolute constant, factoring is done using $O(\log q)$ field operations [von zur Gathen and Gerhard 2013, Chapter 14]. □

Proof of Theorem E(i). By Corollary 5.3, if the G_i are elliptic groups, the $\mathrm{Cent}(t_{G_i})$ are finite extensions of $\mathbb{F}_p$. Write t_{G_i} as a matrix of linear forms $\widetilde{\mathrm{B}}_i \in \mathrm{Mat}_{6m}(\mathbb{F}_p[y_1, \ldots, y_{3m}]_1)$. Use Theorem 6.2(1) to express $\widetilde{\mathrm{B}}_i$ as a matrix of linear forms $\mathrm{B}_i \in \mathrm{Mat}_6(F[y_1, y_2, y_3]_1)$ over the centroid F of $\widetilde{\mathrm{B}}_i$, using $O(m^7)$ field operations. If the algorithm fails at any stage, then G_i is not an elliptic group. Otherwise compute the Pfaffians of B_i. Then apply Lemma 6.5 to decide if the Pfaffians are elliptic curves containing flex points; this uses $O(\log|F|) = O(m \log p)$ field operations. If they are not, then G_i is not isomorphic to some $\mathrm{G}_{E,P}(F)$. □

Now our objective is to develop the algorithms that feed into the algorithm for Theorem 6.8, which is the main algorithm for Theorem E(ii). We first describe some algorithms, which will be used in Theorem 6.8, that use a constant number of field operations.

Lemma 6.6. *Assume* $\mathrm{char}(F) \geqslant 5$. *Given an elliptic curve E in short Weierstrass form, there is an algorithm returning the set of automorphisms* $\mathrm{Aut}_{\mathcal{O}}(E)$ *as a subgroup of* $\mathrm{GL}_3(F)$ *using* $O(\log q)$ *field operations.*

Proof. Algorithm. Let $\mu_n(F)$ be the set of roots of $x^n - 1$ in F. Define $\mathcal{R}$ to be $\mu_2(F)$, $\mu_4(F)$, $\mu_6(F)$ respectively when $j(E) \neq 0, 1728$ or $j(E) = 1728$ or $j(E) = 0$. Return the subset $\{\mathrm{diag}(\omega^2, \omega^3, 1) \mid \omega \in \mathcal{R}\}$ of $\mathrm{GL}_3(F)$.

Correctness. It follows from [Silverman 2009, Theorem III.10.1].

Complexity. Factoring constant-degree univariate polynomials is done using $O(\log q)$ field operations [von zur Gathen and Gerhard 2013, Chapter 14]. □

The following is relevant in view of Remark 2.10.

Proposition 6.7. *Assume* $\mathrm{char}(F) \geqslant 5$. *Given an elliptic curve E in short Weierstrass form and $P \in E(F)$, there is an algorithm returning a generating set for* $\mathrm{Auto}_F(J_{E,P})$ *using* $O(q^{1/4} \log q)$ *field operations.*

Proof. Algorithm. Initialize $\mathcal{X} = \varnothing$. Use Lemma 6.6 to construct $\mathrm{Aut}_{\mathcal{O}}(E)$, and use Lemma 6.5 to get the set R of flexes of E over F. For each $\Omega \in \mathrm{Aut}_{\mathcal{O}}(E)$ fixing P construct a nonzero $(X_\omega, Y_\omega) \in \mathrm{Adj}(J_{E,P}, J_{E,P}(\Omega \boldsymbol{y}))$ and include $(X_\omega, Y_\omega^{-1}, \Omega)$ in $\mathcal{X}$. For each $Q \in R$, let $\tau_Q \in \mathrm{GL}_3(F)$ be the linear map given by translation by Q on E, and construct a nonzero $(X_Q, Y_Q) \in \mathrm{Adj}(J_{E,P}, J_{E,P}(\tau_Q \boldsymbol{y}))$ and include (X_Q, Y_Q^{-1}, τ_Q) in $\mathcal{X}$. Find $a \in F$ such that $\langle a \rangle = F^\times$. Then return $\mathcal{X} \cup \{(aI_3, I_3, aI_3), (I_3, aI_3, aI_3)\}$.

Correctness. As explained in Remark 4.9, the set R is equal to $E[3](F)$. As is evident from Remark 2.10 and the proof of Theorem 5.8, the map $\mathrm{Auto}_F(J_{E,P}) \to \mathrm{Aut}_V^f(\mathfrak{g}_{E,P}(F))$ given by $(X, Y, Z) \mapsto \mathrm{diag}(X, Y, Z)$ is an isomorphism, and thus correctness follows from the arguments there presented.

Complexity. The cardinalities of $\mathrm{Aut}_{\mathcal{O}}(E)$ and $E[3](F) = R$ are bounded from above by 6 and 9, respectively. The complexity is dominated by the complexity to find a primitive element of F. From the theorem of [Shparlinski 1996], finding $a \in F^\times$ such that $\langle a \rangle = F^\times$ can be done in time $O(q^{1/4} \log q)$. $\square$

Theorem 6.8. *Assume* $\mathrm{char}(F) = p \geqslant 5$. *There exists an algorithm that, given a subfield $L \subset F$ and isotropically decomposable* $\mathrm{B}, \mathrm{B}' \in \mathrm{Mat}_6(F[y_1, y_2, y_3]_1)$ *whose Pfaffians define elliptic curves in* $\mathbb{P}^2_F$ *with flex points over L, returns the possibly empty coset* $\Psi\mathrm{Isom}_L(\mathrm{B}, \mathrm{B}')$ *using $O(q)$ field operations.*

Proof. Algorithm. Use Theorem 6.2(2) to rewrite B and B' such that they are isotropically decomposed. Let $\mathrm{M}, \mathrm{M}' \in \mathrm{Mat}_3(F[y_1, y_2, y_3]_1)$ be the top right 3×3 blocks in B and B', respectively. Construct $Z, Z' \in \mathrm{GL}_3(F)$ with the property that both $f = \det(\mathrm{M}(Z\boldsymbol{y}))$ and $f' = \det(\mathrm{M}'(Z'\boldsymbol{y}))$ yield short Weierstrass forms of the curves E and E'.

Set $\mathrm{N} = \mathrm{M}(Z\boldsymbol{y})$ and $\mathrm{N}' = \mathrm{M}'(Z'\boldsymbol{y})$ and find $P \in E(F)$ and $P' \in E'(F)$ such that $\mathrm{Adj}(J_{E,P}, \mathrm{N})$ and $\mathrm{Adj}(J_{E',P'}, \mathrm{N}')$ are nontrivial. Determine if there exists $\sigma \in \mathrm{Gal}(F/L)$ and an isomorphism $\varphi : E' \to \sigma(E)$ of elliptic curves such that $P' \mapsto \sigma(P)$. If no such σ exists, return $\varnothing$; otherwise, let φ be represented by a matrix in $\mathrm{GL}_3(F)$ as given in Lemma 6.6 and choose

- $(X_1, Y_1) \in \mathrm{Adj}(J_{\sigma(E),\sigma(P)}, \mathrm{N}) \setminus \{0\}$,
- $(X_2, Y_2) \in \mathrm{Adj}(J_{E',P'}, \mathrm{N}') \setminus \{0\}$, and
- $(X_3, Y_3) \in \mathrm{Adj}(J_{E',P'}, J_{\sigma(E),\sigma(P)}(\varphi\boldsymbol{y})) \setminus \{0\}$.

Set, moreover, $\alpha = \mathrm{diag}(X_2 X_3^{-1} \sigma X_1^{-1}, Y_2^{-1} Y_3 \sigma Y_1)$ and $\beta = (Z')^{-1} \varphi^{-1} \sigma Z$. Now, use Proposition 6.7 to construct a generating set $\mathcal{X}$ for $\mathrm{Auto}_F(J_{E,P})$ and write

$$\mathcal{Y}_1 = \left\{ \left(\begin{pmatrix} X_1 \gamma X_1^{-1} & 0 \\ 0 & Y_1^{-1} \delta Y_1 \end{pmatrix}, Z^{-1} \varepsilon Z \right) \;\middle|\; (\gamma, \delta, \varepsilon) \in \mathcal{X} \right\}.$$

If $P \in E[2](F)$, then set

$$\mathcal{Y}_2 = \left\{ \left(\begin{pmatrix} a I_3 & b X_1 Y_1 \\ c Y_1^{-1} X_1^{-1} & d I_3 \end{pmatrix}, (ad - bc) I_3 \right) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(F) \right\}. \tag{6-1}$$

If $P \notin E[2](F)$, then set

$$\mathcal{Y}_2 = \left\{ \left(\begin{pmatrix} 0 & X_1 X_0 Y_1 \\ Y_1^{-1} X_0 X_1^{-1} & 0 \end{pmatrix}, Z^{-1} Z_0 Z \right) \;\middle|\; (X_0, Z_0) \text{as in Lemma 5.4} \right\}. \tag{6-2}$$

Return the generating set $\mathcal{Y} = \mathcal{Y}_1 \cup \mathcal{Y}_2$ for $\Psi\mathrm{Isom}_F(\mathrm{B})$ and $(\alpha, \beta) \in \Psi\mathrm{Isom}_L(\mathrm{B}, \mathrm{B}')$.

Correctness. For the existence of the matrices Z and Z' use Remark 4.9. Assume there exists $P \in E(F)$ such that $[\mathrm{N}] = [J_{E,P}]$. By definition, there exist $X, Y \in \mathrm{GL}_3(F)$ such that $X^{\mathrm{t}} \mathrm{N} Y = J_{E,P}$. Thus, $(A, B) \in \mathrm{Adj}(\mathrm{N}, J_{E,P})$ if and only if $(AX, Y^{-1}B) \in \mathrm{Adj}(J_{E,P})$. By Proposition 5.1, the latter is 1-dimensional and all nonzero elements are invertible. Thus, $\mathrm{Adj}(\mathrm{N}, J_{E,P})$ is nontrivial if and only if $[\mathrm{N}] = [J_{E,P}]$. Since $\det(\mathrm{N}) = 0$ defines a short Weierstrass equation and $\mathrm{char}(F) \geqslant 5$, Proposition 4.7 ensures the existence and uniqueness of such a P. A similar argument holds for N' and $J_{E',P'}$.

If there is no isomorphism of $\varphi : E' \to \sigma(E)$ mapping P' to $\sigma(P)$, then Theorem A guarantees that B and B$'$ are not L-pseudoisometric. Otherwise, the isomorphism is linear being represented by a matrix in $\mathrm{GL}_3(F)$. Hence in this case, $J_{E',P'}(\varphi \boldsymbol{y})$ is equivalent to $J_{\sigma(E),\sigma(P)}$, and the adjoint algebra $\mathrm{Adj}(J_{E',P'}(\varphi \boldsymbol{y}), J_{\sigma(E),\sigma(P)})$ is 1-dimensional by an argument similar to the one before. Proposition 6.7 and direct calculations show that $\mathcal{Y} \subset \Psi\mathrm{Isom}_F(\mathrm{B})$ and $(\alpha, \beta) \in \Psi\mathrm{Isom}_L(\mathrm{B}, \mathrm{B}')$. That $\langle \mathcal{Y} \rangle = \Psi\mathrm{Isom}_F(\mathrm{B})$ follows from the proof of Theorem 5.8.

Complexity. The complexity is dominated by listing and finding the unique points P and P'. There are at most $O(q)$ points, and listing the points on an elliptic curve can be done using $O(q)$ field operations. □

Proof of Theorem E(ii). We assume the algorithm for Theorem E(i) has already been carried out successfully. Thus, the matrices B_1 and B_2 associated to t_{G_1} and t_{G_2} are written over their centroids, F, and are decomposable. Now use the algorithm in Theorem 6.8 with $L = \mathbb{F}_p$. □

6.4. *Implementation.* We have implemented the algorithms in this section in the computer algebra system Magma [Bosma et al. 1997], and they are publicly available [Maglione 2022]. The plot in Figure 1 shows the runtimes on an Intel Xeon Gold 6138 2.00 GHz running Magma V2.26-11.

We describe the process shown in Figure 1 from Section 1.6. For each prime-power $q = p^e$ up to 10^5, avoiding integers with $p \in \{2, 3\}$, we construct an elliptic curve in short Weierstrass form $y^2 = x^3 + ax + b$, by choosing $(a, b) \in \mathbb{F}_q^2$ uniformly at random and discarding any pair (a, b) satisfying $4a^3 + 27b^2 = 0$. For each elliptic curve E, we choose $P \in E(\mathbb{F}_q) \setminus \{\mathcal{O}\}$ uniformly at random. After writing $\mathrm{B}_{E,P}$ over $\mathbb{F}_p$, our tensor is still represented with convenient choices of bases. In order to remove this bias, we randomly construct $X \in \mathrm{GL}_{6e}(\mathbb{F}_p)$ and $Z \in \mathrm{GL}_{3e}(\mathbb{F}_p)$, and set $\mathrm{B} = X^{\mathrm{t}} \mathrm{B}_{E,P}(Z\boldsymbol{y})X$. We finally construct generators for the automorphism group of $\mathrm{G}_{\mathrm{B}}(\mathbb{F}_p)$ using Theorem E.

Theorem A gives us a characterization of the isomorphism classes of elliptic p-groups for $p \notin \{2, 3\}$. Such a characterization lends itself more easily to explicit computations. In Table 1, for each prime power $q \in [5, 97]$, with q not equal to 2^e or 3^e, we compute the number of isomorphism classes, denoted by N_q, of the $G = \mathrm{G}_{E,P}(F)$ such that $|G| = q^9$.

The data in Table 1 provides good evidence that the following conjecture seems true; in particular this would imply that the function $p \mapsto N_p$ is quasipolynomial.

q	5	7	11	13	17	19	23	25	29	31	37	41	43
N_q	31	57	131	185	307	381	551	385	871	993	1409	1723	1893
q	47	49	53	59	61	67	71	73	79	83	89	97	
N_q	2255	1393	2863	3539	3785	4557	5111	5405	6321	6971	8011	9509	

Table 1. The number of isomorphism classes N_q of the $\mathrm{G}_{E,P}(F)$.

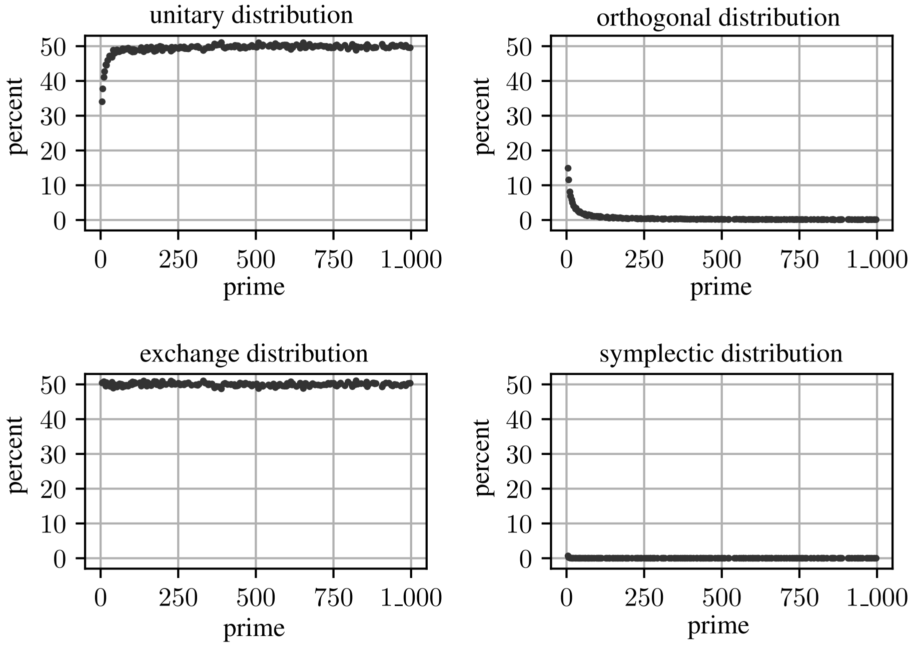

Figure 2. The isomorphism type for the $*$-semisimple part of the adjoint algebra for randomly constructed tensors.

Conjecture 6.9. *For primes $p \geqslant 5$, we have*

$$N_p = p^2 + p - \gcd(p-2, 3) + \gcd(p-1, 4).$$

It is clear that Conjecture 6.9 cannot be true for prime powers: for example,

$$N_{25} = 385 \neq 653 = 25^2 + 25 - \gcd(25-2, 3) + \gcd(25-1, 4).$$

Question 6.10. For fixed e, is $p \mapsto N_{p^e}$ a quasipolynomial?

It may seem that the tensors we consider, namely $\mathrm{B}_{E,P}$, are somewhat rare in general. Indeed, the existence of 3-dimensional totally isotropic subspaces of F^6 should not occur "at random". However, this is not the case. Let $\mathrm{B} \in \mathrm{Mat}_6(F[y_1, y_2, y_3]_1)$ with Pfaffian defining an elliptic curve in $\mathbb{P}_F^2$. By Corollary 3.6, there are four cases for $|\mathcal{T}(\mathrm{B})|$, namely 0, 1, 2, and $q+1$. By Theorem 3.13, if $|\mathcal{T}(\mathrm{B})| \geqslant 1$, then there are three different $*$-semisimple types: $\boldsymbol{O}_1(F)$, $\boldsymbol{X}_1(F)$, and $\boldsymbol{S}_2(F)$. From computer evidence, it seems that $\mathrm{Adj}(\mathrm{B}) \cong \boldsymbol{U}_1(L)$, where L/F is a quadratic extension, whenever $\mathcal{T}(\mathrm{B}) = \varnothing$.

For primes $p \in [3, 1000]$, we constructed 1000 matrices $\mathrm{B} \in \mathrm{Mat}_6(\mathbb{F}_p[y_1, y_2, y_3]_1)$ where $\mathrm{Pf}(\mathrm{B})$ defines an elliptic curve in $\mathbb{P}_{\mathbb{F}_p}^2$. Each B was constructed uniformly at random: there are 36 homogeneous linear polynomials, so we chose 108 elements from $\mathbb{F}_p$ uniformly at random to build B, discarding matrices until they satisfied the required condition. The outcome of the experiment is shown in Figure 2. It seems that, as $p \to \infty$, the probability of $\mathrm{Adj}(\mathrm{B}) \cong \boldsymbol{X}_1(F)$ is equal to 0.5, which seems to also be equal to the probability of $\mathrm{Adj}(\mathrm{B}) \cong \boldsymbol{U}_1(L)$. In other words, it seems that for "random" $\mathrm{B} \in \mathrm{Mat}_6(\mathbb{F}_p[y_1, y_2, y_3]_1)$, we have either $|\mathcal{T}(\mathrm{B})| = 2$ or $|\mathcal{T}(\mathrm{B})| = 0$ at 50% of the time.

Acknowledgements

We wish to thank Daniele Agostini for his precious help in connection to the proof of Theorem A; Mima especially thanks Daniele for always joyfully welcoming her questions. We also thank Fulvio Gesmundo, Carlo Pagano, and Rosa Winter for pointing out [Ng 1995; Duke 1997; Bandini and Paladino 2012] to us. We thank Andrea Bandini for some clarifications around [Bandini and Paladino 2012]. We, moreover, thank Francesco Galuppi, Tobias Rossmann, Christopher Voll for their invaluable comments on an early version of this manuscript. We thank Lars Bügemannskemper for pointing out a typo involving the order of the central automorphisms. We are grateful to the anonymous referees for their careful study of our paper and for their kind and detailed reports, which helped us fix some imprecisions and led to an improvement of the paper.

This project was initiated during a Research in Pairs visit at MFO in March 2022 and was partially supported by the Daimler and Benz Foundation. Maglione was supported by the DFG-Graduiertenkolleg "Mathematical Complexity Reduction" and the DFG grant VO 1248/4-1 (project number 373111162). Stanojkovski was supported by the DFG Project-ID 286237555-TRR 195 and by the Italian program "Rita Levi Montalcini", edition 2020.

References

[Baer 1938] R. Baer, "Groups with abelian central quotient group", *Trans. Amer. Math. Soc.* **44**:3 (1938), 357–386. MR Zbl

[Bandini and Paladino 2012] A. Bandini and L. Paladino, "Number fields generated by the 3-torsion points of an elliptic curve", *Monatsh. Math.* **168**:2 (2012), 157–181. MR Zbl

[Bardestani et al. 2019] M. Bardestani, K. Mallahi-Karai, and H. Salmasian, "Kirillov's orbit method and polynomiality of the faithful dimension of p-groups", *Compos. Math.* **155**:8 (2019), 1618–1654. MR Zbl

[Beauville 2000] A. Beauville, "Determinantal hypersurfaces", *Michigan Math. J.* **48** (2000), 39–64. MR Zbl

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR Zbl

[Boston and Isaacs 2004] N. Boston and I. M. Isaacs, "Class numbers of p-groups of a given order", *J. Algebra* **279**:2 (2004), 810–819. MR Zbl

[Brooksbank and Wilson 2012] P. A. Brooksbank and J. B. Wilson, "Computing isometry groups of Hermitian maps", *Trans. Amer. Math. Soc.* **364**:4 (2012), 1975–1996. MR Zbl

[Brooksbank and Wilson 2015] P. A. Brooksbank and J. B. Wilson, "The module isomorphism problem reconsidered", *J. Algebra* **421** (2015), 541–559. MR Zbl

[Brooksbank et al. 2017] P. A. Brooksbank, J. Maglione, and J. B. Wilson, "A fast isomorphism test for groups whose Lie algebra has genus 2", *J. Algebra* **473** (2017), 545–590. MR Zbl

[Brooksbank et al. 2019] P. A. Brooksbank, E. A. O'Brien, and J. B. Wilson, "Testing isomorphism of graded algebras", *Trans. Amer. Math. Soc.* **372**:11 (2019), 8067–8090. MR Zbl

[Brooksbank et al. 2020] P. A. Brooksbank, J. Maglione, and J. B. Wilson, "Exact sequences of inner automorphisms of tensors", *J. Algebra* **545** (2020), 43–63. MR Zbl

[Cannon and Holt 2003] J. J. Cannon and D. F. Holt, "Automorphism group computation and isomorphism testing in finite groups", *J. Symbolic Comput.* **35**:3 (2003), 241–267. MR Zbl

[Cox et al. 2015] D. A. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*, 4th ed., Springer, 2015. MR Zbl

[Cremona 2003] J. Cremona, "Rational points on curves", course notes, 2003, available at https://www.cise.ufl.edu/research/SpaceTimeUncertainty/Spatial3D/crem03.pdf.

[Duke 1997] W. Duke, "Elliptic curves with no exceptional primes", *C. R. Acad. Sci. Paris Sér. I Math.* **325**:8 (1997), 813–818. MR Zbl

[Eick et al. 2002] B. Eick, C. R. Leedham-Green, and E. A. O'Brien, "Constructing automorphism groups of p-groups", *Comm. Algebra* **30**:5 (2002), 2271–2295. MR Zbl

[Fulton 1969] W. Fulton, *Algebraic curves: an introduction to algebraic geometry*, Benjamin, New York, 1969. MR Zbl

[von zur Gathen and Gerhard 2013] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, 3rd ed., Cambridge Univ. Press, 2013. MR Zbl

[Grunewald and Segal 1984] F. Grunewald and D. Segal, "Reflections on the classification of torsion-free nilpotent groups", pp. 121–158 in *Group theory*, edited by K. W. Gruenberg and J. E. Roseblade, Academic Press, London, 1984. MR Zbl

[Hall 1940] P. Hall, "The classification of prime-power groups", *J. Reine Angew. Math.* **182** (1940), 130–141. MR Zbl

[Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Grad. Texts in Math. **52**, Springer, 1977. MR Zbl

[Hesse 1844] O. Hesse, "Über die Elimination der Variabeln aus drei algebraischen Gleichungen vom zweiten Grade mit zwei Variabeln", *J. Reine Angew. Math.* **28** (1844), 68–96. MR Zbl

[Higman 1960a] G. Higman, "Enumerating p-groups, I: Inequalities", *Proc. Lond. Math. Soc.* (3) **10** (1960), 24–30. MR Zbl

[Higman 1960b] G. Higman, "Enumerating p-groups, II: Problems whose solution is PORC", *Proc. Lond. Math. Soc.* (3) **10** (1960), 566–582. MR Zbl

[Ishitsuka 2017] Y. Ishitsuka, "A positive proportion of cubic curves over $\mathbb{Q}$ admit linear determinantal representations", *J. Ramanujan Math. Soc.* **32**:3 (2017), 231–257. MR Zbl

[Ivanyos and Qiao 2019] G. Ivanyos and Y. Qiao, "Algorithms based on $*$-algebras, and their applications to isomorphism of polynomials with one secret, group isomorphism, and polynomial identity testing", *SIAM J. Comput.* **48**:3 (2019), 926–963. MR Zbl

[Kantor and Luks 1990] W. M. Kantor and E. M. Luks, "Computing in quotient groups", pp. 524–534 in *STOC '90: Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing* (Baltimore, MD, 1990), edited by H. Ortiz, ACM, New York, 1990.

[Lee 2016] S. Lee, "A class of descendant p-groups of order p^9 and Higman's PORC conjecture", *J. Algebra* **468** (2016), 440–447. MR Zbl

[Leedham-Green and Soicher 1998] C. R. Leedham-Green and L. H. Soicher, "Symbolic collection using Deep Thought", *LMS J. Comput. Math.* **1** (1998), 9–24. MR Zbl

[Luks 1992] E. M. Luks, "Computing in solvable matrix groups", pp. 111–120 in *33rd Annual Symposium on Foundations of Computer Science* (Pittsburgh, PA, 1992), IEEE, Los Alamitos, CA, 1992. Zbl

[Maglione 2017] J. Maglione, "Efficient characteristic refinements for finite groups", *J. Symbolic Comput.* **80**:2 (2017), 511–520. MR Zbl

[Maglione 2021] J. Maglione, "Filters compatible with isomorphism testing", *J. Pure Appl. Algebra* **225**:3 (2021), art. id. 106528. MR Zbl

[Maglione 2022] J. Maglione, "EGroups", Magma implementation, 2022, available at https://github.com/joshmaglione/egroups.

[Miller 1978] G. L. Miller, "On the $n^{\log n}$ isomorphism technique", pp. 51–58 in *STOC '78: Proceedings of the Tenth Annual ACM Symposium on Theory of Computing* (San Diego, CA, 1978), ACM, New York, 1978. Zbl

[Neumann 1986] P. M. Neumann, "Some algorithms for computing with finite permutation groups", pp. 59–92 in *Proceedings of groups* (St Andrews, Scotland, 1985), edited by E. F. Robertson and C. M. Campbell, Lond. Math. Soc. Lect. Note Ser. **121**, Cambridge Univ. Press, 1986. MR Zbl

[Ng 1995] K. O. Ng, "The classification of (3, 3, 3) trilinear forms", *J. Reine Angew. Math.* **468** (1995), 49–75. MR Zbl

[O'Brien and Voll 2015] E. A. O'Brien and C. Voll, "Enumerating classes and characters of p-groups", *Trans. Amer. Math. Soc.* **367**:11 (2015), 7775–7796. MR Zbl

[Ravindra and Tripathi 2014] G. V. Ravindra and A. Tripathi, "Torsion points and matrices defining elliptic curves", *Internat. J. Algebra Comput.* **24**:6 (2014), 879–891. MR Zbl

[Rossmann 2020] T. Rossmann, "The average size of the kernel of a matrix and orbits of linear groups, II: Duality", *J. Pure Appl. Algebra* **224**:4 (2020), art. id. 106203. MR Zbl

[Rossmann 2025] T. Rossmann, "On the enumeration of orbits of unipotent groups over finite fields", *Proc. Amer. Math. Soc.* **153**:2 (2025), 479–495. MR Zbl

[Rossmann and Voll 2024] T. Rossmann and C. Voll, *Groups, graphs, and hypergraphs: average sizes of kernels of generic matrices with support constraints*, Mem. Amer. Math. Soc. **1465**, Amer. Math. Soc., Providence, RI, 2024. MR Zbl

[SageMath 2019] *SageMath, Version 8.7*, 2019, available at https://www.sagemath.org.

[du Sautoy 2001] M. du Sautoy, "A nilpotent group and its elliptic curve: non-uniformity of local zeta functions of groups", *Israel J. Math.* **126** (2001), 269–288. MR Zbl

[du Sautoy 2002] M. du Sautoy, "Counting subgroups in nilpotent groups and points on elliptic curves", *J. Reine Angew. Math.* **549** (2002), 1–21. MR Zbl

[du Sautoy and Vaughan-Lee 2012] M. du Sautoy and M. Vaughan-Lee, "Non-PORC behaviour of a class of descendant p-groups", *J. Algebra* **361** (2012), 287–312. MR Zbl

[Seress 2003] Á. Seress, *Permutation group algorithms*, Cambridge Tracts in Math. **152**, Cambridge Univ. Press, 2003. MR Zbl

[Shparlinski 1996] I. Shparlinski, "On finding primitive roots in finite fields", *Theoret. Comput. Sci.* **157**:2 (1996), 273–275. MR Zbl

[Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Grad. Texts in Math. **106**, Springer, 2009. MR Zbl

[Silverman and Tate 2015] J. H. Silverman and J. T. Tate, *Rational points on elliptic curves*, 2nd ed., Springer, 2015. MR Zbl

[Stanojkovski and Voll 2021] M. Stanojkovski and C. Voll, "Hessian matrices, automorphisms of p-groups, and torsion points of elliptic curves", *Math. Ann.* **381**:1-2 (2021), 593–629. MR Zbl

[Vaughan-Lee 2018] M. Vaughan-Lee, "Non-PORC behaviour in groups of order p^7", *J. Algebra* **500** (2018), 30–45. MR Zbl

[Voll 2004] C. Voll, "Zeta functions of groups and enumeration in Bruhat–Tits buildings", *Amer. J. Math.* **126**:5 (2004), 1005–1032. MR Zbl

[Voll 2005] C. Voll, "Functional equations for local normal zeta functions of nilpotent groups", *Geom. Funct. Anal.* **15**:1 (2005), 274–295. MR Zbl

[Weinstein 2016] J. Weinstein, "Reciprocity laws and Galois representations: recent breakthroughs", *Bull. Amer. Math. Soc. (N.S.)* **53**:1 (2016), 1–39. MR Zbl

[Wilson 2012] J. B. Wilson, "Existence, algorithms, and asymptotics of direct product decompositions, I", *Groups Complex. Cryptol.* **4**:1 (2012), 33–72. MR Zbl

[Wilson 2013] J. B. Wilson, "More characteristic subgroups, Lie rings, and isomorphism tests for p-groups", *J. Group Theory* **16**:6 (2013), 875–897. MR

[Wilson 2017] J. B. Wilson, "On automorphisms of groups, rings, and algebras", *Comm. Algebra* **45**:4 (2017), 1452–1478. MR Zbl

[Wyman 1972] B. F. Wyman, "What is a reciprocity law?", *Amer. Math. Monthly* **79** (1972), 571–586. Correction in **80** (1973), 281. MR Zbl

Communicated by Hélène Esnault
Received 2023-04-17 Revised 2024-06-10 Accepted 2024-07-16

joshua.maglione@universityofgalway.ie *School of Mathematical and Statistical Sciences, University of Galway, Galway, Ireland*

mima.stanojkovski@unitn.it *Dipartimento di Matematica, Università di Trento, Trento, Italy*

ALGEBRA AND NUMBER THEORY 19:5 (2025)
https://doi.org/10.2140/ant.2025.19.1007

Malle's conjecture for fair counting functions

Peter Koymans and Carlo Pagano

We show that the naive adaptation of Malle's conjecture to fair counting functions is not true in general.

1. Introduction

1.1. ***Malle's conjecture.*** Number field counting has a rich history in number theory, going back to at least Gauss counting quadratic extensions of $\mathbb{Q}$. The leading conjecture in this field is due to Malle.

Conjecture 1.1 [Malle 2004]. *Let G be a nontrivial finite group and let k be a number field. Then there exists an integer $a(G) \geq 1$, an integer $b(G,k) \geq 0$ and a real number $c(G,k) > 0$ with*

$$|\{K/k : \mathrm{Gal}(K/k) \cong G,\, N_{k/\mathbb{Q}}(\mathrm{Disc}(K/k)) \leq X\}| \sim c(G,k) X^{1/a(G)} (\log X)^{b(G,k)}. \tag{1-1}$$

If we let $\mathrm{Cl}(g)$ be the conjugacy class of an element $g \in G - \{\mathrm{id}\}$ and if we write $g \sim h$ if $\mathrm{Cl}(g)$ and $\mathrm{Cl}(h)$ are equivalent under the cyclotomic action of k, then we have

$$b(G,k) = -1 + n, \tag{1-2}$$

where n is the number of equivalence classes of $G - \{\mathrm{id}\}$ under $\sim$ consisting entirely of elements with minimal order in G.

Although this conjecture has been exceptionally influential, numerous issues have come to light. One problem with Malle's conjecture is that it is not correct with the first counterexample due to Klüners [2005]. However, there are also other undesirable features that are inherently tied with counting by discriminant that we will now discuss.

One desirable feature of a counting function is that the leading constant $c(G,k)$ is an Euler product. This type of leading constants are frequent in rational points counting, and suggest a good compatibility between global and local behavior. In the case of S_n, the leading constant $c(G,k)$ is conjectured to be an Euler product [Bhargava 2007], in which case we say that the *Malle–Bhargava* principle holds. It is however not always the case that the leading constant is an Euler product. This problem already manifests itself when dealing with quartic D_4-extensions, see the work of Cohen, Diaz, y Diaz and Olivier [Cohen et al. 2002] and of Altuğ, Shankar, Varma and Wilson [Altuğ et al. 2021]. In general, it is still unclear when we expect the Malle–Bhargava principle to hold true.

MSC2020: primary 11N45, 11R45; secondary 11R21, 11R29.
Keywords: Malle's conjecture, number fields.

Another related undesirable feature of discriminant counting is the *subfield problem*. When counting by discriminant, it may happen that a positive proportion of the fields counted share a common subfield. This already happens for quartic D_4-extensions, and is the main underlying cause for the failure of the leading constant to be an Euler product.

1.2. ***Fair counting functions.*** The above reasons have led to an increasing interest in *fair counting functions*, first introduced by Wood [2010]. We shall restrict ourselves to the product of ramified primes, which is the most prominent fair counting function. We consider the following naive modification of Malle's conjecture. Write $\mathfrak{f}(K/k)$ for the product of primes of k that ramify in K.

Conjecture 1.2 (folklore adaptation of Malle's conjecture). *Let G be a nontrivial finite group and let k be a number field. Then there exists an integer $b(G,k) \geq 0$ and a real number $c(G,k) > 0$ such that*

$$|\{K/k : \mathrm{Gal}(K/k) \cong G,\ N_{k/\mathbb{Q}}(\mathfrak{f}(K/k)) \leq X\}| \sim c(G,k)X(\log X)^{b(G,k)}. \tag{1-3}$$

If we let $\mathrm{Cl}(g)$ be the conjugacy class of an element $g \in G - \{\mathrm{id}\}$ and if we write $g \sim h$ if $\mathrm{Cl}(g)$ and $\mathrm{Cl}(h)$ are equivalent under the cyclotomic action of k, then we have

$$b(G,k) = -1 + n, \tag{1-4}$$

where n is the number of equivalence classes of $G - \{\mathrm{id}\}$ under $\sim$.

Maki [1993] proved this conjecture for abelian extensions, and Wood [2010] proved the same for any fair counting function and arbitrary finite sets of local conditions. It is important to emphasize that the leading constant $c(G,k)$ is an Euler product and that the subfield problem also disappears in all known cases. An additional benefit is that this counting function is much more natural from a geometric perspective occurring prominently in function field counting, which is rife with geometric techniques.

Number field counting is intimately related to finding the distribution of class groups. Counting by discriminant also leads to problems in this setting, as first uncovered in [Bartel and Lenstra 2020]. Bartel and Lenstra give a counterexample to the Cohen–Martinet heuristics with the root cause being precisely the subfield problem. These reasons strongly suggests that it may be preferable to count by fair counting functions instead of the discriminant.

1.3. ***Results and conjectures.*** Our main result shows that Conjecture 1.2 is not correct.

Theorem 1.3. *There exists an infinite family of nilpotent groups G of nilpotency class 2 such that Conjecture 1.2 fails for the pair $(G, \mathbb{Q})$. More precisely, the constant $b(G, \mathbb{Q})$ in (1-4) is too small.*

Although we have restricted to $\mathbb{Q}$ for simplicity, it is not difficult to adapt our arguments to find many more counterexamples of a similar flavor showing that the above phenomenon persists in a wide number of settings.

Our counterexample is of a genuinely different nature than Klüners' counterexample. Firstly, Klüners takes $G = C_3 \wr C_2$, which is solvable but not nilpotent. Secondly, Klüners' counterexample is no longer a counterexample when counting by product of ramified primes, which was historically another important motivation to count by ramified primes. In fact, Koymans and Pagano [2023, Section 3.2] have previously given strong heuristic evidence that Malle's original conjecture, see Conjecture 1.1, is correct for nilpotent extensions. Thirdly and perhaps most importantly, although both counterexamples proceed by fixing a cyclotomic subextension, Klüners' counterexample relies on the shrinking of the cyclotomic action, while we fundamentally rely on a certain *entanglement of Frobenius* that shrinks the conjugation action.

A novel feature of our work is the first family of counterexamples when counting G-extensions in their regular representation. This phenomenon has never been observed for discriminant counting. All known modifications of Malle's conjecture (such as [Türkelli 2015]) predict no counterexamples when counting G-extensions by discriminant in their regular representation.

We still expect the veracity of the asymptotic in (1-3), but of course not with the naive choice of $b(G, \mathbb{Q})$ from (1-4). It is at present unclear what the right choice of $b(G, \mathbb{Q})$ is in general. We will however make several predictions. We have opted to restrict ourselves to nilpotent extensions as even merely making predictions for number field counting has proven to be a deceptively difficult task.

To this end, let $\phi : G \twoheadrightarrow H$ be a surjective homomorphism, let $\chi(\text{cyc}) : G_{\mathbb{Q}} \to (\mathbb{Z}/|G|\mathbb{Z})^*$ be the cyclotomic character and let $r : (\mathbb{Z}/|G|\mathbb{Z})^* \twoheadrightarrow H$ be a surjection. We define

$$\text{Epi}_{(H,\phi)}(G_{\mathbb{Q}}, G)$$

be the set of continuous surjective homomorphisms $\psi : G_{\mathbb{Q}} \twoheadrightarrow G$ satisfying the equations

$$\phi \circ \psi = r \circ \chi(\text{cyc}), \quad \mathbb{Q}(\psi) \cap \mathbb{Q}(\zeta_{|G|}) = \mathbb{Q}(\phi \circ \psi).$$

We write $G \times_H (\mathbb{Z}/|G|\mathbb{Z})^* \subseteq G \times (\mathbb{Z}/|G|\mathbb{Z})^*$ for the subgroup consisting of pairs (g, α) such that $\phi(g) = r(\alpha)$. We let $G \times (\mathbb{Z}/|G|\mathbb{Z})^*$ act on $\ker(\phi) - \{\text{id}\}$ by sending n to $gn^{\alpha}g^{-1}$. We restrict this action to the subgroup $G \times_H (\mathbb{Z}/|G|\mathbb{Z})^*$, and we denote by

$$b_{(H,\phi)}(G) := |(\ker(\phi) - \{\text{id}\})/(G \times_H (\mathbb{Z}/|G|\mathbb{Z})^*)|$$

the resulting number of equivalence classes.

Conjecture 1.4 (Conjecture 5.1). *Let G be a nilpotent group. For each H, ϕ as above, there exists a positive constant $c_{(H,\phi)}(G)$ such that*

$$|\{\psi \in \text{Epi}_{(H,\phi)}(G_{\mathbb{Q}}, G) : \mathfrak{f}(\psi) \leq X\}| \sim c_{(H,\phi)}(G) \cdot X \cdot \log(X)^{b_{(H,\phi)}(G)-1}.$$

Conjecture 1.5 (Conjecture 5.5). *Let G be a nilpotent group with $|G|$ odd. Then the leading constant $c_{(H,\phi)}(G)$ satisfies the Malle–Bhargava principle.*

For the precise computation of the leading constant provided by the Malle–Bhargava principle, we refer to Conjecture 5.5. It is tempting to speculate that both conjectures are true in a much wider generality, which we shall leave as an open question. However, Conjecture 5.5 does not hold when $|G|$ is even, in which case a rational correction factor is needed.

We will now explicate Theorem 1.3, in particular the construction of the infinite family G. We take $Q_n = \mathbb{Z}/3\mathbb{Z} \oplus (\mathbb{Z}/9\mathbb{Z})^n$. We let $\pi_0 : Q_n \to \mathbb{Z}/3\mathbb{Z}$ be the projection on the first $\mathbb{Z}/3\mathbb{Z}$ and we let $\pi_i : Q_n \to \mathbb{Z}/3\mathbb{Z}$ be the projection on the i-th $\mathbb{Z}/9\mathbb{Z}$ composed with the quotient map $\mathbb{Z}/9\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$. We introduce the 2-cocycles

$$\theta_i(\sigma, \tau) := \pi_0(\sigma) \cdot \pi_i(\tau) \in H^2(Q_n, \mathbb{Z}/3\mathbb{Z})$$

and $\theta := (\theta_1, \dots, \theta_n) \in H^2(Q_n, (\mathbb{Z}/3\mathbb{Z})^n)$. Given such a θ, we have a corresponding central exact sequence given by

$$1 \to (\mathbb{Z}/3\mathbb{Z})^n \to G_n \to Q_n \to 1.$$

In our proofs, we will choose the family $(G_n)_{n \geq 2}$ for the infinite family of Theorem 1.3. In the process we will also prove a special case of Conjectures 1.4 and 1.5.

Theorem 1.6 (Theorem 3.4). *Let G_n be as above and write $q_n : G_n \to Q_n$ for the natural quotient map. Let $H_n := \mathbb{Z}/3\mathbb{Z}$ and let $\phi := \pi_0 \circ q_n$. Let $\rho : G_{\mathbb{Q}} \to \mathbb{Z}/3\mathbb{Z}$ be any character such that the fixed field of the kernel equals $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. Then we have*

$$\sum_{\substack{\psi \in \mathrm{Epi}(G_{\mathbb{Q}}, G_n) \\ \pi_0 \circ q_n \circ \psi = \rho \\ \mathfrak{f}(\psi) \leq X}} 1 \sim 27^n \cdot \frac{X \cdot (\log X)^{\alpha - 1}}{3 \cdot \Gamma(\alpha)} \cdot c_0,$$

where $\alpha := (9^n - 1)/3 + (27^n - 1)/6$ and c_0 equals the conditionally convergent Euler product

$$c_0 := \prod_p \left(1 + \frac{(9^n - 1)\mathbf{1}_{p \equiv 4,7 \bmod 9} + (27^n - 1)\mathbf{1}_{p \equiv 1 \bmod 9}}{p}\right)\left(1 - \frac{1}{p}\right)^{\alpha}.$$

One pleasant feature is that $\ker(\phi) \cong (\mathbb{Z}/9\mathbb{Z})^n \oplus (\mathbb{Z}/3\mathbb{Z})^n$ is abelian despite the fact that G_n is not. It is no coincidence that the logarithmic exponent matches exactly the logarithmic exponent when counting $(\mathbb{Z}/9\mathbb{Z})^n \oplus (\mathbb{Z}/3\mathbb{Z})^n$-extensions. In fact, once one fixes the subextension $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, we have the remarkable property that any $G_n/[G_n, G_n]$-extension lifts to a G_n-extension. This is the crux of our counterexample stemming from Lemma 2.1. Once we have proven Theorem 1.6 in Section 3, the computation of $b(G_n, \mathbb{Q})$ in Section 4 immediately gives Theorem 1.3.

In fact, it is plausible that one can use [Alberts and O'Dorney 2021, Theorem 1.1] or [Darda and Yasuda 2023, Theorem 1.3.3] to prove Conjectures 1.4 and 1.5 as soon as $\ker(\phi)$ is abelian, with substantial work required to deduce explicitly from those works the leading constant c_0 and the logarithmic exponent α. We have opted to give a different proof to keep our work completely self-contained.

We remark that if H and ϕ are trivial, then $b_{(H,\phi)}(G)$ equals the right-hand side of (1-4). In particular, we predict that the full Malle–Bhargava principle holds when counting tame, nilpotent G-extensions with $|G|$ odd. We emphasize that, once one accounts for the counterexamples found in Theorem 1.3, all good properties of fair counting functions are restored again: the leading constant is an Euler product and the subfield problem disappears.

1.4. ***Comparison with previous results and conjectures.*** Malle's original conjecture has been proven over $\mathbb{Q}$ for a handful of specific groups namely for:

- Cubic S_3-extensions [Davenport and Heilbronn 1971].
- Quartic S_4-extensions and quintic S_5-extensions [Bhargava 2005; 2010].
- Sextic S_3-extensions [Belabas and Fouvry 2010; Bhargava and Wood 2008].
- Abelian extensions [Wright 1989].
- Direct products $G \times A$ with $G \in \{S_3, S_4, S_5\}$ and A abelian [Masri et al. 2020], building on the earlier work [Wang 2021].
- Quartic D_4-extensions [Cohen et al. 2002].
- Nonic Heisenberg extensions [Fouvry and Koymans 2021].
- Certain wreath products [Klüners 2012].
- Nilpotent groups such that all minimal order elements are central [Koymans and Pagano 2023].

In many situations we have upper and lower bounds for number field counting instead of asymptotics. This comprises a vast literature as well, including work of Alberts [2021], Klüners and Malle [2004], Ellenberg and Venkatesh [2006], Couveignes [2020] and Lemke Oliver and Thorne [2022].

Of particular relevance to our work is the recent spur of other modifications of Malle's conjecture. This was initiated by Türkelli [2015] for discriminant counting, who modified Conjecture 1.1 to account for Klüners' counterexample. Our prediction for $b_{(H,\phi)}(G)$ is a direct parallel of Türkelli's modification.

Gundlach [2022, Conjecture 1.5] proposed a variant of Malle's conjecture where one counts by multiple fair invariants. He avoids our counterexamples by demanding that this invariant lies in the range $(\delta X, X)$ for some $\delta > 0$. Our conjecture however does not impose this condition, which necessitates a more thorough treatment of the logarithmic exponent $b_{(H,\phi)}(G)$.

Darda and Yasuda [2023, Conjecture 1.3.1] propose a far reaching conjecture for counting points on stacks by a wide class of height functions. Their conjecture is similar in spirit than ours but substantially less precise: our conjecture is more precise under what circumstances the logarithmic exponent may increase and also more precise about the leading constant; with no prediction being made in [loc. cit.]. We remark that none of the aforementioned works [Darda and Yasuda 2023; Gundlach 2022; Türkelli 2015] make a prediction about the leading constant $c_{(H,\phi)}(G)$.

1.5. ***Overview of the paper.*** The key result for our counterexample is Lemma 2.1. This lemma shows that the group G_n has the key property that all $G_n/[G_n, G_n]$-extensions lift to a G_n-extension once one fixes a suitable cyclotomic subextension. We will exploit Lemma 2.1 to show in Section 3 that the count of $\psi \in \mathrm{Hom}(G_{\mathbb{Q}}, G_n)$, containing this suitably constructed cyclotomic subextension, equals the number of abelian $(\mathbb{Z}/9\mathbb{Z})^n \oplus (\mathbb{Z}/3\mathbb{Z})^n$-extensions. In Section 4 we will compute the naive Malle constant $b(G_n, \mathbb{Q})$. These results immediately give Theorem 1.3. In our final Section 5 we motivate Conjectures 1.4 and 1.5.

2. The construction

We fix in the rest of the paper an algebraic closure $\mathbb{Q}^{\text{sep}}$ of $\mathbb{Q}$ and for each place v an algebraic closure $\mathbb{Q}_v^{\text{sep}}$ of $\mathbb{Q}_v$. We furthermore fix an embedding

$$i_v : \mathbb{Q}^{\text{sep}} \to \mathbb{Q}_v^{\text{sep}},$$

providing us with an embedding

$$i_v^* : G_{\mathbb{Q}_v} \to G_{\mathbb{Q}}.$$

We denote by $\mathcal{G}(3)$ the pro-3 completion of a profinite group $\mathcal{G}$. We fix a choice of the cyclotomic character

$$\chi_{\text{cyc}}(3) : G_{\mathbb{Q}} \twoheadrightarrow \mathbb{Z}_3.$$

For each prime number p congruent to 1 modulo 3, we fix an element $\sigma_p' \in G_{\mathbb{Q}_p}$ such that its image in $G_{\mathbb{Q}_p}(3)$ is a topological generator of the inertia subgroup. We denote by σ_p the image of σ_p' in $G_{\mathbb{Q}}(3)$ by applying i_p^* followed by the natural projection map $G_{\mathbb{Q}} \to G_{\mathbb{Q}}(3)$. We fix any element σ_3 of $G_{\mathbb{Q}}(3)$ with $\chi_{\text{cyc}}(3)(\sigma_3) = 1$ and coming from the inertia subgroup of $G_{\mathbb{Q}_3}$ in the manner just described above.

We define

$$\mathfrak{G} := \{\sigma_p : p \equiv 1 \bmod 3\} \cup \{\sigma_3\} \subseteq G_{\mathbb{Q}}(3).$$

For each p congruent to 1 modulo 3, we put $\chi_p : G_{\mathbb{Q}} \to \mathbb{Z}/3\mathbb{Z}$ to be the unique character which ramifies only at p and with $\chi_p(\sigma_p) = 1$. We define χ_3 to be the reduction modulo 3 of $\chi_{\text{cyc}}(3)$. Furthermore, for each p congruent to 1 modulo 9, we put $\psi_p : G_{\mathbb{Q}} \to \mathbb{Z}/9\mathbb{Z}$ to be the unique character which ramifies only at p and with $\psi_p(\sigma_p) = 1$. We set ψ_3 to be the reduction modulo 9 of $\chi_{\text{cyc}}(3)$. Then the set

$$\{\chi_p : p \equiv 0, 1 \bmod 3\}$$

is a basis for $\text{Hom}(G_{\mathbb{Q}}(3), \mathbb{Z}/3\mathbb{Z})$, which is dual to $\mathfrak{G}$. It follows that $\mathfrak{G}$ is a minimal set of topological generators for $G_{\mathbb{Q}}(3)$.

For a continuous homomorphism $\psi : G_{\mathbb{Q}} \to \mathcal{G}$, where $\mathcal{G}$ is a profinite group, we define

$$\mathbb{Q}(\psi) := (\mathbb{Q}^{\text{sep}})^{\ker(\psi)}.$$

In the case $\mathcal{G}$ is a finite group, we denote by $\mathfrak{f}(\psi)$ the product of the finite rational primes ramifying in $\mathbb{Q}(\psi)/\mathbb{Q}$. Likewise, for $\psi : G_{\mathbb{Q}_p} \to \mathcal{G}$, we define $\mathfrak{f}(\psi)$ to be p in the case ψ is ramified and 1 in the case ψ is unramified.

Consider $Q_n = \mathbb{Z}/3\mathbb{Z} \oplus (\mathbb{Z}/9\mathbb{Z})^n$. Write $\pi_0 : Q_n \to \mathbb{Z}/3\mathbb{Z}$ for the projection on the first $\mathbb{Z}/3\mathbb{Z}$ and write $\pi_i : Q_n \to \mathbb{Z}/3\mathbb{Z}$ for the projection on the i-th $\mathbb{Z}/9\mathbb{Z}$ followed by the quotient map $\mathbb{Z}/9\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$. We define

$$\theta_i(\sigma, \tau) := \pi_0(\sigma) \cdot \pi_i(\tau) \in H^2(Q_n, \mathbb{Z}/3\mathbb{Z})$$

and $\theta := (\theta_1, \ldots, \theta_n) \in H^2(Q_n, (\mathbb{Z}/3\mathbb{Z})^n)$. Given such a θ, we may attach a central extension

$$1 \to (\mathbb{Z}/3\mathbb{Z})^n \to G_n \to Q_n \to 1.$$

We will show, for sufficiently large n, that G_n is a counterexample.

From now on we will consider all our abelian groups as discrete $G_{\mathbb{Q}}$-modules with trivial action. Given $\phi \in \mathrm{Hom}(G_{\mathbb{Q}}, Q_n)$, we write $\theta_{i,\phi} \in H^2(G_{\mathbb{Q}}, \mathbb{Z}/3\mathbb{Z})$ and $\theta_\phi \in H^2(G_{\mathbb{Q}}, (\mathbb{Z}/3\mathbb{Z})^n)$ for the inflation of θ_i and θ to $G_{\mathbb{Q}}$ using ϕ. The following lemma is the crux of the counterexample. Informally speaking, it shows that any homomorphism $\phi : G_{\mathbb{Q}} \to Q_n$ satisfying $\pi_0 \circ \phi \in \{\chi_3, 2\chi_3\}$, i.e., $\mathbb{Q}(\pi_0 \circ \phi) = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, lifts to G_n. This will be the source of the abundance of G_n-extensions.

Lemma 2.1. *Let $\phi \in \mathrm{Hom}(G_{\mathbb{Q}}, Q_n)$ be such that $\mathbb{Q}(\pi_0 \circ \phi) = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. Then there exists a homomorphism $\psi : G_{\mathbb{Q}} \to G_n$ lifting ϕ.*

Proof. Note that G_n is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^n \times_\theta Q_n$, where multiplication is given by

$$(c_1, a_1) *_\theta (c_2, a_2) = (c_1 + c_2 + \theta(a_1, a_2), a_1 + a_2).$$

Any lift $\psi : G_{\mathbb{Q}} \to G_n$ of ϕ is of the shape (ψ', ϕ) for some map $\psi' : G_{\mathbb{Q}} \to (\mathbb{Z}/3\mathbb{Z})^n$. Imposing that ψ is a homomorphism means precisely that θ_ϕ is trivial in $H^2(G_{\mathbb{Q}}, (\mathbb{Z}/3\mathbb{Z})^n)$, which is the case if and only if each $\theta_{i,\phi}$ is trivial in $H^2(G_{\mathbb{Q}}, \mathbb{Z}/3\mathbb{Z})$.

Therefore it suffices to show that $\theta_{i,\phi}$ is trivial in $H^2(G_{\mathbb{Q}}, \mathbb{Z}/3\mathbb{Z})$ for each i. By class field theory we have an injection

$$H^2(G_{\mathbb{Q}}, \mathbb{Z}/3\mathbb{Z}) \to \bigoplus_v H^2(G_{\mathbb{Q}_v}, \mathbb{Z}/3\mathbb{Z}).$$

Now let v be a place of $\mathbb{Q}$. We will check that the restriction of $\theta_{i,\phi}$ is trivial at v. If v is real, then $H^2(G_{\mathbb{Q}_v}, \mathbb{Z}/3\mathbb{Z}) = 0$. If $v = (3)$, then we also have $H^2(G_{\mathbb{Q}_v}, \mathbb{Z}/3\mathbb{Z}) = 0$ by a well-known result of Shafarevich. Using local Tate duality as in [Neukirch et al. 2000, Theorem 7.2.6], Shafarevich's result follows immediately from $H^2(G_{\mathbb{Q}_3}, \mathbb{Z}/3\mathbb{Z}) \cong H^0(G_{\mathbb{Q}_3}, \mu_3) = 0$.

We define K_i to be the fixed field of $\pi_{0,i} \circ \phi$, where $\pi_{0,i} : Q_n \to (\mathbb{Z}/3\mathbb{Z})^2$ is the homomorphism given by

$$\pi_{0,i}(a) = (\pi_0(a), \pi_i(a)).$$

If v is unramified in K_i, then the restriction of $\theta_{i,\phi}$ to $G_{\mathbb{Q}_v}$ factors through the maximal unramified extension of $\mathbb{Q}_v$, therefore giving a class in $H^2(\hat{\mathbb{Z}}, \mathbb{Z}/3\mathbb{Z}) = 0$.

It remains to treat finite places v, coprime to 3, that are ramified in K_i. Recall that $\theta_{i,\phi}$ is the class of the 2-cochain $c(\sigma, \tau)$ given by

$$(\sigma, \tau) \mapsto \pi_0(\phi(\sigma)) \cdot \pi_i(\phi(\tau)).$$

We claim that $\pi_0(\phi(\sigma))$ is the zero map when restricted to $G_{\mathbb{Q}_v}$. This implies that $c(\sigma, \tau)$ is also the zero map when restricted to $G_{\mathbb{Q}_v}$. In particular, $\theta_{i,\phi}$ is trivial in $H^2(G_{\mathbb{Q}_v}, \mathbb{Z}/3\mathbb{Z})$, and thus the lemma is a consequence of the claim.

In order to prove the claim, observe that our assumptions imply that v ramifies in $\pi_i \circ \phi$ but not in $\pi_0 \circ \phi = \rho$, which is ramified only at 3. Since $v \neq (3)$ and since $\pi_i \circ \phi$ lifts to a $\mathbb{Z}/9\mathbb{Z}$-extension, class field theory over $\mathbb{Q}$ shows that $v \equiv 1 \bmod 9$. But then v splits completely in $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, which gives the claim. □

3. Finding many lifts

Call $q_n : G_n \to Q_n$ the natural quotient map.

Definition 3.1. We define $\mathcal{G}_{n,\mathrm{bad}}$ to be the set of tuples $(v_g)_{g \in G_n - \{\mathrm{id}\}}$ satisfying the following conditions:

- v_g is a positive squarefree integer for every $g \in G_n - \{\mathrm{id}\}$.
- v_g and v_h are coprime for every $g, h \in G_n - \{\mathrm{id}\}$ with $g \neq h$.
- If $p \mid v_g$ for some $g \in G_n - \{\mathrm{id}\}$ satisfying $\pi_0(q_n(g)) = 0$, then $p \equiv 1 \mod \mathrm{ord}(g)$.
- We have
$$\prod_{\substack{g \in G_n - \{\mathrm{id}\} \\ \pi_0(q_n(g)) \neq 0}} v_g = 3.$$

Lemma 3.2. *Let $g \in G_n$ and suppose that $q_n(g) \neq 0$. Then* $\mathrm{ord}(g) = \mathrm{ord}(q_n(g))$.

Proof. Write $G_n = (\mathbb{Z}/3\mathbb{Z})^n \times_\theta Q_n$, write $g = (c, q_n(g))$ and write $m = \mathrm{ord}(q_n(g))$. Then a calculation using the group law on G_n given by θ shows that
$$g^m = \left(\sum_{j=1}^{m-1} \theta(q_n(g), q_n(g)^j), 0\right).$$
Now observe that
$$\sum_{j=1}^{m-1} \theta(q_n(g), q_n(g)^j) = \left(\sum_{j=1}^{m-1} \pi_0(q_n(g)) \cdot \pi_1(q_n(g)^j), \dots, \sum_{j=1}^{m-1} \pi_0(q_n(g)) \cdot \pi_n(q_n(g)^j)\right).$$
Since we have $\sum_{j=1}^{m-1} \pi_i(q_n(g)^j) = \pi_i(q_n(g)) \sum_{j=1}^{m-1} j = 0$, the lemma follows. □

Following the Koymans–Pagano parametrization technique [Koymans and Pagano 2023] yields the following key result. For the convenience of the reader we give a direct proof of this special case from scratch.

Theorem 3.3. *There is a bijection* Par *between $\mathcal{G}_{n,\mathrm{bad}}$ and the subset of $\psi \in \mathrm{Hom}(G_{\mathbb{Q}}, G_n)$ such that $\mathbb{Q}(\pi_0 \circ q_n \circ \psi) = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. Writing $\mathfrak{f}(\psi)$ for the product of ramified primes of a homomorphism ψ, we have*
$$\mathfrak{f}(\mathrm{Par}((v_g)_{g \in G_n - \{\mathrm{id}\}})) = \prod_{g \in G_n - \{\mathrm{id}\}} v_g. \tag{3-1}$$
Furthermore, the homomorphism $\mathrm{Par}((v_g)_{g \in G_n - \{\mathrm{id}\}}) : G_{\mathbb{Q}} \to G_n$ *is surjective if and only if*
$$\langle q_n(\{g \in G_n - \{\mathrm{id}\} : v_g \neq 1\}) \rangle = Q_n. \tag{3-2}$$

Proof. Let us define $\mathrm{Hom}_{n,\mathrm{bad}}$ to be the set of continuous homomorphisms $\psi : G_{\mathbb{Q}}(3) \to G_n$ with the property that
$$\mathbb{Q}(\pi_0 \circ q_n \circ \psi) = \mathbb{Q}(\zeta_9 + \zeta_9^{-1}).$$

We begin by constructing a map $\mathrm{Ev} : \mathrm{Hom}_{n,\mathrm{bad}} \to \mathcal{G}_{n,\mathrm{bad}}$ in the following manner. Given $\psi \in \mathrm{Hom}_{n,\mathrm{bad}}$, we consider the vector

$$(v_g)_{g \in G_n - \{\mathrm{id}\}}$$

consisting of positive squarefree numbers divisible only by primes congruent to 0, 1 modulo 3 uniquely defined through the property

$$p \mid v_g \quad \Longleftrightarrow \quad \psi(\sigma_p) = g.$$

Let us check that Ev indeed maps $\mathrm{Hom}_{n,\mathrm{bad}}$ to $\mathcal{G}_{n,\mathrm{bad}}$. Since ψ is a function, it follows that the vector $(v_g)_{g \in G_n - \{\mathrm{id}\}}$ consists of pairwise coprime squarefree integers by construction. In other words, the first two points of Definition 3.1 are taken care of. Let us verify the third point and distinguish for that purpose two cases. Suppose first that $q_n(g) = 0$. Then $\mathrm{ord}(g) = 3$, so that the condition becomes $p \equiv 1 \bmod 3$, which is automatically satisfied as primes $p \equiv 2 \bmod 3$ are unramified in 3-extensions. Suppose now that $q_n(g) \neq 0$. Then by Lemma 3.2 we know that $\mathrm{ord}(g) = \mathrm{ord}(q_n(g))$. Hence we need to show that $p \equiv 1 \bmod \mathrm{ord}(q_n(g))$. The map $q_n \circ \psi \circ i_p^*$ induces a continuous homomorphism

$$G_{\mathbb{Q}_p} \to G_{\mathbb{Q}_p}^{\mathrm{ab}} \to Q_n,$$

sending σ_p' to $q_n(g)$. But the order of the image of σ_p' in an abelian extension of $\mathbb{Q}_p$ is always a divisor of $p - 1$ so that $p \equiv 1 \bmod \mathrm{ord}(q_n(g))$ as desired.

Let us now show that the vector $(v_g)_{g \in G_n - \{\mathrm{id}\}}$ satisfies the fourth point of Definition 3.1. Observe that for each prime $p \equiv 1 \bmod 3$ we have $\pi_0 \circ q_n \circ \psi(\sigma_p) \in \{\chi_3(\sigma_p), 2 \cdot \chi_3(\sigma_p)\} = \{0\}$. It follows that the variables v_g, with $\pi_0(q_n(g)) \neq 0$, are all equal to 1 or 3. Since we have shown that they are pairwise coprime, at most one of them equals 3, namely $\psi(\sigma_3)$. This gives the desired fourth point of Definition 3.1.

We will now show that (3-1) holds. Indeed, 3 is certainly both a divisor of $\mathfrak{f}(\psi)$ and $\prod_{g \in G_n - \{\mathrm{id}\}} v_g$, since the extension ramifies at 3 and we have just verified the fourth bullet point of Definition 3.1. For a prime $p \equiv 1 \bmod 3$, we have that the ramification index of $\mathbb{Q}^{\ker(\psi)}/\mathbb{Q}$ at p equals precisely the order of $\psi(\sigma_p)$. Primes congruent to 2 modulo 3 are always unramified in a 3-extension.

We now observe that $\mathrm{Ev}(\psi)$ determines the value of ψ on $\mathfrak{G}$, which is a set of topological generators, and therefore $\mathrm{Ev}(\psi)$ determines ψ. In other words, the map Ev is injective. Furthermore, the fact that $\mathfrak{G}$ is a set of topological generators gives at once that

$$\mathrm{im}(\psi) := \langle \psi(\mathfrak{G}) \rangle = \langle \{g \in G_n - \{\mathrm{id}\} : v_g \neq 1\} \rangle.$$

In particular, ψ is surjective if and only if $G_n = \langle \{g \in G_n - \{\mathrm{id}\} : v_g \neq 1\} \rangle$. Recall that a set generates a nilpotent group if and only if it generates the abelianization. Then the elementary observation that Q_n is the abelianization of G_n yields (3-2).

We are only left with showing that Ev is surjective. We will proceed in 3 steps. Let $(v_g)_{g \in G_n - \{\mathrm{id}\}}$ be in $\mathcal{G}_{n,\mathrm{bad}}$:

Step 1: Define $\psi^{\mathrm{ab}} := (\psi_i^{\mathrm{ab}})_{i=0}^n : G_{\mathbb{Q}} \to Q_n$ using the formula

$$\psi_i^{\mathrm{ab}} := \begin{cases} \pi_0(q_n(g_0)) \cdot \chi_3 & \text{for } i = 0, \\ \sum_{g \in G_n - \{\mathrm{id}\}} \sum_{p \mid v_g} \mu_i(g) \cdot \psi_p & \text{for } 1 \leq i \leq n, \end{cases}$$

where g_0 is the unique element of $G_n - \{\mathrm{id}\}$ with $v_{g_0} = 3$, where $\mu_i : G_n \to Q_n \to \mathbb{Z}/9\mathbb{Z}$ is the projection map, where ψ_p is defined in Section 2 and where $\cdot$ denotes the usual multiplication in $\mathbb{Z}/3\mathbb{Z}$, respectively $\mathbb{Z}/9\mathbb{Z}$.

Step 2: We have $\pi_0 \circ \psi^{\mathrm{ab}} = \pi_0(q_n(g_0)) \cdot \chi_3$ by construction. Therefore we have that ψ^{ab} can be lifted to a homomorphism $\psi : G_{\mathbb{Q}} \to G_n$ thanks to Lemma 2.1. The choice of such a lift consists precisely of the choice of a vector of continuous 1-cochains $(\phi_i)_{i=1}^n$ with each $\phi_i : G_{\mathbb{Q}} \to \mathbb{Z}/3\mathbb{Z}$ fulfilling the property

$$d\phi_i(\sigma, \tau) = \theta_i(\psi^{\mathrm{ab}}(\sigma), \psi^{\mathrm{ab}}(\tau)) = \theta_{i,\psi^{\mathrm{ab}}}(\sigma, \tau),$$

where $d\phi_i(\sigma, \tau) = \phi_i(\sigma\tau) - \phi_i(\sigma) - \phi_i(\tau)$. Indeed, such a vector completes the map ψ^{ab} into a set-theoretic map $((\phi_i)_{i=1}^n, \psi^{\mathrm{ab}}) : G_{\mathbb{Q}} \to G_n$, which is a group homomorphism precisely owing to the cocycle equation. Conversely, given a lift ψ, we have that $\phi_i := \rho_i \circ \psi$ provides the desired 1-cochains, where $\rho_i : G_n \to \mathbb{Z}/3\mathbb{Z}$ is the projection on the i-th $\mathbb{Z}/3\mathbb{Z}$ in $(\mathbb{Z}/3\mathbb{Z})^n \times_\theta Q_n$ (note that ρ_i is not a group homomorphism).

We next define

$$\phi_i(\mathrm{clean}) := \phi_i - \phi_i(\sigma_3) \cdot \chi_3 - \sum_{p \equiv 1 \bmod 3} \phi_i(\sigma_p) \cdot \chi_p,$$

which now vanishes at all the elements of $\mathfrak{G}$ (observe that the sum is finite, since ϕ_i vanishes on all but finitely many σ_p by continuity).

Step 3: We now define

$$\phi_i(\mathrm{twist}) := \phi_i(\mathrm{clean}) + \sum_{g \in G_n - \{\mathrm{id}\}} \rho_i(g) \cdot \sum_{p \mid v_g} \chi_p.$$

This gives us a homomorphism

$$\psi(\mathrm{twist}) := ((\phi_i(\mathrm{twist}))_{i=1}^n, \psi^{\mathrm{ab}}) : G_{\mathbb{Q}} \to G_n$$

satisfying by construction that $\psi(\mathrm{twist})(\sigma_p) = g$ if and only if $p \mid v_g$. Therefore

$$\mathrm{Ev}(\psi(\mathrm{twist})) = (v_g)_{g \in G_n - \{\mathrm{id}\}}.$$

This shows that the map Ev is also surjective. Putting $\mathrm{Par} := \mathrm{Ev}^{-1}$ finishes the proof. $\square$

The properties (3-1) and (3-2) are the core features of the Koymans–Pagano parametrization method [Koymans and Pagano 2023]. Using [Granville and Koukoulopoulos 2019, Theorem 1], we get the following result.

Theorem 3.4. *We have*

$$\sum_{\substack{\psi\in\mathrm{Hom}(G_{\mathbb{Q}},G_n)\\ \pi_0\circ q_n\circ\psi\in\{\chi_3,2\chi_3\}\\ \mathfrak{f}(\psi)\le X}} 1 \sim 2\cdot 27^n\cdot\frac{X\cdot(\log X)^{\alpha-1}}{3\cdot\Gamma(\alpha)}\cdot c_0,$$

where

$$\alpha := \sum_{\substack{g\in G_n-\{\mathrm{id}\}\\ \pi_0(q_n(g))=0}}\frac{1}{\varphi(\mathrm{ord}(g))} = \frac{3^n-1}{2}+3^n\cdot\left(\frac{9^n-3^n}{6}+\frac{3^n-1}{2}\right) = \frac{9^n-1}{3}+\frac{27^n-1}{6}$$

and c_0 equals the conditionally convergent Euler product

$$c_0 := \prod_p\left(1+\frac{(9^n-1)\mathbf{1}_{p\equiv 4,7 \bmod 9}+(27^n-1)\mathbf{1}_{p\equiv 1 \bmod 9}}{p}\right)\left(1-\frac{1}{p}\right)^{\alpha}.$$

The same result is true if $\mathrm{Hom}(G_{\mathbb{Q}},G_n)$ *is replaced by* $\mathrm{Epi}(G_{\mathbb{Q}},G_n)$.

Proof. We will first prove the $\mathrm{Hom}(G_{\mathbb{Q}},G_n)$ case. By Theorem 3.3 we have

$$\sum_{\substack{\psi\in\mathrm{Hom}(G_{\mathbb{Q}},G_n)\\ \pi_0\circ q_n\circ\psi\in\{\chi_3,2\chi_3\}\\ \mathfrak{f}(\psi)\le X}} 1 = \sum_{\substack{(v_g)_{g\in G_n-\{\mathrm{id}\}}\in\mathcal{G}_{n,\mathrm{bad}}\\ \prod_{g\in G_n-\{\mathrm{id}\}} v_g\le X}} 1.$$

Recall that

$$\prod_{\substack{g\in G_n-\{\mathrm{id}\}\\ \pi_0(q_n(g))\neq 0}} v_g = 3.$$

Write T_n for the subset of $g\in G_n-\{\mathrm{id}\}$ with $\pi_0(q_n(g))=0$. Since there are $2\cdot 27^n$ elements $g\in G_n-\{\mathrm{id}\}$ with $\pi_0(q_n(g))\neq 0$, we obtain that

$$\sum_{\substack{(v_g)_{g\in G_n-\{\mathrm{id}\}}\in\mathcal{G}_{n,\mathrm{bad}}\\ \prod_{g\in G_n-\{\mathrm{id}\}} v_g\le X}} 1 = 2\cdot 27^n \sum_{\substack{(v_g)_{g\in T_n}\\ \prod_{g\in T_n} v_g\le X/3\\ p\mid v_g\Rightarrow p\equiv 1 \bmod \mathrm{ord}(g)}} \mu^2\left(\prod_{g\in T_n} v_g\right).$$

Writing $m := \prod_{g\in T_n} v_g$, this transforms the sum into

$$2\cdot 27^n \sum_{\substack{(v_g)_{g\in T_n}\\ \prod_{g\in T_n} v_g\le X/3\\ p\mid v_g\Rightarrow p\equiv 1 \bmod \mathrm{ord}(g)}} \mu^2\left(\prod_{g\in T_n} v_g\right) = 2\cdot 27^n\sum_{m\le X/3} f(m),$$

where $f(m)$ is the multiplicative function supported on squarefree integers and given on primes by

$$f(p) = (9^n-1)\mathbf{1}_{p\equiv 4,7 \bmod 9}+(27^n-1)\mathbf{1}_{p\equiv 1 \bmod 9}$$

thanks to Lemma 3.2. The average of f on primes is equal to α, and the theorem now follows from [Granville and Koukoulopoulos 2019, Theorem 1].

To deal with $\mathrm{Epi}(G_{\mathbb{Q}}, G_n)$, let S be a subset of T_n and consider the subsum

$$N_1(X, S) := \sum_{\substack{(v_g)_{g \in T_n} \\ \prod_{g \in G_n - \{\mathrm{id}\}} v_g \leq X/3 \\ p \mid v_g \Rightarrow p \equiv 1 \bmod \mathrm{ord}(g) \\ v_g = 1 \Longleftrightarrow g \in S}} \mu^2\biggl(\prod_{g \in T_n} v_g\biggr). \tag{3-3}$$

This dissects the original sum into $2^{|T_n|}$ subsums. Furthermore, S determines whether the resulting map will be surjective or not thanks to Theorem 3.3. Following the argument for the homomorphism case, one may use [Granville and Koukoulopoulos 2019, Theorem 1] to extract an asymptotic for sums of the shape

$$N_2(X, S) := \sum_{\substack{(v_g)_{g \in T_n} \\ \prod_{g \in G_n - \{\mathrm{id}\}} v_g \leq X/3 \\ p \mid v_g \Rightarrow p \equiv 1 \bmod \mathrm{ord}(g) \\ g \in S \Rightarrow v_g = 1}} \mu^2\biggl(\prod_{g \in T_n} v_g\biggr)$$

for every subset S of T_n. By [loc. cit., Theorem 1], we see that

$$N_2(X, \varnothing) \sim 2 \cdot 27^n \cdot \frac{X \cdot (\log X)^{\alpha - 1}}{3 \cdot \Gamma(\alpha)} \cdot c_0$$

and $N_2(X, S) = o(X(\log X)^{\alpha-1})$ for $S \neq \varnothing$. But the sums in (3-3) are linear combinations of such sums. More precisely, there holds

$$N_1(X, S) = \sum_{S \subseteq S'} (-1)^{|S'| - |S|} N_2(X, S').$$

This includes the term $N_2(X, \varnothing)$ if and only if $S = \varnothing$. Therefore we also have

$$N_1(X, \varnothing) \sim 2 \cdot 27^n \cdot \frac{X \cdot (\log X)^{\alpha - 1}}{3 \cdot \Gamma(\alpha)} \cdot c_0$$

and $N_1(X, S) = o(X(\log X)^{\alpha-1})$ for $S \neq \varnothing$. Since the number of epimorphisms is exactly equal to

$$\sum_{\substack{S \subseteq T_n \\ T_n - S \text{ generates } \ker(\pi_0 \circ q_n)}} N_1(X, S),$$

this proves the theorem. $\square$

4. Counting conjugacy classes

Define for $g \in G$ and $\alpha \in (\mathbb{Z}/\operatorname{ord}(g)\mathbb{Z})^*$ the set

$$S_{g,\alpha} := \{h \in G : hgh^{-1} = g^\alpha\}.$$

Informally, one may think of $S_{g,\alpha}$ as the admissible Frobenius elements given that an inertia element is sent to g and $p \equiv \alpha \bmod \operatorname{ord}(g)$. Given $g \in G$ and a number field k, we may canonically identify $\operatorname{Gal}(k(\zeta_{\operatorname{ord}(g)})/k)$ as a subgroup of $(\mathbb{Z}/\operatorname{ord}(g)\mathbb{Z})^*$. We will write this group as $T(g,k)$. The next proposition gives an explicit formula for the naive Malle constant in terms of $S_{g,\alpha}$.

Proposition 4.1. *We have*

$$b(G,k) := -1 + \sum_{g \in G - \{\mathrm{id}\}} \frac{1}{[k(\zeta_{\operatorname{ord}(g)}) : k]} \sum_{\alpha \in T(g,k)} \frac{|S_{g,\alpha}|}{|G|}. \tag{4-1}$$

Proof. Observe that

$$\sum_{g \in G - \{\mathrm{id}\}} \frac{1}{[k(\zeta_{\operatorname{ord}(g)}) : k]} \sum_{\alpha \in T(g,k)} \frac{|S_{g,\alpha}|}{|G|} = \sum_{g \in G - \{\mathrm{id}\}} \frac{|\{\alpha \in T(g,k) : S_{g,\alpha} \neq \varnothing\}|}{[k(\zeta_{\operatorname{ord}(g)}) : k] \cdot |\mathrm{Cl}(g)|}.$$

For elements $g, h \in G$, recall that $g \sim h$ if $\mathrm{Cl}(g)$ is equivalent to $\mathrm{Cl}(h)$ under the cyclotomic action and also recall that $b(G,k)$ is the number of equivalence classes of $\sim$. We claim that

$$\frac{|\{\alpha \in T(g,k) : S_{g,\alpha} \neq \varnothing\}|}{[k(\zeta_{\operatorname{ord}(g)}) : k] \cdot |\mathrm{Cl}(g)|} = \frac{1}{|[g]|}. \tag{4-2}$$

But this follows from the Orbit-stabilizer theorem by letting $T(g,k)$ act on the set $X := \{\mathrm{Cl}(g^\alpha) : \alpha \in T(g,k)\}$. Indeed, first observe that

$$|[g]| = |X| \cdot |\mathrm{Cl}(g)|.$$

Since the action is transitive by construction, we get for every $x \in X$

$$|X| = |\mathrm{Orb}(x)| = \frac{[k(\zeta_{\operatorname{ord}(g)}) : k]}{|\mathrm{Stab}(x)|}.$$

Observing that $|\mathrm{Stab}(x)| = |\mathrm{Stab}(\mathrm{Cl}(g))|$ is precisely $|\{\alpha \in T(g,k) : S_{g,\alpha} \neq \varnothing\}|$, (4-2) follows. Therefore the naive Malle constant is equal to

$$b(G,k) = -1 + \sum_{g \in G - \{\mathrm{id}\}} \frac{|\{\alpha \in T(g,k) : S_{g,\alpha} \neq \varnothing\}|}{[k(\zeta_{\operatorname{ord}(g)}) : k] \cdot |\mathrm{Cl}(g)|} = -1 + |(G - \{\mathrm{id}\})/\sim|,$$

as desired. □

We now calculate (4-1) in the special case of $G = G_n$ and $k = \mathbb{Q}$. Let $g \in G_n$. If $q_n(g) = 0$, then we have $\operatorname{ord}(g) = 3$ and

$$S_{g,\alpha} = \begin{cases} G_n & \text{if } \alpha \equiv 1 \bmod 3, \\ \varnothing & \text{otherwise.} \end{cases} \tag{4-3}$$

Now suppose that $q_n(g) \neq 0$. If $h \in S_{g,\alpha}$, we have by definition

$$hgh^{-1} = g^\alpha.$$

Applying q_n to the above expression and recalling Lemma 3.2, we see that $S_{g,\alpha} = \varnothing$ unless $\alpha \equiv 1 \bmod \operatorname{ord}(g)$. Fixing g, we will now compute $S_{g,1 \bmod \operatorname{ord}(g)}$, which is precisely the set of $h \in G_n$ commuting with g.

Observe that the map $f_g : Q_n \to (\mathbb{Z}/3\mathbb{Z})^n$ given by lifting $a \in Q_n$ to an element $h \in G_n$ and then computing

$$hgh^{-1}g^{-1}$$

is a well-defined homomorphism, i.e., does not depend on the choice of lift. Writing out the multiplication rule for G_n given by θ explicitly, we see that this homomorphism equals

$$a \mapsto \big(\pi_0(a) \cdot \pi_i(q_n(g)) - \pi_0(q_n(g)) \cdot \pi_i(a)\big)_{1 \le i \le n}.$$

We will now distinguish two cases. If $\pi_0(q_n(g)) \neq 0$, then the homomorphism f_g is surjective. If instead $\pi_0(q_n(g)) = 0$, then the image of the homomorphism f_g has dimension 0 if $\pi_i(q_n(g)) = 0$ for all i and dimension 1 otherwise.

Note that the homomorphism f_g depends only on $q_n(g)$. Furthermore, we have the key identity

$$|S_{g,1 \bmod \operatorname{ord}(g)}| = 3^n \cdot |\ker(f_g)| = \begin{cases} 3 \cdot 9^n & \text{if } \pi_0(q_n(g)) \neq 0, \\ 27^n & \text{if } \pi_0(q_n(g)) = 0 \text{ and } \exists i : \pi_i(q_n(g)) \neq 0, \\ 3 \cdot 27^n & \text{if } \pi_0(q_n(g)) = 0 \text{ and } \forall i : \pi_i(q_n(g)) = 0. \end{cases} \tag{4-4}$$

Therefore we split the sum

$$\sum_{g \in G_n - \{\mathrm{id}\}} \frac{1}{\varphi(\operatorname{ord}(g))} \sum_{\alpha \in (\mathbb{Z}/\operatorname{ord}(g)\mathbb{Z})^*} \frac{|S_{g,\alpha}|}{|G_n|} = \sum_{g \in G_n - \{\mathrm{id}\}} \frac{1}{\varphi(\operatorname{ord}(g))} \cdot \frac{|S_{g,1 \bmod \operatorname{ord}(g)}|}{|G_n|}$$

in four pieces, namely the piece where $q_n(g) = 0$, the piece where $\pi_0(q_n(g)) \neq 0$, the piece where $\pi_0(q_n(g)) = 0$ and $\pi_i(q_n(g)) \neq 0$ for some i, and the piece where $\pi_0(q_n(g)) = 0$, $q_n(g) \neq 0$ and $\pi_i(q_n(g)) = 0$ for all i. The contribution from $q_n(g) = 0$ equals

$$\sum_{\substack{g \in G_n - \{\mathrm{id}\} \\ q_n(g) = 0}} \frac{1}{\varphi(\operatorname{ord}(g))} \cdot \frac{|S_{g,1 \bmod \operatorname{ord}(g)}|}{|G_n|} = \frac{3^n - 1}{2} \tag{4-5}$$

by (4-3). Using Lemma 3.2, we see that the number of elements of G_n with $\pi_0(q_n(g)) \neq 0$ with order 3 is $2 \cdot 3^n \cdot 3^n$, while the number of elements of order 9 is $2 \cdot 3^n \cdot (9^n - 3^n)$. The contribution from $\pi_0(q_n(g)) \neq 0$ becomes

$$\sum_{\substack{g \in G_n - \{\mathrm{id}\} \\ \pi_0(q_n(g)) \neq 0}} \frac{1}{\varphi(\operatorname{ord}(g))} \cdot \frac{|S_{g,1 \bmod \operatorname{ord}(g)}|}{|G_n|} = \left(2 \cdot 3^n \cdot \frac{9^n - 3^n}{6} + 2 \cdot 3^n \cdot \frac{3^n}{2}\right) \cdot \frac{1}{3^n} = 2 \cdot \frac{9^n - 3^n}{6} + 3^n \tag{4-6}$$

by (4-4). Finally, we treat the contribution from $\pi_0(q_n(g)) = 0$ but $q_n(g) \neq 0$. Firstly, if $\pi_i(q_n(g)) = 0$ for all i, then $\operatorname{ord}(g) = 3$. There are $3^n \cdot (3^n - 1)$ such elements, and they contribute

$$\sum_{\substack{g \in G_n - \{\mathrm{id}\} \\ q_n(g) \neq 0 \\ \pi_0(q_n(g))=0 \\ \forall i : \pi_i(q_n(g))=0}} \frac{1}{\varphi(\operatorname{ord}(g))} \cdot \frac{|S_{g,1 \bmod \operatorname{ord}(g)}|}{|G_n|} = 3^n \cdot \frac{3^n - 1}{2} \tag{4-7}$$

to the total thanks to (4-4). Now suppose that $\pi_i(q_n(g)) \neq 0$ for some i. Such g have order 9 and there are $3^n \cdot (9^n - 3^n)$ such g. This yields

$$\sum_{\substack{g \in G_n - \{\mathrm{id}\} \\ q_n(g) \neq 0 \\ \pi_0(q_n(g))=0 \\ \exists i : \pi_i(q_n(g))\neq 0}} \frac{1}{\varphi(\operatorname{ord}(g))} \cdot \frac{|S_{g,1 \bmod \operatorname{ord}(g)}|}{|G_n|} = 3^n \cdot \frac{9^n - 3^n}{6} \cdot \frac{1}{3} \tag{4-8}$$

once more due to (4-4). Adding up the contributions from (4-5), (4-6), (4-7) and (4-8) gives the following theorem.

Theorem 4.2. *For all $n \geq 1$ there holds*

$$b(G_n, \mathbb{Q}) + 1 = \frac{3^n - 1}{2} + 2 \cdot \frac{9^n - 3^n}{6} + 3^n + 3^n \cdot \frac{3^n - 1}{2} + 3^n \cdot \frac{9^n - 3^n}{6} \cdot \frac{1}{3}. \tag{4-9}$$

Observe that the logarithmic exponent of Theorem 3.4 is strictly larger than $b(G_n, \mathbb{Q})$ for all $n \geq 2$. This immediately gives Theorem 1.3.

5. A modified Malle conjecture

Let G be a finite nilpotent group and suppose that we have the following diagram:

$$\begin{tikzcd} G \arrow[dr, two heads, "\phi"] & \\ & H \\ (\mathbb{Z}/|G|\mathbb{Z})^* \arrow[ur, two heads, "r"] & \end{tikzcd}$$

For the rest of this section, $\chi(\mathrm{cyc}) : G_{\mathbb{Q}} \to (\mathbb{Z}/|G|\mathbb{Z})^*$ denotes the cyclotomic character. We now define

$$\operatorname{Epi}_{(H,\phi)}(G_{\mathbb{Q}}, G)$$

to be the set of continuous surjective homomorphisms $\psi : G_{\mathbb{Q}} \twoheadrightarrow G$ satisfying the equations

$$\phi \circ \psi = r \circ \chi(\mathrm{cyc}), \quad \mathbb{Q}(\psi) \cap \mathbb{Q}(\zeta_{|G|}) = \mathbb{Q}(\phi \circ \psi),$$

i.e., we are only considering those ψ with a fixed wildly ramified cyclotomic subextension. In particular, we have the following diagram:

$$\begin{tikzcd} & G \arrow[dr, two heads, "\phi"] & \\ G_{\mathbb{Q}} \arrow[ur, two heads, "\psi"] \arrow[dr, two heads, "\chi\,(\mathrm{cyc})"] & & H \\ & (\mathbb{Z}/|G|\mathbb{Z})^* \arrow[ur, two heads, "r"] & \end{tikzcd}$$

We denote by $G \times_H (\mathbb{Z}/|G|\mathbb{Z})^* \subseteq G \times (\mathbb{Z}/|G|\mathbb{Z})^*$ the subgroup consisting of pairs (g, α) satisfying

$$\phi(g) = r(\alpha).$$

The group $G \times (\mathbb{Z}/|G|\mathbb{Z})^*$ acts on $\ker(\phi) - \{\mathrm{id}\}$ by sending n to $gn^{\alpha^{-1}}g^{-1}$. Restricting this action to $G \times_H (\mathbb{Z}/|G|\mathbb{Z})^*$, we denote by

$$b_{(H,\phi)}(G) := |(\ker(\phi) - \{\mathrm{id}\})/(G \times_H (\mathbb{Z}/|G|\mathbb{Z})^*)|$$

the size of the quotient space. We propose the following conjecture. We thank Jiuya Wang for pointing out that the counting function in Conjecture 5.1 can be zero in some circumstances.

Conjecture 5.1. *Let G be a nilpotent group. For each H, ϕ as above, then either $\mathrm{Epi}_{(H,\phi)}(G_{\mathbb{Q}}, G)$ is empty or there exists a positive constant $c_{(H,\phi)}(G)$ such that*

$$|\{\psi \in \mathrm{Epi}_{(H,\phi)}(G_{\mathbb{Q}}, G) : \mathfrak{f}(\psi) \le X\}| \sim c_{(H,\phi)}(G) \cdot X \cdot \log(X)^{b_{(H,\phi)}(G)-1}.$$

In the following remark we compare this conjecture with the naive adaptation of Malle's conjecture and with Theorem 3.4.

Remark 5.2. (a) We can recover Malle's original exponent as follows. If one takes $H = \{\mathrm{id}\}$, one trivially has that $b_{(H,\phi)}(G) = b(G)$. In particular, Conjecture 5.1 predicts that one can rescue Malle's conjecture in the case one considers the family of extensions that are linearly disjoint from $\mathbb{Q}(\zeta_{|G|})$.

(b) We have restricted ourselves to maps $r : (\mathbb{Z}/|G|\mathbb{Z})^* \twoheadrightarrow H$, but in principle one could consider maps $r : (\mathbb{Z}/|G|^j\mathbb{Z})^* \twoheadrightarrow H$ for every $j \ge 2$ as well. Using that powering with elements $\alpha \equiv 1 \bmod |G|$ is the identity map on G, one can check that this does not lead to higher logarithmic exponents than the ones in our conjecture.

(c) We can recover the exponent in Theorem 3.4 as follows. Let H be the order-3 quotient of $(\mathbb{Z}/9\mathbb{Z})^*$. Fix an identification $i : \mathbb{Z}/3\mathbb{Z} \to H$ and let $\phi := i \circ \pi_0 \circ q_n$. It is easy to verify that α in Theorem 3.4 equals exactly $b_{(H,\phi)}(G_n)$.

(d) It is worthwhile to compare our conjecture with work of Alberts; see Section 3.4, and specifically Conjecture 3.10, of [Alberts 2021]. Both conjectures predict that the correct logarithmic exponent is the maximum of the logarithmic exponents obtained by fixing some collection of subextensions and then applying Türkelli's adaptation to each such subextension. The work of Alberts allows for arbitrary groups G, while our conjecture is more restrictive on G. However, our conjecture is more precise about both the leading constant and the set of subextensions to consider.

We remark that one may reinterpret the exponents $b_{(H,\phi)}(G)$ as an adaptation, to the product of ramified primes, of Türkelli's modification of Malle's conjecture [Türkelli 2015]. Indeed, observe that the fibered product $G \times_H (\mathbb{Z}/|G|\mathbb{Z})^*$ certainly contains $\ker(\phi) \times \{1\}$. Hence the $G \times_H (\mathbb{Z}/|G|\mathbb{Z})^*$-equivalence relation is a further equivalence relation on $\ker(\phi)$-conjugacy classes in $\ker(\phi)$. This further equivalence relation is obtained by acting on a $\ker(\phi)$-conjugacy class via a pair (g, α) with $\phi(g) = r(\alpha)$. A moment's reflection shows that this comes down to the twisted $(\mathbb{Z}/|G|\mathbb{Z})^*$-action on the set of $\ker(\phi)$-conjugacy classes of $\ker(\phi)$ given in [loc. cit., page 198].

Remark 5.3. A nilpotent group G is always the product of its p-Sylow subgroups G_p. So the example in Theorem 3.4 might give the misleading impression that $b_{(H,\phi)}(G) > b(G, \mathbb{Q})$ can only occur by fixing at G_p some character ramified at p. However, choosing the central extension

$$0 \to (\mathbb{Z}/2\mathbb{Z})^n \to G_n \to (\mathbb{Z}/2\mathbb{Z})^{n+1} \times (\mathbb{Z}/3\mathbb{Z})^n \to 0,$$

given by the cocycles

$$\theta_i(\sigma, \tau) := \pi_0(\sigma) \cdot \pi_i(\tau)$$

for $1 \le i \le n$, also leads to examples. Here π_i denotes the projection map on the i-th copy of $\mathbb{Z}/2\mathbb{Z}$. Indeed, one may take $H := \mathbb{Z}/2\mathbb{Z}$, $\phi := \pi_0$ and r such that $\mathbb{Q}(r \circ \chi(\text{cyc})) = \mathbb{Q}(\sqrt{-3})$. Then we have

$$b_{(H,\phi)}(G_n) = \frac{12^n}{2} + O(6^n),$$

while

$$b(G_n, \mathbb{Q}) = \frac{12^n}{4} + O(6^n),$$

hence giving an example for n sufficiently large. We leave the details of this alternative example to the interested reader.

Finally, we adapt the so-called Malle–Bhargava heuristic principle [Bhargava 2007] within the family $\mathrm{Epi}_{(H,\phi)}(G_{\mathbb{Q}}, G)$, in order to specify the leading constant $c_{(H,\phi)}(G)$ in the case $|G|$ is *odd*. To this end, for a prime number p and for G, H, ϕ as above, we denote by

$$\mathrm{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)$$

the set of homomorphisms $\psi : G_{\mathbb{Q}_p} \to G$ such that $\phi \circ \psi = r \circ \chi(\text{cyc}) \circ i_p^*$. The Malle–Bhargava principle states that if one writes the following Euler product

$$F(s) := \prod_p \left(\frac{1}{|\ker(\phi)|} \cdot \sum_{\psi \in \mathrm{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)} \mathfrak{f}(\psi)^{-s} \right),$$

as a Dirichlet series

$$F(s) := \sum_{n \ge 1} \frac{f(n)}{n^s},$$

then one expects the asymptotic

$$\sum_{n\le X} f(n) \sim |\{\psi \in \mathrm{Epi}_{(H,\phi)}(G_{\mathbb{Q}}, G) : \mathfrak{f}(\psi) \le X\}|.$$

With this principle in mind, let us now compute the left hand side. For $g \in G$ and $\alpha \in (\mathbb{Z}/|G|\mathbb{Z})^*$, we define

$$S_{(H,\phi)}(g, \alpha) := \{h \in G : hgh^{-1} = g^{\alpha} \text{ and } \phi(h) = r(\alpha)\}.$$

For a profinite group $\mathcal{G}$, we denote by $\mathcal{G}(p)$ the pro-p completion of $\mathcal{G}$. Likewise, for a continuous homomorphism $\varphi : \mathcal{G}_1 \to \mathcal{G}_2$ of profinite groups, we denote by $\varphi(p)$ the induced map between pro-p completions. We define $\mathcal{G}(\text{non-}p)$ to be the product of the pro-q completions of $\mathcal{G}$ as q runs over prime divisors of $|G|$ not equal to p. Given a continuous homomorphism $\varphi : \mathcal{G}_1 \to \mathcal{G}_2$, there is a natural induced homomorphism $\varphi(\text{non-}p)$. Write $f : H \to H(p)$ and $g : H \to H(\text{non-}p)$ for the natural surjective maps so that the product map (f, g) is an isomorphism owing to the fact that H is nilpotent.

We fix for each prime number p a generator τ_p of the image of the inertia subgroup of $G_{\mathbb{Q}_p}$ in the quotient $g \circ r \circ \chi(\text{cyc}) \circ i_p^*$: this is a cyclic group because tame inertia is cyclic.

Proposition 5.4. *Notation as immediately above, we have that*

$$\sum_{n\le X} f(n) \sim c_{(H,\phi)}(G) \cdot X \cdot \log(X)^{b_{(H,\phi)}(G)-1},$$

where $c_{(H,\phi)}(G)$ is the conditionally convergent product

$$c_{(H,\phi)}(G) := \frac{1}{\Gamma(b_{(H,\phi)}(G))} \times \alpha_1 \times \alpha_2 \times \alpha_3,$$

where

$$\alpha_1 := \prod_{p \mid \mathfrak{f}(r\circ\chi(\text{cyc}))} \left(\frac{|\ker(\phi(p))|}{p}\right) \cdot \left(\frac{\sum_{g\in\phi(\text{non-}p)^{-1}(\tau_p)} |S_{(H(\text{non-}p),\phi(\text{non-}p))}(g, p)|}{|\ker(\phi(\text{non-}p))|}\right)\left(1-\frac{1}{p}\right)^{b_{(H,\phi)}(G)},$$

$$\alpha_2 := \prod_{\substack{p \mid |G| \\ p \nmid \mathfrak{f}(r\circ\chi(\text{cyc}))}} \left(1 + \frac{|\ker(\phi(p))|\left(\frac{\sum_{g\in\ker(\phi(\text{non-}p))} |S_{(H(\text{non-}p),\phi(\text{non-}p))}(g,p)|}{|\ker(\phi(\text{non-}p))|}\right) - 1}{p}\right)\left(1-\frac{1}{p}\right)^{b_{(H,\phi)}(G)},$$

$$\alpha_3 := \prod_{p \nmid |G|} \left(1 + \frac{\sum_{g\in\ker(\phi)-\{\text{id}\}} |S_{(H,\phi)}(g, p)|}{|\ker(\phi)| \cdot p}\right)\left(1-\frac{1}{p}\right)^{b_{(H,\phi)}(G)}.$$

Proof. Note that f is supported on squarefree integers and multiplicative away from primes dividing $|G|$. The proposition will ultimately follow from [Granville and Koukoulopoulos 2019, Theorem 1], with the exponent of $\log(X)$ being the average of f on primes. Let us start by showing that this equals $b_{(H,\phi)}(G)$. We compute

$$\frac{1}{|\ker(\phi)| \cdot \varphi(|G|)} \cdot \sum_{\substack{g\in\ker(\phi)-\{\text{id}\} \\ \alpha\in(\mathbb{Z}/|G|\mathbb{Z})^*}} |S_{(H,\phi)}(g, \alpha)|.$$

Observe that $|\ker(\phi)| \cdot \varphi(|G|) = |G \times_H (\mathbb{Z}/|G|\mathbb{Z})^*|$. We can therefore rewrite the sum as

$$\frac{1}{|G \times_H (\mathbb{Z}/|G|\mathbb{Z})^*|} \cdot \sum_{(h,\alpha) \in G \times_H (\mathbb{Z}/|G|\mathbb{Z})^*} |\{g \in \ker(\phi) - \{\mathrm{id}\} : hgh^{-1} = g^{\alpha}\}| = b_{(H,\phi)}(G)$$

by Burnside's lemma.

It remains to examine the local factors of the leading constant. In [Granville and Koukoulopoulos 2019], the authors do so by rewriting $F(s)$ as

$$F(s) = \frac{F(s)}{\zeta_{\mathbb{Q}}(s)^{b_{(H,\phi)}(G)}} \cdot \zeta_{\mathbb{Q}}(s)^{b_{(H,\phi)}(G)},$$

in order to obtain the leading coefficient as a conditionally convergent Euler product. This is the reason for the occurrence of the term $(1 - 1/p)^{b_{(H,\phi)}(G)}$ in our formulas. We now wish to explain the remaining contributors:

The constant $\boldsymbol{\alpha_1}$: Suppose that $p \mid \mathfrak{f}(r \circ \chi(\mathrm{cyc}))$. Then the local contribution is precisely

$$\frac{1}{p \cdot |\ker(\phi)|} \cdot |\mathrm{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)|.$$

Recalling that these are nilpotent groups, we see that we can split the count in the numerator Sylow by Sylow. Therefore we have that

$$|\mathrm{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)| = T_p \times T_{\text{non-}p},$$

where T_p equals the number of continuous homomorphisms $\psi : G_{\mathbb{Q}_p} \to G(p)$ such that

$$\phi(p) \circ \psi = f \circ r \circ \chi(\mathrm{cyc}) \circ i_p^*,$$

while $T_{\text{non-}p}$ equals the number of continuous homomorphisms $\psi : G_{\mathbb{Q}_p} \to G(\text{non-}p)$ such that

$$\phi(\text{non-}p) \circ \psi = g \circ r \circ \chi(\mathrm{cyc}) \circ i_p^*.$$

Note that $\psi : G_{\mathbb{Q}_p} \to G(p)$ factors through $G_{\mathbb{Q}_p}(p)$ and recall that $G_{\mathbb{Q}_p}(p)$ is isomorphic to a free pro-p group on 2 generators. It follows that T_p equals the number of pairs of elements in $G(p)$ having prescribed value of $\phi(p)$. Therefore

$$T_p = |\ker(\phi(p))|^2.$$

Note that any map $\psi : G_{\mathbb{Q}_p} \to G(\text{non-}p)$ must factor through $G_{\mathbb{Q}_p}^{\mathrm{tame}}$. Recall that

$$G_{\mathbb{Q}_p}^{\mathrm{tame}} \simeq_{\text{top.gr.}} \Big(\prod_{\ell \neq p} \mathbb{Z}_\ell\Big) \rtimes \hat{\mathbb{Z}},$$

where the topological generator 1 of the group $\hat{\mathbb{Z}}$ acts by multiplication by p on $\prod_{\ell \neq p} \mathbb{Z}_\ell$. Both groups in this direct product are pro-cyclic. Hence the cardinality

$$T_{\text{non-}p}$$

equals the number of possible choices for two fixed generators. Once we prescribe that a generator of $\prod_{\ell \neq p} \mathbb{Z}_\ell$ goes to an element g of $\phi(\text{non-}p)^{-1}(\tau_p) \in G(\text{non-}p)$, we have that the generator 1 of $\hat{\mathbb{Z}}$ has to be sent in $S_{(H(\text{non-}p),\phi(\text{non-}p))}(g, p) \subseteq G(\text{non-}p)$. And conversely any choice of such a pair gives rise to a valid homomorphism. This proves that

$$T_{\text{non-}p} = \left(\sum_{g \in \phi(\text{non-}p)^{-1}(\tau_p)} |S_{(H(\text{non-}p),\phi(\text{non-}p))}(g, p)| \right),$$

which gives us the desired conclusion on α_1.

The constant α_2: Suppose that $p \mid |G|$ and $p \nmid \mathfrak{f}(r \circ \chi)$. Then splitting the local factor

$$\frac{1}{|\ker(\phi)|} \cdot \sum_{\psi \in \text{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)} \mathfrak{f}(\psi)^{-1},$$

into unramified and ramified ψ, we get precisely

$$1 + \frac{|\{\psi \text{ ramified and } \psi \in \text{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)\}|}{p \cdot |\ker(\phi)|}.$$

This is because there are precisely $|\ker(\phi)|$ unramified ones. Indeed, the Galois group of the maximal unramified extension of $\mathbb{Q}_p$ is topologically free on one generator and therefore the unramified elements of $\text{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)$ correspond to the choices of an element of G with prescribed image under ϕ.

Now we can use again the count of unramified classes in $\text{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)$ to obtain that

$$|\{\psi \text{ ramified and } \psi \in \text{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)\}| = |\text{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)| - |\ker(\phi)|.$$

But we have computed in the evaluation of α_1 that

$$|\text{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)| = |\ker(\phi(p))|^2 \left(\sum_{g \in \phi(\text{non-}p)^{-1}(\tau_p)} |S_{(H(\text{non-}p),\phi(\text{non-}p))}(g, p)| \right).$$

Since $p \nmid \mathfrak{f}(r \circ \chi(\text{cyc}))$, we have $r \circ \chi(\text{cyc}) \circ i_p^*(I_p) = \{1\}$ and thus $\phi(\text{non-}p)^{-1}(\tau_p) = \ker(\phi(\text{non-}p))$. This gives the desired formula.

The constant α_3: Since p does not divide $|G|$, we now have that all the homomorphisms will be tame. In particular, this implies that the image of a generator of tame inertia has to be in $\ker(\phi)$. The total contribution from unramified homomorphisms is again 1, as already articulated above. The one from ramified ones comes precisely in the same way we have explained in the computation of α_1. □

With the above in mind, we are ready to make the following conjecture.

Conjecture 5.5. *Suppose G is odd and nilpotent. Then Conjecture 5.1 holds with*

$$c_{(H,\phi)}(G) := \frac{1}{\Gamma(b_{(H,\phi)}(G))} \times \alpha_1 \times \alpha_2 \times \alpha_3,$$

where α_i are as in Proposition 5.4.

It is readily verified that Theorem 3.4 is a special case of Conjecture 5.5, with the choice of G, H, ϕ as explained in Remark 5.2. The extra factor 2 in Theorem 3.4 accounts for the fact that one may also choose another identification in Remark 5.2. The factor $\frac{27^n}{3}$ is the local factor at 3 and the constant c_0 therein is the product of the tame factors along with the factor $\left(\frac{2}{3}\right)^{\alpha}$.

The conjecture can be extended also for a finite prescribed set of local conditions by modifying accordingly the local factors defining $F(s)$, namely summing $\mathfrak{f}(\psi)^{-s}$ only among the prescribed local homomorphisms ψ. In particular, if one runs only over tame extensions, one gets the simpler leading constant

$$\prod_{p\,|\,|G|}\left(1-\frac{1}{p}\right)^{b_{(H,\phi)}(G)} \times \prod_{p\nmid |G|}\left(1+\frac{\sum_{g\in\ker(\phi)-\{\mathrm{id}\}}|S_{(H,\phi)}(g,p)|}{|\ker(\phi)|\cdot p}\right)\left(1-\frac{1}{p}\right)^{b_{(H,\phi)}(G)}.$$

We have excluded the groups of even cardinality from Conjecture 5.5, since one can prove that the same conjecture would fail already for the dihedral group on 8 elements, and even among tamely ramified extensions. In this case the leading constant is likely to be an Euler product times a rational correction factor to account for quadratic reciprocity. If also wild extensions are considered, then even further modifications may be needed by Grunwald–Wang-type of obstructions. These problems at 2 correspond to the unspecified constant $C(G)$ in [Bhargava 2007, Equation (8.6), page 17].

Acknowledgements

Koymans gratefully acknowledges the support of Dr. Max Rössler, the Walter Haefner foundation and the ETH Zürich foundation. The authors would like to thank Ratko Darda for fruitful discussions and the anonymous referee for their careful reading of the manuscript.

References

[Alberts 2021] B. Alberts, "Statistics of the first Galois cohomology group: a refinement of Malle's conjecture", *Algebra Number Theory* **15**:10 (2021), 2513–2569. MR Zbl

[Alberts and O'Dorney 2021] B. Alberts and E. O'Dorney, "Harmonic analysis and statistics of the first Galois cohomology group", *Res. Math. Sci.* **8**:3 (2021), art. id. 50. Correction in **10**:3 (2023), art. id. 31. MR Zbl

[Altuğ et al. 2021] S. A. Altuğ, A. Shankar, I. Varma, and K. H. Wilson, "The number of D_4-fields ordered by conductor", *J. Eur. Math. Soc.* **23**:8 (2021), 2733–2785. MR Zbl

[Bartel and Lenstra 2020] A. Bartel and H. W. Lenstra, Jr., "On class groups of random number fields", *Proc. Lond. Math. Soc.* (3) **121**:4 (2020), 927–953. MR Zbl

[Belabas and Fouvry 2010] K. Belabas and É. Fouvry, "Discriminants cubiques et progressions arithmétiques", *Int. J. Number Theory* **6**:7 (2010), 1491–1529. MR Zbl

[Bhargava 2005] M. Bhargava, "The density of discriminants of quartic rings and fields", *Ann. of Math.* (2) **162**:2 (2005), 1031–1063. MR Zbl

[Bhargava 2007] M. Bhargava, "Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants", *Int. Math. Res. Not.* **2007**:17 (2007), art. id. rnm052. MR Zbl

[Bhargava 2010] M. Bhargava, "The density of discriminants of quintic rings and fields", *Ann. of Math.* (2) **172**:3 (2010), 1559–1591. MR Zbl

[Bhargava and Wood 2008] M. Bhargava and M. M. Wood, "The density of discriminants of S_3-sextic number fields", *Proc. Amer. Math. Soc.* **136**:5 (2008), 1581–1587. MR Zbl

[Cohen et al. 2002] H. Cohen, F. Diaz y Diaz, and M. Olivier, "Enumerating quartic dihedral extensions of $\mathbb{Q}$", *Compos. Math.* **133**:1 (2002), 65–93. MR Zbl

[Couveignes 2020] J.-M. Couveignes, "Enumerating number fields", *Ann. of Math.* (2) **192**:2 (2020), 487–497. MR

[Darda and Yasuda 2023] R. Darda and T. Yasuda, "Torsors for finite group schemes of bounded height", *J. Lond. Math. Soc.* (2) **108**:3 (2023), 1275–1331. MR Zbl

[Davenport and Heilbronn 1971] H. Davenport and H. Heilbronn, "On the density of discriminants of cubic fields, II", *Proc. Roy. Soc. Lond. Ser. A* **322**:1551 (1971), 405–420. MR Zbl

[Ellenberg and Venkatesh 2006] J. S. Ellenberg and A. Venkatesh, "The number of extensions of a number field with fixed degree and bounded discriminant", *Ann. of Math.* (2) **163**:2 (2006), 723–741. MR Zbl

[Fouvry and Koymans 2021] É. Fouvry and P. Koymans, "Malle's conjecture for nonic Heisenberg extensions", preprint, 2021. arXiv 2102.09465

[Granville and Koukoulopoulos 2019] A. Granville and D. Koukoulopoulos, "Beyond the LSD method for the partial sums of multiplicative functions", *Ramanujan J.* **49**:2 (2019), 287–319. MR Zbl

[Gundlach 2022] F. Gundlach, "Malle's conjecture with multiple invariants", preprint, 2022. arXiv 2211.16698

[Klüners 2005] J. Klüners, "A counterexample to Malle's conjecture on the asymptotics of discriminants", *C. R. Math. Acad. Sci. Paris* **340**:6 (2005), 411–414. MR

[Klüners 2012] J. Klüners, "The distribution of number fields with wreath products as Galois groups", *Int. J. Number Theory* **8**:3 (2012), 845–858. MR Zbl

[Klüners and Malle 2004] J. Klüners and G. Malle, "Counting nilpotent Galois extensions", *J. Reine Angew. Math.* **572** (2004), 1–26. MR Zbl

[Koymans and Pagano 2023] P. Koymans and C. Pagano, "On Malle's conjecture for nilpotent groups", *Trans. Amer. Math. Soc. Ser. B* **10** (2023), 310–354. MR Zbl

[Lemke Oliver and Thorne 2022] R. J. Lemke Oliver and F. Thorne, "Upper bounds on number fields of given degree and bounded discriminant", *Duke Math. J.* **171**:15 (2022), 3077–3087. MR Zbl

[Mäki 1993] S. Mäki, "The conductor density of abelian number fields", *J. Lond. Math. Soc.* (2) **47**:1 (1993), 18–30. MR Zbl

[Malle 2004] G. Malle, "On the distribution of Galois groups, II", *Exp. Math.* **13**:2 (2004), 129–135. MR Zbl

[Masri et al. 2020] R. Masri, F. Thorne, W.-L. Tsai, and J. Wang, "Malle's conjecture for $G \times A$ with $G = S_3, S_4, S_5$", preprint, 2020. arXiv 2004.04651

[Neukirch et al. 2000] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Grundl. Math. Wissen. **323**, Springer, 2000. MR Zbl

[Türkelli 2015] S. Türkelli, "Connected components of Hurwitz schemes and Malle's conjecture", *J. Number Theory* **155** (2015), 163–201. MR Zbl

[Wang 2021] J. Wang, "Malle's conjecture for $S_n \times A$ for $n = 3, 4, 5$", *Compos. Math.* **157**:1 (2021), 83–121. MR Zbl

[Wood 2010] M. M. Wood, "On the probabilities of local behaviors in abelian field extensions", *Compos. Math.* **146**:1 (2010), 102–128. MR Zbl

[Wright 1989] D. J. Wright, "Distribution of discriminants of abelian extensions", *Proc. Lond. Math. Soc.* (3) **58**:1 (1989), 17–50. MR Zbl

Communicated by Melanie Matchett Wood
Received 2023-09-18 Revised 2024-04-22 Accepted 2024-06-15

peter.koymans@eth-its.ethz.ch *Institute for Theoretical Studies, ETH Zurich, Zurich, Switzerland*

carlo.pagano@concordia.ca *Department of Mathematics and Statistics, Concordia University, Montreal, Quebec, Canada*

mathematical sciences publishers

ALGEBRA AND NUMBER THEORY 19:5 (2025)
https://doi.org/10.2140/ant.2025.19.1029

Syzygies of tangent-developable surfaces and K3 carpets via secant varieties

Jinhyung Park

We give simple geometric proofs of Aprodu, Farkas, Papadima, Raicu and Weyman's theorem on syzygies of tangent-developable surfaces of rational normal curves and Raicu and Sam's result on syzygies of K3 carpets. As a consequence, we obtain a quick proof of Green's conjecture for general curves of genus g over an algebraically closed field $\Bbbk$ with $\mathrm{char}(\Bbbk) = 0$ or $\mathrm{char}(\Bbbk) \geq \lfloor (g-1)/2 \rfloor$. Our approach provides a new way to study tangent-developable surfaces in general. Along the way, we show the arithmetic normality of tangent-developable surfaces of arbitrary smooth projective curves of large degree.

1. Introduction

Let C be a smooth projective curve of genus $g \geq 3$ over the field $\mathbb{C}$ of complex numbers. If $\mathrm{Cliff}(C) \geq 1$, i.e., C is nonhyperelliptic, then K_C is very ample. In this case, Noether's theorem says that the canonical curve $C \subseteq \mathbb{P}^{g-1}$ is projectively normal. Petri's theorem states that if $\mathrm{Cliff}(C) \geq 2$, then the defining ideal $I_{C|\mathbb{P}^{g-1}}$ of C in $\mathbb{P}^{g-1}$ is generated by quadrics. To generalize classical theorems of Noether and Petri, Green [1984, Conjecture 5.1] formulated a very famous conjecture that predicts

$$K_{p,2}(C, K_C) = 0 \quad \text{for } 0 \leq p \leq \mathrm{Cliff}(C) - 1.$$

By the Green–Lazarsfeld nonvanishing theorem [Green 1984, Appendix], we have $K_{p,2}(C, K_C) \neq 0$ for $\mathrm{Cliff}(C) \leq p \leq g-3$. Then Green's conjecture determines the shape of the minimal free resolution of the canonical ring $R(C, K_C) = \bigoplus_{m \in \mathbb{Z}} H^0(C, mK_C)$ (see [Aprodu and Nagel 2010, Remark 4.19]). Although the conjecture is still open, Voisin [2002; 2005] resolved the general curve case in the early 2000s. To prove the generic Green conjecture, it suffices to exhibit one curve of each genus for which the assertion holds. If $S \subseteq \mathbb{P}^g$ is a K3 surface of degree $2g-2$, then its general hyperplane section is a canonical curve $C \subseteq \mathbb{P}^{g-1}$ and $K_{p,2}(S, \mathscr{O}_S(1)) = K_{p,2}(C, K_C)$. Based on the Hilbert scheme interpretation of Koszul cohomology, Voisin accomplished sophisticated cohomology computations on Hilbert schemes of K3 surfaces to show $K_{p,2}(S, \mathscr{O}_S(1)) = 0$. For an introduction to Voisin's work; see [Aprodu and Nagel 2010]. Recently, Kemeny [2021] gave a simpler proof of Voisin's theorem for even-genus case and a streamlined version of her arguments for the odd-genus case.

Park was partially supported by the National Research Foundation (NRF) funded by the Korea government (MSIT) (RS-2021-NR061320 and RS-2022-NR119741).
MSC2020: 14N05, 14N07, 13D02.
Keywords: tangent-developable surfaces, K3 carpets, secant varieties, syzygies.

Prior to Voisin's work, O'Grady and Buchweitz–Schreyer independently observed that one could use the *tangent-developable surface* $T \subseteq \mathbb{P}^g$ of a rational normal curve of degree g to solve Green's conjecture for general curves of genus g (see [Eisenbud 1992]). Note that $T \subseteq \mathbb{P}^g$ is arithmetically Cohen–Macaulay as for a K3 surface. One can actually view T as a degeneration of a K3 surface (see [Aprodu et al. 2019, Remark 6.6]). A general hyperplane section of T is a canonically embedded g-cuspidal rational curve $\overline{C} \subseteq \mathbb{P}^{g-1}$ of degree $2g-2$, which is a degeneration of a general canonical curve $C \subseteq \mathbb{P}^{g-1}$ with $\mathrm{Cliff}(C) = \lfloor (g-1)/2 \rfloor$. By the upper semicontinuity of graded Betti numbers, $K_{p,2}(\overline{C}, \mathscr{O}_{\overline{C}}(1)) = K_{p,2}(T, \mathscr{O}_T(1)) = 0$ implies $K_{p,2}(C, K_C) = 0$ (see [loc. cit., Section 6]). The required vanishing of $K_{p,2}(T, \mathscr{O}_T(1))$ for confirming the generic Green conjecture was finally established by Aprodu, Farkas, Papadima, Raicu and Weyman [loc. cit.] just a few years ago. Their important result gives not only an alternative proof of the generic Green conjecture but also an extension to positive characteristic. This circle of ideas is surveyed in [Ein and Lazarsfeld 2020]. In this paper, we give a simple geometric proof of the main result of [Aprodu et al. 2019].

Theorem 1.1. *Let $T \subseteq \mathbb{P}^g$ be the tangent-developable surface of a rational normal curve of degree $g \geq 3$ over an algebraically closed field $\Bbbk$ with $\mathrm{char}(\Bbbk) = 0$ or $\mathrm{char}(\Bbbk) \geq (g+2)/2$. Then*

$$K_{p,2}(T, \mathscr{O}_T(1)) = 0 \quad \textit{for } 0 \leq p \leq \lfloor (g-3)/2 \rfloor.$$

The proof of Theorem 1.1 in [Aprodu et al. 2019] goes as follows. We have a short exact sequence

$$0 \longrightarrow \mathscr{O}_T \longrightarrow \nu_* \mathscr{O}_{\widetilde{T}} \longrightarrow \omega_{\mathbb{P}^1} \longrightarrow 0,$$

where $\nu : \widetilde{T} = \mathbb{P}^1 \times \mathbb{P}^1 \to T$ is a resolution of singularities. Then it is elementary to see that

$$K_{p,2}(T, \mathscr{O}_T(1)) = \mathrm{coker}\big(K_{p,1}(T, \nu_* \mathscr{O}_{\widetilde{T}}; \mathscr{O}_T(1)) \xrightarrow{\gamma} K_{p,1}(\mathbb{P}^1, \omega_{\mathbb{P}^1}; \mathscr{O}_{\mathbb{P}^1}(g))\big).$$

Let $U := H^0(\mathbb{P}^1, \mathscr{O}_{\mathbb{P}^1}(1))$, $V := D^{p+2}U$, $W := D^{2p+2}U$, and $q := g - p - 3$. The authors of [Aprodu et al. 2019] devoted considerable effort to show that γ arises as the composition

$$S^q V \otimes W \xrightarrow{\mathrm{id}_{S^q V} \otimes \Delta} S^q V \otimes \textstyle\bigwedge^2 V \xrightarrow{\delta} \ker(S^{q+1} V \otimes V \xrightarrow{\delta} S^{q+2} V), \tag{1-1}$$

where Δ is the *co-Wahl map* and δ is the *Koszul differential*. To achieve this, they established an explicit characteristic-free Hermite reciprocity for $\mathfrak{sl}_2$-representations, and they carried out complicated algebraic computations. Now, $K_{p,2}(T, \mathscr{O}_T(1))$ is the homology of a complex

$$S^q V \otimes W \xrightarrow{\gamma} S^{q+1} V \otimes V \xrightarrow{\delta} S^{q+2} V.$$

This homology, denoted by $W_q(V, W)$, is the degree-q piece of the *Koszul module* (or *Weyman module*) associated to (V, W). It is enough to prove that

$$W_q(V, W) = 0 \quad \text{for } q \geq p. \tag{1-2}$$

The vanishing result (1-2) was first proved in characteristic zero in [Aprodu et al. 2022] by an application of Bott vanishing, and the argument is extended in [Aprodu et al. 2019] to positive characteristics.

Our strategy to prove Theorem 1.1 is essentially the same as that of [Aprodu et al. 2019], but our geometric approach utilizing the *secant variety* $\Sigma \subseteq \mathbb{P}^g$ of a rational normal curve C of degree g provides a substantial simplification of the proof. The tangent surface T is a Weil divisor on Σ, and $\widetilde{T}$ is a Cartier divisor on B, where $\beta : B \to \Sigma$ is the blow-up of Σ along C with the exceptional divisor $Z = \mathbb{P}^1 \times \mathbb{P}^1$. Letting $M_H := \beta^* M_{\mathscr{O}_\Sigma(1)}$, we realize (1-1) as maps induced in cohomology of vector bundles on B (see (3-1)):

$$H^1\big(\widetilde{T}, \textstyle\bigwedge^{p+2} M_H|_{\widetilde{T}}\big) \xrightarrow{\alpha} H^2\big(B, \textstyle\bigwedge^{p+2} M_H \otimes \omega_B(Z)\big) \xrightarrow{\delta} H^2\big(Z, \omega_{\mathbb{P}^1} \boxtimes \textstyle\bigwedge^{p+2} M_L \otimes \omega_{\mathbb{P}^1}\big).$$

This was previously asked in [Aprodu et al. 2019, last paragraph on p. 666]. There is a rank-2 vector bundle E on $\mathbb{P}^2$ such that $B = \mathbb{P}(E)$. If $\pi : B \to \mathbb{P}^2$ is the canonical fibration, then $Q := \pi(\widetilde{T})$ is a smooth conic and $\widetilde{T} = \mathbb{P}(E|_Q)$. It is easy to check that $\alpha = \mathrm{id}_{S^q V} \otimes \Delta$, where Δ is the dual of the restriction map $H^0(\mathbb{P}^2, \mathscr{O}_{\mathbb{P}^2}(p+1)) \to H^0(Q, \mathscr{O}_Q(p+1))$. Put $M_E := \pi_* M_H$ and $\sigma := \pi|_Z$. The map δ is naturally factored as

$$\begin{array}{ccccc}
H^2\big(B, \bigwedge^{p+2} M_H \otimes \omega_B(Z)\big) & \xrightarrow{\mathrm{id}_{S^q V} \otimes \iota} & H^2\big(Z, \sigma^* \bigwedge^{p+2} M_E \otimes (\omega_{\mathbb{P}^1} \boxtimes \omega_{\mathbb{P}^1})\big) & \xrightarrow{m \otimes \mathrm{id}_V} & H^2\big(Z, \omega_{\mathbb{P}^1} \boxtimes \bigwedge^{p+2} M_L \otimes \omega_{\mathbb{P}^1}\big) \\
\| & & \| & & \| \\
S^q V \otimes \bigwedge^2 V & & S^q V \otimes V \otimes V & & S^{q+1} V \otimes V
\end{array}$$

where ι is the canonical injection and m is the multiplication map identified with

$$H^1(\mathbb{P}^{p+2} \times \mathbb{P}^1, \mathscr{O}_{\mathbb{P}^{p+2}}(q) \boxtimes \omega_{\mathbb{P}^1}(-p-2)) \longrightarrow H^1(\mathbb{P}^{p+2} \times \mathbb{P}^1, \mathscr{O}_{\mathbb{P}^{p+2}}(q+1) \boxtimes \omega_{\mathbb{P}^1}).$$

Without any lengthy computation, we quickly obtain the key part of [Aprodu et al. 2019] — the descriptions of the maps in (1-1) (see Lemma 3.1). This provides a conceptual explanation of the difficult computation in [loc. cit.] and a geometric understanding of syzygies of T in $\mathbb{P}^g$ as expected in [loc. cit., last paragraph on p. 666]. Next, regarding $V = H^0(\mathbb{P}^{p+2}, \mathscr{O}_{\mathbb{P}^{p+2}}(1))$, we give a direct proof of (1-2) using vector bundles on $\mathbb{P}^{p+2}$. This part of the proof is largely equivalent to the original proof in [Aprodu et al. 2019; 2022].[1] Put $M_V := M_{\mathscr{O}_{\mathbb{P}^{p+2}}(1)}$. Then (1-1) can be identified with

$$W \otimes H^0(\mathbb{P}^{p+2}, \mathscr{O}_{\mathbb{P}^{p+2}}(q)) \longrightarrow \textstyle\bigwedge^2 V \otimes H^0(\mathbb{P}^{p+2}, \mathscr{O}_{\mathbb{P}^{p+2}}(q)) \longrightarrow H^0(\mathbb{P}^{p+2}, M_V(q+1)).$$

Under the assumption $\mathrm{char}(\Bbbk) = 0$ or $\mathrm{char}(\Bbbk) \geq (g+2)/2$, we show that $W \otimes \mathscr{O}_{\mathbb{P}^{p+2}} \to M_V(1)$ is surjective and its kernel is $(p+1)$-regular in the sense of Castelnuovo and Mumford. This implies (1-2). Here the characteristic assumption plays a crucial role (see Remark 3.3).

It is worth noting that the characteristic assumption on the field $\Bbbk$ in Theorem 1.1 cannot be improved. If $2 \leq \mathrm{char}(\Bbbk) \leq (g+1)/2$, then $K_{\lfloor (g-3)/2 \rfloor, 2}(T, \mathscr{O}_T(1)) \neq 0$ (see [Aprodu et al. 2019, Remark 5.17]). Theorem 1.1 implies the generic Green conjecture for general curves of genus g when $\mathrm{char}(\Bbbk) = 0$ or $\mathrm{char}(\Bbbk) \geq (g+2)/2$, but this is not optimal. Raicu and Sam [2022, Theorem 1.5] recently obtained a sharp result that Green's conjecture holds for general curves of genus g when $\mathrm{char}(\Bbbk) = 0$ or $\mathrm{char}(\Bbbk) \geq \lfloor (g-1)/2 \rfloor$. This confirms a conjecture of Eisenbud and Schreyer [2019, Conjecture 1.1]. For the failure of Green's

[1] After writing the paper, the author learned from Claudiu Raicu [2021] that a similar argument proving (1-2) directly on projective spaces is given in his lecture notes based on Robert Lazarsfeld's suggestion.

conjecture in small characteristic, see [Eisenbud and Schreyer 2019; Schreyer 1986]. It has long been known that the generic Green conjecture would follow from the canonical ribbon conjecture [Bayer and Eisenbud 1995]. A *canonical ribbon* is a hyperplane section of a $K3$ *carpet* $X = X(a, b) \subseteq \mathbb{P}^{a+b+1}$ for integers $b \geq a \geq 1$, which is a unique double structure on a rational normal surface scroll $S(a, b) \subseteq \mathbb{P}^{a+b+1}$ of type (a, b) such that $\omega_X = \mathscr{O}_X$ and $h^1(X, \mathscr{O}_X) = 0$ (see [Gallego and Purnaprajna 1997, Theorem 1.3]). The K3 carpet X is a degeneration of a K3 surface of degree $2(a + b)$, and a canonical ribbon is a degeneration of a general canonical curve C of genus $a+b+1$ with $\mathrm{Cliff}(C) = a$. By extending algebraic arguments of [Aprodu et al. 2019], Raicu and Sam [2022, Theorem 1.1] proved $K_{p,2}(X, \mathscr{O}_X(1)) = 0$ for $0 \leq p \leq a-1$ when $\mathrm{char}(\Bbbk) = 0$ or $\mathrm{char}(\Bbbk) \geq a$. This implies the canonical ribbon conjecture and hence the generic Green conjecture (see [loc. cit., Section 6]). However, for settling Eisenbud and Schreyer conjecture, we only need to consider the case $a = \lfloor (g-1)/2 \rfloor$ and $b = \lfloor g/2 \rfloor$, and we recover [loc. cit., Theorem 1.1] for this case here.

Theorem 1.2. *Let $X = X(\lfloor (g-1)/2 \rfloor, \lfloor g/2 \rfloor) \subseteq \mathbb{P}^g$ be a $K3$ carpet with $g \geq 3$ over an algebraically closed field $\Bbbk$ with* $\mathrm{char}(\Bbbk) = 0$ *or* $\mathrm{char}(\Bbbk) \geq \lfloor (g-1)/2 \rfloor$ *and* $\mathrm{char}(\Bbbk) \neq 2$. *Then*

$$K_{p,2}(X, \mathscr{O}_X(1)) = 0 \quad \textit{for } 0 \leq p \leq \lfloor (g-3)/2 \rfloor.$$

In particular, Green's conjecture holds for general curves of genus g over $\Bbbk$.

Recall that Schreyer [1986] verified Green's conjecture for every curve of genus $g \leq 6$ over an algebraically closed field of arbitrary characteristic. In the theorem, if $g \geq 7$, then the condition $\mathrm{char}(\Bbbk) \neq 2$ is redundant. Our proof of Theorem 1.2 is essentially different from that of [Raicu and Sam 2022] but surprisingly the same as that of Theorem 1.1. The key point is that the K3 carpet X in the theorem is a Weil divisor linearly equivalent to the tangent-developable surface T on the secant variety Σ. Thus X is a degeneration of the tangent surface T. The proof of Theorem 1.1 works for X, and the characteristic assumption on $\Bbbk$ for (1-2) with another W can be improved. Consequently, we obtain a very quick proof of the generic Green conjecture and Eisenbud and Schreyer's conjecture.

In view of Theorem 1.1, it is quite natural to study syzygies of tangent-developable surfaces of smooth projective curves of genus $g \geq 1$. However, there was no research in this direction to the best of the author's knowledge. As a first step, we show the arithmetic normality, and compute the Castelnuovo–Mumford regularity.

Theorem 1.3. *Let C be a smooth projective curve of genus $g \geq 1$ over an algebraically closed field of characteristic zero, L be a line bundle on C with* $\deg L \geq 4g + 3$, *and T be the tangent-developable surface of C embedded in $\mathbb{P}^r$ by $|L|$. Then $T \subseteq \mathbb{P}^r$ is arithmetically normal but not arithmetically Cohen–Macaulay, and $H^i(T, \mathscr{O}_T(m)) = 0$ for $i > 0$, $m > 0$ but $H^1(T, \mathscr{O}_T) \neq 0$, $H^2(T, \mathscr{O}_T) \neq 0$. In particular*, $\operatorname{reg} \mathscr{O}_T = 3$, *and* $\operatorname{reg} \mathscr{I}_{T|\mathbb{P}^r} = 4$.

To prove the theorem, we develop new techniques based on the methods for secant varieties in [Ein et al. 2020]. Along with our proof of Theorem 1.1, this provides a general framework for syzygies of tangent-developable surfaces. First, we show that the dualizing sheaf ω_T is trivial (Proposition 2.5). The hard part of the proof of Theorem 1.3 is to check the 2-normality of $T \subseteq \mathbb{P}^r$, which is turned out to be equivalent to $H^1(C \times C, (L \boxtimes L)(-3D)) = 0$, where D is the diagonal of $C \times C$. This cohomology vanishing was established by Bertram, Ein and Lazarsfeld [Bertram et al. 1991] when $\deg L \geq 4g+3$. This degree condition is optimal: If $\deg L = 4g+2$, then $T \subseteq \mathbb{P}^r$ is arithmetically normal if and only if C is neither elliptic nor hyperelliptic (see Remark 4.4). We will discuss some conjectures on syzygies of tangent-developable surfaces at the end of Section 4.

After setting notation and presenting basic facts in Section 2, we prove Theorems 1.1 and 1.2 in Section 3 and Theorem 1.3 in Section 4. Throughout the paper, we work over an algebraically closed field $\Bbbk$ of arbitrary characteristic unless otherwise stated.

2. Preliminaries

2.1. ***Syzygies.*** Let X be a projective scheme, B be a coherent sheaf on X, and L be a very ample line bundle on X. Put $V := H^0(X, L)$. The *Koszul cohomology* $K_{p,q}(X, B; L)$ is the cohomology of the Koszul-type complex

$$\textstyle\bigwedge^{p+1} V \otimes H^0(X, B \otimes L^{q-1}) \longrightarrow \bigwedge^{p} V \otimes H^0(X, B \otimes L^{q}) \longrightarrow \bigwedge^{p-1} V \otimes H^0(X, B \otimes L^{q+1}).$$

When $B = \mathscr{O}_X$, we put $K_{p,q}(X, L) := K_{p,q}(X, \mathscr{O}_X; L)$ and $\kappa_{p,q}(X, L) := \dim_{\Bbbk} K_{p,q}(X, L)$. Let $S := \bigoplus_{m \geq 0} S^m V$. Then the graded S-module $R(X, B; L) := \bigoplus_{m \in \mathbb{Z}} H^0(X, B \otimes L^m)$ admits a minimal free resolution

$$0 \longleftarrow R(X, B; L) \longleftarrow E_0 \longleftarrow E_1 \longleftarrow \cdots \longleftarrow E_r \longleftarrow 0,$$

where $E_p = \bigoplus_q K_{p,q}(X, B; L) \otimes_{\Bbbk} S(-p-q)$. We may think that $K_{p,q}(X, B; L)$ is the space of p-th syzygies of weight q. For a globally generated vector bundle E on X, we denote by M_E the kernel of the evaluation map $H^0(X, E) \otimes \mathscr{O}_X \to E$. The following is well known.

Proposition 2.1 (see [Park 2022, Proposition 2.1]). *Assume that $H^i(X, B \otimes L^m) = 0$ for $i > 0$ and $m > 0$. For $q \geq 2$, we have $K_{p,q}(X, B; L) = H^{q-1}\big(X, \bigwedge^{p+q-1} M_L \otimes B \otimes L\big)$. If furthermore $H^{q-1}(X, B) = H^q(X, B) = 0$, then $K_{p,q}(X, B; L) = H^q\big(X, \bigwedge^{p+q} M_L \otimes B\big)$.*

2.2. ***Castelnuovo–Mumford regularity.*** A coherent sheaf $\mathscr{F}$ on $\mathbb{P}^n$ is said to be *m-regular* if

$$H^i(\mathbb{P}^n, \mathscr{F}(m-i)) = 0$$

for $i > 0$. By Mumford's theorem [Lazarsfeld 2004, Theorem 1.8.3], if $\mathscr{F}$ is m-regular, then $\mathscr{F}$ is $(m+1)$-regular. The *Castelnuovo–Mumford regularity* $\operatorname{reg} \mathscr{F}$ is the minimum m such that $\mathscr{F}$ is m-regular. If $\mathscr{F}$ fits into an exact sequence $\cdots \to \mathscr{F}_2 \to \mathscr{F}_1 \to \mathscr{F}_0 \to \mathscr{F} \to 0$ of coherent sheaves on $\mathbb{P}^n$ and $\mathscr{F}_i$ is $(m+i)$-regular for each $i \geq 0$, then $\mathscr{F}$ is m-regular [loc. cit., Example 1.8.7]. If $\mathscr{F}$ is m-regular and E is an m'-regular vector bundle on $\mathbb{P}^n$, then $\mathscr{F} \otimes E$ is $(m+m')$-regular [loc. cit., Proposition 1.8.9]. We can think of the regularity of a coherent sheaf $\mathscr{G}$ on a closed subscheme $X \subseteq \mathbb{P}^n$ by regarding $\mathscr{G}$ as a sheaf on $\mathbb{P}^n$.

2.3. ***Multilinear algebra.*** Let V be a finite-dimensional vector space over $\Bbbk$. The symmetric group $\mathfrak{S}_n$ naturally acts on $V^{\otimes n}$ by permuting the factors. The *divided power* $D^n V$ is the subspace

$$\{\omega \in V^{\otimes n} \mid \sigma(\omega) = \omega \text{ for all } \sigma \in \mathfrak{S}_n\} \subseteq T^n V,$$

and the *symmetric power* $S^n V$ is the quotient of $V^{\otimes n}$ by the span of $\sigma(\omega) - \omega$ for all $\omega \in V^{\otimes n}$ and $\sigma \in \mathfrak{S}_n$. We have a natural identification $D^n V = (S^n V^\vee)^\vee$. By composing the inclusion of $D^n V$ into $V^{\otimes n}$ with the projection onto $S^n V$, we get a natural map $D^n V \to S^n V$. This is an isomorphism if $\operatorname{char}(\Bbbk) = 0$ or $\operatorname{char}(\Bbbk) > n$, but it may be neither injective nor surjective in general. The *wedge product* $\bigwedge^n V$ is the quotient of $V^{\otimes n}$ by the span of $v_1 \otimes \cdots \otimes v_n$ for all $v_1, \dots, v_n \in V$ with $v_i = v_j$ for some $i \neq j$. We write $v_1 \wedge \cdots \wedge v_n$ for the class of $v_1 \otimes \cdots \otimes v_n$ in the quotient. There is a natural inclusion $\bigwedge^n V \to V^{\otimes n}$ given by $v_1 \wedge \cdots \wedge v_n \mapsto \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma)\sigma(v_1 \otimes \cdots \otimes v_n)$. This gives a splitting of the quotient map $V^{\otimes n} \to \bigwedge^n V$ if and only if $\operatorname{char}(\Bbbk) = 0$ or $\operatorname{char}(\Bbbk) > n$. We refer to [Aprodu et al. 2019, Section 3] for more details.

2.4. ***Projective spaces.*** Throughout the paper, we put $U := H^0(\mathbb{P}^1, \mathscr{O}_{\mathbb{P}^1}(1))$, and fix a basis $1, x$ of U. The monomials $1, x, \dots, x^d$ form a basis of $S^d U$, and the divided power monomials $x^{(0)}, x^{(1)}, \dots, x^{(d)}$ form a basis of $D^d U$. Let $1, y$ be the dual basis of $U^\vee$ to $1, x$. There is a natural identification $U^\vee = \bigwedge^2 U \otimes U^\vee = U$ sending $1, y$ to $-x, 1$. Then $H^0(\mathbb{P}^1, \mathscr{O}_{\mathbb{P}^1}(d)) = S^d U$ and $H^1(\mathbb{P}^1, \mathscr{O}_{\mathbb{P}^1}(-d-2)) = D^d U$. Note that $M_{\mathscr{O}_{\mathbb{P}^1}(d)} = S^{d-1} U \otimes \mathscr{O}_{\mathbb{P}^1}(-1)$.

We may regard $\mathbb{P}^n$ as the symmetric product of $\mathbb{P}^1$. By permuting the components, $\mathfrak{S}_n$ acts on the ordinary product $(\mathbb{P}^1)^n$, and the line bundle $\mathscr{O}_{\mathbb{P}^1}(d)^{\boxtimes n}$ on $(\mathbb{P}^1)^n$ descends to a line bundle $T_{n, \mathscr{O}_{\mathbb{P}^1}(d)} = \mathscr{O}_{\mathbb{P}^n}(d)$ on $\mathbb{P}^n$ in such a way that $q_n^* T_{n, \mathscr{O}_{\mathbb{P}^1}(d)} = \mathscr{O}_{\mathbb{P}^1}(d)^{\boxtimes n}$, where $q_n : (\mathbb{P}^1)^n \to \mathbb{P}^n$ is the quotient map. Then $H^0(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(d)) = D^n S^d U$. Since $H^0(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(1)) = D^n U$, we get $H^0(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(d)) = S^d D^n U$. This gives *Hermite reciprocity* $D^n S^d U = S^d D^n U$. If the action of $\mathfrak{S}_n$ on $(\mathbb{P}^1)^n$ is alternating, then $\mathscr{O}_{\mathbb{P}^1}(d)^{\boxtimes n}$ descends to $N_{n, \mathscr{O}_{\mathbb{P}^1}(d)} = \mathscr{O}_{\mathbb{P}^n}(d-n+1)$ and $H^0(\mathbb{P}^n, \mathscr{O}_{\mathbb{P}^n}(d-n+1)) = \bigwedge^n S^d U$. This gives another *Hermite reciprocity*

$$\bigwedge^n S^d U = S^{d-n+1} D^n U. \tag{2-1}$$

See [Aprodu et al. 2019, Remark 3.2] and [Park 2022, Subsection 2.3]. Our Hermite reciprocity coincides with the explicit map constructed in [Aprodu et al. 2019, Section 3] (see [Raicu and Sam 2021]), but we will not use this fact.

Let D_n be the image of the injective map $\mathbb{P}^{n-1} \times \mathbb{P}^1 \to \mathbb{P}^n \times \mathbb{P}^1$ given by $(\xi, z) \mapsto (\xi + z, z)$. Note that the effective divisor D_n on $\mathbb{P}^n \times \mathbb{P}^1$ is defined by

$$\sum_{i=0}^{n} (-1)^i (x^0 \wedge \cdots \wedge \widehat{x^i} \wedge \cdots \wedge x^n) \otimes x^i \in \bigwedge^n S^n U \otimes S^n U = H^0(\mathbb{P}^n \times \mathbb{P}^1, \mathscr{O}_{\mathbb{P}^n}(1) \boxtimes \mathscr{O}_{\mathbb{P}^1}(n)).$$

Consider the short exact sequence

$$0 \longrightarrow \mathscr{O}_{\mathbb{P}^n}(d-1) \boxtimes \mathscr{O}_{\mathbb{P}^1}(-n) \xrightarrow{\cdot D_n} \mathscr{O}_{\mathbb{P}^n}(d) \boxtimes \mathscr{O}_{\mathbb{P}^1} \longrightarrow \mathscr{O}_{\mathbb{P}^{n-1}}(d) \boxtimes \mathscr{O}_{\mathbb{P}^1}(d) \longrightarrow 0. \tag{2-2}$$

Pushing forward to $\mathbb{P}^1$ yields a short exact sequence

$$0 \longrightarrow \bigwedge^n M_{\mathscr{O}_{\mathbb{P}^1}(d+n-1)} \longrightarrow \bigwedge^n S^{d+n-1} U \otimes \mathscr{O}_{\mathbb{P}^1} \longrightarrow \bigwedge^{n-1} M_{\mathscr{O}_{\mathbb{P}^1}(d+n-1)} \otimes \mathscr{O}_{\mathbb{P}^1}(d+n-1) \longrightarrow 0.$$

On the other hand, D_n can be also defined by

$$\sum_{i=0}^{n}(-1)^i x^{(n-i)} \otimes x^i \in D^n U \otimes S^n U = H^0(\mathbb{P}^n \times \mathbb{P}^1, \mathscr{O}_{\mathbb{P}^n}(1) \boxtimes \mathscr{O}_{\mathbb{P}^1}(n)).$$

Then we see that the map

$$\begin{tikzcd} H^1(\mathbb{P}^n \times \mathbb{P}^1, \mathscr{O}_{\mathbb{P}^n}(d-1) \boxtimes \omega_{\mathbb{P}^1}(-n)) \arrow[r, "\cdot D_n"] \arrow[d, equal] & H^1(\mathbb{P}^n \times \mathbb{P}^1, \mathscr{O}_{\mathbb{P}^n}(d) \boxtimes \omega_{\mathbb{P}^1}) \arrow[d, equal] \\ S^{d-1} D^n U \otimes D^n U & S^d D^n U \end{tikzcd} \tag{2-3}$$

is given by $f \otimes x^{(i)} \mapsto (-1)^n f x^{(i)}$. We simply regard this as the multiplication map.

2.5. ***Secant varieties.*** We recall the set-up of [Ein et al. 2020; 2021], and we present some preliminary results. Let C be a smooth projective curve of genus $g \geq 0$, and L be a line bundle on C with $\deg L \geq 2g+3$.[2] We assume $\operatorname{char}(\Bbbk) = 0$ whenever $g \geq 1$. We denote by $C^2 = C \times C$ the ordinary product of C and by $C_2 = C^2/\mathfrak{S}_2$ the symmetric product of C. The quotient map $\sigma : C^2 \to C_2$ is given by $(x, y) \mapsto x+y$. If we regard C_2 as the Hilbert scheme of two points on C, then σ is the universal family. For any line bundle A on C, there is a line bundle T_A on C_2 such that $\sigma^* T_A = A \boxtimes A$. Let D be the diagonal of C^2, and $Q := \sigma(D)$. Then $Q \cong C$ unless $g = 0$ and $\operatorname{char}(\Bbbk) = 2$. We may write $Q = 2\delta$ for some divisor δ on C_2. Note that $\sigma^*\delta = D$ and $\sigma_* \mathscr{O}_{C^2} = \mathscr{O}_{C_2}(-\delta) \oplus \mathscr{O}_C$ (see [Ein et al. 2020, Lemma 3.5]). We can write $K_{C_2} = T_{K_C}(-\delta)$. Consider the *tautological bundle* $E := \sigma_*(\mathscr{O}_C \boxtimes L)$ on C_2. We have $\operatorname{rank} E = 2$ and $\det E = T_L(-\delta)$. Let $B := \mathbb{P}(E)$, and $\pi : B \to C_2$ be the canonical fibration. As $H^0(C_2, E) = H^0(C, L)$ and E is globally generated, $|\mathscr{O}_{\mathbb{P}(E)}(1)|$ induces a map $\beta : B \to \mathbb{P}^r = \mathbb{P}H^0(C, L)$. Then $\Sigma := \beta(B)$ is the *secant variety* of C in $\mathbb{P}^r$, and $\beta : B \to \Sigma$ is the blow-up of Σ along C (see [Ein et al. 2021, Theorem 1.1]). Unless $g = 0$ and $\deg L = 3$ (in this case $\Sigma = \mathbb{P}^3$), $\operatorname{Sing} \Sigma = C$ and $\beta : B \to \Sigma$ is a resolution of singularities. Let $Z := \beta^{-1}(C) \cong C^2$. Then $\pi|_Z : Z \to C_2$ is just σ, and $\beta|_Z : Z = C \times C \to C$ is the second projection:

$$\begin{tikzcd} Z = C \times C \arrow[r, hook] \arrow[dr, "\sigma"'] & B = \mathbb{P}(E) \arrow[r, "\beta"] \arrow[d, "\pi"] & \Sigma \subseteq \mathbb{P}^r \\ & C_2 & \end{tikzcd}$$

Theorem 2.2 [Ein et al. 2020, Theorems 1.1 and 1.2]. *$\Sigma \subseteq \mathbb{P}^r$ is arithmetically Cohen–Macaulay. If $g = 0$, then Σ has rational singularities and* $\operatorname{reg} \mathscr{O}_\Sigma = 2$. *If $g \geq 1$ and* $\operatorname{char}(\Bbbk) = 0$, *then Σ has normal Du Bois singularities and* $\operatorname{reg} \mathscr{O}_\Sigma = 4$.

Pick $H \in |\mathscr{O}_{\mathbb{P}(E)}(1)|$. We may write $K_B = -2H + \pi^* T_{K_C+L}(-2\delta)$ and $Z = 2H - \pi^* T_L(-2\delta)$. Take $\bar{S} \in |2\delta|$. Let $\widetilde{S} := \pi^{-1}(\bar{S}) = \mathbb{P}(E|_{\bar{S}})$, and $S := \beta(\widetilde{S})$. We are mostly interested in the case $\bar{S} = Q$. In fact, Q is a unique member in $|2\delta|$ when $g \geq 2$. Note that $\dim |2\delta| = 5$ when $g = 0$ and $\dim |2\delta| = 1$ when $g = 1$. Assume that $\operatorname{char}(\Bbbk) \neq 2$ when $g = 0$. Note that $M_E|_Q = N^\vee_{C|\mathbb{P}^r} \otimes L$ and $E|_Q = \mathscr{P}^1(L)$ is the first

[2] It is assumed that $\operatorname{char}(\Bbbk) = 0$ in [Ein et al. 2020; 2021], but everything works when $g = 0$ and $\operatorname{char}(\Bbbk) \geq 0$ (see also [Raicu and Sam 2021]).

jet bundle. By [Kaji 1986, Corollary 1.18], $\mathscr{P}^1(L)$ is the unique nontrivial extension of L by $\omega_C \otimes L$ when $\mathrm{char}(\Bbbk) \nmid \deg L$. Let $\widetilde{T} := \pi^{-1}(Q)$. Then $T := \beta(\widetilde{T})$ is the *tangent-developable surface* of C in $\mathbb{P}^r$, and T has cuspidal singularities along C. Note that $\nu := \beta|_{\widetilde{T}} : \widetilde{T} \to T$ is a resolution of singularities and T is Cohen–Macaulay.

Proposition 2.3. $\deg S = 2\deg L + 2g - 2$.

Proof. We have $\deg S = (H|_{\widetilde{S}})^2 = (\det E) \cdot \overline{S} = 2\deg L + 2g - 2$. □

Recall from [Ein et al. 2020, Theorem 5.2] that $\beta_*\mathscr{O}_B(-Z) = \mathscr{I}_{C|\Sigma}$ and $R^1\beta_*\mathscr{O}_B(-Z) = 0$.

Lemma 2.4. *$\beta_*\mathscr{O}_B(-\widetilde{S} - Z) = \mathscr{I}_{S|\Sigma}$ and $R^1\beta_*\mathscr{O}_B(-\widetilde{S} - Z) = 0$.*

Proof. As $\beta_*\mathscr{O}_Z(-\widetilde{S}) = 0$, we have $\beta_*\mathscr{O}_B(-\widetilde{S} - Z) = \beta_*\mathscr{O}_B(-\widetilde{S}) = \mathscr{I}_{S|\Sigma}$. For the second assertion, following [loc. cit., proof of Theorem 5.2(2)], we show that $R^1\beta_*\mathscr{O}_B(-\widetilde{S} - Z)_x = 0$ for any $x \in C \subseteq \Sigma$. Let $F := \beta^{-1}(x) \cong C$. By the formal function theorem, it suffices to prove that

$$H^1(F, \mathscr{O}_B(-\widetilde{S} - Z) \otimes \mathscr{O}_B/\mathscr{I}^m_{F|B}) = 0 \quad \text{for } m \geq 1.$$

It is enough to check that

$$H^1(F, \mathscr{O}_B(-\widetilde{S} - Z) \otimes \mathscr{I}^m_{F|B}/\mathscr{I}^{m+1}_{F|B}) = 0 \quad \text{for } m \geq 0.$$

As $(-\widetilde{S} - Z)|_Z = (L \boxtimes -L)(-4D)$ and F is a fiber of the second projection $Z = C \times C \to C$, we have $\mathscr{O}_B(-\widetilde{S} - Z)|_F = L(-4x)$. Note that $\mathscr{I}^m_{F|B}/\mathscr{I}^{m+1}_{F|B} = S^m N^\vee_{F|B}$. Recall from [Ein et al. 2020, Proposition 3.13] that $N^\vee_{F|B} = \mathscr{O}_C \oplus L(-2x)$. The problem is then reduced to verifying that

$$H^1(C, (m+1)L + (-4 - 2m)x) = 0 \quad \text{for } m \geq 0.$$

This vanishing holds since $\deg((m+1)L + (-4-2m)x) \geq (m+1)(2g+3) - 4 - 2m \geq 2g - 1$. □

Consider the following commutative diagram with short exact sequences:

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathscr{O}_B(-\widetilde{S} - Z) \arrow[r, "\cdot Z"] \arrow[d, equal] & \mathscr{O}_B(-\widetilde{S}) \arrow[r] \arrow[d, "\cdot \widetilde{S}"] & \mathscr{O}_Z(-2D) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathscr{O}_B(-\widetilde{S} - Z) \arrow[r, "\cdot \widetilde{S}+Z"'] & \mathscr{O}_B \arrow[r] \arrow[d] & \mathscr{O}_{\widetilde{S}+Z} \arrow[r] \arrow[d] & 0 \\
 & & \mathscr{O}_{\widetilde{S}} \arrow[r, equal] \arrow[d] & \mathscr{O}_{\widetilde{S}} \arrow[d] & \\
 & & 0 & 0 &
\end{tikzcd} \tag{2-4}$$

By Lemma 2.4, applying β_* to the second-row exact sequence in (2-4), we find $\beta_*\mathscr{O}_{\widetilde{S}+Z} = \mathscr{O}_S$ and $R^1\beta_*\mathscr{O}_{\widetilde{S}+Z} = R^1\beta_*\mathscr{O}_B = H^1(C, \mathscr{O}_C) \otimes \mathscr{O}_C$, and we get a short exact sequence

$$0 \longrightarrow \beta_*\mathscr{O}_B(-\widetilde{S} - Z) \longrightarrow \mathscr{O}_\Sigma \longrightarrow \mathscr{O}_S \longrightarrow 0. \tag{2-5}$$

Note that

$$R^1\beta_*\mathscr{O}_{\widetilde{S}+Z} = R^1\beta_*\mathscr{O}_B = R^1(\beta|_Z)_*\mathscr{O}_Z = R^1(\beta|_Z)_*\mathscr{O}_Z(-D).$$

The kernel of the map $R^1(\beta|_Z)_*\mathscr{O}_Z(-2D) \to R^1(\beta|_Z)_*\mathscr{O}_Z(-D)$ is $\mathscr{O}_D(-D|_D) = \omega_C$. By applying β_* to the rightmost vertical exact sequence in (2-4), we get a short exact sequence

$$0 \longrightarrow \mathscr{O}_S \longrightarrow \beta_*\mathscr{O}_{\widetilde{S}} \longrightarrow \omega_C \longrightarrow 0. \tag{2-6}$$

Proposition 2.5. *The dualizing sheaf ω_S is trivial.*

Proof. Consider two short exact sequences

$$0 \longrightarrow \omega_B \longrightarrow \omega_B(Z) \longrightarrow \omega_Z \longrightarrow 0 \quad \text{and} \quad 0 \longrightarrow \omega_B \longrightarrow \omega_B(\widetilde{S}) \longrightarrow \omega_{\widetilde{S}} \longrightarrow 0. \tag{2-7}$$

By Theorem 2.2 for $g = 0$ and Grauert–Riemenschneider vanishing for $g \geq 1$, we have $R^1\beta_*\omega_B = 0$. Then $R^1\beta_*\omega_B(Z) = R^1\beta_*\omega_Z = \omega_C$ and $R^1\beta_*\omega_B(\widetilde{S}) = 0$. By taking $-\otimes\mathscr{O}_B(\widetilde{S})$ to the left of (2-7), we see that $R^1\beta_*\omega_B(\widetilde{S}+Z) = 0$. When $g = 0$, we have $\beta_*\omega_B(Z) = \beta_*\omega_B = \omega_\Sigma$ by Theorem 2.2. When $g \geq 1$, Theorem 2.2 and [Kovács et al. 2010, Theorem 1.1] show that $\beta_*\omega_B(Z) = \omega_\Sigma$. As $\omega_{\widetilde{S}}(Z|_{\widetilde{S}}) = \mathscr{O}_{\widetilde{S}}$, applying β_* to the short exact sequence with the consideration of (2-6),

$$0 \longrightarrow \omega_B(Z) \xrightarrow{\cdot\widetilde{S}} \omega_B(\widetilde{S}+Z) \longrightarrow \mathscr{O}_{\widetilde{S}} \longrightarrow 0,$$

we obtain a short exact sequence

$$0 \longrightarrow \omega_\Sigma \longrightarrow \beta_*\omega_B(\widetilde{S}+Z) \longrightarrow \mathscr{O}_S \longrightarrow 0.$$

On the other hand, applying $\mathscr{H}om_\Sigma(-, \omega_\Sigma)$ to (2-5), we get a short exact sequence

$$0 \longrightarrow \omega_\Sigma \longrightarrow \mathscr{H}om_\Sigma(\beta_*\mathscr{O}_B(-\widetilde{S}-Z), \omega_\Sigma) \longrightarrow \omega_S \longrightarrow 0$$

since Σ is Cohen–Macaulay. Notice that

$$\mathscr{H}om_\Sigma(\beta_*\mathscr{O}_B(-\widetilde{S}-Z), \omega_\Sigma) = \mathscr{H}om_\Sigma(\beta_*\mathscr{O}_B(-\widetilde{S}), \omega_\Sigma) = \beta_*\omega_B(\widetilde{S}+Z).$$

Hence we conclude that $\omega_S = \mathscr{O}_S$. □

Remark 2.6. When $g = 0$ and $S = T$ is the tangent-developable surface, the above proposition was shown in [Aprodu et al. 2019, Corollary 5.16]. When $g = 1$ and $\deg L = 5$, applying the Serre construction to the tangent-developable surface T in $\mathbb{P}^4$, Hulek [1986, Chapter VII] gave a new construction of the Horrocks–Mumford bundle on $\mathbb{P}^4$.

2.6. ***Rational curve case.*** Assume that $\operatorname{char}(\Bbbk) \neq 2$. Let $C \subseteq \mathbb{P}^g$ be a rational normal curve of degree $g \geq 3$, and $L := \mathscr{O}_{\mathbb{P}^1}(g)$. When we consider a rational normal curve, g is not the genus but the degree. Note that $C_2 = \mathbb{P}^2$ and $\mathscr{O}_{\mathbb{P}^2}(\delta) = \mathscr{O}_{\mathbb{P}^2}(1)$. We have $T_{\mathscr{O}_{\mathbb{P}^1}(d)} = \mathscr{O}_{\mathbb{P}^2}(d)$, and put $N_{\mathscr{O}_{\mathbb{P}^1}(d)} := T_{\mathscr{O}_{\mathbb{P}^1}(d)}(-\delta) = \mathscr{O}_{\mathbb{P}^2}(d-1)$.

Then $\sigma^* T_{\mathscr{O}_{\mathbb{P}^1}(d)} = \mathscr{O}_{\mathbb{P}^1}(d) \boxtimes \mathscr{O}_{\mathbb{P}^1}(d)$ and $\sigma^* N_{\mathscr{O}_{\mathbb{P}^1}(d)} = \mathscr{O}_{\mathbb{P}^1}(d-1) \boxtimes \mathscr{O}_{\mathbb{P}^1}(d-1)$. Note that $\pi_* \mathscr{O}_B(-Z) = 0$ and $R^1\pi_* \mathscr{O}_B(-Z) = \mathscr{O}_{\mathbb{P}^2}(-\delta)$. By applying π_* to the short exact sequence

$$0 \longrightarrow \mathscr{O}_B(-Z) \xrightarrow{\cdot Z} \mathscr{O}_B \longrightarrow \mathscr{O}_Z \longrightarrow 0, \tag{2-8}$$

we get a splitting short exact sequence

$$0 \longrightarrow \mathscr{O}_{\mathbb{P}^2} \longrightarrow \sigma_* \mathscr{O}_Z \longrightarrow \mathscr{O}_{\mathbb{P}^2}(-\delta) \longrightarrow 0.$$

Then we obtain the following canonically splitting short exact sequence:

$$\begin{array}{ccccccccc} 0 \longrightarrow & H^0(\mathbb{P}^2, T_{\mathscr{O}_{\mathbb{P}^1}(d)}) & \longrightarrow & H^0(\mathbb{P}^1 \times \mathbb{P}^1, \mathscr{O}_{\mathbb{P}^1}(d) \boxtimes \mathscr{O}_{\mathbb{P}^1}(d)) & \longrightarrow & H^0(\mathbb{P}^2, N_{\mathscr{O}_{\mathbb{P}^1}(d)}) & \longrightarrow 0 \\ & \| & & \| & & \| & \\ & D^2 S^d U & & S^d U \otimes S^d U & & \bigwedge^2 S^d U & \end{array} \tag{2-9}$$

Lemma 2.7. $M_E = S^{g-2}U \otimes \mathscr{O}_{\mathbb{P}^2}(-1)$.

Proof. Recall that there is an injective map $D_2 = \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^2 \times \mathbb{P}^1$. Let $p_1 : \mathbb{P}^2 \times \mathbb{P}^1 \to \mathbb{P}^2$ be the first projection. Then $(p_1)|_{D_2} = \sigma$. By applying $p_{1,*}$ to the short exact sequence

$$0 \longrightarrow \mathscr{O}_{\mathbb{P}^2}(-1) \boxtimes \mathscr{O}_{\mathbb{P}^1}(g-2) \xrightarrow{\cdot D_2} \mathscr{O}_{\mathbb{P}^2} \boxtimes \mathscr{O}_{\mathbb{P}^1}(g) \longrightarrow \mathscr{O}_{\mathbb{P}^1} \boxtimes \mathscr{O}_{\mathbb{P}^1}(g) \longrightarrow 0,$$

we get a short exact sequence

$$0 \longrightarrow S^{g-2}U \otimes \mathscr{O}_{\mathbb{P}^2}(-1) \longrightarrow S^g U \otimes \mathscr{O}_{\mathbb{P}^2} \longrightarrow E \longrightarrow 0,$$

where $H^0(\mathbb{P}^2, E) \otimes \mathscr{O}_{\mathbb{P}^2} = S^g U \otimes \mathscr{O}_{\mathbb{P}^2} \to E$ is the evaluation map. Thus the lemma follows. □

Proposition 2.8. (1) $K_B + \widetilde{S} + Z = 0$.

(2) *$S \subseteq \mathbb{P}^g$ is arithmetically Cohen–Macaulay and* $\operatorname{reg} \mathscr{O}_S = 3$.

(3) *The Hilbert function of $S \subseteq \mathbb{P}^g$ is given by $H_S(t) = (g-1)t^2 + 2$ for $t \geq 1$.*

Proof. The assertion (1) follows from the direct computation

$$K_B + \widetilde{S} + Z = (-2H + \pi^* \mathscr{O}_{\mathbb{P}^2}(g-4)) + \pi^* \mathscr{O}_{\mathbb{P}^2}(2) + (2H - \pi^* \mathscr{O}_{\mathbb{P}^2}(g-2)) = 0.$$

As $\beta_* \mathscr{O}_B(-\widetilde{S} - Z) = \beta_* \omega_B = \omega_\Sigma$ by Theorem 2.2, the short exact sequence (2-5) is

$$0 \longrightarrow \omega_\Sigma \longrightarrow \mathscr{O}_\Sigma \longrightarrow \mathscr{O}_S \longrightarrow 0. \tag{2-10}$$

By Theorem 2.2, we readily obtain (2). Now, $H_T(t)$ agrees with the Hilbert polynomial $P_S(t)$ for $t \geq 1$. Note that det $P_S(t) = 2$ and the leading coefficient of $P_T(t)$ is $(\deg S)/2 = g-1$. As $P_S(0) = \chi(\mathscr{O}_S) = 2$ and $P_S(1) = g+1$, we get (3). □

When $S = T$ is the tangent-developable surface, Proposition 2.8(2) was first shown by Schreyer [1983, Proposition 6.1] (see also [Aprodu et al. 2019, Theorem 5.1]). Observe that $S \subseteq \mathbb{P}^g$ has the same Hilbert polynomial with a K3 surface of degree $2g-2$ in $\mathbb{P}^g$.

Suppose that $\bar{S}=Q$. Here $Q=\sigma(D)$ is a smooth conic in $\mathbb{P}^2$. When $\mathrm{char}(\Bbbk)=0$ or $\mathrm{char}(\Bbbk)\geq(g+2)/2$, [Kaji 1986, Corollary 1.18] implies that $E|_Q=\mathscr{O}_{\mathbb{P}^1}(g-1)\oplus\mathscr{O}_{\mathbb{P}^1}(g-1)$. In this case, $\widetilde{T}=\mathbb{P}^1\times\mathbb{P}^1$, and $\mathscr{O}_{\widetilde{T}}(H|_{\widetilde{T}})=\mathscr{O}_{\mathbb{P}^1}(g-1)\boxtimes\mathscr{O}_{\mathbb{P}^1}(1)$. When $\mathrm{char}(\Bbbk)\mid g$, [loc. cit., Corollary 1.18] implies that $\widetilde{T}\neq\mathbb{P}^1\times\mathbb{P}^1$. However, we always have $Z=\mathbb{P}^1\times\mathbb{P}^1$. Now, consider the following short exact sequence:

$$\begin{array}{ccccccccc} 0 \longrightarrow & H^0(\mathbb{P}^2,\mathscr{O}_{\mathbb{P}^2}(d-1)) & \xrightarrow{\cdot Q} & H^0(\mathbb{P}^2,\mathscr{O}_{\mathbb{P}^2}(d+1)) & \longrightarrow & H^0(Q,\mathscr{O}_Q(d+1)) & \longrightarrow 0 \\ & \| & & \| & & \| & \\ & \bigwedge^2 S^dU & & \bigwedge^2 S^{d+2}U & & S^{2d+2}U & \end{array} \tag{2-11}$$

Since $\sigma^*Q=2D$ and the diagonal D of $\mathbb{P}^1\times\mathbb{P}^1$ is defined by

$$x\otimes 1-1\otimes x\in U\otimes U=H^0(\mathbb{P}^1\times\mathbb{P}^1,\mathscr{O}_{\mathbb{P}^1}(1)\boxtimes\mathscr{O}_{\mathbb{P}^1}(1)),$$

the inclusion $H^0(\mathbb{P}^2,\mathscr{O}_{\mathbb{P}^2}(d-1))\to H^0(\mathbb{P}^2,\mathscr{O}_{\mathbb{P}^2}(d+1))$ in (2-11) is

$$\textstyle\bigwedge^2 S^dU\longrightarrow\bigwedge^2 S^{d+2}U,\quad x^i\wedge x^j\longmapsto x^{i+2}\wedge x^j-2x^{i+1}\wedge x^{j+1}+x^i\wedge x^{j+2}.$$

The surjection $H^0(\mathbb{P}^2,\mathscr{O}_{\mathbb{P}^2}(d+1))\to H^0(Q,\mathscr{O}_Q(d+1))$ in (2-11) is

$$\mu_{d+2}:\textstyle\bigwedge^2 S^{d+2}U\longrightarrow S^{2d+2}U,\quad x^i\wedge x^j\longmapsto(i-j)x^{i+j-1}, \tag{2-12}$$

which is the *Wahl map* (or the *Gaussian map*). See [Bertram et al. 1991; Wahl 1990] for details on Wahl maps.

Suppose that $\bar{S}=2\ell$, where $\ell\subseteq\mathbb{P}^2$ is a line meeting Q at two distinct points. We may write $E|_\ell=\mathscr{O}_{\mathbb{P}^1}(a)\oplus\mathscr{O}_{\mathbb{P}^1}(b)$ for some integers $b\geq a\geq 1$. As $\det E=N_L=\mathscr{O}_{\mathbb{P}^2}(g-1)$, we have $a+b=g-1$. Note that $\sigma^{-1}(\ell)=\mathbb{P}^1$ and $\sigma|_{\sigma^{-1}(\ell)}:\sigma^{-1}(\ell)\to\ell$ is a two-to-one map. By restricting the short exact sequence

$$0\longrightarrow\mathscr{O}_{\mathbb{P}^1}(g-1)\boxtimes\mathscr{O}_{\mathbb{P}^1}(-1)\longrightarrow\sigma^*E\longrightarrow\mathscr{O}_{\mathbb{P}^1}\boxtimes\mathscr{O}_{\mathbb{P}^1}(g)\longrightarrow 0$$

to $\sigma^{-1}(\ell)$, we get a short exact sequence

$$0\longrightarrow\mathscr{O}_{\mathbb{P}^1}(g-2)\longrightarrow\mathscr{O}_{\mathbb{P}^1}(2a)\oplus\mathscr{O}_{\mathbb{P}^1}(2b)\longrightarrow\mathscr{O}_{\mathbb{P}^1}(g)\longrightarrow 0.$$

It follows that $(a,b)=(\lfloor(g-1)/2\rfloor,\lfloor g/2\rfloor)$. Then S is a double structure on a rational normal surface scroll $S(a,b)=\mathbb{P}(E|_\ell)\subseteq\mathbb{P}^g$. Recall that $H^1(S,\mathscr{O}_S)=0$ and $\omega_S=\mathscr{O}_S$. Thus $S=X(\lfloor(g-1)/2\rfloor,\lfloor g/2\rfloor)\subseteq\mathbb{P}^g$ is a $K3$ *carpet* (see [Gallego and Purnaprajna 1997, Definition 1.2 and Theorem 1.3][3]). On the other hand, consider the following short exact sequence:

$$\begin{array}{ccccccccc} 0 \longrightarrow & H^0(\mathbb{P}^2,\mathscr{O}_{\mathbb{P}^2}(d-1)) & \xrightarrow{\cdot 2\ell} & H^0(\mathbb{P}^2,\mathscr{O}_{\mathbb{P}^2}(d+1)) & \longrightarrow & H^0(2\ell,\mathscr{O}_{2\ell}(d+1)) & \longrightarrow 0 \\ & \| & & \| & & & \\ & \bigwedge^2 S^dU & & \bigwedge^2 S^{d+2}U & & & \end{array} \tag{2-13}$$

[3] The proof of [Gallego and Purnaprajna 1997, Theorem 1.3] also works in positive characteristic.

We may assume that $\sigma^{-1}(\ell)$ in $\mathbb{P}^1\times\mathbb{P}^1$ is defined by

$$x\otimes 1+1\otimes x\in U\otimes U=H^0(\mathbb{P}^1\times\mathbb{P}^1,\mathscr{O}_{\mathbb{P}^1}(1)\boxtimes\mathscr{O}_{\mathbb{P}^1}(1)).$$

Then the inclusion $H^0(\mathbb{P}^2,\mathscr{O}_{\mathbb{P}^2}(d-1))\to H^0(\mathbb{P}^2,\mathscr{O}_{\mathbb{P}^2}(d+1))$ in (2-13) is

$$\textstyle\bigwedge^2 S^dU\longrightarrow \bigwedge^2 S^{d+2}U,\quad x^i\wedge x^j\longmapsto x^{i+2}\wedge x^j+2x^{i+1}\wedge x^{j+1}+x^i\wedge x^{j+2}.$$

It is a direct summand of the inclusion

$$H^0(\mathbb{P}^1\times\mathbb{P}^1,\mathscr{O}_{\mathbb{P}^1}(d)\boxtimes\mathscr{O}_{\mathbb{P}^1}(d))\xrightarrow{\cdot 2\sigma^{-1}(\ell)}H^0(\mathbb{P}^1\times\mathbb{P}^1,\mathscr{O}_{\mathbb{P}^1}(d+2)\boxtimes\mathscr{O}_{\mathbb{P}^1}(d+2))$$

whose cokernel is $S^{2d+2}U\oplus S^{2d+4}U$. The surjection $H^0(\mathbb{P}^2,\mathscr{O}_{\mathbb{P}^2}(d+1))\to H^0(2\ell,\mathscr{O}_{2\ell}(d+1))$ in (2-13) factors through

$$\tau_{d+2}:\textstyle\bigwedge^2 S^{d+2}U\longrightarrow \begin{matrix}S^{2d+2}U\\ \oplus\\ S^{2d+4}U\end{matrix},\quad x^i\wedge x^j\longmapsto\begin{cases}((-1)^i(i-j)x^{i+j-1},0) & \text{if } i\equiv j \pmod 2,\\ (0,(-1)^ix^{i+j}) & \text{if } i\not\equiv j \pmod 2,\end{cases}\tag{2-14}$$

in such a way that $\mathrm{im}(\tau_{d+2})$ injects into $H^0(2\ell,\mathscr{O}_{2\ell}(d+1))$.

3. Proofs of Theorems 1.1 and 1.2

Assume that $\mathrm{char}(\Bbbk)\neq 2$. Let $C\subseteq\mathbb{P}^g$ be a rational normal curve of degree $g\geq 3$, and $L:=\mathscr{O}_{\mathbb{P}^1}(g)$. We use the notation in Section 2. From (2-10), we see that

$$K_{p,2}(S,\mathscr{O}_S(1))=\mathrm{coker}\big(K_{p,2}(\Sigma,K_\Sigma;\mathscr{O}_\Sigma(1))\xrightarrow{\rho_{p+2}}K_{p,2}(\Sigma,\mathscr{O}_\Sigma(1))\big).$$

Thus $K_{p,2}(S,\mathscr{O}_S(1))=0$ if and only if ρ_{p+2} is surjective. Recall from Theorem 2.2 that Σ has rational singularities. As $\beta^*M_{\mathscr{O}_\Sigma(1)}=M_H$, by Proposition 2.1, we find

$$K_{p,2}(\Sigma,K_\Sigma;\mathscr{O}_\Sigma(1))=H^2\big(\Sigma,\textstyle\bigwedge^{p+2}M_{\mathscr{O}_\Sigma(1)}\otimes\omega_\Sigma\big)=H^2\big(B,\bigwedge^{p+2}M_H\otimes\omega_B\big),$$
$$K_{p,2}(\Sigma,\mathscr{O}_\Sigma(1))=H^2\big(\Sigma,\textstyle\bigwedge^{p+2}M_{\mathscr{O}_\Sigma(1)}\big)=H^2\big(B,\bigwedge^{p+2}M_H\big).$$

In (2-4), we have $-\widetilde{S}-Z=K_B$, $-\widetilde{S}=K_B+Z$, $-2D=K_Z$. Then ρ_{p+2} fits into the following commutative diagram with exact sequences induced from (2-4):

$$\begin{tikzcd}
& H^1\big(\widetilde{S},\bigwedge^{p+2}M_H|_{\widetilde{S}}\big) \arrow[d, hook, "\alpha_{p+2}"'] \arrow[dr, "\gamma_{p+2}"] & \\
H^2\big(B,\bigwedge^{p+2}M_H\otimes\omega_B\big) \arrow[r, hook] \arrow[dr, "\rho_{p+2}"'] & H^2\big(B,\bigwedge^{p+2}M_H\otimes\omega_B(Z)\big) \arrow[r, "\delta_{p+2}"'] \arrow[d, two heads] & H^2\big(Z,\omega_{\mathbb{P}^1}\boxtimes\bigwedge^{p+2}M_L\otimes\omega_{\mathbb{P}^1}\big) \\
& H^2\big(B,\bigwedge^{p+2}M_H\big) &
\end{tikzcd}\tag{3-1}$$

It is easy to check that ρ_{p+2} is surjective if and only if $\gamma_{p+2}=\delta_{p+2}\circ\alpha_{p+2}$ surjects onto $\mathrm{im}(\delta_{p+2})$. We shall prove the latter for $0\leq p\leq\lfloor(g-3)/2\rfloor$ when $S=T$ is the tangent-developable surface and

$S=X(\lfloor (g-1)/2\rfloor, \lfloor g/2\rfloor)$ is a K3 carpet. To this end, we first describe $\gamma_{p+2}=\delta_{p+2}\circ\alpha_{p+2}$. Let $q:=g-p-3,\ V:=D^{p+2}U,\ W:=H^1(\bar{S},\mathscr{O}_{\bar{S}}(-p-2))$.

Lemma 3.1. *The map γ_{p+2} is the composition*

$$S^qV\otimes W\xrightarrow{\alpha_{p+2}} S^qV\otimes\textstyle\bigwedge^2 V\xrightarrow{\delta_{p+2}} S^{q+1}V\otimes V$$

such that δ_{p+2} is the Koszul differential given by $f\otimes(x^{(i)}\wedge x^{(j)})\longmapsto fx^{(i)}\otimes x^{(j)}-fx^{(j)}\otimes x^{(i)}$ and $\alpha_{p+2}=\mathrm{id}_{S^qV}\otimes\Delta_{p+2}$, where Δ_{p+2} fits into the short exact sequence[4]

$$0\longrightarrow H^1(\bar{S},\mathscr{O}_{\bar{S}}(-p-2))\xrightarrow{\Delta_{p+2}} H^2(\mathbb{P}^2,\mathscr{O}_{\mathbb{P}^2}(-p-2)(-\bar{S}))\xrightarrow{\cdot\bar{S}} H^2(\mathbb{P}^2,\mathscr{O}_{\mathbb{P}^2}(-p-2))\longrightarrow 0.$$

Proof. First, we give a description of α_{p+2}. As $\pi_*M_H=M_E$, we have a short exact sequence

$$0\longrightarrow \pi^*M_E\longrightarrow M_H\longrightarrow \mathscr{O}_B(-H)\otimes\pi^*N_L\longrightarrow 0. \tag{3-2}$$

Then we get $\pi_*\bigwedge^{p+2}M_H=\bigwedge^{p+2}M_E$ and $R^1\pi_*\bigwedge^{p+2}M_H=0$. By restricting (3-2) to $\widetilde{S}$, we also get $(\pi|_{\widetilde{S}})_*\bigwedge^{p+2}M_H|_{\widetilde{S}}=\bigwedge^{p+2}M_E|_{\bar{S}}$ and $R^1(\pi|_{\widetilde{S}})_*\bigwedge^{p+2}M_H|_{\widetilde{S}}=0$. Recall from Lemma 2.7 that $M_E=S^{g-2}U\otimes\mathscr{O}_{\mathbb{P}^2}(-1)$. Thus we find

$$\begin{aligned}
H^1\big(\widetilde{S},\textstyle\bigwedge^{p+2}M_H|_{\widetilde{S}}\big)&=H^1\big(\bar{S},\textstyle\bigwedge^{p+2}M_E|_{\bar{S}}\big)=\textstyle\bigwedge^{p+2}S^{g-2}U\otimes H^1(\bar{S},\mathscr{O}_{\bar{S}}(-p-2)),\\
H^2\big(B,\textstyle\bigwedge^{p+2}M_H\otimes\omega_B(Z)\big)&=H^2\big(\mathbb{P}^2,\textstyle\bigwedge^{p+2}M_E\otimes\mathscr{O}_{\mathbb{P}^2}(-\bar{S})\big)=\textstyle\bigwedge^{p+2}S^{g-2}U\otimes H^2(\mathbb{P}^2,\mathscr{O}_{\mathbb{P}^2}(-p-2)(-\bar{S})),\\
H^2\big(B,\textstyle\bigwedge^{p+2}M_H\big)f&=H^2\big(\mathbb{P}^2,\textstyle\bigwedge^{p+2}M_E\big)=\textstyle\bigwedge^{p+2}S^{g-2}U\otimes H^2(\mathbb{P}^2,\mathscr{O}_{\mathbb{P}^2}(-p-2)).
\end{aligned}$$

By considering the vertical short exact sequence in (3-1), we obtain $\alpha_{p+2}=\mathrm{id}_{\bigwedge^{p+2}S^{g-2}U}\otimes\Delta_{p+2}$. By Hermite reciprocity (2-1), we have $\bigwedge^{p+2}S^{g-2}U=S^qV$.

To describe δ_{p+2}, we restrict (3-2) to Z to get a short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \sigma^*M_E \arrow[r] \arrow[d, equal] & \mathscr{O}_{\mathbb{P}^1}\boxtimes M_L \arrow[r] \arrow[d, equal] & (\mathscr{O}_{\mathbb{P}^1}\boxtimes -L)\otimes\sigma^*N_L \arrow[r] \arrow[d, equal] & 0\\
& M_{\mathscr{O}_{\mathbb{P}^1}(g-1)}\boxtimes\mathscr{O}_{\mathbb{P}^1}(-1) & S^{g-1}U\otimes\mathscr{O}_{\mathbb{P}^1}\boxtimes\mathscr{O}_{\mathbb{P}^1}(-1) & \mathscr{O}_{\mathbb{P}^1}(g-1)\boxtimes\mathscr{O}_{\mathbb{P}^1}(-1) &
\end{tikzcd}$$

where the maps are the identity on $\mathscr{O}_{\mathbb{P}^1}(-1)$ and the map $S^{g-1}U\otimes\mathscr{O}_{\mathbb{P}^1}\to\mathscr{O}_{\mathbb{P}^1}(g-1)$ is the evaluation map. The induced map $H^2\big(Z,\sigma^*\bigwedge^{p+2}M_E\otimes\omega_Z\big)\to H^2\big(Z,\omega_{\mathbb{P}^1}\boxtimes\bigwedge^{p+2}M_L\otimes\omega_{\mathbb{P}^1}\big)$ can be written as $\delta'_{p+2}\otimes\mathrm{id}_V$, where

$$\delta'_{p+2}:H^1\big(\mathbb{P}^1,\textstyle\bigwedge^{p+2}M_{\mathscr{O}_{\mathbb{P}^1}(g-1)}\otimes\omega_{\mathbb{P}^1}\big)\longrightarrow\textstyle\bigwedge^{p+2}S^{g-1}U\otimes H^1(\mathbb{P}^1,\omega_{\mathbb{P}^1})$$

and $V=D^{p+2}U=H^1(\mathbb{P}^1,\omega_{\mathbb{P}^1}(-p-2))$. By considering the push-forward of (2-2) to $\mathbb{P}^1$, we can identify δ'_{p+2} with

$$H^1(\mathbb{P}^{p+2}\times\mathbb{P}^1,\mathscr{O}_{\mathbb{P}^{p+2}}(g-p-3)\boxtimes\omega_{\mathbb{P}^1}(-p-2))\xrightarrow{\cdot D_{p+2}} H^1(\mathbb{P}^{p+2}\times\mathbb{P}^1,\mathscr{O}_{\mathbb{P}^{p+2}}(g-p-2)\boxtimes\omega_{\mathbb{P}^1}).$$

[4] When $S=T$, one can easily confirm that the map γ in the Introduction coincides with the map γ_{p+2} by replacing the range by $\mathrm{im}(\delta_{p+2})=K_{p,1}(\mathbb{P}^1,\omega_{\mathbb{P}^1};\mathscr{O}_{\mathbb{P}^1}(g))$. In this case, Δ_{p+2} can be thought of as the dual of the Wahl map μ_{p+2}.

This is the map (2-3) with $n = p+2$ and $d = g-p-2 = q+1$, so $\delta'_{p+2} : S^q V \otimes V \to S^{q+1} V$ is the multiplication map, where we use Hermite reciprocity (2-1) to have that

$$H^1\big(\mathbb{P}^1, \textstyle\bigwedge^{p+2} M_{\mathscr{O}_{\mathbb{P}^1}(g-1)} \otimes \omega_{\mathbb{P}^1}\big) = \textstyle\bigwedge^{p+2} S^{g-2} U \otimes D^{p+2} U = S^q V \otimes V,$$
$$\textstyle\bigwedge^{p+2} S^{g-1} U \otimes H^1(\mathbb{P}^1, \omega_{\mathbb{P}^1}) = \textstyle\bigwedge^{p+2} S^{g-1} U = S^{q+1} V.$$

Now, consider the following commutative diagram with short exact sequences:

$$\begin{tikzcd}
0 \arrow[r] & \pi^* M_E \otimes \mathscr{O}_B(-Z) \arrow[r, "\cdot Z"] \arrow[d] & \pi^* M_E \arrow[r] \arrow[d] & \sigma^* M_E \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M_H \otimes \mathscr{O}_B(-Z) \arrow[r, "\cdot Z"'] & M_H \arrow[r] & \mathscr{O}_{\mathbb{P}^1} \boxtimes M_L \arrow[r] & 0
\end{tikzcd}$$

The top row is $(S^{g-2} U \otimes \pi^* \mathscr{O}_{\mathbb{P}^2}(-1)) \otimes$ (2-8). The diagram induces the following commutative diagram:

$$\begin{tikzcd}
H^2\big(B, \pi^* \textstyle\bigwedge^{p+2} M_E \otimes \omega_B(Z)\big) \arrow[r, hook, "\mathrm{id}_{S^q V} \otimes \iota_V"] \arrow[d, equal] & H^2\big(Z, \sigma^* \textstyle\bigwedge^{p+2} M_E \otimes \omega_Z\big) \arrow[d, "\delta'_{p+2} \otimes \mathrm{id}_V"] \\
H^2\big(B, \textstyle\bigwedge^{p+2} M_H \otimes \omega_B(Z)\big) \arrow[r, "\delta_{p+2}"'] & H^2\big(Z, \omega_{\mathbb{P}^1} \boxtimes \textstyle\bigwedge^{p+2} M_L \otimes \omega_{\mathbb{P}^1}\big)
\end{tikzcd}$$

Recalling $\omega_B(Z) = \pi^* \omega_{\mathbb{P}^2}(1)$ and $\bigwedge^{p+2} S^{g-2} U = S^q V$, we have

$$H^2\big(B, \pi^* \textstyle\bigwedge^{p+2} M_E \otimes \omega_B(Z)\big) = S^q V \otimes H^0(\mathbb{P}^2, \mathscr{O}_{\mathbb{P}^2}(p+1))^\vee,$$
$$H^2\big(Z, \sigma^* \textstyle\bigwedge^{p+2} M_E \otimes \omega_Z\big) = S^q V \otimes H^0(Z, \mathscr{O}_{\mathbb{P}^1}(p+2) \boxtimes \mathscr{O}_{\mathbb{P}^1}(p+2))^\vee.$$

By considering (2-8), we see that the upper horizontal injection in the above commutative diagram can be written as $\mathrm{id}_{S^q V} \otimes \iota_V$, where

$$\iota_V : H^2(\mathbb{P}^2, \omega_{\mathbb{P}^2}(-p-1)) \longrightarrow H^2\big(Z, (\mathscr{O}_{\mathbb{P}^1}(-p-2) \boxtimes \mathscr{O}_{\mathbb{P}^1}(-p-2)) \otimes \omega_Z\big)$$

is the dual of the canonical surjection in (2-9) with $d = p+2$. In other words, the map $\iota_V : \bigwedge^2 V \to V \otimes V$ is given by $\iota_V(x^{(i)} \wedge x^{(j)}) = x^{(i)} \otimes x^{(j)} - x^{(j)} \otimes x^{(i)}$. Hence we conclude that $\delta_{p+2} = (\delta'_{p+2} \otimes \mathrm{id}_V) \circ (\mathrm{id}_{S^q V} \otimes \iota_V) : S^q V \otimes \bigwedge^2 V \to S^{q+1} V \otimes V$ is the Koszul differential. □

From now on, we consider $\gamma_{p+2} : W \otimes S^q V \to \mathrm{im}(\delta_{p+2})$ (the target $S^{q+1} V \otimes V$ is replaced by $\mathrm{im}(\delta_{p+2})$). Our aim is to show the surjectivity of γ_{p+2} for $0 \le p \le \lfloor (g-3)/2 \rfloor$.[5] Viewing $V = H^0(\mathbb{P}^{p+2}, \mathscr{O}_{\mathbb{P}^{p+2}}(1))$ and putting $M_V := M_{\mathscr{O}_{\mathbb{P}^{p+2}}(1)}$, we have a short exact sequence

$$0 \longrightarrow \textstyle\bigwedge^2 M_V \longrightarrow \textstyle\bigwedge^2 V \otimes \mathscr{O}_{\mathbb{P}^{p+2}} \longrightarrow M_V(1) \longrightarrow 0.$$

Consider the composition

$$W \otimes \mathscr{O}_{\mathbb{P}^{p+2}} \xrightarrow{\Delta_{p+2} \otimes \mathrm{id}_{\mathscr{O}_{\mathbb{P}^{p+2}}}} \textstyle\bigwedge^2 V \otimes \mathscr{O}_{\mathbb{P}^{p+2}} \longrightarrow M_V(1). \tag{3-3}$$

[5] The Koszul complex $S^q V \otimes \bigwedge^2 V \to S^{q+1} V \otimes V \to S^{q+2} V$ is exact, so $\mathrm{im}(\delta_{p+2}) = \ker(S^{q+1} V \otimes V \to S^{q+2} V)$. Thus the surjectivity of γ_{p+2} for $0 \le p \le \lfloor (g-3)/2 \rfloor$ is equivalent to (1-2): $W_q(V, W) = 0$ for $q = g-p-3 \ge p \ge 0$.

Lemma 3.2. *Assume that* $\operatorname{char}(\Bbbk) = 0$ *or* $\operatorname{char}(\Bbbk) \geq \lfloor (g-1)/2 \rfloor$. *If the composition* (3-3) *is surjective, then* γ_{p+2} *is surjective for* $0 \leq p \leq \lfloor (g-3)/2 \rfloor$.

Proof. We can form a short exact sequence

$$0 \longrightarrow K \longrightarrow W \otimes \mathscr{O}_{\mathbb{P}^{p+2}} \xrightarrow{(3\text{-}3)} M_V(1) \longrightarrow 0, \tag{3-4}$$

where K is a vector bundle with $\operatorname{rank} K = p+1$ and $\det K = \mathscr{O}_{\mathbb{P}^{p+2}}(-p-1)$. Notice that γ_{p+2} is the $k = q$ case of the map

$$\gamma_k' : W \otimes H^0(\mathbb{P}^{p+2}, \mathscr{O}_{\mathbb{P}^{p+2}}(k)) \longrightarrow H^0(\mathbb{P}^{p+2}, M_V(k+1)).$$

As $q = g-p-3 \geq p$, it suffices to show the surjectivity of γ_k' for $k \geq p$. To this end, consider the dual of (3-4):

$$0 \longrightarrow M_V^\vee(-1) \longrightarrow W^\vee \otimes \mathscr{O}_{\mathbb{P}^{p+2}} \longrightarrow K^\vee \longrightarrow 0.$$

Since $M_V^\vee(-1)$ is 1-regular and $W^\vee \otimes \mathscr{O}_{\mathbb{P}^{p+2}}$ is 0-regular, it follows that $K^\vee$ is 0-regular. Then $(K^\vee)^{\otimes p}$ is 0-regular, and so is $\bigwedge^p K^\vee$ because $\operatorname{char}(\Bbbk) = 0$ or $\operatorname{char}(\Bbbk) \geq \lfloor (g-1)/2 \rfloor \geq p+1$. Thus $K = \bigwedge^p K^\vee \otimes \det K$ is $(p+1)$-regular, and hence, γ_k' is surjective for $k \geq p$. □

It only remains to prove that the composition (3-3) is surjective. The second map in (3-3) is just the globalization of the map

$$\textstyle\bigwedge^2 V \longrightarrow V_h, \quad x^{(i)} \wedge x^{(j)} \longmapsto a_j x^{(i)} - a_i x^{(j)},$$

where V_h is the kernel of a nonzero linear functional $h := \sum_{i=0}^{p+2} a_i y^i \in V^\vee = S^{p+2} U^\vee$. We now regard $h = \sum_{i=0}^{p+2} b_i x^i \in S^{p+2} U$, where $b_i = (-1)^i a_{p+2-i}$. The surjectivity of (3-3) is equivalent to the injectivity of the composition of the dual maps

$$V_h^\vee \longrightarrow \textstyle\bigwedge^2 V^\vee \xrightarrow{\Delta_{p+2}^\vee} W^\vee. \tag{3-5}$$

The image of $V_h^\vee$ in $\bigwedge^2 V^\vee$ is spanned by $v_j := x^j \wedge h$ for $j = 0, \dots, d-1, d+1, \dots, p+2$, where $d := \deg h$. Recall that $\Delta_{p+2}^\vee$ is the restriction map $H^0(\mathbb{P}^2, \mathscr{O}_{\mathbb{P}^2}(p+1)) \to H^0(\bar{S}, \mathscr{O}_{\bar{S}}(p+1))$.

Proof of Theorem 1.1. We consider the case $\bar{S} = Q$. In this case, $\Delta_{p+2}^\vee = \mu_{p+2}$ (see (2-12)). We have $\Delta_{p+2}^\vee(v_j) = \sum_{i=0}^d (j-i) b_i x^{i+j-1}$. As $\operatorname{char}(\Bbbk) = 0$ or $\operatorname{char}(\Bbbk) \geq (g+2)/2 \geq p+3$, we get $\deg(\Delta_{p+2}^\vee(v_j)) = d+j-1$. This implies that

$$\Delta_{p+2}^\vee(v_0), \dots, \Delta_{p+2}^\vee(v_{d-1}), \Delta_{p+2}^\vee(v_{d+1}), \dots, \Delta_{p+2}^\vee(v_{p+2}) \text{ are linearly independent.}$$

Thus the composition (3-5) is injective. □

Proof of Theorem 1.2. We consider the case $\bar{S} = 2\ell$. In this case, $\Delta_{p+2}^\vee$ factors through τ_{p+2} (see (2-14)). Write $\tau_{p+2}(v_j) = (u_j, w_j)$. By Proposition 2.8 (2), we only need to deal with the case $p \geq 1$. As $\operatorname{char}(\Bbbk) = 0$ or $\operatorname{char}(\Bbbk) \geq \lfloor (g-1)/2 \rfloor \geq (p+3)/2$, we have

$$\begin{aligned} &\deg u_j = d+j-1 \quad \text{and} \quad \deg w_j \leq d+j-1 \quad \text{when } d \equiv j \pmod 2, \\ &\deg u_j \leq d+j-2 \quad \text{and} \quad \deg w_j = d+j \qquad \text{when } d \not\equiv j \pmod 2. \end{aligned}$$

This implies

$$\tau_{p+2}(v_0), \dots, \tau_{p+2}(v_{d-1}), \tau_{p+2}(v_{d+1}), \dots, \tau_{p+2}(v_{p+2}) \text{ are linearly independent.}$$

Thus the composition (3-5) is injective. □

Remark 3.3. The characteristic assumption in Theorem 1.1 is used to prove the injectivity of (3-5). If $k := \mathrm{char}(\Bbbk) \le p+2$, then (3-5) is not injective for $h = 1$. Indeed, $x^k \wedge 1 \neq 0$ in $\bigwedge^2 V^\vee$ is sent to 0 in $W^\vee$. The characteristic assumption in Theorem 1.2 is used in Lemma 3.2.

Remark 3.4. By the duality theorem, $K_{p,q}(S, \mathscr{O}_S(1)) = K_{g-p-2,3-q}(S, \mathscr{O}_S(1))^\vee$. In the situation of Theorem 1.1 or Theorem 1.2, we have

$$K_{p,1}(S, \mathscr{O}_S(1)) = 0 \quad \text{for } p \ge \lfloor g/2 \rfloor.$$

As $K_{p+1,1}(S, \mathscr{O}_S(1)) = \ker(\rho_{p+2}) = \ker(\gamma_{p+2})$ and γ_{p+2} is surjective for $0 \le p \le \lfloor (g-3)/2 \rfloor$, we can compute $\kappa_{p,1}(S, \mathscr{O}_S(1))$ for $0 \le p \le \lfloor (g-1)/2 \rfloor$. Note that $K_{p,0}(S, \mathscr{O}_S(1)) \neq 0$ if and only if $p = 0$. In this case, $\kappa_{0,0}(S, \mathscr{O}_S(1)) = 1$. Thus we can completely determine all graded Betti numbers $\kappa_{p,q}(S, \mathscr{O}_S(1))$.

4. Proof of Theorem 1.3

Assume that $\mathrm{char}(\Bbbk) = 0$. Let $C \subseteq \mathbb{P}^r$ be a smooth projective curve of genus $g \ge 1$ embedded by $|L|$, where L is a line bundle on C with $\deg L \ge 2g+3$. We use the notation in Section 2. Recall from Theorem 2.2 that $\Sigma \subseteq \mathbb{P}^r$ is arithmetically Cohen–Macaulay and $H^3(\Sigma, \mathscr{O}_\Sigma(m)) = 0$ for $m > 0$. By considering (2-5) and Lemma 2.4, we see that

$$\begin{aligned} H^i(T, \mathscr{O}_T(m)) &= H^{i+1}(B, \mathscr{O}_B(mH - \widetilde{T} - Z)) \quad \text{for } i \ge 1,\ m \ge 1, \\ T \subseteq \mathbb{P}^r \text{ is } m\text{-normal} \quad &\iff \quad H^1(B, \mathscr{O}_B(mH - \widetilde{T} - Z)) = 0. \end{aligned} \tag{4-1}$$

Note that $mH - \widetilde{T} - Z = (m-2)H + \pi^* T_L(-4\delta)$. Thus $R^1\pi_*\mathscr{O}_B(mH - \widetilde{T} - Z) = 0$ for $m \ge 1$. When $m = 1$, we have $H^j(B, \mathscr{O}_B(H - \widetilde{T} - Z)) = 0$ for $j > 0$ since $\pi_*\mathscr{O}_B(H - \widetilde{T} - Z) = 0$. When $m = 2$, we have $H^j(B, \mathscr{O}_B(2H - \widetilde{T} - Z)) = H^j(C_2, T_L(-4\delta))$ for $j > 0$. Recall that $\sigma_*\mathscr{O}_Z = \mathscr{O}_{C_2} \oplus \mathscr{O}_{C_2}(-\delta)$. Then we have $\sigma_*(L \boxtimes L)(-kD) = T_L(-(k+1)\delta) \oplus T_L(-k\delta)$.

Lemma 4.1. *$H^i(T, \mathscr{O}_T(m)) = 0$ for $i > 0$, $m > 0$, and $h^1(T, \mathscr{O}_T) = 2g$, $h^2(T, \mathscr{O}_T) = 1$. In particular,* $\operatorname{reg} \mathscr{O}_T = 3$.

Proof. By (2-6) and Proposition 2.5, $h^1(T, \mathscr{O}_T) = 2g$ and $h^2(T, \mathscr{O}_T) = 1$. It suffices to prove that $H^i(T, \mathscr{O}_T(m)) = 0$ for $i = 1$, $m = 1, 2$ and $i = 2$, $m = 1$. Indeed, this implies $\operatorname{reg} \mathscr{O}_T = 3$. By (4-1), we need to check that $H^j(B, \mathscr{O}_B(mH - \widetilde{T} - Z)) = 0$ for $j = 2$, $m = 1, 2$ and $j = 3$, $m = 1$. As the required vanishing is trivial when $m = 1$, it is enough to show that $H^2(C^2, (L \boxtimes L)(-3D)) = 0$. Observe that $R^1 p_*(L \boxtimes L)(-3D) = 0$, where $p : C \times C \to C$ is a projection map. Then

$$H^2(C^2, (L \boxtimes L)(-3D)) = H^2(C, p_*(L \boxtimes L)(-3D)) = 0.$$ □

As $T \subseteq \mathbb{P}^r$ is linearly normal and $h^1(T, \mathscr{O}_T) = 2g$, a general hyperplane section of the tangent-developable surface $T \subseteq \mathbb{P}^r$ is obtained from an isomorphic projection of an $(r+g)$-cuspidal curve of geometric genus g canonically embedded in $\mathbb{P}^{r+2g-1}$.

Lemma 4.2. *Suppose* $\deg L \geq 3g+2$. *Then* 2*-normality of* $T \subseteq \mathbb{P}^r$ *is equivalent to*

$$H^1(C \times C, (L \boxtimes L)(-3D)) = 0.$$

Proof. By (4-1), 2-normality of $T \subseteq \mathbb{P}^r$ is equivalent to $H^1(C_2, T_L(-4\delta)) = 0$. By [Bertram et al. 1991, Theorem 1(i)], $H^1(C^2, (L \boxtimes L)(-2D)) = 0$. It follows that $H^1(C_2, T_L(-3\delta)) = 0$. Then $H^1(C_2, T_L(-4\delta)) = 0$ if and only if $H^1(C^2, (L \boxtimes L)(-3D)) = 0$. □

Proposition 4.3. $K_{p,3}(T, \mathscr{O}_T(1)) = 0$ *for* $0 \leq p \leq r-3$, *and* $\kappa_{r-2,3}(T, \mathscr{O}_T(1)) = 1$.

Proof. By Proposition 2.1 and Lemma 4.1, $K_{p,3}(T, \mathscr{O}_T(1)) = H^2\big(T, \bigwedge^{p+2} M_{\mathscr{O}_T(1)} \otimes \mathscr{O}_T(1)\big)$. Note that $\omega_T = \mathscr{O}_T$ (Proposition 2.5) and $\bigwedge^{p+2} M^\vee_{\mathscr{O}_T(1)} = \bigwedge^{r-p-2} M_{\mathscr{O}_T(1)} \otimes \mathscr{O}_T(1)$. By Serre duality, we have

$$H^2\big(T, \textstyle\bigwedge^{p+2} M_{\mathscr{O}_T(1)} \otimes \mathscr{O}_T(1)\big) = H^0\big(T, \textstyle\bigwedge^{p+2} M^\vee_{\mathscr{O}_T(1)} \otimes \mathscr{O}_T(-1)\big)^\vee = H^0\big(T, \textstyle\bigwedge^{r-p-2} M_{\mathscr{O}_T(1)}\big)^\vee.$$

Then the proposition immediately follows. □

Proof of Theorem 1.3. By Lemma 4.1, it suffices to show that $T \subseteq \mathbb{P}^r$ is m-normal for $m = 1, 2, 3$. Indeed, this together with $\operatorname{reg} \mathscr{O}_T = 3$ implies $\operatorname{reg} \mathscr{I}_{T|\mathbb{P}^r} = 4$, and thus, $T \subseteq \mathbb{P}^r$ is m-normal for $m \geq 1$. In view of (4-1), $T \subseteq \mathbb{P}^r$ is trivially 1-normal. For the 2-normality, we assume that $\deg L \geq 4g+3$. Then [Bertram et al. 1991, Theorem 1.7(i)] says that $H^1(C \times C, (L \boxtimes L)(-3D)) = 0$, so the 2-normality of $T \subseteq \mathbb{P}^r$ follows from Lemma 4.2. Now, 3-normality of $T \subseteq \mathbb{P}^r$ is equivalent to $K_{0,3}(T, \mathscr{O}_T(1)) = 0$, but this is a special case of Proposition 4.3. □

Remark 4.4. In Theorem 1.3, the degree condition $\deg L \geq 4g+3$ is only used to show that $T \subseteq \mathbb{P}^r$ is 2-normal. If $\deg L = 4g+2$, then by Lemma 4.2 and [Bertram et al. 1991, Theorem 1.7(ii), (iii)], $T \subseteq \mathbb{P}^r$ is 2-normal (and arithmetically normal) if and only if $g \geq 3$ and C is nonhyperelliptic. More generally, using the results in [Bertram et al. 1991, Section 1] and [Pareschi 1995, Theorem 3.8(b)], one can prove that if $\deg L \geq 4g+3-\operatorname{Cliff}(C)$, then $T \subseteq \mathbb{P}^r$ is arithmetically normal.

Corollary 4.5. *Suppose that* $\deg L \geq 4g+3$. *Then the Hilbert function of* $T \subseteq \mathbb{P}^r$ *is given by* $H_T(t) = (\deg L + g - 1)t^2 + 2 - 2g$ *for* $t \geq 1$. *In particular*, $\kappa_{1,1}(T, \mathscr{O}_T(1)) = (r-2)(r-3)/2 - 6g$.

Proof. By Theorem 1.3, $H_T(t)$ coincides with the Hilbert polynomial $P_T(t)$ for $t \geq 1$. We know that $\deg P_T(t) = 2$ and the leading coefficient of $P_T(t)$ is $(\deg T)/2 = \deg L + g - 1$. As $P_T(0) = \chi(\mathscr{O}_T) = 2-2g$ and $P_T(1) = h^0(C, L) = \deg L - g + 1$, we easily get the assertion. The last assertion follows from $\kappa_{1,1}(T, \mathscr{O}_T(1)) = h^0(\mathbb{P}^r, \mathscr{I}_{T|\mathbb{P}^r}(2)) = \binom{r+2}{2} - H_T(2)$. □

Assume that $\deg L \geq 4g+3$. Notice that (see Proposition 4.3)

$$K_{p,0}(T, \mathscr{O}_T(1)) \neq 0 \iff p = 0 \quad (\kappa_{0,0}(T, \mathscr{O}_T(1)) = 1),$$
$$K_{p,3}(T, \mathscr{O}_T(1)) \neq 0 \iff p = r-2 \quad (\kappa_{r-2,3}(T, \mathscr{O}_T(1)) = 1).$$

It would be exceedingly interesting to study vanishing/nonvanishing behaviors of $K_{p,1}(T,\mathscr{O}_T(1))$ and $K_{p,2}(T,\mathscr{O}_T(1))$ as the positivity of L grows. For a possible generalization of Theorem 1.1 (see also Remark 3.4), one may hope the following.

Conjecture 4.6. $K_{p,1}(T,\mathscr{O}_T(1))=0$ *for* $p\geq\lfloor(\deg L-3g)/2\rfloor$.

We have $\kappa_{p,1}(T,\mathscr{O}_T(1))\leq\kappa_{p,1}(C,L)$. Thus $K_{p,1}(T,\mathscr{O}_T(1))=0$ at least for $p\geq r-1$ (or for $p\geq r-\operatorname{gon}(C)+1$ by [Rathmann 2016, Theorem 1.1]). We find

$$\kappa_{r-2,2}(T,\mathscr{O}_T(1))=2g(r+1),\quad \kappa_{r-1,2}(T,\mathscr{O}_T(1))=2g.$$

If Conjecture 4.6 holds, then we can compute $\kappa_{p,2}(T,\mathscr{O}_T(1))$ for $\lfloor(\deg L-3g-2)/2\rfloor\leq p\leq r-1$.

Concerning vanishing of $K_{p,2}(T,\mathscr{O}_T(1))$, in view of Theorems 1.1 and 1.3, one may ask whether

$$K_{p,2}(T,\mathscr{O}_T(1))=0\quad\text{for } 0\leq p\leq\lfloor(\deg L-4g-3)/2\rfloor. \tag{4-2}$$

Suppose that $g=1$. Observe that T has the same Hilbert polynomial with an abelian surface of degree $2\deg L$ and T is a degeneration of an abelian surface with polarization $(1,\deg L)$ (see [Gross and Popescu 1998, Theorem 3.1]). Notice that (4-2) is similar to Gross and Popescu's conjecture [1998, conjecture on p. 375]. However, Example 4.8(1) shows that (4-2) is not true even for $g=1$ and $p=1$. The correct expectation might be the following.

Conjecture 4.7. *Suppose that* $g=1$. *Then* $K_{p,2}(T,\mathscr{O}_T(1))=0$ *for* $0\leq p\leq\lfloor(\deg L-7)/3\rfloor$.

This conjecture would imply that a general $(1,d)$-polarized abelian surface satisfies the property N_p for $0\leq p\leq\lfloor(d-7)/3\rfloor$.

In general, it is tempting to guess that

$$K_{p,2}(T,\mathscr{O}_T(1))=0\quad\text{for } 0\leq p\leq\lfloor(\deg L-4g-3)/(g+2)\rfloor, \tag{4-3}$$

but it is hard to make a precise prediction at this moment.

Example 4.8. Let $q_1,\dots,q_m$ be minimal generators of the ideal $I_{C|\mathbb{P}^r}\subseteq\boldsymbol{k}[x_0,\dots,x_r]$. Then $\widetilde{T}$ is defined by q_i and $\sum_{j=0}^r(\partial q_i/\partial x_j)y_j$ for $1\leq i\leq m$ in $\mathbb{P}^r\times\mathbb{P}^r$, and $T=q(\widetilde{T})\subseteq\mathbb{P}^r$, where $q:\mathbb{P}^r\times\mathbb{P}^r\to\mathbb{P}^r$ is the second projection. Using Macaulay2, we can compute the Betti table of T in $\mathbb{P}^r$ whenever r is reasonably not so big.

(1) Let $C:=Z(z_0^3-z_0z_2^2-z_1^2z_2)\subseteq\mathbb{P}^2$ be an elliptic curve. There is a point $x\in C$ such that $\mathscr{O}_C(1)=\mathscr{O}_C(3x)$. Consider the embedding $C\subseteq\mathbb{P}^{d-1}$ given by $|\mathscr{O}_C(dx)|$ for $d\geq 3$. The computation of the Betti table of the tangent-developable surface T of C in $\mathbb{P}^{d-1}$ confirms Conjectures 4.6 and 4.7 when $7\leq d\leq 16$. For these cases, the predictions are sharp. The Betti tables of T in $\mathbb{P}^{d-1}$ for $d=9,10$ are as follows:

	0	1	2	3	4	5	6	7
0	1	-	-	-	-	-	-	-
1	-	9	3	-	-	-	-	-
2	-	6	81	171	165	81	18	2
3	-	-	-	-	-	-	1	-

	0	1	2	3	4	5	6	7	8
0	1	-	-	-	-	-	-	-	-
1	-	15	20	-	-	-	-	-	-
2	-	-	70	252	350	260	105	20	2
3	-	-	-	-	-	-	-	1	-

(2) Let $C \subseteq \mathbb{P}^1 \times \mathbb{P}^1$ be a smooth projective curve of genus 2 defined by

$$x^2 \otimes (x^3+1) + 1 \otimes (x^2 - x) \in S^2U \otimes S^3U = H^0(\mathbb{P}^1 \times \mathbb{P}^1, \mathscr{O}_{\mathbb{P}^1}(2) \boxtimes \mathscr{O}_{\mathbb{P}^1}(3)).$$

Consider the embedding $C \subseteq \mathbb{P}^{11}$ given by $|(\mathscr{O}_{\mathbb{P}^1}(3) \boxtimes \mathscr{O}_{\mathbb{P}^1}(2))|_C|$. Note that $\deg C = 13$. The Betti table of the tangent-developable surface T of C in $\mathbb{P}^{11}$ is the following:

	0	1	2	3	4	5	6	7	8	9	10
0	1	-	-	-	-	-	-	-	-	-	-
1	-	24	48	-	-	-	-	-	-	-	-
2	-	-	153	864	1848	2304	1827	928	288	48	4
3	-	-	-	-	-	-	-	-	-	1	-

We can confirm Conjecture 4.6 and (4-2) for this case, and we see that the expectation (4-3) is not sharp when $g \geq 2$.

Acknowledgements

This paper grew out of attempts to understand the algebraic arguments of [Aprodu et al. 2019; Raicu and Sam 2022] in a geometric way, so the present author wishes to express his deep gratitude to the authors of those papers, particularly to Claudiu Raicu for valuable comments. The author is grateful to Lawrence Ein, Sijong Kwak, Robert Lazarsfeld, and Wenbo Niu, he is indebted to Daniele Agostini for introducing [Gross and Popescu 1998], and he benefited from interesting discussions about Macaulay2 computations in Example 4.8 with Kiryong Chung and Jong In Han.

References

[Aprodu and Nagel 2010] M. Aprodu and J. Nagel, *Koszul cohomology and algebraic geometry*, Univ. Lect. Ser. **52**, Amer. Math. Soc., Providence, RI, 2010. MR Zbl

[Aprodu et al. 2019] M. Aprodu, G. Farkas, Ş. Papadima, C. Raicu, and J. Weyman, "Koszul modules and Green's conjecture", *Invent. Math.* **218**:3 (2019), 657–720. MR Zbl

[Aprodu et al. 2022] M. Aprodu, G. Farkas, Ş. Papadima, C. Raicu, and J. Weyman, "Topological invariants of groups and Koszul modules", *Duke Math. J.* **171**:10 (2022), 2013–2046. MR Zbl

[Bayer and Eisenbud 1995] D. Bayer and D. Eisenbud, "Ribbons and their canonical embeddings", *Trans. Amer. Math. Soc.* **347**:3 (1995), 719–756. MR Zbl

[Bertram et al. 1991] A. Bertram, L. Ein, and R. Lazarsfeld, "Surjectivity of Gaussian maps for line bundles of large degree on curves", pp. 15–25 in *Algebraic geometry* (Chicago, IL, 1989), edited by S. Bloch et al., Lecture Notes in Math. **1479**, Springer, 1991. MR Zbl

[Ein and Lazarsfeld 2020] L. Ein and R. Lazarsfeld, "Tangent developable surfaces and the equations defining algebraic curves", *Bull. Amer. Math. Soc.* (*N.S.*) **57**:1 (2020), 23–38. MR Zbl

[Ein et al. 2020] L. Ein, W. Niu, and J. Park, "Singularities and syzygies of secant varieties of nonsingular projective curves", *Invent. Math.* **222**:2 (2020), 615–665. MR Zbl

[Ein et al. 2021] L. Ein, W. Niu, and J. Park, "On blowup of secant varieties of curves", *Electron. Res. Arch.* **29**:6 (2021), 3649–3654. MR Zbl

[Eisenbud 1992] D. Eisenbud, "Green's conjecture: an orientation for algebraists", pp. 51–78 in *Free resolutions in commutative algebra and algebraic geometry* (Sundance, UT, 1990), edited by D. Eisenbud and C. Huneke, Res. Notes Math. **2**, Jones & Bartlett, Boston, MA, 1992. MR Zbl

[Eisenbud and Schreyer 2019] D. Eisenbud and F.-O. Schreyer, "Equations and syzygies of K3 carpets and unions of scrolls", *Acta Math. Vietnam.* **44**:1 (2019), 3–29. MR Zbl

[Gallego and Purnaprajna 1997] F. J. Gallego and B. P. Purnaprajna, "Degenerations of K3 surfaces in projective space", *Trans. Amer. Math. Soc.* **349**:6 (1997), 2477–2492. MR Zbl

[Green 1984] M. L. Green, "Koszul cohomology and the geometry of projective varieties", *J. Differential Geom.* **19**:1 (1984), 125–171. MR

[Gross and Popescu 1998] M. Gross and S. Popescu, "Equations of $(1, d)$-polarized abelian surfaces", *Math. Ann.* **310**:2 (1998), 333–377. MR Zbl

[Hulek 1986] K. Hulek, *Projective geometry of elliptic curves*, Astérisque **137**, Soc. Math. France, Paris, 1986. MR Zbl

[Kaji 1986] H. Kaji, "On the tangentially degenerate curves", *J. Lond. Math. Soc.* (2) **33**:3 (1986), 430–440. MR Zbl

[Kemeny 2021] M. Kemeny, "Universal secant bundles and syzygies of canonical curves", *Invent. Math.* **223**:3 (2021), 995–1026. MR Zbl

[Kovács et al. 2010] S. J. Kovács, K. Schwede, and K. E. Smith, "The canonical sheaf of Du Bois singularities", *Adv. Math.* **224**:4 (2010), 1618–1640. MR Zbl

[Lazarsfeld 2004] R. Lazarsfeld, *Positivity in algebraic geometry, I: Classical setting: line bundles and linear series*, Ergebnisse der Math. (3) **48**, Springer, 2004. MR Zbl

[Pareschi 1995] G. Pareschi, "Gaussian maps and multiplication maps on certain projective varieties", *Compos. Math.* **98**:3 (1995), 219–268. MR Zbl

[Park 2022] J. Park, "Asymptotic vanishing of syzygies of algebraic varieties", *Commun. Am. Math. Soc.* **2** (2022), 133–148. MR Zbl

[Raicu 2021] C. Raicu, "Koszul modules", pp. 33–57 in *Recent developments in commutative algebra* (Trento, Italy, 2019), edited by A. Conca et al., Lecture Notes in Math. **2283**, Springer, 2021. MR Zbl

[Raicu and Sam 2021] C. Raicu and S. V Sam, "Hermite reciprocity and Schwarzenberger bundles", pp. 689–721 in *Commutative algebra*, edited by I. Peeva, Springer, 2021. MR Zbl

[Raicu and Sam 2022] C. Raicu and S. V Sam, "Bi-graded Koszul modules, K3 carpets, and Green's conjecture", *Compos. Math.* **158**:1 (2022), 33–56. MR Zbl

[Rathmann 2016] J. Rathmann, "An effective bound for the gonality conjecture", preprint, 2016. arXiv 1604.06072

[Schreyer 1983] F. O. Schreyer, *Syzygies of curves with special pencils*, Ph.D. thesis, Brandeis University, 1983, available at https://www.proquest.com/docview/303128625.

[Schreyer 1986] F.-O. Schreyer, "Syzygies of canonical curves and special linear series", *Math. Ann.* **275**:1 (1986), 105–137. MR Zbl

[Voisin 2002] C. Voisin, "Green's generic syzygy conjecture for curves of even genus lying on a K3 surface", *J. Eur. Math. Soc.* **4**:4 (2002), 363–404. MR Zbl

[Voisin 2005] C. Voisin, "Green's canonical syzygy conjecture for generic curves of odd genus", *Compos. Math.* **141**:5 (2005), 1163–1190. MR Zbl

[Wahl 1990] J. Wahl, "Gaussian maps on algebraic curves", *J. Differential Geom.* **32**:1 (1990), 77–98. MR Zbl

Communicated by Gavril Farkas
Received 2024-04-28 Accepted 2024-07-16

parkjh13@kaist.ac.kr Department of Mathematical Sciences, KAIST, Daejeon, South Korea

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

Originality. Submission of a manuscript acknowledges that the manuscript is original and and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles in *ANT* are usually in English, but articles written in other languages are welcome.

Length There is no a priori limit on the length of an *ANT* article, but *ANT* considers long articles only if the significance-to-length ratio is appropriate. Very long manuscripts might be more suitable elsewhere as a memoir instead of a journal article.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

Format. Authors are encouraged to use LaTeX but submissions in other varieties of TeX, and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of BibTeX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@msp.org with details about how your graphics were generated.

White space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Algebra & Number Theory

Volume 19 No. 5 2025