Algebra & Number Theory

Volume 17
2023
No. 9

msp

Algebra & Number Theory

msp.org/ant

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

The subscription price for 2023 is US $485/year for the electronic version, and $705/year (+$65, 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/

msp

ALGEBRA AND NUMBER THEORY 17:9 (2023)
https://doi.org/10.2140/ant.2023.17.1533

Unipotent ℓ-blocks for simply connected p-adic groups

Thomas Lanard

Let F be a nonarchimedean local field and G the F-points of a connected simply connected reductive group over F. We study the unipotent ℓ-blocks of G, for $\ell \neq p$. To that end, we introduce the notion of $(d, 1)$-series for finite reductive groups. These series form a partition of the irreducible representations and are defined using Harish-Chandra theory and d-Harish-Chandra theory. The ℓ-blocks are then constructed using these $(d, 1)$-series, with d the order of q modulo ℓ, and consistent systems of idempotents on the Bruhat–Tits building of G. We also describe the stable ℓ-block decomposition of the depth zero category of an unramified classical group.

Introduction

Let F be a nonarchimedean local field and k its residue field. Let q be the cardinal of k and p its characteristic. Let $\boldsymbol{G}$ be a connected reductive group over F and denote by $G := \boldsymbol{G}(F)$ the F-points of $\boldsymbol{G}$.

Let $\mathrm{Rep}_{\mathbb{C}}(G)$ be the category of smooth representations of G with complex coefficients. One way to study this category is to decompose it in a minimal product of subcategories, called blocks, and describe them. Bernstein [2] solved this problem by describing the blocks with inertial classes of cuspidal support.

Congruences between automorphic forms were used to solve remarkable problems of arithmetic-geometry. Hence, it becomes natural to study the smooth representations of p-adic groups with coefficients in $\bar{\mathbb{Z}}_\ell$, for ℓ a prime number different from p. In the same way, we would like to have a decomposition of their category $\mathrm{Rep}_{\bar{\mathbb{Z}}_\ell}(G)$ into ℓ-blocks. However, we do not have a result like the Bernstein decomposition, for the ℓ-blocks. A decomposition of $\mathrm{Rep}_{\bar{\mathbb{F}}_\ell}(\mathrm{GL}_n(F))$ into blocks was proved by Vignéras [28] (see also

MSC2020: primary 22E50; secondary 20C20, 20C33, 20G05, 20G25, 20G40.

Keywords: l-blocks, modular representations of p-adic groups, unipotent representations, Deligne–Lusztig, d-Harish-Chandra theory, stable l-blocks.

the work of Sécherre and Stevens [27] for inner forms of $\mathrm{GL}_n(F)$). After that, Helm [14] reached a decomposition into ℓ-blocks of $\mathrm{Rep}_{\overline{\mathbb{Z}}_\ell}(\mathrm{GL}_n(F))$. He describes these ℓ-blocks with the notion of mod ℓ inertial supercuspidal support. Apart from GL_n and its inner forms, we don't know much about the ℓ-blocks.

The decomposition of Bernstein and Vignéras–Helm both use the "unicity of the supercuspidal support", which is true for GL_n and in the complex case, but not in general. Therefore, a new strategy to study the ℓ-blocks is needed. A new method, using consistent systems of idempotents on the Bruhat–Tits building, was used in [9] to construct in depth zero the ℓ-blocks for GL_n. Then, this was used in [18] and [19] to obtain decompositions of the depth zero category over $\overline{\mathbb{Z}}_\ell$, for a group which is split over an unramified extension of F. These decompositions are constructed using Deligne–Lusztig theory. They present a lot of interesting properties and links with the local Langlands correspondence, but they are not blocks in general, just unions of blocks.

In this paper, we deal with two problems, the study of the unipotent ℓ-blocks and the stable ℓ-blocks for unramified classical groups.

Let us start by the unipotent ℓ-blocks. Let $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Q}}_\ell}(G)$ be the subcategory of unipotent representations. Using [19] (with the system of conjugacy classes composed of the trivial representation for every polysimplex), we also get a ℓ-unipotent category over $\overline{\mathbb{Z}}_\ell$: $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(G)$. The unipotent ℓ-blocks are the ℓ-blocks of $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(G)$.

In [19], the idempotents are constructed using Deligne–Lusztig theory. A first difficulty for an ℓ-block decomposition is that Deligne–Lusztig theory does not produce primitives idempotents. Moreover, replacing naively Deligne–Lusztig idempotents by primitive central ones won't produce consistent systems of idempotents for the p-adic group. This is why we introduce for G, a finite reductive group over k, the notion of a $(d, 1)$-series. A $(d, 1)$-series will be a minimal set of irreducible characters with the property that it is a union of Harish-Chandra series (in order to get p-adic blocks) and that the idempotent associated has integer coefficients (to get a decomposition over $\overline{\mathbb{Z}}_\ell$).

Let $(\mathbf{G}, \mathsf{F})$ be a connected reductive group over k. The ℓ-blocks of $\mathbf{G}^{\mathsf{F}}$ are then described using d-cuspidal pairs; see [4] and [6]. For an integer d, a d-split Levi subgroup is the centralizer of a F stable torus $\mathbf{G}$, such that the cardinal of $\mathbf{T}^{\mathsf{F}}$ is a power of $\Phi_d(q)$, where Φ_d is the d-th cyclotomic polynomial. The usual Harish-Chandra induction and restriction is then replaced by the Deligne–Lusztig induction and restriction from these d-split Levi subgroups. An irreducible character χ is said to be d-cuspidal if and only if ${}^*\mathcal{R}^{\mathbf{G}}_{\mathbf{L}\subseteq\mathbf{P}}\chi = 0$ for every proper d-split Levi subgroup $\mathbf{L}$ and every parabolic $\mathbf{P}$ admitting $\mathbf{L}$ as Levi subgroup. Let d be the order of q modulo ℓ. Then we get a bijection (with some restrictions on ℓ) between conjugacy classes of pairs $(\mathbf{M}, \chi)$, consisting of a d-split Levi $\mathbf{M}$ and a d-cuspidal character of $\mathbf{M}^{\mathsf{F}}$, and ℓ-blocks of $\mathbf{G}^{\mathsf{F}}$.

We define a $(d, 1)$-set to be a subset of $\mathrm{Irr}(\mathbf{G}^{\mathsf{F}})$ which is both a union of Harish-Chandra series and of d-series (that is a set of characters having the same d-cuspidal support). A $(d, 1)$-series is then a $(d, 1)$-set with no proper nonempty $(d, 1)$-subset. In Theorem 3.6.1, we completely compute the unipotent $(d, 1)$-series of $\mathbf{G}^{\mathsf{F}}$.

Let BT be the semisimple Bruhat–Tits building associated to G. For $\sigma \in \mathrm{BT}$, we denote by $\bar{\mathsf{G}}_\sigma$ the reductive quotient of G at σ, which is a connected reductive group over k. Let $\mathcal{T}(G)$ be the set of G-conjugacy classes of pairs (σ, π), where $\sigma \in \mathrm{BT}$ and π is an irreducible cuspidal representation of $\bar{\mathsf{G}}_\sigma$. The work of Morris [26] shows that to an element $\mathfrak{t} \in \mathcal{T}(G)$ we can associate $\mathrm{Rep}^{\mathfrak{t}}_{\overline{\mathbb{Q}}_\ell}(G)$, a union of blocks of depth zero. We define an equivalence relation $\sim$ on $\mathcal{T}(G)$ (see Section 2.2 for more details) such that $\mathrm{Rep}^{\mathfrak{t}}_{\overline{\mathbb{Q}}_\ell}(G) = \mathrm{Rep}^{\mathfrak{t}'}_{\overline{\mathbb{Q}}_\ell}(G)$ if and only if $\mathfrak{t} \sim \mathfrak{t}'$. Denote by $[\mathfrak{t}]$ the equivalence class of $\mathfrak{t}$. Hence, we get a decomposition of the depth zero category

$$\mathrm{Rep}^0_{\overline{\mathbb{Q}}_\ell}(G) = \prod_{[\mathfrak{t}] \in \mathcal{T}(G)/\sim} \mathrm{Rep}^{[\mathfrak{t}]}_{\overline{\mathbb{Q}}_\ell}(G).$$

Moreover, when G is semisimple and simply connected, the categories $\mathrm{Rep}^{[\mathfrak{t}]}_{\overline{\mathbb{Q}}_\ell}(G)$ are blocks.

We also denote by $\mathcal{T}^{\mathrm{un}}(G)$ the subset of $\mathcal{T}(G)$ of pairs (σ, π) with π unipotent, and $\mathcal{T}^{\mathrm{un}}_\ell(G)$ the subset of $\mathcal{T}(G)$ of pairs (σ, π) with π in a Deligne–Lusztig series associated with a semisimple conjugacy class in $\bar{\mathsf{G}}^*_\sigma$ of order a power of ℓ. The equivalence relation $\sim$ is trivial on $\mathcal{T}^{\mathrm{un}}(G)$ (see Remark 4.1.1). We have $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Q}}_\ell}(G) = \prod_{\mathfrak{t} \in \mathcal{T}^{\mathrm{un}}(G)} \mathrm{Rep}^{[\mathfrak{t}]}_{\overline{\mathbb{Q}}_\ell}(G)$ and $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(G) \cap \mathrm{Rep}_{\overline{\mathbb{Q}}_\ell}(G) = \prod_{[\mathfrak{t}] \in \mathcal{T}^{\mathrm{un}}_\ell(G)/\sim} \mathrm{Rep}^{[\mathfrak{t}]}_{\overline{\mathbb{Q}}_\ell}(G)$ (see the remark below for the definition of the intersection).

Remark 0.0.1. Let B be a direct factor subcategory of $\mathrm{Rep}_{\overline{\mathbb{Z}}_\ell}(G)$ and $e \in \mathcal{Z}_{\overline{\mathbb{Z}}_\ell}(G)$ be the corresponding idempotent in the center of $\mathrm{Rep}_{\overline{\mathbb{Z}}_\ell}(G)$. We then denote by $B \cap \mathrm{Rep}_{\overline{\mathbb{Q}}_\ell}(G)$ the direct factor of $\mathrm{Rep}_{\overline{\mathbb{Q}}_\ell}(G)$ cut out by $e \in \mathcal{Z}_{\overline{\mathbb{Z}}_\ell}(G) \subseteq \mathcal{Z}_{\overline{\mathbb{Q}}_\ell}(G)$.

Now, let us come back to the ℓ-block.

Theorem. *Let ℓ be a prime different from p. Assume that G is semisimple and simply connected. Let R be an ℓ-block of* $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(G)$. *Then R is characterized by the nonempty intersection $R \cap \mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Q}}_\ell}(G)$.*

Thus, we need to describe the intersection of the ℓ-blocks and the unipotent category. To achieve that, we define an equivalence relation on $\mathcal{T}^{\mathrm{un}}(G)$ in the following way. Let d be the order of q modulo ℓ. Let $\mathfrak{t}$ and $\mathfrak{t}'$ be two elements of $\mathcal{T}^{\mathrm{un}}(G)$ and $\omega \in \mathrm{BT}$. Then we say that $\mathfrak{t} \sim_{\ell,\omega} \mathfrak{t}'$ if and only if $\mathfrak{t} = \mathfrak{t}'$ or there exist (σ, π) and (τ, π') such that $\mathfrak{t} = [\sigma, \pi]$, $\mathfrak{t}' = [\tau, \pi']$, ω is a face of σ and τ, and the Harish-Chandra series in $\bar{\mathsf{G}}_\omega$ corresponding to the cuspidal pairs $(\bar{\mathsf{G}}_\sigma, \pi)$ and $(\bar{\mathsf{G}}_\tau, \pi')$ are both contained in the same $(d, 1)$-series. Note that by our computation of the $(d, 1)$-series, for $\mathfrak{t}$ and ω fixed, we know explicitly the set of $\mathfrak{t}' \in \mathcal{T}^{\mathrm{un}}(G)$ such that $\mathfrak{t} \sim_{\ell,\omega} \mathfrak{t}'$. Now we define $\sim_\ell$, an equivalence relation on $\mathcal{T}^{\mathrm{un}}(G)$ by $\mathfrak{t} \sim_\ell \mathfrak{t}'$ if and only if there exist $\omega_1, \ldots, \omega_r \in \mathrm{BT}$ and $\mathfrak{t}_1, \ldots, \mathfrak{t}_{r-1} \in \mathcal{T}^{\mathrm{un}}(G)$ such that $\mathfrak{t} \sim_{\ell,\omega_1} \mathfrak{t}_1 \sim_{\ell,\omega_2} \mathfrak{t}_2 \cdots \sim_{\ell,\omega_r} \mathfrak{t}'$. We write $[\mathfrak{t}]_\ell$ for the equivalence class of $\mathfrak{t}$.

Theorem. *Let ℓ be an odd prime number, different from p, such that $\ell \geq 5$ if a group of exceptional type ($^3\boldsymbol{D}_4$, $\boldsymbol{G}_2$, $\boldsymbol{F}_4$, $\boldsymbol{E}_6$, $^2\boldsymbol{E}_6$, $\boldsymbol{E}_7$) is involved in a reductive quotient and $\ell \geq 7$ if $\boldsymbol{E}_8$ is involved in a reductive quotient. To each equivalence class $[\mathfrak{t}]_\ell \in \mathcal{T}^{\mathrm{un}}(G)/\sim_\ell$, we can associate* $\mathrm{Rep}^{[\mathfrak{t}]_\ell}_{\overline{\mathbb{Z}}_\ell}(G)$ *a Serre subcategory of* $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(G)$, *constructed with a consistent system of idempotents such that*:

(1) *We have a decomposition*

$$\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(G) = \prod_{[\mathfrak{t}]_\ell \in \mathcal{T}^{\mathrm{un}}(G)/\sim_\ell} \mathrm{Rep}^{[\mathfrak{t}]_\ell}_{\overline{\mathbb{Z}}_\ell}(G).$$

(2) $\mathrm{Rep}^{[\mathfrak{t}]_\ell}_{\overline{\mathbb{Z}}_\ell}(G) \cap \mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Q}}_\ell}(G) = \prod_{\mathfrak{u}\in[\mathfrak{t}]_\ell} \mathrm{Rep}^{\mathfrak{u}}_{\overline{\mathbb{Q}}_\ell}(G)$.

(3) *We also have a description of* $\mathrm{Rep}^{[\mathfrak{t}]_\ell}_{\overline{\mathbb{Z}}_\ell}(G) \cap \mathrm{Rep}_{\overline{\mathbb{Q}}_\ell}(G)$. *Let* $(\sigma, \chi) \in \mathcal{T}^{\mathrm{un}}_\ell(G)$. *Let* $\mathfrak{t}$ *be a semisimple conjugacy class in* $\overline{G}^*_\sigma$ *of order a power of* ℓ, *such that* χ *is in the Deligne–Lusztig series associated to* $\mathfrak{t}$. *Let* $\overline{G}_\sigma(t)$ *be a Levi in* $\overline{G}_\sigma$ *dual to* $C_{\overline{G}^*_\sigma}(t)^\circ$, *the connected centralizer of* t, P *be a parabolic subgroup with Levi component* $\overline{G}_\sigma(t)$, $\hat{t}$ *be a linear character of* $\overline{G}_\sigma(t)$ *associated to* t *by duality*, *and* χ_t *be a unipotent character in* $\overline{G}_\sigma(t)$ *such that* $\langle \chi, \mathcal{R}^{\overline{G}_\sigma}_{\overline{G}_\sigma(t)\subseteq P}(\hat{t}\chi_t)\rangle \neq 0$. *Let* π *be an irreducible component of* $\mathcal{R}^{\overline{G}_\sigma}_{\overline{G}_\sigma(t)\subseteq P}(\chi_t)$. *Let* $(\overline{G}_\tau, \lambda)$ *be the cuspidal support of* π. *Then*

$$\mathrm{Rep}^{(\sigma,\chi)}_{\overline{\mathbb{Q}}_\ell}(G) \subseteq \mathrm{Rep}^{[(\tau,\lambda)]_\ell}_{\overline{\mathbb{Z}}_\ell}(G) \cap \mathrm{Rep}_{\overline{\mathbb{Q}}_\ell}(G).$$

(4) *When* G *is semisimple and simply connected*, *the categories* $\mathrm{Rep}^{[\mathfrak{t}]_\ell}_{\overline{\mathbb{Z}}_\ell}(G)$ *are* ℓ*-blocks.*

We also obtain results for the bad prime $\ell = 2$ in some special cases (which include classical groups).

Theorem. *Let* G *be a semisimple and simply connected group such that all the reductive quotients only involve types among* $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$ *and* $\boldsymbol{D}$, *and* $p \neq 2$. *Then* $\mathrm{Rep}^{1}_{\overline{\mathbb{Z}}_2}(G)$ *is a* 2*-block.*

As mentioned before, we can compute explicitly the equivalence relation $\sim_{\ell,\omega}$, so we can also know $\sim_\ell$. We work out a few examples here, where we make $\sim_\ell$ explicit, hence also the unipotent ℓ-blocks.

Theorem. *Let* G *be a semisimple and simply connected group*:

(1) *If* ℓ *is banal* (*see Definition 2.2.5*), *then the unipotent* ℓ*-blocks are indexed by* $\mathcal{T}^{\mathrm{un}}(G)$.

(2) *If* ℓ *divides* $q-1$ *and satisfies the conditions of the previous theorem*, *then* $\sim_\ell$ *is the trivial relation and the unipotent* ℓ*-blocks are indexed by* $\mathcal{T}^{\mathrm{un}}(G)$. *Moreover*, *the intersection of an* ℓ*-block with* $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Q}}_\ell}(G)$ *is a Bernstein block.*

(3) *If* $G = \mathrm{SL}_n(F)$ *then* $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(\mathrm{SL}_n(F))$ *is an* ℓ*-block.*

We also work out the case $G = \mathrm{Sp}_{2n}(F)$, but to do that we require a few more notations.

Let $\mathcal{S}^{\mathrm{un}}(G) := \{(s,s') \in \mathbb{N}^2, s(s+1)+s'(s'+1) \leq n\}$. To $(s,s') \in \mathcal{S}^{\mathrm{un}}(G)$ we can associate $\mathfrak{t}(s,s') = (\sigma(s,s'), \pi(s,s')) \in \mathcal{T}^{\mathrm{un}}(G)$, such that the reductive quotient at $\sigma(s,s')$ is $\mathrm{GL}_1(k)^{n-s(s+1)+s'(s'+1)} \times \mathrm{Sp}_{2s(s+1)}(k) \times \mathrm{Sp}_{2s'(s'+1)}(k)$ and $\pi(s,s')$ is the unique unipotent irreducible cuspidal representation in this group. The map $(s,s') \mapsto \mathfrak{t}(s,s')$ gives a bijection between $\mathcal{S}^{\mathrm{un}}(G)$ and $\mathcal{T}^{\mathrm{un}}(G)$. Also denote by $\mathcal{S}_c$ the set

$$\mathcal{S}_c = \left\{(s,s') \in \mathcal{S}^{\mathrm{un}}(G), \left\{ \begin{array}{l} s(s+1)+s'(s'-1) > n - d/2 \\ s'(s'+1)+s(s-1) > n - d/2 \end{array} \right\}\right\}.$$

Putting together the previous theorems and making the equivalence relation explicit, we obtain the following description of the unipotent ℓ-blocks of $\mathrm{Sp}_{2n}(F)$.

Theorem. *Let ℓ be prime not dividing q:*

(1) *If $\ell = 2$: $\mathrm{Rep}^1_{\overline{\mathbb{Z}}_2}(\mathrm{Sp}_{2n}(F))$ is a 2-block.*

(2) *If $\ell \neq 2$. Let d be the order of q modulo ℓ:*

(a) *If d is odd, $\sim_\ell$ is the trivial equivalence relation giving the following decomposition into ℓ-blocks*

$$\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(\mathrm{Sp}_{2n}(F)) = \prod_{\mathfrak{t}\in\mathcal{T}^{\mathrm{un}}(G)} \mathrm{Rep}^{[\mathfrak{t}]_\ell}_{\overline{\mathbb{Z}}_\ell}(\mathrm{Sp}_{2n}(F)).$$

(b) *If d is even, the equivalence classes of $\sim_\ell$ are the singletons $\{\mathfrak{t}(s,s')\}$ for $(s,s') \in \mathcal{S}_c$ and $\{\mathfrak{t}(s,s'), (s,s') \in \mathcal{S}^{\mathrm{un}}(G) \setminus \mathcal{S}_c\}$ thus giving the ℓ-block decomposition*

$$\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(\mathrm{Sp}_{2n}(F)) = \mathrm{Rep}^{[\mathfrak{t}(0,0)]_\ell}_{\overline{\mathbb{Z}}_\ell}(\mathrm{Sp}_{2n}(F)) \times \prod_{(s,s')\in\mathcal{S}_c} \mathrm{Rep}^{[\mathfrak{t}(s,s')]_\ell}_{\overline{\mathbb{Z}}_\ell}(\mathrm{Sp}_{2n}(F)).$$

Remark. (1) In the case d odd, or d even and $(s,s') \in \mathcal{S}_c$, we see that the intersection of an ℓ-block with $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Q}}_\ell}(G)$ is a Bernstein block.

(2) If $\ell > n$, in the case d even and $(s,s') \in \mathcal{S}_c$, then $\mathrm{Rep}^{[\mathfrak{t}(s,s')]_\ell}_{\overline{\mathbb{Z}}_\ell}(\mathrm{Sp}_{2n}(F)) \cap \mathrm{Rep}_{\overline{\mathbb{Q}}_\ell}(G)$ is a Bernstein block.

Let us now turn to the study of the stable ℓ-blocks. Let G be a classical unramified group. In this case we have the local Langlands correspondence [1; 13; 15; 17; 25]. The block decomposition is not compatible with the local Langlands correspondence, two irreducible representations may have the same Langlands parameter but may not be in the same block. However, we can look for the "stable" blocks, which are the smallest direct factors subcategories stable by the local Langlands correspondence. These categories correspond to the primitive idempotents in the stable Bernstein center, as defined in [12]. In [19], the decomposition into stable blocks of the depth zero category is given by

$$\mathrm{Rep}^0_{\overline{\mathbb{Q}}_\ell}(G) = \prod_{(\phi,\sigma)\in\widetilde{\Phi}_m(I_F^{\overline{\mathbb{Q}}_\ell}, {}^L\boldsymbol{G})} \mathrm{Rep}^{(\phi,\sigma)}_{\overline{\mathbb{Q}}_\ell}(G)$$

where the set $\widetilde{\Phi}_m(I_F^{\overline{\mathbb{Q}}_\ell}, {}^L\boldsymbol{G})$ is defined in [19, Definition 4.4.2]. An analogous decomposition is given over $\overline{\mathbb{Z}}_\ell$ and we prove here that this is the stable ℓ-block decomposition.

Theorem. *Let G be an unramified classical group and $p \neq 2$. Then the decomposition of* [19]

$$\mathrm{Rep}^0_{\overline{\mathbb{Z}}_\ell}(G) = \prod_{(\phi,\sigma)\in\widetilde{\Phi}_m(I_F^{\overline{\mathbb{Z}}_\ell}, {}^L\boldsymbol{G})} \mathrm{Rep}^{(\phi,\sigma)}_{\overline{\mathbb{Z}}_\ell}(G).$$

is the decomposition of $\mathrm{Rep}^0_{\overline{\mathbb{Z}}_\ell}(G)$ into stable ℓ-blocks, that is, these categories correspond to primitive integral idempotent in the stable Bernstein center.

1. Notations

Let F be a nonarchimedean local field and k its residue field. Let q be the cardinal of k and p its characteristic.

We will be interested in reductive groups over F and over k. In order not to confuse the two settings, we will use the font $\boldsymbol{G}$ for a connected reductive group over F and $\mathbf{G}$ for a connected reductive group over k.

Let $\boldsymbol{G}$ be a connected reductive group over F. We denote by $G := \boldsymbol{G}(F)$ the F-points of $\boldsymbol{G}$. If Λ is a ring where p is invertible, then we will write $\mathrm{Rep}_\Lambda(G)$ for the abelian category of smooth representations of G with coefficients in Λ. The full subcategory of representations of depth zero will be denoted by $\mathrm{Rep}^0_\Lambda(G)$ (see Definition 2.1.3).

In the same way, if $\mathbf{G}$ is a connected reductive group over k, we denote by $\mathsf{G} := \mathbf{G}(k)$ the group of its k-points. This group can be seen as $\mathsf{G} := \mathbf{G}(\bar{k})^{\mathsf{F}}$, the group of fixed points of a Frobenius automorphism F. If $\mathbf{P}$ is a parabolic subgroup admitting $\mathbf{M}$ a F-stable Levi subgroup, we will write $\mathcal{R}^{\mathbf{G}}_{\mathbf{M}\subseteq\mathbf{P}}$ for the Deligne–Lusztig induction from M to G; defined in [10]. It is a map between spaces of virtual representations $\mathcal{R}^{\mathbf{G}}_{\mathbf{M}\subseteq\mathbf{P}} : \mathbb{Z}\,\mathrm{Irr}(\mathsf{M}) \to \mathbb{Z}\,\mathrm{Irr}(\mathsf{G})$. When $\mathbf{P}$ is also F-stable, since the Deligne–Lusztig induction is the same as the Harish-Chandra induction, we will also use $i^{\mathsf{G}}_{\mathsf{M}\subseteq\mathsf{P}}$ and $r^{\mathsf{G}}_{\mathsf{M}\subseteq\mathsf{P}}$ for the Harish-Chandra induction and restriction. Let $\mathbf{G}^*$ be in duality with $\mathbf{G}$, a duality defined over k, with Frobenius F on $\mathbf{G}^*$.

In all this paper, ℓ will be a prime number not dividing q. We shall assume that choices have been made, once and for all, of isomorphisms of $\bar{k}^*$ with $(\mathbb{Q}/\mathbb{Z})_{p'}$ and of $\bar{k}^*$ with the group of roots of unity of order prime to p in $\overline{\mathbb{Q}}_\ell$.

2. Bernstein blocks

Let G be the F-points of a connected reductive group. When the field of coefficients is $\overline{\mathbb{Q}}_\ell$ (or $\mathbb{C}$), the blocks of G are well known thanks to the theory of Bernstein [2]. In this paper, the ℓ-blocks of G will be constructed using consistent systems of idempotents on the Bruhat–Tits building of G. The purpose of this section is to explain, in the case where G is semisimple and simply connected, how we can recover Bernstein blocks using consistent systems of idempotents.

2.1. ***Consistent systems of idempotents.*** In this section, we recall the basic definitions and properties of systems of idempotents.

Let BT be the semisimple Bruhat–Tits building associated to G. This is a polysimplicial complex and we denote by BT_0 the set of vertices, that is of polysimplices of dimension 0. We will usually use Latin letters $x, y, \ldots$ for vertices and Greek letters $\sigma, \tau, \ldots$ for polysimplices. We can define an order relation on BT by $\sigma \leq \tau$ if σ is a face of τ. Two vertices x and y are adjacent if there exists a polysimplex σ such that $x \leq \sigma$ and $y \leq \sigma$.

Let Λ be a ring where p is invertible. We fix a Haar measure on G and denote by $\mathcal{H}_\Lambda(G)$ the Hecke algebra with coefficients in Λ, that is the algebra of functions from G to Λ locally constant with compact support.

Definition 2.1.1 [24, Definition 2.1]. A system of idempotents $e = (e_x)_{x\in \mathrm{BT}_0}$ of $\mathcal{H}_\Lambda(G)$ is said to be consistent if the following properties are satisfied:

(1) $e_x e_y = e_y e_x$ when x and y are adjacent.

(2) $e_x e_z e_y = e_x e_y$ when z is adjacent to x and in the polysimplicial hull of x and y.

(3) $e_{gx} = g e_x g^{-1}$ for all $x \in \mathrm{BT}_0$ and $g \in G$.

If $e = (e_x)_{x\in \mathrm{BT}_0}$ is a consistent system of idempotent, then for $\sigma \in \mathrm{BT}$ we can define $e_\sigma := \prod_x e_x$, where the product is taken over the vertices x such that $x \leq \sigma$.

Consistent systems of idempotents are very interesting because we have the following theorem due to Meyer and Solleveld.

Theorem 2.1.2 [24, Theorem 3.1]. *Let $e = (e_x)_{x\in \mathrm{BT}_0}$ a consistent system of idempotents, then the full subcategory $\mathrm{Rep}^e_\Lambda(G)$ of objects V of $\mathrm{Rep}_\Lambda(G)$ such that $V = \sum_{x\in \mathrm{BT}_0} e_x V$ is a Serre subcategory.*

It may not be easy to check the conditions of consistency. But, if we are working with the subcategory of depth zero representations, we can find in [18] the notion of 0-consistent, which implies consistency, and is easier to check.

Let $\sigma \in \mathrm{BT}$. We denote by G°_σ the parahoric subgroup at σ and by G^+_σ its pro-p-radical. The quotient, $\bar{\mathsf{G}}_\sigma$, is then the group of k-points of a connected reductive group $\bar{\mathbf{G}}_\sigma$ defined over k.

If $\sigma \in \mathrm{BT}$ is a polysimplex, then G^+_σ defines an idempotent $e^+_\sigma \in \mathcal{H}_{\mathbb{Z}[1/p]}(G)$ by $e^+_\sigma = \mu(G^+_\sigma)^{-1}\chi_{G^+_\sigma}$, where μ is our fixed Haar measure and $\chi_{G^+_\sigma}$ is the characteristic function of G^+_σ. The system of idempotents $(e^+_x)_{x\in \mathrm{BT}_0}$ is consistent and cuts out the category of depth zero.

Definition 2.1.3. An object V of $\mathrm{Rep}_\Lambda(G)$ has depth zero if $V = \sum_{x\in \mathrm{BT}_0} e^+_x V$.

In other words, with the notations of Theorem 2.1.2, the depth zero category is $\mathrm{Rep}^0_\Lambda(G) = \mathrm{Rep}^{e^+}_\Lambda(G)$, with $e^+ = (e^+_x)_{x\in \mathrm{BT}_0}$.

Definition 2.1.4 [18, Definition 1.0.5]. We say that a system $(e_\sigma)_{\sigma\in \mathrm{BT}}$ is 0-consistent if:

(1) $e_{gx} = g e_x g^{-1}$ for all $x \in \mathrm{BT}_0$ and $g \in G$.

(2) $e_\sigma = e^+_\sigma e_x = e_x e^+_\sigma$ for $x \in \mathrm{BT}_0$ and $\sigma \in \mathrm{BT}$ such that $x \leq \sigma$.

Proposition 2.1.5 [18, Proposition 1.0.6]. *If $(e_\sigma)_{\sigma\in \mathrm{BT}}$ is a 0-consistent system of idempotents, then it is consistent.*

Let us give two examples of systems of idempotents which are 0-consistent. Let $\sigma \in \mathrm{BT}$. Let $\mathcal{E}(\bar{\mathsf{G}}_\sigma, 1)$ be the Deligne–Lusztig series associated with the trivial conjugacy class, that is the set of unipotent characters in $\bar{\mathsf{G}}_\sigma$. Let $e_{1,\bar{\mathsf{G}}_\sigma}$, be the central idempotent in $\bar{\mathbb{Q}}_\ell[\bar{\mathsf{G}}_\sigma]$ that cuts out $\mathcal{E}(\bar{\mathsf{G}}_\sigma, 1)$. Thanks to the isomorphism $G^\circ_\sigma/G^+_\sigma \xrightarrow{\sim} \bar{\mathsf{G}}_\sigma$, we can pull back $e_{1,\bar{\mathsf{G}}_\sigma}$ to an idempotent $e_{1,\sigma} \in \mathcal{H}_{\bar{\mathbb{Q}}_\ell}(G^\circ_\sigma)$. The system $e_1 = (e_{1,\sigma})_{\sigma\in \mathrm{BT}}$ is then 0-consistent; see [18, Proposition 2.3.2]. Thus it defines $\mathrm{Rep}^{\mathrm{un}}_{\bar{\mathbb{Q}}_\ell}(G)$ the full-subcategory of $\mathrm{Rep}_{\bar{\mathbb{Q}}_\ell}(G)$ of unipotent representations.

In the same way, let $\mathcal{E}_\ell(\bar{\mathsf{G}}_\sigma, 1)$ be the union of the $\mathcal{E}(\bar{\mathsf{G}}_\sigma, t)$, where t is a semisimple conjugacy class in the dual of $\bar{\mathsf{G}}_\sigma$, of order a power of ℓ. By [3] Theorem A' and Remark 11.3, the idempotent that cuts out this series is in $\bar{\mathbb{Z}}_\ell[\bar{\mathsf{G}}_\sigma]$. We can then pull it back to get $e^\ell_{1,\sigma} \in \mathcal{H}_{\bar{\mathbb{Z}}_\ell}(G^\circ_\sigma)$. This system $e^\ell_1 = (e^\ell_{1,\sigma})_{\sigma\in \mathrm{BT}}$ is also 0-consistent and defines the ℓ-unipotent subcategory $\mathrm{Rep}^{\mathrm{un}}_{\bar{\mathbb{Z}}_\ell}(G)$.

2.2. ***Bernstein blocks with system of idempotents.*** In this section, we want to reinterpret the Bernstein blocks of depth zero (that is the blocks over $\bar{\mathbb{Q}}_\ell$ or $\mathbb{C}$), in terms of consistent systems of idempotents. To do that, we will construct a 0-consistent system of idempotents from unrefined depth zero types, hence subcategories of $\mathrm{Rep}^0_{\bar{\mathbb{Q}}_\ell}(G)$. When G is semisimple and simply connected, these categories will be blocks.

We define, as in [20], "unrefined depth zero types" to be the pairs (σ, π), where $\sigma \in \mathrm{BT}$ and π is an irreducible cuspidal representation of $\bar{\mathsf{G}}_\sigma$. Let $\mathcal{T}(G)$ be the set of unrefined depth zero types, up to G-conjugacy.

If $\sigma, \tau \in \mathrm{BT}$ are two polysimplices with $\tau \leq \sigma$, we can see $\bar{\mathsf{G}}_\sigma$ as a Levi subgroup of $\bar{\mathsf{G}}_\tau$. Let $\mathfrak{t}$ and $\mathfrak{t}'$ be two elements of $\mathcal{T}(G)$ and $\omega \in \mathrm{BT}$. Then we say that $\mathfrak{t} \sim_\omega \mathfrak{t}'$ if and only if $\mathfrak{t} = \mathfrak{t}'$ or there exist (σ, π) and (τ, π') such that $\mathfrak{t} = [\sigma, \pi]$, $\mathfrak{t}' = [\tau, \pi']$, ω is a face of σ and τ, and the cuspidal pairs $(\bar{\mathsf{G}}_\sigma, \pi)$ and $(\bar{\mathsf{G}}_\tau, \pi')$ are conjugated in $\bar{\mathsf{G}}_\omega$. Now we define $\sim$, an equivalence relation on $\mathcal{T}(G)$ by $\mathfrak{t} \sim \mathfrak{t}'$ if and only if there exist $\omega_1, \dots, \omega_r \in \mathrm{BT}$ and $\mathfrak{t}_1, \dots, \mathfrak{t}_{r-1} \in \mathcal{T}(G)$ such that $\mathfrak{t} \sim_{\omega_1} \mathfrak{t}_1 \sim_{\omega_2} \mathfrak{t}_2 \cdots \sim_{\omega_r} \mathfrak{t}'$. We write $[\mathfrak{t}]$ for the equivalence class of $\mathfrak{t}$.

If G is a connected reductive group over k, then the theory of Harish-Chandra allows us to partition $\mathrm{Irr}(\mathsf{G})$ according to cuspidal support $[\mathsf{M}, \pi]$:

$$\mathrm{Irr}(\mathsf{G}) = \bigsqcup \mathrm{Irr}_{(\mathsf{M},\pi)}(\mathsf{G}).$$

Now we construct from $[\mathfrak{t}] \in \mathcal{T}(G)/\sim$ a system of idempotents $e_{[\mathfrak{t}]}$ in the following way. Let $\tau \in \mathrm{BT}$ and define $e^\tau_{[\mathfrak{t}]} \in \bar{\mathbb{Q}}_\ell[\bar{\mathsf{G}}_\tau]$ the idempotent that cuts out the union of $\mathrm{Irr}_{(\bar{\mathsf{G}}_\sigma,\pi)}(\bar{\mathsf{G}}_\tau)$ for every $[\sigma, \pi] \in [\mathfrak{t}]$ with $\tau \leq \sigma$. We can then pull pack $e^\tau_{[\mathfrak{t}]}$ to an idempotent $e_{[\mathfrak{t}],\tau} \in \mathcal{H}_{\bar{\mathbb{Q}}_\ell}(G^\circ_\tau) \subseteq \mathcal{H}_{\bar{\mathbb{Q}}_\ell}(G)$, giving us $e_{[\mathfrak{t}]}$ a system of idempotents.

Lemma 2.2.1. *Let $x \in \mathrm{BT}_0$, $\sigma \in \mathrm{BT}$ with $x \leq \sigma$. We have the following properties*:

(1) $e^+_\sigma = \sum_{[\mathfrak{t}]\in\mathcal{T}(G)/\sim} e_{[\mathfrak{t}],\sigma}$.

(2) *For all $\mathfrak{t}, \mathfrak{t}' \in \mathcal{T}(G)$ with $[\mathfrak{t}] \neq [\mathfrak{t}']$, $e_{[\mathfrak{t}],x} e_{[\mathfrak{t}'],\sigma} = 0$.*

Proof. (1) The partition $\mathrm{Irr}(\bar{\mathsf{G}}_\sigma) = \bigsqcup \mathrm{Irr}_{(\mathsf{M},\pi)}(\bar{\mathsf{G}}_\sigma)$ and the fact that each $\mathrm{Irr}_{(\mathsf{M},\pi)}(\bar{\mathsf{G}}_\sigma)$ can be written as $\mathrm{Irr}_{(\mathsf{M},\pi)}(\bar{\mathsf{G}}_\sigma) = \mathrm{Irr}_{(\bar{\mathsf{G}}_\tau,\pi)}(\bar{\mathsf{G}}_\sigma)$ for a polysimplex $\tau \geq \sigma$ show the wanted equality.

(2) The group $\bar{\mathsf{G}}_\sigma$ is a Levi quotient of a parabolic P_σ of $\bar{\mathsf{G}}_x$, and we denote by U_σ the unipotent radical of P_σ. The idempotent $e_{[\mathfrak{t}'],\sigma} \in \mathcal{H}_{\bar{\mathbb{Q}}_\ell}(G^\circ_\sigma) \subseteq \mathcal{H}_{\bar{\mathbb{Q}}_\ell}(G^\circ_x)$ gives us in $\bar{\mathbb{Q}}_\ell[\bar{\mathsf{G}}_x]$ the idempotent $e_{\mathsf{U}_\sigma} e^\sigma_{[\mathfrak{t}']}$, where e_{U_σ} is the idempotent which averages along the group U_σ. We have to prove that $e^x_{[\mathfrak{t}]} e_{\mathsf{U}_\sigma} e^\sigma_{[\mathfrak{t}']} = 0$ in $\bar{\mathbb{Q}}_\ell[\bar{\mathsf{G}}_x]$. But $\bar{\mathbb{Q}}_\ell[\bar{\mathsf{G}}_x] e_{\mathsf{U}_\sigma} e^\sigma_{[\mathfrak{t}']}$ is the parabolic induction from $\bar{\mathsf{G}}_\sigma$ to $\bar{\mathsf{G}}_x$ of the module $\bar{\mathbb{Q}}_\ell[\bar{\mathsf{G}}_\sigma] e^\sigma_{[\mathfrak{t}']}$. Since $[\mathfrak{t}] \neq [\mathfrak{t}']$ no representation in $\mathrm{Irr}_{(\bar{\mathsf{G}}_\tau,\pi)}(\bar{\mathsf{G}}_x)$, with $[\tau, \pi] \in [\mathfrak{t}]$ can be in the induction of a representation in $\mathrm{Irr}_{(\bar{\mathsf{G}}_{\tau'},\pi')}(\bar{\mathsf{G}}_\sigma)$ with $[\tau', \pi'] \in [\mathfrak{t}']$. Hence $e^x_{[\mathfrak{t}]} e_{\mathsf{U}_\sigma} e^\sigma_{[\mathfrak{t}']} = 0$. □

Proposition 2.2.2. *The system of idempotents $e_{[\mathfrak{t}]}$ is 0-consistent.*

Proof. An element $\mathfrak{t} \in \mathcal{T}(G)$ is defined up to G-conjugacy, hence $e_{[\mathfrak{t}]}$ is G-equivariant. Let $x \in \mathrm{BT}_0$ and $\sigma \in \mathrm{BT}$ such that $x \leq \sigma$. We have to prove that $e_{[\mathfrak{t}],\sigma} = e_\sigma^+ e_{[\mathfrak{t}],x}$. By 1. in 2.2.1 we have that $e_\sigma^+ = \sum_{[\mathfrak{t}']\in\mathcal{T}(G)/\sim} e_{[\mathfrak{t}'],\sigma}$. Hence, $e_{[\mathfrak{t}],x}e_\sigma^+ = \sum_{[\mathfrak{t}']\in\mathcal{T}(G)/\sim} e_{[\mathfrak{t}],x}e_{[\mathfrak{t}'],\sigma}$. Now by 2. in 2.2.1, we have that if $[\mathfrak{t}] \neq [\mathfrak{t}']$ then $e_{[\mathfrak{t}],x}e_{[\mathfrak{t}'],\sigma} = 0$. So $e_{[\mathfrak{t}],x}e_\sigma^+ = e_{[\mathfrak{t}],x}e_{[\mathfrak{t}],\sigma}$. In the same way, $e_{[\mathfrak{t}],x}e_{[\mathfrak{t}],\sigma} = e_x^+ e_{[\mathfrak{t}],\sigma}$. So, $e_{[\mathfrak{t}],x}e_\sigma^+ = e_{[\mathfrak{t}],x}e_{[\mathfrak{t}],\sigma} = e_x^+ e_{[\mathfrak{t}],\sigma} = e_x^+ e_\sigma^+ e_{[\mathfrak{t}],\sigma} = e_\sigma^+ e_{[\mathfrak{t}],\sigma} = e_{[\mathfrak{t}],\sigma}$. □

Let $\mathfrak{t} \in \mathcal{T}(G)$. We denote by $\mathrm{Rep}^{[\mathfrak{t}]}_{\overline{\mathbb{Q}}_\ell}(G)$ the category associated with $e_{[\mathfrak{t}]}$.

Proposition 2.2.3. *We have the decomposition*

$$\mathrm{Rep}^0_{\overline{\mathbb{Q}}_\ell}(G) = \prod_{[\mathfrak{t}]\in\mathcal{T}(G)/\sim} \mathrm{Rep}^{[\mathfrak{t}]}_{\overline{\mathbb{Q}}_\ell}(G).$$

Proof. The proof is similar to the proof of [18, Proposition 2.3.5]. Property 2 in Lemma 2.2.1 shows that these categories are pairwise orthogonal and property 1. in Lemma 2.2.1 shows that the product if $\mathrm{Rep}^0_{\overline{\mathbb{Q}}_\ell}(G)$. □

Theorem 2.2.4. *If G is semisimple and simply connected the category $\mathrm{Rep}^{[\mathfrak{t}]}_{\overline{\mathbb{Q}}_\ell}(G)$ is a block.*

Proof. When G is semisimple and simply connected, Theorem 4.9 of [26] shows that we have a bijection between $\mathcal{T}(G)/\sim$ and level zero Bernstein blocks. We then deduce from Proposition 2.2.3 that $\mathrm{Rep}^0_{\overline{\mathbb{Q}}_\ell}(G) = \prod_{[\mathfrak{t}]\in\mathcal{T}(G)/\sim} \mathrm{Rep}^{[\mathfrak{t}]}_{\overline{\mathbb{Q}}_\ell}(G)$ is the decomposition of $\mathrm{Rep}^0_{\overline{\mathbb{Q}}_\ell}(G)$ into Bernstein blocks. □

We would like to do the same thing to construct ℓ-blocks. The simplest case is when ℓ is banal.

Definition 2.2.5. We say that a prime number $\ell \neq p$ is banal when for every vertex $x \in \mathrm{BT}_0$, ℓ does not divide the cardinal of $\overline{\mathsf{G}}_x$.

Therefore, when ℓ is banal each idempotent $e_{[\mathfrak{t}]}$ is in $\mathcal{H}_{\overline{\mathbb{Z}}_\ell}(G)$. Thus we have a decomposition

$$\mathrm{Rep}^0_{\overline{\mathbb{Z}}_\ell}(G) = \prod_{[\mathfrak{t}]\in\mathcal{T}(G)/\sim} \mathrm{Rep}^{[\mathfrak{t}]}_{\overline{\mathbb{Z}}_\ell}(G)$$

and the following theorem.

Theorem 2.2.6. *If G is semisimple and simply connected, and ℓ is banal, the category $\mathrm{Rep}^{[\mathfrak{t}]}_{\overline{\mathbb{Z}}_\ell}(G)$ is an ℓ-block.*

In the general case, the idempotents do not have coefficients in $\overline{\mathbb{Z}}_\ell$. The topic of the followings sections will be to explain how to sum these idempotents to get idempotents with integral coefficients.

3. $(d, 1)$-theory

We have seen in Section 2.2 how to construct the Bernstein blocks with consistent systems of idempotents when we have a simply connected group. To construct ℓ-blocks, we need to produce central idempotents for finite reductive groups with coefficients in $\overline{\mathbb{Z}}_\ell$. In this section, we introduce the notion of a $(d, 1)$-set.

This is a subset of $\mathrm{Irr}(\mathsf{G})$ which is a union of Harish-Chandra series and gives a central idempotent with coefficients in $\bar{\mathbb{Z}}_\ell$. These $(d, 1)$-sets will be used in the next sections to describe the unipotent ℓ-blocks for simply connected p-adic groups.

This section will only deal with finite reductive groups. Let us take $(\mathbf{G}, \mathsf{F})$ a connected reductive group defined over k, and let $\mathsf{G} := (\mathbf{G})^{\mathsf{F}}$. We recall that $q = |k|$. We will define the $(d, 1)$-set and $(d, 1)$-series, then explain how to compute them, and to finish, we will show that they behave well with respect to Harish-Chandra induction and Deligne–Lusztig induction from particular Levi subgroups.

3.1. ***Unipotent ℓ-blocks for finite reductive groups.*** We recall in this section the theory of ℓ-blocks for a finite connected reductive group. These blocks will be constructed using a modified Harish-Chandra induction called d-Harish-Chandra induction, defined using Deligne–Lusztig theory.

For each connected reductive group $(\mathbf{G}, \mathsf{F})$ over k, there exists a unique polynomial $P_{\mathsf{G}} \in \mathbb{Z}[x]$ called the polynomial order of $\mathbf{G}$ (see, for example, [4] section 1.A) with the property that there is $a \geq 1$ such that $|\mathbf{G}^{\mathsf{F}^m}| = P_{\mathsf{G}}(q^m)$ for all $m \geq 1$ such that $m \equiv 1 \pmod a$. The prime factors of P_{G} distinct from x are cyclotomic polynomials. Let $d \geq 1$ be an integer and Φ_d the corresponding cyclotomic polynomial. We say that $\mathbf{T}$ is a Φ_d-subgroup if $\mathbf{T}$ is a F-stable torus of $\mathbf{G}$ whose polynomial order is a power of Φ_d. A d-split Levi subgroups of $\mathbf{G}$ is the centralizer in $\mathbf{G}$ of some Φ_d-subgroup of $\mathbf{G}$.

Let $\chi \in \mathrm{Irr}(\mathsf{G})$ be an ordinary irreducible character. We say that χ is d-cuspidal if and only if ${}^*\mathcal{R}^{\mathbf{G}}_{\mathbf{L}\subseteq\mathbf{P}}\chi = 0$ for every proper d-split Levi subgroup $\mathbf{L}$ and every parabolic $\mathbf{P}$ admitting $\mathbf{L}$ as Levi subgroup.

A "unipotent d-pair" is a pair $(\mathbf{L}, \lambda)$ where $\mathbf{L}$ is a d-split Levi and λ is a unipotent character of $\mathbf{L}$. Such a pair is said to be cuspidal if λ is cuspidal. We define an order on unipotent d-pairs by $(\mathbf{M}, \mu) \preceq (\mathbf{L}, \lambda)$ if $\mathbf{M}$ is a Levi subgroup of $\mathbf{L}$ and there is a parabolic subgroup $\mathbf{P}$ of $\mathbf{L}$ admitting $\mathbf{M}$ as a Levi such that $\langle \lambda, \mathcal{R}^{\mathbf{L}}_{\mathbf{M}\subseteq\mathbf{P}}(\mu)\rangle \neq 0$. For $(\mathbf{L}, \lambda)$ a unipotent d-cuspidal pair, let us define $\mathcal{E}(\mathsf{G}, (\mathbf{L}, \lambda))$ to be the subset of $\mathcal{E}(\mathsf{G}, 1)$ of characters χ such that $(\mathbf{L}, \lambda) \preceq (\mathbf{G}, \chi)$. We call $\mathcal{E}(\mathsf{G}, (\mathbf{L}, \lambda))$ a d-series.

Theorem 3.1.1 [4, Theorem 3.2(1)]. *For each d, the sets $\mathcal{E}(\mathsf{G}, (\mathbf{L}, \lambda))$ (where $(\mathbf{L}, \lambda)$ runs over a complete set of representatives of G-conjugacy classes of unipotent d-cuspidal pairs) partition $\mathcal{E}(\mathsf{G}, 1)$.*

An ℓ-block is a primitive idempotent in the center $Z(\bar{\mathbb{Z}}_\ell[\mathsf{G}])$ of the group algebra $\bar{\mathbb{Z}}_\ell[\mathsf{G}]$. For b an ℓ-block, we denote by $\mathrm{Irr}(b)$ the subset of $\mathrm{Irr}(\mathsf{G})$ that is cuts out by the idempotent b. This defines a partition $\mathrm{Irr}(\mathsf{G}) = \bigsqcup_b \mathrm{Irr}(b)$. The ℓ-unipotent series $\mathcal{E}_\ell(\mathsf{G}, 1)$, defined as the union of the $\mathcal{E}(\mathsf{G}, t)$ with t of order a power of ℓ, defines a central idempotent in $\bar{\mathbb{Z}}_\ell[\mathsf{G}]$ [3, Theorem A' and Remark 11.3], hence it is a union of ℓ-blocks: $\mathcal{E}_\ell(\mathsf{G}, 1) = \bigsqcup_b \mathrm{Irr}(b)$. We will call these blocks the unipotent ℓ-blocks.

Let ℓ be a prime number not diving q. We will say that ℓ satisfies the condition $(*)$ if

$$\ell \text{ is odd, } \ell \text{ is good for } \mathbf{G} \text{ and } \ell \neq 3 \text{ if } {}^3\boldsymbol{D}_4 \text{ is involved in } (\mathbf{G}, \mathsf{F}). \tag{$*$}$$

Let us summarize the condition of being good and $(*)$ in a table

Types	$\boldsymbol{A}_n$, ${}^2\boldsymbol{A}_n$	$\boldsymbol{B}_n$, $\boldsymbol{C}_n$, $\boldsymbol{D}_n$, ${}^2\boldsymbol{D}_n$	${}^3\boldsymbol{D}_4$	$\boldsymbol{G}_2$, $\boldsymbol{F}_4$, $\boldsymbol{E}_6$, ${}^2\boldsymbol{E}_6$, $\boldsymbol{E}_7$	$\boldsymbol{E}_8$
bad ℓ	$\varnothing$	$\{2\}$	$\{2\}$	$\{2, 3\}$	$\{2, 3, 5\}$
$(*)$	$\ell \geq 3$	$\ell \geq 3$	$\ell \geq 5$	$\ell \geq 5$	$\ell \geq 7$

Theorem 3.1.2 [5, Theorem 4.4]. *We assume that ℓ satisfies $(*)$ and let d be the order of q modulo ℓ. Then there is a bijection*

$$(\boldsymbol{L}, \lambda) \mapsto b(\boldsymbol{L}, \lambda),$$

between the set of $\mathbf{G}$-conjugacy classes of unipotent d-cuspidal pairs of $\mathbf{G}$ and the set of unipotent ℓ-blocks.

Moreover, we have that $\mathrm{Irr}(b(\boldsymbol{L}, \lambda)) \cap \mathcal{E}(\mathbf{G}, 1) = \{\chi, (\boldsymbol{L}, \lambda) \preceq (\boldsymbol{G}, \chi)\}$.

If b is a unipotent ℓ-block, then the knowledge of $\mathrm{Irr}(b) \cap \mathcal{E}(\mathbf{G}, 1)$ is enough to describe all the characters in $\mathrm{Irr}(b)$. To explain this, we need a few more notations.

Let $t \in \mathbf{G}^*$ be a semisimple element of order a power of ℓ. Let ℓ be a good prime for $\mathbf{G}$. Then $C_{\mathbf{G}^*}(t)^\circ$ is a Levi subgroup; see for example [5, Proposition 2.1]. Let $\mathbf{G}(t)$ be a Levi subgroup in $\mathbf{G}$ in duality with $C_{\mathbf{G}^*}(t)^\circ$ over k and $\mathbf{P}$ be a parabolic subgroup with Levi component $\mathbf{G}(t)$.

Since t is a central element of $(C_{\mathbf{G}^*}(t)^\circ)^{\mathsf{F}}$, by [11, Proposition 13.30], there exists a linear character $\hat{t} \in \mathrm{Irr}(\mathbf{G}(t))$ such that the tensor product with $\hat{t}$ defines a bijection from $\mathcal{E}(\mathbf{G}(t), 1)$ to $\mathcal{E}(\mathbf{G}(t), t)$. Let $\chi \in \mathcal{E}(\mathbf{G}, t)$. Then, by the Jordan decomposition in the case of nonconnected center (defined in [23]) there exists $\chi_t \in \mathcal{E}(\mathbf{G}(t), 1)$ such that $\langle \chi, \mathcal{R}^{\mathbf{G}}_{\mathbf{G}(t)\subseteq\mathbf{P}}(\hat{t}\chi_t)\rangle \neq 0$.

Theorem 3.1.3 [5, Theorem 4.4]. *Let ℓ be a prime good for $\mathbf{G}$. Let $\chi \in \mathcal{E}(\mathbf{G}, t)$, for t a semisimple conjugacy class in $\mathbf{G}^*$ of order a power of ℓ. Let b be the ℓ-block such that $\chi \in \mathrm{Irr}(b)$. Let $\boldsymbol{G}(t)$ be a F-stable Levi in $\boldsymbol{G}$ dual to $C_{\boldsymbol{G}^*}(t)^\circ$, $\boldsymbol{P}$ be a parabolic subgroup with Levi component $\boldsymbol{G}(t)$, and $\chi_t \in \mathcal{E}(\mathbf{G}(t), 1)$ such that $\langle \chi, \mathcal{R}^{\mathbf{G}}_{\mathbf{G}(t)\subseteq\boldsymbol{P}}(\hat{t}\chi_t)\rangle \neq 0$. For any such $(\boldsymbol{G}(t), \boldsymbol{P}, \chi_t)$ associated to χ, all the irreducible components of $\mathcal{R}^{\mathbf{G}}_{\mathbf{G}(t)\subseteq\boldsymbol{P}}(\chi_t)$ are in* $\mathrm{Irr}(b) \cap \mathcal{E}(\mathbf{G}, 1)$.

Let $(\mathbf{L}, \lambda)$ be a unipotent d-cuspidal pair. Then we define the ℓ-extension of the d-series $\mathcal{E}(\mathbf{G}, (\mathbf{L}, \lambda))$ as the subset $\mathcal{E}_\ell(\mathbf{G}, (\mathbf{L}, \lambda)) \subseteq \mathcal{E}_\ell(\mathbf{G}, 1)$ of characters $\chi \in \mathcal{E}_\ell(\mathbf{G}, 1)$ such that, with the notation of Theorem 3.1.3, all the irreducible components of $\mathcal{R}^{\mathbf{G}}_{\mathbf{G}(t)\subseteq\mathbf{P}}(\chi_t)$ are in $\mathcal{E}(\mathbf{G}, (\mathbf{L}, \lambda))$. Hence, if ℓ satisfies $(*)$, then $\mathcal{E}_\ell(\mathbf{G}, (\mathbf{L}, \lambda)) = \mathrm{Irr}(b(\mathbf{L}, \lambda))$.

3.2. $(d, 1)$-*series*. We have seen in Section 2.2 that in order to construct Bernstein blocks we needed to decompose $\mathrm{Irr}(\mathbf{G})$ as Harish-Chandra series. But to get ℓ-blocks we need to decompose it as d-series, as seen in Section 3.1. In this section, we will introduce $(d, 1)$-series, which will give a partition of $\mathrm{Irr}(\mathbf{G})$ into subsets which are both a union of Harish-Chandra series and a union of d-series.

First, let us remark that 1-series are just Harish-Chandra series, so from now on we will speak of 1-split Levi, 1-cuspidal pairs and 1-series when we want to talk about "normal" Levi subgroup, cuspidal pairs and Harish-Chandra series.

Definition 3.2.1. We define a $(d, 1)$-set to be a subset of $\mathrm{Irr}(\mathbf{G})$ which is a union of 1-series and a union of d-series. A $(d, 1)$-series is then a $(d, 1)$-set with no proper nonempty $(d, 1)$-subset.

A $(d, 1)$-set, respectively a $(d, 1)$-series, included in $\mathcal{E}(\mathbf{G}, 1)$ will be called a unipotent $(d, 1)$-set, respectively a unipotent $(d, 1)$-series.

Remark 3.2.2. (1) By Theorem 3.1.1 $\mathcal{E}(\mathbf{G}, 1)$ is a $(d, 1)$-set, so the unipotent $(d, 1)$-series give a partition of $\mathcal{E}(\mathbf{G}, 1)$.

(2) If Φ_d does not divide P_{G}, then the only Φ_d-torus is the trivial one. Hence the $(d,1)$-series are just the 1-series.

Let $\mathcal{E}$ be a unipotent $(d,1)$-series. Since $\mathcal{E}$ can be written as a union of d-series $\mathcal{E} = \bigsqcup_i \mathcal{E}_i$, we can define the ℓ-extension of a $(d,1)$-series by

$$\mathcal{E}_\ell := \bigsqcup_i \mathcal{E}_{i,\ell}.$$

We want to compute the unipotent $(d,1)$-series. The first step is to reduce to the case of simple groups.

To every orbit ω of F on the set of connected components of the Dynkin diagram of $\mathbf{G}$ there corresponds a well defined F-stable subgroup $\mathbf{G}'_\omega$ of $[\mathbf{G},\mathbf{G}]$ and a component $\mathbf{G}_\omega = Z^\circ(\mathbf{G})\mathbf{G}'_\omega$ of $\mathbf{G}$. The finite group $(\mathbf{G}_\omega/Z(\mathbf{G}_\omega))^{\mathsf{F}}$ is characterized by its simple type $\{\boldsymbol{A}_n, {}^2\boldsymbol{A}_n, \boldsymbol{B}_n, \boldsymbol{C}_n, \boldsymbol{D}_n, {}^2\boldsymbol{D}_n, {}^3\boldsymbol{D}_4, \boldsymbol{G}_2, \boldsymbol{F}_4, \boldsymbol{E}_6, {}^2\boldsymbol{E}_6, \boldsymbol{E}_7, \boldsymbol{E}_8\}$ and an extension field $\mathbb{F}_{q^{m(\omega)}}$ of $\mathbb{F}_q$ of degree $m(\omega)$ equal to the length of the orbit of ω. Moreover, when $\mathbf{G} = \mathbf{G}_{ad}$, where $\mathbf{G}_{ad}$ denotes the adjoint group of $\mathbf{G}$, then it is a direct product of its components.

Let us begin, by showing how to reduce to $\mathbf{G}$ of adjoint type.

Proposition 3.2.3. *Let $\pi : \boldsymbol{G} \to \boldsymbol{G}_{ad}$ be the reduction map modulo $Z(\boldsymbol{G})$. Then π induces a bijection between $\mathcal{E}(G_{ad},1)$ and $\mathcal{E}(G,1)$ which commutes with the Deligne–Lusztig induction and preserves unipotent $(d,1)$-series.*

Proof. This follows from [4, Proposition 1.36] and [4, Remark 1.25]. □

Let $a \in \mathbb{N}^*$. Denote by $(\mathbf{G}^{(a)}, \mathsf{F}^{(a)})$ the restriction of scalars (or Weil restriction) of $(\mathbf{G},\mathsf{F})$ from $\mathbb{F}_{q^a}$ to $\mathbb{F}_q$. This is a reductive group defined over $\mathbb{F}_q$ characterized by the property: for any $\mathbb{F}_q$-algebra A we have $\mathbf{G}^{(a)}(A) = \mathbf{G}(A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^a})$. In particular, $(\mathbf{G}^{(a)})^{\mathsf{F}^{(a)}} = \mathbf{G}^{\mathsf{F}^a}$ (that is $\mathbf{G}^{(a)}(\mathbb{F}_q) = \mathbf{G}(\mathbb{F}_{q^a})$). Moreover, the isomorphism $(\mathbf{G}^{(a)})^{\mathsf{F}^{(a)}} \simeq \mathbf{G}^{\mathsf{F}^a}$ "commutes" with the Deligne–Lusztig induction and map isomorphically $\mathcal{E}((\mathbf{G}^{(a)})^{\mathsf{F}^{(a)}},1)$ to $\mathcal{E}(\mathbf{G}^{\mathsf{F}^a},1)$. Now a group of adjoint type is a direct product of restriction of scalars of simple groups. Let us take a look at the behavior of $(d,1)$-series with respect to restriction of scalars.

Proposition 3.2.4. *Let $a \in \mathbb{N}^*$. We have a bijection between the $(d,1)$-series in $\mathcal{E}((\boldsymbol{G}^{(a)})^{\mathsf{F}^{(a)}},1)$ and the $(d/\gcd(d,a),1)$-series in $\mathcal{E}(\boldsymbol{G}^{\mathsf{F}^a},1)$.*

Proof. If p is a prime number, then

$$\Phi_n(x^p) = \begin{cases} \Phi_{pn}(x) & \text{if } p \mid n, \\ \Phi_{pn}(x)\Phi_n(x) & \text{otherwise.} \end{cases}$$

From that we can deduce what is $\Phi_n(x^a)$. We write $a = a_n a'_n$, with a'_n relatively prime with n and all the prime numbers dividing a_n also divide n. Then we have

$$\Phi_n(x^a) = \prod_{k \mid a'_n} \Phi_{ka_n n}(x).$$

Let us prove that $\Phi_d(x)$ divides $\Phi_n(x^a)$ if and only if $n = d/\gcd(d,a)$.

First assume that $n = d/\gcd(d,a)$. Hence, we want to prove that there exists $k \mid a'_n$ such that $ka_n = \gcd(d,a)$. If $p^e \mid a_n$, then $p \mid n = d/\gcd(d,a)$. So, $\nu_p(d) \geq \nu_p(a)$, where ν_p is the p-adic valuation. Hence,

$v_p(\gcd(d,a)) = v_p(a) = v_p(a_n)$. Thus $a_n \mid \gcd(d,a)$. Let $k = \gcd(d,a)/a_n$. It remains to prove that $k \mid a'_n$. We have that $k \mid a$ and if $p \mid k$, then $p \nmid a_n$ since it would imply that $v_p(\gcd(d,a)) = v_p(a) = v_p(a_n)$ and a contradiction. Hence $k \mid a'_n$.

Now, let us assume that there exist n and k, such that $k \mid a'_n$ and $ka_n n = d$. We want to prove that $n = d/\gcd(d,a)$. It is enough to prove that $ka_n = \gcd(d,a)$. First $k \mid a'_n$ and since a_n and a'_n are relatively prime, $k \mid a$. We also have that $ka_n \mid d$, thus $ka_n \mid \gcd(d,a)$. Now, if $p^e \mid \gcd(d,a)$, then $p^e \mid a = a_n a'_n$. If $p^e \mid a_n$, then $p^e \mid ka_n$. If not, $p^e \mid a'_n$. Thus $p \nmid n$. But since $p^e \mid d = ka_n n$, we have that $p^e \mid k$ and $p^e \mid ka_n$. We conclude that $ka_n = \gcd(d,a)$.

We have just proved that $\Phi_d(x) \mid \Phi_n(x^a)$ if and only if $n = d/\gcd(d,a)$. As a result, if $\mathbf{T}'$ is a torus in $\mathbf{G}^{(a)}$, then $\mathbf{T}'$ is a d-torus in $\mathbf{G}^{(a)}$ if and only if it is the maximal d-subtorus of $\mathbf{T}^{(a)}$, for $\mathbf{T}$ a $d/\gcd(d,a)$-torus of $\mathbf{G}$. Thus the d-split Levi subgroup of $\mathbf{G}^{(a)}$ are of the form $\mathbf{L}^{(a)}$ for $\mathbf{L}$ a $d/\gcd(d,a)$-split Levi subgroup of $\mathbf{G}$. We then conclude the proof with the following commutative diagram of [4, Proposition 1.37]:

$$\begin{array}{ccc} \mathbb{Z}\mathcal{E}((\mathbf{G}^{(a)})^{\mathsf{F}^{(a)}}, 1) & \xrightarrow{\sim} & \mathbb{Z}\mathcal{E}(\mathbf{G}^{\mathsf{F}^a}, 1) \\ {\scriptstyle \mathcal{R}^{\mathbf{G}^{(a)}}_{\mathbf{L}^{(a)}}}\uparrow & & \uparrow{\scriptstyle \mathcal{R}^{\mathbf{G}}_{\mathbf{L}}} \\ \mathbb{Z}\mathcal{E}((\mathbf{L}^{(a)})^{\mathsf{F}^{(a)}}, 1) & \xrightarrow{\sim} & \mathbb{Z}\mathcal{E}(\mathbf{L}^{\mathsf{F}^a}, 1) \end{array}$$

□

To compute the $(d,1)$-series of $\mathcal{E}(\mathsf{G},1)$, Proposition 3.2.3 allows us to reduce to the case where G is adjoint. Now, an adjoint group can be written as a product of restriction of scalars of simple groups. The $(d,1)$-series of a direct product is the product of the $(d,1)$-series. Hence by Proposition 3.2.4, we can compute the unipotent $(d,1)$-series of G, if we know them for simple groups. This is what we do in the following sections.

3.3. ***Computation of $(d,1)$-series for type A_n and ${}^2A_n$.*** In this section, we want to compute the unipotent $(d,1)$-series for groups of type $\boldsymbol{A}_n$ and ${}^2\boldsymbol{A}_n$.

Let us start by explaining what the d-series are. First, let G be of type $\boldsymbol{A}_n$. The unipotent characters are in bijection with partitions of $n+1$. On partitions, there is the well defined notion of d-hook and of d-core; see for example [16, Chapter 2.7]. The proof of Theorem 3.2 in [4] then shows the following proposition.

Proposition 3.3.1. *The d-cuspidal unipotent characters are precisely those where the partition is itself a d-core. Moreover, two characters are in the same d-series if and only if they have the same d-core.*

In order to get the result for groups of type ${}^2\boldsymbol{A}_n$, we will use an "Ennola"-duality. We use here the notation of [4]. Let $\mathbb{G} = (\Gamma, W\phi)$ be a generic finite reductive group [4, Section 1.A]. We can then define $\mathbb{G}^-$ by

$$\mathbb{G}^- := (\Gamma, W(-\phi)).$$

To $\mathbb{G}$ we can associate a finite set $\mathrm{Uch}(\mathbb{G})$ [4, Theorem 1.26] which is in bijection with the set of unipotent characters of $\mathsf{G} = \mathbb{G}(q)$.

Theorem 3.3.2 [4, Theorem 3.3]. *There exists a natural bijective isometry $\sigma^{\mathbb{G}} : \mathbb{Z}\,\mathrm{Uch}(\mathbb{G}) \to \mathbb{Z}\,\mathrm{Uch}(\mathbb{G}^-)$ such that whenever $\mathbb{L}$ is d-split for some d, the following diagram is commutative*:

$$\begin{array}{ccc} \mathbb{Z}\,\mathrm{Uch}(\mathbb{G}) & \xrightarrow{\sigma^{\mathbb{G}}} & \mathbb{Z}\,\mathrm{Uch}(\mathbb{G}^-) \\ \mathcal{R}_{\mathbb{L}}^{\mathbb{G}} \uparrow & & \mathcal{R}_{\mathbb{L}^-}^{\mathbb{G}^-} \uparrow \\ \mathbb{Z}\,\mathrm{Uch}(\mathbb{L}) & \xrightarrow{\sigma^{\mathbb{L}}} & \mathbb{Z}\,\mathrm{Uch}(\mathbb{L}^-) \end{array}$$

Note that if $\mathbb{G}(q)$ is of rational type $(\boldsymbol{A}_n, q)$ then $\mathbb{G}^-(q)$ is of rational type $({}^2\boldsymbol{A}_n, q)$. In particular, we see that the unipotent characters for ${}^2\boldsymbol{A}_n$ are still parametrized by partitions of $n+1$. If $\mathbb{T}$ is a generic torus with polynomial order $\Phi_d(x)$, $\mathbb{T}^-$ has polynomial order $\Phi_d(-x)$. The map $\mathbb{L} \mapsto \mathbb{L}^-$ is a bijection between $\Phi_d(x)$-subgroup of ${}^2\boldsymbol{A}_n$ and $\Phi_d(-x)$-subgroup of $\boldsymbol{A}_n$. Now, for $d > 2$, we have that $\Phi_d(-x) = \Phi_{2d}(x)$ if d is odd, $\Phi_d(-x) = \Phi_{d/2}(x)$ if d is congruent to 2 modulo 4 and $\Phi_d(-x) = \Phi_d(x)$ if d is divisible by 4. Let d' be the integer defined by

$$d' = \begin{cases} 2d & \text{if } d \text{ is odd,} \\ d/2 & \text{if } d \equiv 2 \pmod 4, \\ d & \text{if } d \equiv 0 \pmod{4k}. \end{cases}$$

By Theorem 3.3.2 the d-series of ${}^2\boldsymbol{A}_n$ correspond to d'-series of $\boldsymbol{A}_n$ which are given by Proposition 3.3.1.

Remark 3.3.3. If d is the order of q modulo ℓ then d' is the order of $-q$ modulo ℓ.

In both cases, it is very important to be able to compute hooks and cores of partitions. In order to make the computation easier, and also to match with the following Section 3.4, we will use the notion of a β-set instead of a partition.

A β-set is a subset $\lambda \subseteq \mathbb{N}$, and we will write $\lambda = (x_1\, x_2\, \cdots\, x_a)$ with $x_1 < x_2 < \cdots < x_a$. We define the rank of a β-set by $\mathrm{rank}(\lambda) = \sum_{i=1}^{a} x_i - a(a-1)/2$. We define an equivalence relation on the β-sets by $(x_1\, x_2\, \cdots\, x_a) \sim (0\, x_1 + 1\, x_2 + 1\, \cdots\, x_a + 1)$. The rank is invariant by this equivalence relation hence can be extended to equivalence classes. Now, a partition $a_1 \leq \cdots \leq a_k$ of $n+1$ can be sent to a β-set of rank $n+1$ defined by $\lambda = (a_1\, a_2 + 1\, a_3 + 2\, \cdots\, a_k + (k-1))$ and this gives us a bijection between partitions of $n+1$ and equivalence classes of β-set of rank $n+1$.

Let λ and λ' be two β-sets. We say that λ' is obtained from λ by a d-hook if there exists $x \in \lambda$ such that $x - d \notin \lambda$ and $\lambda' = \lambda \setminus \{x\} \cup \{x - d\}$. The d-core of λ is then the β-set without d-hook obtained from λ by repetitively removing d-hooks.

Lemma 3.3.4 [16, Lemma 2.7.13]. *Let λ, λ' be two β-sets and α, α' be two partitions corresponding respectively to λ, λ'. Then α' is obtained from α by a d-hook if and only if λ' is obtained from λ by a d-hook.*

Now we have everything we need to compute the unipotent $(d, 1)$-series for type $\boldsymbol{A}_n$ and ${}^2\boldsymbol{A}_n$.

For a group G of type $\boldsymbol{A}_n$, this is easy because there is no unipotent cuspidal representation. Hence, there is only one unipotent 1-series $\mathcal{E}(G, 1)$ which is thus a $(d, 1)$-series.

Proposition 3.3.5. *If G is of type* $\boldsymbol{A}_n$, $\mathcal{E}(G, 1)$ *is a* $(d, 1)$*-series.*

Now, we assume that G is of type ${}^2\boldsymbol{A}_n$. We saw previously that two β-sets are in the same d-series if and only if they have the same d'-core and that they are in the same 1-series if and only if they have the same 2-core.

Remark 3.3.6. As we will see below, there are two different behaviors of the $(d, 1)$-series depending on the parity of d'. When we will apply these results to ℓ-modular representations theory, d will be the order of q modulo ℓ. The primes ℓ such that d' is even are called *linear* and when d' is odd they are called *unitary*.

The first case to consider is when d' is even (linear prime case). We then have the following result.

Proposition 3.3.7. *If* d' *is even* (*linear prime case*) *then the unipotent* $(d, 1)$*-series for type* ${}^2\boldsymbol{A}_n$ *are the unipotent* 1*-series.*

Proof. If d' is even, removing a d'-hook to a β-set can be obtained by removing $d'/2$ 2-hooks, hence the unipotent $(d, 1)$-series are the unipotent 1-series. □

Now, let us assume that d' is odd (unitary prime case).

Let λ be a β-set with finite cardinal. Let o be the number of odd numbers in λ and e be the number of even numbers. We define the defect of λ by $\mathrm{defect}(\lambda) = o - e$ if $o \geq e$ and $e - o - 1$ if $o < e$. The defect is invariant under the equivalence relation and we extend it to equivalence classes.

The 2-core of a β-set is of the form $(1\,3 \cdots 2k+1)$ (possibly $\varnothing$) which all have different defect. Moreover, removing a 2-hook does not change the defect of a β-set, so the defect of a β-set determines its 2-core, hence it characterizes the 1-series. Adding a 2-hook increase the rank of a β-set by 2. Therefore, we get the following lemma.

Lemma 3.3.8. *There exists a* β*-set of rank* m *and defect* k *if and only if* $m - k(k+1)/2$ *is even and positive.*

Let $[\lambda]$ be an equivalence class of β-sets. We define $\max([\lambda])$ to be 0 if $(0) \in [\lambda]$ and $\max([\lambda]) := \max(\lambda')$ where λ' is the unique β-set in $[\lambda]$ such that $0 \notin \lambda'$ if $(0) \notin [\lambda]$. Then $\max([\lambda])$ is the length of the largest hook in $[\lambda]$.

Lemma 3.3.9. *Let* $k \geq 0$ *and* $m \geq 1$ *such that* $m - k(k+1)/2$ *is even and positive. We have*

$$\max\{\max([\lambda]), \mathrm{defect}(\lambda) = k, \mathrm{rank}(\lambda) = m\} = \begin{cases} m - (k^2 - 3k + 2)/2 & \text{if } k \geq 1, \\ m & \text{if } k = 0. \end{cases}$$

Proof. A β-set of rank m and defect k is obtained by $1/2(m - k(k+1)/2)$ 2-hooks from $(1\,3 \cdots (2k-1))$. Each 2-hook increase the maximum of the coefficients by at most 2, giving us the result. □

Definition 3.3.10. Let us define for G of type ${}^2\boldsymbol{A}_n$,

$$k(\mathsf{G}, d) := \max\{k \geq 1, (k^2 - 3k + 2)/2 \leq n + 1 - d\}$$

if it exists and -1 otherwise.

From Lemma 3.3.9, $k(\mathsf{G}, d)$ is the greatest integer k such that there exists λ of defect k and rank $n+1$ having a hook of length at least d. In particular, if λ has defect $k > k(\mathsf{G}, d)$ and rank $n+1$ then it is a d-core.

Proposition 3.3.11. *Assume that d' is odd (unitary prime case) and G is of type ${}^2\boldsymbol{A}_n$. Then, the unipotent 1-series with defect strictly greater than $k(\mathsf{G}, d')$ are $(d, 1)$-series, composed uniquely of d-cuspidal representations, and the union of the unipotent 1-series with defect lower or equal to $k(\mathsf{G}, d')$ is a $(d, 1)$-series.*

Proof. The β-sets of rank $n+1$ and defect strictly greater than $k(\mathsf{G}, d')$ are all d'-core. Therefore the corresponding unipotent characters are d-cuspidal. Thus the unipotent 1-series with defect strictly greater than $k(\mathsf{G}, d')$ are $(d, 1)$-series.

Since $\mathcal{E}(\mathsf{G}, 1)$ is a $(d, 1)$-set, we have that the union of the unipotent 1-series with defect lower or equal to $k(\mathsf{G}, d')$ is a $(d, 1)$-set. It remains to prove that it is a $(d, 1)$-series. Let $k \leq k(\mathsf{G}, d')$. Let us assume that $k \geq 3$. Let $\lambda := (1\,3\,\cdots\,(2k-3)\,(n+1-(k^2-3k+2)/2))$ be a β-set of defect k and rank $n+1$. Let u be an odd number, $1 \leq u \leq 2k-3$ such that $u+d' \neq n+1-(k^2-3k+2)/2-d'$ (such a u exists since there are more than two odd numbers between 1 and $2k-3$). Let $\lambda' := (1\,3\,\cdots\,u+d'\,\cdots\,(2k-3)\,(n+1-(k^2-3k+2)/2-d'))$ (with a possible permutation of the coefficients so that they are written in the correct order). The β-set λ' is obtain from λ by removing a d'-hook and then adding a d'-hook. Hence λ and λ' are in the same d-series. Since d' is odd, if $k \geq 4$ then $\mathrm{defect}(\lambda') = k-4$ and if $k = 3$, $\mathrm{defect}(\lambda') = 0$. Hence the unipotent 1-series with defect $k \geq 4$ are in the same $(d, 1)$-series as the unipotent 1-series with defect $k-4$. We have the same result for defects 0 and 3. Thus to prove the result, we are left with the 1-series of defect 1 and 2. By Lemma 3.3.8, depending on the parity of n, we can only have simultaneously β-sets of rank $n+1$ and defects 0, 3 or defects 1, 2. Therefore, we need to prove that, if they exist, the β-sets with defects 1, 2 are in the same $(d, 1)$-series.

If there are β-sets of rank $n+1$ with defects 1, 2. We start by assuming that $n \neq 4$. Either $n \neq 2d'$ or $n \neq 4+2d'$. If $n \neq 2d'$ then we take $\lambda = (1\,n+1)$ and $\lambda' = (1+d'\,n+1-d')$, with $\mathrm{defect}(\lambda) = 2$ and $\mathrm{defect}(\lambda') = 1$. If $n \neq 4+2d'$ then we take $\lambda = (3\,n-1)$ and $\lambda' = (3+d'\,n-1-d')$, with $\mathrm{defect}(\lambda) = 2$ and $\mathrm{defect}(\lambda') = 1$ (we can note here that we can well assume that $d' \leq n-1$ because if not then $d' \geq (n+1)$ and we can use the previous case since $n \neq 2d'$). So we are left with $n = 4$. We can then have $d' = 1, 3$ or 5. If $d' = 1$, every β-set has the same 1-core, so the result follows. If $d' = 3$, we take $\lambda = (1\,3\,4)$ and $\lambda' = (1\,2\,3\,5)$. Finally, if $d' = 5$ we take $\lambda = (5)$ and $\lambda' = (1\,5)$. □

In the case d' odd, We will write $\mathcal{E}_1^d(\mathsf{G})$ for the union of the unipotent 1-series of defect lower or equal to $k(\mathsf{G}, d')$. Thus, if it is not empty, $\mathcal{E}_1^d(\mathsf{G})$ is the unipotent $(d, 1)$-series containing the trivial representation.

3.4. *Computation of $(d, 1)$-series for classical groups.* In this section we compute the unipotent $(d, 1)$-series for groups of type $\boldsymbol{B}_n$, $\boldsymbol{C}_n$, $\boldsymbol{D}_n$ and ${}^2\boldsymbol{D}_n$.

Just as before, let us start by studying d-series. When G is a classical group we have a classification of unipotent characters with the notion of symbols that we recall here. Furthermore, with these symbols, we can describe the decomposition into d-series of Theorem 3.1.1.

A symbol is an unordered set $\{S, T\}$ of two subsets $S, T \subseteq \mathbb{N}$. We write such a symbol in the following way

$$\Sigma = \begin{pmatrix} x_1 & \cdots & x_a \\ y_1 & \cdots & y_b \end{pmatrix}$$

with $x_1 < \cdots < x_a$, $y_1 < \cdots < y_b$ and $S = \{x_1, \ldots, x_a\}$, $T = \{y_1, \ldots, y_b\}$. Two symbols are said to be equivalent if they can be transformed into each other by a sequence of steps

$$\begin{pmatrix} x_1 & \cdots & x_a \\ y_1 & \cdots & y_b \end{pmatrix} \sim \begin{pmatrix} 0 & x_1+1 & \cdots & x_a+1 \\ 0 & y_1+1 & \cdots & y_b+1 \end{pmatrix}$$

or by interchanging the rows.

We define the defect of Σ by $\mathrm{defect}(\Sigma) = |a-b|$ and its rank by

$$\mathrm{rank}(\Sigma) = \sum_{i=1}^{a} x_i + \sum_{i=1}^{b} y_i - \left[\left(\frac{a+b-1}{2}\right)^2\right].$$

These two notions can be defined on the equivalence classes of symbols.

If G is a group of type $\boldsymbol{B}_n$, $\boldsymbol{C}_n$, $\boldsymbol{D}_n$ or ${}^2\boldsymbol{D}_n$, Lusztig has shown that the unipotent characters may be parametrized by these symbols; see [21]. The unipotent characters of groups of type $\boldsymbol{B}_n$ or $\boldsymbol{C}_n$ are in bijection with the equivalence classes of symbols of rank n and odd defect. For the groups of type $\boldsymbol{D}_n$, the unipotent characters are parametrized by classes of symbols of rank n and defect divisible by 4 (except that if the two rows are identical, two characters correspond to the same symbol). And the unipotent characters of groups of type ${}^2\boldsymbol{D}_n$ are in bijection with symbols of rank n and defect congruent 2 $(\mathrm{mod}\, 4)$.

Let $\{S, T\}$ be a symbol and $d \geq 1$ an integer. If there exists $x \in S$ such that $x + d \notin S$, or $y \in T$ with $y + d \notin T$, then the symbol $\{S \setminus \{x\} \cup \{x+d\}, T\}$ or $\{S, T \setminus \{y\} \cup \{y+d\}\}$, is said to be obtained from $\{S, T\}$ by adding a d-hook. We define the d-core of $\{S, T\}$ as the symbol $\{U, V\}$ without d-hook obtained from $\{S, T\}$ by removing a sequence of d-hooks.

In the same way, if there exists $x \in S$ such that $x + d \notin T$, or $y \in T$ with $y + d \notin S$, then the symbol $\{S \setminus \{x\}, T \cup \{x+d\}\}$ or $\{S \cup \{y+d\}, T \setminus \{y\}\}$, is said to be obtained from $\{S, T\}$ by adding a d-cohook. And we define like previously the d-cocore of $\{S, T\}$.

Proposition 3.4.1. (1) *If d is odd, then the d-cuspidal unipotent characters are precisely those where Σ is itself a d-core. Moreover, two characters are in the same d-series if and only if they have the same d-core.*

(2) *If d is even, then the d-cuspidal unipotent characters are precisely those where Σ is itself a $d/2$-cocore. Moreover, two characters are in the same d-series if and only if they have the same $d/2$-cocore.*

Proof. This is proved in the proof of Theorem 3.2 in [4]. □

Now let us compute the unipotent $(d, 1)$-series. The first case is when d is odd (the linear prime case). To obtain the d-series we need to take the d-core of the symbols by the Proposition 3.4.1. We also obtain the 1-series by taking the 1-core. But two symbols which have the same d-core have the same 1-core, so each unipotent 1-series is a $(d, 1)$-series.

Proposition 3.4.2. *If d is odd (linear prime case), the unipotent $(d, 1)$-series are the unipotent 1-series.*

Now, assume that d is even (unitary prime case). This case is a little bit more complicated because we need to take the $d/2$-cocore for the d-series and the 1-core for the 1-series. We will do a proof similar to the case of ${}^2\boldsymbol{A}_n$ done in Section 3.3.

Let Σ be a symbol. We define $\max(\Sigma)$ to be $\max(\Sigma) := 0$ if $\Sigma \sim \{\varnothing, \varnothing\}$, and otherwise $\max(\Sigma) := \max(S \cup T)$ where $\{S, T\}$ is the unique symbol equivalent to Σ with $0 \notin S \cap T$. Note that $\max(\Sigma)$ is the longest length of a hook or cohook in Σ.

Lemma 3.4.3. *Let $k \geq 0$ and $n \geq 1$ such that $n \geq (k^2-1)/4$. We have*

$$\max\{\max(\Sigma), \operatorname{defect}(\Sigma) = k, \operatorname{rank}(\Sigma) = n\} = \begin{cases} n - (k^2 - 4k + 3)/4 & \text{if } k \text{ is odd}, \\ n - (k^2 - 4k + 4)/4 & \text{if } k \text{ is even}, k \neq 0, \\ n & \text{if } k = 0. \end{cases}$$

Proof. Every symbol of defect k is obtained from $\Sigma_k = \left(\begin{smallmatrix} 0 & \cdots & k-1 \end{smallmatrix}\right)$, for $k \geq 1$, and $\Sigma_0 = \{\varnothing, \varnothing\}$, for $k = 0$, by adding 1-hooks. Each 1-hook increases the rank of 1. So in order to get a symbol of rank n, we need to do $m := n - \operatorname{rank}(\Sigma_k)$ 1-hooks. Note that, for $k \geq 1$,

$$\operatorname{rank}(\Sigma_k) = \frac{(k-1)k}{2} - \left[\left(\frac{k-1}{2}\right)^2\right] = \begin{cases} (k^2-1)/4 & \text{if } k \text{ is odd}, \\ k^2/4 & \text{if } k \text{ is even}, \end{cases}$$

and $\operatorname{rank}(\Sigma_0) = 0$. Remark also, that the hypothesis $n \geq (k^2-1)/4$ is equivalent to $m \geq 0$. Each 1-hook increases the maximum of the coefficients by at most one, so $\max\{\max(\Sigma), \operatorname{defect}(\Sigma) = k\} = k - 1 + m$, for $k \geq 1$, and m for $k = 0$ (we have equality by adding the 1-hooks on the last coefficient on the top row). □

Let us define an integer $k(\mathsf{G}, d)$ in the following way.

Definition 3.4.4. If G is of type $\boldsymbol{B}_n$ or $\boldsymbol{C}_n$ we define

$$k(\mathsf{G}, d) = \max\{k \geq 1, k \text{ odd}, (k^2 - 4k + 3)/4 \leq n - d/2\}$$

if it exists and $k(\mathsf{G}, d) = -1$ otherwise.

If G is of type $\boldsymbol{D}_n$ or ${}^2\boldsymbol{D}_n$ then in the same way

$$k(\mathsf{G}, d) = \max\{k \geq 2, k \text{ even}, (k^2 - 4k + 4)/4 \leq n - d/2\}$$

if it exists and $k(\mathsf{G}, d) = -1$ otherwise.

As in the case of ${}^2\boldsymbol{A}_n$, by Lemma 3.4.3 we see that $k(\mathsf{G}, d)$ is the greatest integer k such that there exists Σ of defect k and rank n having a cohook of length at least d. In particular, if $\mathrm{defect}(\Sigma) > k(\mathsf{G}, d)$ then Σ is a d-cocore.

Remark 3.4.5. Two symbols are in the same 1-series if and only if they have the same 1-core by Proposition 3.4.1. But removing a 1-hook does not change the defect of a symbol. Hence, every symbol in a 1-series has the same defect. Moreover, the 1-core of a symbol is of the form $\binom{0\ \cdots\ k-1}{}$ where k is the defect of the symbol (or $\{\varnothing, \varnothing\}$ when the defect is 0). Hence, two symbols are in the same 1-series if and only if they have the same defect. And the defect associated with a 1-series is the defect of the cuspidal representation associated to this 1-series.

We have the following partition of $\mathcal{E}(\mathsf{G}, 1)$ into $(d, 1)$-series.

Proposition 3.4.6. *If d is even (unitary prime case), the unipotent 1-series with defect strictly greater than $k(\mathsf{G}, d)$ are $(d, 1)$-series, composed uniquely of d-cuspidal representations, and the union of the unipotent 1-series with defect lower or equal to $k(\mathsf{G}, d)$ is a $(d, 1)$-series.*

Proof. Let $k > k(\mathsf{G}, d)$ and a unipotent 1-series with defect k. Then by definition of $k(\mathsf{G}, d)$ and with Lemma 3.4.3, $d/2$ is strictly greater than every coefficient in every symbol in the 1-series chosen. Hence, this 1-series is composed of d-cuspidal representations, so is a $(d, 1)$-series.

We also deduce from that, that the union of the unipotent 1-series with defect lower or equal to $k(\mathsf{G}, d)$ is a $(d, 1)$-set. It remains to prove that this is a $(d, 1)$-series. Let $3 \leq k \leq k(\mathsf{G}, d)$ such that there is a unipotent 1-series with defect k. We want to prove that the unipotent 1-series with defect k is in the same $(d, 1)$-series as a unipotent 1-series with defect strictly less than k, which will finish the proof. Let $\Sigma_k = \binom{0\ \cdots\ k-1}{}$ and $m = n - \mathrm{rank}(\Sigma_k)$ as in the proof of Lemma 3.4.3. Then the symbol

$$\Sigma = \begin{pmatrix} 0 & \cdots & k-2 & k-1+m \\ & & & \end{pmatrix}$$

has defect k and rank n so is in the 1-series chosen. Now by definition of $k(\mathsf{G}, d)$, $d/2 \leq k-1+m$, we can then remove a $d/2$-cohook from Σ to get

$$\Sigma' = \begin{pmatrix} 0 & \cdots & k-2 \\ k-1+m-d/2 & & \end{pmatrix}.$$

Let $v \in \{0, \ldots, k-2\}$ such that $v + d/2 \neq k-1+m-d/2$. Then we can add a $d/2$-cohook to Σ' to obtain

$$\Sigma'' = \begin{pmatrix} 0 & \cdots & v-1 & v+1 & \cdots & k-2 \\ k-1+m-d/2 & v+d/2 & & & & \end{pmatrix}$$

(we possibly have to swap the numbers in the lower row so that they are written in the good order). The symbol Σ'' is a symbol of defect $k-4$ if $k > 3$ and $k-2$ if $k = 3$, which has the same $d/2$-cocore as Σ. Hence, Σ and Σ are in the same $(d, 1)$-series, and $\mathrm{defect}(\Sigma') < \mathrm{defect}(\Sigma)$. □

As before, when d is even, we write $\mathcal{E}_1^d(\mathsf{G})$ for the union of the 1-series of defect lower or equal to $k(\mathsf{G}, d)$, which is, if not empty, the $(d, 1)$-series containing the trivial representation.

3.5. ***Computation of* $(d, 1)$*-series for exceptional groups.*** We have computed the unipotent $(d, 1)$-series for groups of type $\boldsymbol{A}$ and for classical groups. We are left with groups of exceptional type, that is of type ${}^3\boldsymbol{D}_4$, $\boldsymbol{G}_2$, $\boldsymbol{F}_4$, $\boldsymbol{E}_6$, ${}^2\boldsymbol{E}_6$, $\boldsymbol{E}_7$ and $\boldsymbol{E}_8$.

Unfortunately, we do not have a nice classification with partitions or symbols like for groups of types $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$ and $\boldsymbol{D}$. However, since we are working with groups with bounded rank, we can do a case by case analysis. We will summarize the result in Tables 1 and 2. We need to explain the notations used. To keep the notation as simple as possible, we are writing the unipotent $(d, 1)$-series in terms of 1-series. We will write a 1-series by the corresponding 1-cuspidal representation of the 1-split Levi defining this series. The notations for the cuspidal representations are the notations of [8, Section 13.9]. So for example for $\boldsymbol{F}_4$, we have a (2,1)-series

$$\{1, \boldsymbol{B}_2, \boldsymbol{F}_4[-1], \boldsymbol{F}_4[i], \boldsymbol{F}_4''[1]\}.$$

This set is composed of the principal series (denoted by 1), the characters coming from the unipotent cuspidal character of $\boldsymbol{B}_2$ (denoted by $\boldsymbol{B}_2$) and 3 cuspidal representations of $\boldsymbol{F}_4$:

$$\boldsymbol{F}_4[-1], \quad \boldsymbol{F}_4[i] \quad \text{and} \quad \boldsymbol{F}_4''[1].$$

Thus

$$\{1, \boldsymbol{B}_2, \boldsymbol{F}_4[-1], \boldsymbol{F}_4[i], \boldsymbol{F}_4''[1]\}$$

denotes a set composed of 33 unipotent characters.

If a d does not appear in Tables 1 and 2, it means that the unipotent $(d, 1)$-series are the unipotent 1-series.

Proposition 3.5.1. *The unipotent* $(d, 1)$*-series for groups of exceptional types are written in the Tables 1 and 2.*

Proof. In [8, Section 13.9] we can find tables for the unipotent characters of groups of exceptional types and the partitions into 1-series. So to compute the unipotent $(d, 1)$-series, we need to know about the d-series. In [4], we find in Tables 1 and 2 a list of the d-series $\mathcal{E}(\mathsf{G}, (\mathsf{L}, \lambda))$, where (L, λ) is a unipotent d-cuspidal pair and L is not a torus. So we are missing the cases of L a torus (hence λ is trivial). However, in the case $\mathsf{L} = \mathsf{T}$ of a torus, the Deligne–Lusztig induction $\mathcal{R}_{\mathsf{T}}^{\mathsf{G}}$ is known by the work of Lusztig. Hence combining all the computations, we prove the results of Tables 1 and 2. □

3.6. ***Summary for unipotent* $(d, 1)$*-series.*** In this section, we summarize all the computations of the unipotent $(d, 1)$-series.

First let us recall some definition. For an integer d we define d' by

$$d' = \begin{cases} 2d & \text{if } d \text{ is odd,} \\ d/2 & \text{if } d \equiv 2 \pmod 4, \\ d & \text{if } d \equiv 0 \pmod 4. \end{cases}$$

group	d	unipotent $(d, 1)$-series
$\boldsymbol{G}_2$	2	$\{1, \boldsymbol{G}_2[1], \boldsymbol{G}_2[-1]\}, \{\boldsymbol{G}_2[\theta]\}, \{\boldsymbol{G}_2[\theta^2]\}$
	3	$\{1, \boldsymbol{G}_2[1], \boldsymbol{G}_2[\theta], \boldsymbol{G}_2[\theta^2]\}, \{\boldsymbol{G}_2[-1]\}$
	6	$\{1, \boldsymbol{G}_2[-1], \boldsymbol{G}_2[\theta], \boldsymbol{G}_2[\theta^2]\}, \{\boldsymbol{G}_2[1]\}$
${}^3\boldsymbol{D}_4$	2, 6	$\{1, {}^3\boldsymbol{D}_4[1], {}^3\boldsymbol{D}_4[-1]\}$
	3	$\{1, {}^3\boldsymbol{D}_4[1]\}, \{{}^3\boldsymbol{D}_4[-1]\}$
	12	$\{1, {}^3\boldsymbol{D}_4[-1]\}, \{{}^3\boldsymbol{D}_4[1]\}$
$\boldsymbol{F}_4$	2	$\{1, \boldsymbol{B}_2, \boldsymbol{F}_4[-1], \boldsymbol{F}_4[i], \boldsymbol{F}_4''[1]\}, \{\boldsymbol{F}_4[-i]\}, \{\boldsymbol{F}_4[\theta]\}, \{\boldsymbol{F}_4[\theta^2]\}, \{\boldsymbol{F}_4'[1]\}$
	3	$\{1, \boldsymbol{F}_4[\theta], \boldsymbol{F}_4[\theta^2], \boldsymbol{F}_4'[1]\}, \{\boldsymbol{B}_2\}, \{\boldsymbol{F}_4[-i]\}, \{\boldsymbol{F}_4[-1]\}, \{\boldsymbol{F}_4[i]\}, \{\boldsymbol{F}_4''[1]\}$
	4	$\{1, \boldsymbol{B}_2, \boldsymbol{F}_4[-i], \boldsymbol{F}_4[i], \boldsymbol{F}_4'[1], \boldsymbol{F}_4''[1]\}, \{\boldsymbol{F}_4[-1]\}, \{\boldsymbol{F}_4[\theta]\}, \{\boldsymbol{F}_4[\theta^2]\}$
	6	$\{1, \boldsymbol{B}_2, \boldsymbol{F}_4[-1], \boldsymbol{F}_4[\theta], \boldsymbol{F}_4[\theta^2], \boldsymbol{F}_4'[1]\}, \{\boldsymbol{F}_4[-i]\}, \{\boldsymbol{F}_4[i]\}, \{\boldsymbol{F}_4''[1]\}$
	8	$\{1, \boldsymbol{F}_4[-1], \boldsymbol{F}_4[-i], \boldsymbol{F}_4[i]\}, \{\boldsymbol{B}_2\}, \{\boldsymbol{F}_4'[1]\}, \{\boldsymbol{F}_4[\theta]\}, \{\boldsymbol{F}_4[\theta^2]\}, \{\boldsymbol{F}_4''[1]\}$
	12	$\{1, \boldsymbol{B}_2, \boldsymbol{F}_4[-i], \boldsymbol{F}_4[i], \boldsymbol{F}_4[\theta], \boldsymbol{F}_4[\theta^2]\}, \{\boldsymbol{F}_4[-1]\}, \{\boldsymbol{F}_4'[1]\}, \{\boldsymbol{F}_4''[1]\}$
$\boldsymbol{E}_6$	2, 4, 8	$\{1, \boldsymbol{D}_4\}, \{\boldsymbol{E}_6[\theta]\}, \{\boldsymbol{E}_6[\theta^2]\}$
	3, 9	$\{1, \boldsymbol{E}_6[\theta], \boldsymbol{E}_6[\theta^2]\}, \{\boldsymbol{D}_4\}$
	5	$\{1\}, \{\boldsymbol{D}_4\}, \{\boldsymbol{E}_6[\theta]\}, \{\boldsymbol{E}_6[\theta^2]\}$
	6, 12	$\{1, \boldsymbol{D}_4, \boldsymbol{E}_6[\theta], \boldsymbol{E}_6[\theta^2]\}$
$\boldsymbol{E}_7$	2, 10, 14	$\{1, \boldsymbol{D}_4, \boldsymbol{E}_7[\xi], \boldsymbol{E}_7[-\xi]\}, \{\boldsymbol{E}_6[\theta]\}, \{\boldsymbol{E}_6[\theta^2]\}$
	3, 9	$\{1, \boldsymbol{E}_6[\theta], \boldsymbol{E}_6[\theta^2]\}, \{\boldsymbol{D}_4\}, \{\boldsymbol{E}_7[\xi]\}, \{\boldsymbol{E}_7[-\xi]\}$
	4, 8	$\{1, \boldsymbol{D}_4\}, \{\boldsymbol{E}_6[\theta]\}, \{\boldsymbol{E}_6[\theta^2]\}, \{\boldsymbol{E}_7[\xi]\}, \{\boldsymbol{E}_7[-\xi]\}$
	5, 7	$\{1\}, \{\boldsymbol{D}_4\}, \{\boldsymbol{E}_6[\theta]\}, \{\boldsymbol{E}_6[\theta^2]\}, \{\boldsymbol{E}_7[\xi]\}, \{\boldsymbol{E}_7[-\xi]\}$
	6, 18	$\{1, \boldsymbol{D}_4, \boldsymbol{E}_6[\theta], \boldsymbol{E}_6[\theta^2], \boldsymbol{E}_7[\xi], \boldsymbol{E}_7[-\xi]\}$
	12	$\{1, \boldsymbol{D}_4, \boldsymbol{E}_6[\theta], \boldsymbol{E}_6[\theta^2]\}, \{\boldsymbol{E}_7[\xi]\}, \{\boldsymbol{E}_7[-\xi]\}$
$\boldsymbol{E}_8$	2	$\{1, \boldsymbol{D}_4, \boldsymbol{E}_7[\xi], \boldsymbol{E}_7[-\xi], \boldsymbol{E}_8[-1], \boldsymbol{E}_8'[1], \boldsymbol{E}_8''[1]\}, \{\boldsymbol{E}_6[\theta], \boldsymbol{E}_8[-\theta], \boldsymbol{E}_8[\theta]\},$ $\{\boldsymbol{E}_6[\theta^2], \boldsymbol{E}_8[\theta^2], \boldsymbol{E}_8[-\theta^2]\}, \{\boldsymbol{E}_8[-i]\}, \{\boldsymbol{E}_8[\zeta^4]\}, \{\boldsymbol{E}_8[\zeta^3]\}, \{\boldsymbol{E}_8[\zeta^2]\}, \{\boldsymbol{E}_8[\zeta]\}, \{\boldsymbol{E}_8[i]\}$
	3	$\{1, \boldsymbol{E}_6[\theta], \boldsymbol{E}_6[\theta^2], \boldsymbol{E}_8[\theta^2], \boldsymbol{E}_8[\theta], \boldsymbol{E}_8'[1]\}, \{\boldsymbol{D}_4, \boldsymbol{E}_8[-1], \boldsymbol{E}_8[-\theta^2], \boldsymbol{E}_8[-\theta]\},$ $\{\boldsymbol{E}_7[-\xi]\}, \{\boldsymbol{E}_7[\xi]\}, \{\boldsymbol{E}_8''[1]\}, \{\boldsymbol{E}_8[-i]\}, \{\boldsymbol{E}_8[\zeta^4]\}, \{\boldsymbol{E}_8[\zeta^3]\}, \{\boldsymbol{E}_8[\zeta^2]\}, \{\boldsymbol{E}_8[\zeta]\}, \{\boldsymbol{E}_8[i]\}$
	4	$\{1, \boldsymbol{D}_4, \boldsymbol{E}_8[-i], \boldsymbol{E}_8[i], \boldsymbol{E}_8'[1], \boldsymbol{E}_8''[1]\}, \{\boldsymbol{E}_7[-\xi]\}, \{\boldsymbol{E}_7[\xi]\}, \{\boldsymbol{E}_6[\theta]\}, \{\boldsymbol{E}_6[\theta^2]\}, \{\boldsymbol{E}_8[\zeta^4]\},$ $\{\boldsymbol{E}_8[\zeta^3]\}, \{\boldsymbol{E}_8[\zeta^2]\}, \{\boldsymbol{E}_8[\zeta]\}, \{\boldsymbol{E}_8[-1]\}, \{\boldsymbol{E}_8[-\theta]\}, \{\boldsymbol{E}_8[\theta]\}, \{\boldsymbol{E}_8[\theta^2]\}, \{\boldsymbol{E}_8[-\theta^2]\}$
	5	$\{1, \boldsymbol{E}_8[\zeta^4], \boldsymbol{E}_8[\zeta^3], \boldsymbol{E}_8[\zeta^2], \boldsymbol{E}_8[\zeta], \boldsymbol{E}_8'[1]\}, \{\boldsymbol{E}_7[-\xi]\}, \{\boldsymbol{E}_7[\xi]\}, \{\boldsymbol{D}_4\}, \{\boldsymbol{E}_6[\theta]\}, \{\boldsymbol{E}_6[\theta^2]\},$ $\{\boldsymbol{E}_8[-i]\}, \{\boldsymbol{E}_8[i]\}, \{\boldsymbol{E}_8''[1]\}, \{\boldsymbol{E}_8[-1]\}, \{\boldsymbol{E}_8[-\theta]\}, \{\boldsymbol{E}_8[\theta]\}, \{\boldsymbol{E}_8[\theta^2]\}, \{\boldsymbol{E}_8[-\theta^2]\}$
	6	$\{1, \boldsymbol{E}_7[-\xi], \boldsymbol{E}_7[\xi], \boldsymbol{D}_4, \boldsymbol{E}_6[\theta], \boldsymbol{E}_6[\theta^2], \boldsymbol{E}_8[-1], \boldsymbol{E}_8[-\theta^2], \boldsymbol{E}_8[-\theta], \boldsymbol{E}_8[\theta^2],$ $\boldsymbol{E}_8[\theta], \boldsymbol{E}_8'[1], \boldsymbol{E}_8''[1]\}, \{\boldsymbol{E}_8[-i]\}, \{\boldsymbol{E}_8[\zeta^4]\}, \{\boldsymbol{E}_8[\zeta^3]\}, \{\boldsymbol{E}_8[\zeta^2]\}, \{\boldsymbol{E}_8[\zeta]\}, \{\boldsymbol{E}_8[i]\}$

Table 1. Unipotent $(d, 1)$-series for groups of exceptional types.

We also have defined $k(\mathsf{G}, d)$ by

$$k(\mathsf{G}, d) = \begin{cases} \max\{k \geq 1, (k^2 - 3k + 2)/2 \leq n + 1 - d\} & \text{for type } {}^2\boldsymbol{A}_n, \\ \max\{k \geq 1, k \text{ odd}, (k^2 - 4k + 3)/4 \leq n - d/2\} & \text{for types } \boldsymbol{B}_n, \boldsymbol{C}_n, \\ \max\{k \geq 2, k \text{ even}, (k^2 - 4k + 4)/4 \leq n - d/2\} & \text{for types } \boldsymbol{D}_n, {}^2\boldsymbol{D}_n, \end{cases}$$

if it exists and -1 otherwise.

group	d	unipotent $(d, 1)$-series
$\boldsymbol{E}_8$	7	$\{1\}, \{\boldsymbol{D}_4\}, \{\boldsymbol{E}_7[-\xi]\}, \{\boldsymbol{E}_7[\xi]\}, \{\boldsymbol{E}_6[\theta]\}, \{\boldsymbol{E}_6[\theta^2]\}, \{\boldsymbol{E}_8[-i]\}, \{\boldsymbol{E}_8[i]\}, \{\boldsymbol{E}'_8[1]\}, \{\boldsymbol{E}''_8[1]\}, \{\boldsymbol{E}_8[\zeta^4]\}, \{\boldsymbol{E}_8[\zeta^3]\}, \{\boldsymbol{E}_8[\zeta^2]\}, \{\boldsymbol{E}_8[\zeta]\}, \{\boldsymbol{E}_8[-1]\}, \{\boldsymbol{E}_8[-\theta]\}, \{\boldsymbol{E}_8[\theta]\}, \{\boldsymbol{E}_8[\theta^2]\}, \{\boldsymbol{E}_8[-\theta^2]\}$
	8	$\{1, \boldsymbol{D}_4, \boldsymbol{E}_8[-1], \boldsymbol{E}_8[-i], \boldsymbol{E}_8[i]\}, \{\boldsymbol{E}_7[-\xi]\}, \{\boldsymbol{E}_7[\xi]\}, \{\boldsymbol{E}_6[\theta]\}, \{\boldsymbol{E}_6[\theta^2]\}, \{\boldsymbol{E}_8[\zeta^4]\}, \{\boldsymbol{E}_8[\zeta^3]\}, \{\boldsymbol{E}_8[\zeta^2]\}, \{\boldsymbol{E}_8[\zeta]\}, \{\boldsymbol{E}'_8[1]\}, \{\boldsymbol{E}_8[-\theta]\}, \{\boldsymbol{E}_8[\theta]\}, \{\boldsymbol{E}_8[\theta^2]\}, \{\boldsymbol{E}_8[-\theta^2]\}, \{\boldsymbol{E}''_8[1]\}$
	9	$\{1, \boldsymbol{E}_6[\theta], \boldsymbol{E}_6[\theta^2]\}, \{\boldsymbol{D}_4\}, \{\boldsymbol{E}_7[-\xi]\}, \{\boldsymbol{E}_7[\xi]\}, \{\boldsymbol{E}_8[-i]\}, \{\boldsymbol{E}_8[i]\}, \{\boldsymbol{E}'_8[1]\}, \{\boldsymbol{E}''_8[1]\}, \{\boldsymbol{E}_8[\zeta^4]\}, \{\boldsymbol{E}_8[\zeta^3]\}, \{\boldsymbol{E}_8[\zeta^2]\}, \{\boldsymbol{E}_8[\zeta]\}, \{\boldsymbol{E}_8[-1]\}, \{\boldsymbol{E}_8[-\theta]\}, \{\boldsymbol{E}_8[\theta]\}, \{\boldsymbol{E}_8[\theta^2]\}, \{\boldsymbol{E}_8[-\theta^2]\}$
	10	$\{1, \boldsymbol{E}_7[-\xi], \boldsymbol{E}_7[\xi], \boldsymbol{D}_4, \boldsymbol{E}_8[-1], \boldsymbol{E}_8[\zeta^4], \boldsymbol{E}_8[\zeta^3], \boldsymbol{E}_8[\zeta^2], \boldsymbol{E}_8[\zeta], \boldsymbol{E}''_8[1]\}, \{\boldsymbol{E}_6[\theta]\}, \{\boldsymbol{E}_6[\theta^2]\}, \{\boldsymbol{E}_8[-i]\}, \{\boldsymbol{E}_8[i]\}, \{\boldsymbol{E}'_8[1]\}, \{\boldsymbol{E}_8[-\theta]\}, \{\boldsymbol{E}_8[\theta]\}, \{\boldsymbol{E}_8[\theta^2]\}, \{\boldsymbol{E}_8[-\theta^2]\}$
	12	$\{1, \boldsymbol{D}_4, \boldsymbol{E}_6[\theta], \boldsymbol{E}_6[\theta^2], \boldsymbol{E}_8[-1], \boldsymbol{E}_8[-\theta^2], \boldsymbol{E}_8[-\theta], \boldsymbol{E}_8[-i], \boldsymbol{E}_8[\theta^2], \boldsymbol{E}_8[\theta], \boldsymbol{E}_8[i], \boldsymbol{E}''_8[1]\}, \{\boldsymbol{E}_7[-\xi]\}, \{\boldsymbol{E}_7[\xi]\}, \{\boldsymbol{E}'_8[1]\}, \{\boldsymbol{E}_8[\zeta^4]\}, \{\boldsymbol{E}_8[\zeta^3]\}, \{\boldsymbol{E}_8[\zeta^2]\}, \{\boldsymbol{E}_8[\zeta]\}$
	14	$\{1, \boldsymbol{E}_7[-\xi], \boldsymbol{E}_7[\xi], \boldsymbol{D}_4\}, \{\boldsymbol{E}_6[\theta]\}, \{\boldsymbol{E}_6[\theta^2]\}, \{\boldsymbol{E}_8[-i]\}, \{\boldsymbol{E}_8[i]\}, \{\boldsymbol{E}'_8[1]\}, \{\boldsymbol{E}''_8[1]\}, \{\boldsymbol{E}_8[\zeta^4]\}, \{\boldsymbol{E}_8[\zeta^3]\}, \{\boldsymbol{E}_8[\zeta^2]\}, \{\boldsymbol{E}_8[\zeta]\}, \{\boldsymbol{E}_8[-1]\}, \{\boldsymbol{E}_8[-\theta]\}, \{\boldsymbol{E}_8[\theta]\}, \{\boldsymbol{E}_8[\theta^2]\}, \{\boldsymbol{E}_8[-\theta^2]\}$
	15	$\{1, \boldsymbol{E}_6[\theta], \boldsymbol{E}_6[\theta^2], \boldsymbol{E}_8[\theta^2], \boldsymbol{E}_8[\theta], \boldsymbol{E}_8[\zeta^4], \boldsymbol{E}_8[\zeta^3], \boldsymbol{E}_8[\zeta^2], \boldsymbol{E}_8[\zeta]\}, \{\boldsymbol{D}_4\}, \{\boldsymbol{E}_7[-\xi]\}, \{\boldsymbol{E}_7[\xi]\}, \{\boldsymbol{E}_8[-i]\}, \{\boldsymbol{E}_8[i]\}, \{\boldsymbol{E}'_8[1]\}, \{\boldsymbol{E}''_8[1]\}, \{\boldsymbol{E}_8[-1]\}, \{\boldsymbol{E}_8[-\theta]\}, \{\boldsymbol{E}_8[-\theta^2]\}$
	18	$\{1, \boldsymbol{E}_7[-\xi], \boldsymbol{E}_7[\xi], \boldsymbol{D}_4, \boldsymbol{E}_6[\theta], \boldsymbol{E}_6[\theta^2], \boldsymbol{E}_8[-\theta^2], \boldsymbol{E}_8[-\theta], \boldsymbol{E}_8[\theta^2], \boldsymbol{E}_8[\theta]\}, \{\boldsymbol{E}_8[-i]\}, \{\boldsymbol{E}_8[i]\}, \{\boldsymbol{E}'_8[1]\}, \{\boldsymbol{E}''_8[1]\}, \{\boldsymbol{E}_8[\zeta^4]\}, \{\boldsymbol{E}_8[\zeta^3]\}, \{\boldsymbol{E}_8[\zeta^2]\}, \{\boldsymbol{E}_8[\zeta]\}, \{\boldsymbol{E}_8[-1]\}$
	20	$\{1, \boldsymbol{D}_4, \boldsymbol{E}_8[-i], \boldsymbol{E}_8[\zeta^4], \boldsymbol{E}_8[\zeta^3], \boldsymbol{E}_8[\zeta^2], \boldsymbol{E}_8[\zeta], \boldsymbol{E}_8[i]\}, \{\boldsymbol{E}_7[-\xi]\}, \{\boldsymbol{E}_7[\xi]\}, \{\boldsymbol{E}_6[\theta]\}, \{\boldsymbol{E}_6[\theta^2]\}, \{\boldsymbol{E}'_8[1]\}, \{\boldsymbol{E}''_8[1]\}, \{\boldsymbol{E}_8[-1]\}, \{\boldsymbol{E}_8[-\theta]\}, \{\boldsymbol{E}_8[\theta]\}, \{\boldsymbol{E}_8[\theta^2]\}, \{\boldsymbol{E}_8[-\theta^2]\}$
	24	$\{1, \boldsymbol{D}_4, \boldsymbol{E}_6[\theta], \boldsymbol{E}_6[\theta^2], \boldsymbol{E}_8[-\theta^2], \boldsymbol{E}_8[-\theta], \boldsymbol{E}_8[-i], \boldsymbol{E}_8[i]\}, \{\boldsymbol{E}_7[-\xi]\}, \{\boldsymbol{E}_7[\xi]\}, \{\boldsymbol{E}'_8[1]\}, \{\boldsymbol{E}''_8[1]\}, \{\boldsymbol{E}_8[\zeta^4]\}, \{\boldsymbol{E}_8[\zeta^3]\}, \{\boldsymbol{E}_8[\zeta^2]\}, \{\boldsymbol{E}_8[\zeta]\}, \{\boldsymbol{E}_8[-1]\}, \{\boldsymbol{E}_8[\theta]\}, \{\boldsymbol{E}_8[\theta^2]\}$
	30	$\{1, \boldsymbol{E}_7[-\xi], \boldsymbol{E}_7[\xi], \boldsymbol{D}_4, \boldsymbol{E}_6[\theta], \boldsymbol{E}_6[\theta^2], \boldsymbol{E}_8[-\theta^2], \boldsymbol{E}_8[-\theta], \boldsymbol{E}_8[\zeta^4], \boldsymbol{E}_8[\zeta^3], \boldsymbol{E}_8[\zeta^2], \boldsymbol{E}_8[\zeta]\}, \{\boldsymbol{E}_8[-i]\}, \{\boldsymbol{E}_8[i]\}, \{\boldsymbol{E}'_8[1]\}, \{\boldsymbol{E}''_8[1]\}, \{\boldsymbol{E}_8[-1]\}, \{\boldsymbol{E}_8[\theta]\}, \{\boldsymbol{E}_8[\theta^2]\}$
${}^2\boldsymbol{E}_6$	2	$\{1, {}^2\boldsymbol{A}_5, {}^2\boldsymbol{E}_6[1]\}, \{{}^2\boldsymbol{E}_6[\theta]\}, \{{}^2\boldsymbol{E}_6[\theta^2]\}$
	3	$\{1, {}^2\boldsymbol{E}_6[1], {}^2\boldsymbol{E}_6[\theta], {}^2\boldsymbol{E}_6[\theta^2]\}, \{{}^2\boldsymbol{A}_5\}$
	4	$\{1, {}^2\boldsymbol{E}_6[1]\}, \{{}^2\boldsymbol{A}_5\}, \{{}^2\boldsymbol{E}_6[\theta]\}, \{{}^2\boldsymbol{E}_6[\theta^2]\}$
	6	$\{1, {}^2\boldsymbol{A}_5, {}^2\boldsymbol{E}_6[1], {}^2\boldsymbol{E}_6[\theta], {}^2\boldsymbol{E}_6[\theta^2]\}$
	8	$\{1\}, \{{}^2\boldsymbol{A}_5\}, \{{}^2\boldsymbol{E}_6[1]\}, \{{}^2\boldsymbol{E}_6[\theta]\}, \{{}^2\boldsymbol{E}_6[\theta^2]\}$
	10	$\{1, {}^2\boldsymbol{A}_5\}, \{{}^2\boldsymbol{E}_6[1]\}, \{{}^2\boldsymbol{E}_6[\theta]\}, \{{}^2\boldsymbol{E}_6[\theta^2]\}$
	12	$\{1, {}^2\boldsymbol{E}_6[\theta], {}^2\boldsymbol{E}_6[\theta^2]\}, \{{}^2\boldsymbol{A}_5\}, \{{}^2\boldsymbol{E}_6[1]\}$
	18	$\{1, {}^2\boldsymbol{A}_5, {}^2\boldsymbol{E}_6[\theta], {}^2\boldsymbol{E}_6[\theta^2]\}, \{{}^2\boldsymbol{E}_6[1]\}$

Table 2. Unipotent $(d, 1)$-series for groups of exceptional types.

Theorem 3.6.1. *The unipotent* $(d, 1)$*-series are given by the following cases*:

(1) *Type* $\boldsymbol{A}_n$: $\mathcal{E}(G, 1)$ *is a* $(d, 1)$*-series.*

(2) *Type* ${}^2\boldsymbol{A}_n$:

(a) d' *even* (*linear prime case*): *the unipotent* $(d, 1)$*-series are the unipotent* 1*-series.*

(b) d' *odd* (*unitary prime case*): *the* $(d, 1)$*-series are*,

- *the unipotent* 1*-series with defect strictly greater than* $k(G, d')$ (*composed uniquely of* d*-cuspidal representations*);
- $\mathcal{E}_1^d(G)$, *the union of the unipotent* 1*-series with defect lower or equal to* $k(G, d')$.

(3) *Type* $\boldsymbol{B}_n$, $\boldsymbol{C}_n$, $\boldsymbol{D}_n$ *and* ${}^2\boldsymbol{D}_n$:

(a) d *odd* (*linear prime case*): *the unipotent* $(d, 1)$*-series are the unipotent* 1*-series.*

(b) d *even* (*unitary prime case*): *the* $(d, 1)$*-series are*:

- *The unipotent* 1*-series with defect strictly greater than* $k(G, d)$ (*composed uniquely of* d*-cuspidal representations*).
- $\mathcal{E}_1^d(G)$, *the union of the unipotent* 1*-series with defect lower or equal to* $k(G, d)$.

(4) *Type* ${}^3\boldsymbol{D}_4$, $\boldsymbol{G}_2$, $\boldsymbol{F}_4$, $\boldsymbol{E}_6$, ${}^2\boldsymbol{E}_6$, $\boldsymbol{E}_7$ *and* $\boldsymbol{E}_8$: *the unipotent* $(d, 1)$*-series are given by Tables 1 and 2.*

3.7. ***Induction and restriction of*** $\boldsymbol{(d, 1)}$***-series.*** Now that we know how to compute the unipotent $(d, 1)$-series, we want to prove that they are compatible with Harish-Chandra induction and restriction. In particular, it will be fundamental in order to construct unipotent ℓ-blocks of p-adic groups, to prove that Harish-Chandra restriction commutes with taking the ℓ-extension of unipotent $(d, 1)$-series.

Let $\mathbf{M}$ be a F-stable Levi of $\mathbf{G}$ and $\mathcal{E}$ a subset of Irr(M). We denote by $\mathcal{R}^{\mathbf{G}}_{\mathbf{M}}(\mathcal{E})$ the set of irreducible characters π of G such that there exists $\sigma \in \mathcal{E}$ satisfying $\langle \pi, \mathcal{R}^{\mathbf{G}}_{\mathbf{M}\subseteq\mathbf{P}}(\sigma)\rangle \neq 0$, for $\mathbf{P}$ a parabolic subgroup admitting $\mathbf{M}$ as a Levi subgroup. When $\mathbf{M}$ is a 1-split Levi of $\mathbf{G}$, we will simply use the notation $i^{\mathsf{G}}_{\mathsf{M}}(\mathcal{E})$. In the same way, for any 1-split Levi $\mathbf{M}$ of $\mathbf{G}$ and $\mathcal{E}'$ a subset of Irr(G), $r^{\mathsf{G}}_{\mathsf{M}}(\mathcal{E}')$ denotes the set of characters σ such that there exists $\pi \in \mathcal{E}'$ satisfying $\langle \sigma, r^{\mathsf{G}}_{\mathsf{M}\subseteq\mathsf{P}}(\pi)\rangle \neq 0$.

The $(d, 1)$-series are a union of 1-series and of d-series. We know that the Harish-Chandra induction of a 1-series is included in a 1-series. But there is no nice result for the Harish-Chandra induction of a d-series. The following results have for goal to prove that the $(d, 1)$-series behave well regarding Harish-Chandra induction.

Lemma 3.7.1. *Let* $\mathbf{M}$ *be a* 1*-split Levi of* $\mathbf{G}$ *and* $\mathcal{E} \subseteq \mathcal{E}(M, 1)$ *a* $(d, 1)$*-series. Then* $i^{\mathsf{G}}_{M}(\mathcal{E})$ *is included in a* $(d, 1)$*-series.*

Proof. By Propositions 3.2.3 and 3.2.4, we can assume that $\mathbf{G}$ is simple:

(1) If $\mathbf{G}$ is of type $\boldsymbol{A}_n$, then $\mathcal{E}(\mathsf{G}, 1)$ is a $(d, 1)$-series so we have the result.

(2) If $\mathbf{G}$ is of type $\boldsymbol{B}_n$, $\boldsymbol{C}_n$, $\boldsymbol{D}_n$ or ${}^2\boldsymbol{D}_n$. The Levi $\mathbf{M}$ has type $\mathrm{GL}_{n_1} \times \cdots \times \mathrm{GL}_{n_r} \times \mathbf{H}$ where $\mathbf{H}$ as the same type as $\mathbf{G}$. We deduce that $\mathcal{E} \simeq \mathcal{E}(\mathrm{GL}_{n_1}(q), 1) \times \cdots \times \mathcal{E}(\mathrm{GL}_{n_r}(q), 1) \times \mathcal{E}_H$, where $\mathcal{E}_H$ is a $(d, 1)$-series of H. We need to differentiate the case d odd and d even.

If d is odd, then $\mathcal{E}_H$ is a 1-series by Proposition 3.4.2 and so is $\mathcal{E}$. The set $i^{\mathsf{G}}_{\mathsf{M}}(\mathcal{E})$ is thus included in a 1-series and so in a $(d, 1)$-series.

If d is even, then by Proposition 3.4.6, $\mathcal{E}_H$ is either a 1-series or $\mathcal{E}_H = \mathcal{E}_1^d(\mathsf{H})$, where $\mathcal{E}_1^d(\mathsf{H})$ is the union of the 1-series with defect lower or equal to $k(\mathsf{H}, d)$. If it is a 1-series, we have the result like previously. And if $\mathcal{E}_H = \mathcal{E}_1^d(\mathsf{H})$, since $k(\mathsf{H}, d) \leq k(\mathsf{G}, d)$ and the fact that the induction preserves the defect, $i^{\mathsf{G}}_{\mathsf{M}}(\mathcal{E}) \subseteq \mathcal{E}_1^d(\mathsf{G})$ which is a $(d, 1)$-series.

(3) If $\mathbf{G}$ is of type ${}^2\boldsymbol{A}_n$. Using "Ennola"-duality, $\mathbf{M}$ corresponds to a 2-split Levi of GL_n, and the unipotent $(d, 1)$-series correspond to $(d', 2)$-series. The proof is then the same as in (2) regarding that d' is odd or even.

(4) If $\mathbf{G}$ is of exceptional type. The proof mainly consists of checking case by case the result using Tables 1 and 2. We explain here the arguments to do so.

The first case to remark is when all the unipotent $(d, 1)$-series not containing the trivial representation are composed uniquely of 1-cuspidal representations. In this case, we have directly the result. This happens for approximately half the cases by looking at Tables 1 and 2 and deals completely with $\boldsymbol{G}_2$ and ${}^3\boldsymbol{D}_4$. Now, when d is odd, and the Levi $\mathbf{M}$ has only component of types $\boldsymbol{A}_n$, $\boldsymbol{B}_n$, $\boldsymbol{C}_n$, $\boldsymbol{D}_n$ or ${}^2\boldsymbol{D}_n$, we know that the unipotent $(d, 1)$-series are 1-series. Since the induction of a 1-series from a 1-split Levi is included in a 1-series, we get the result. This is enough to deal with $\boldsymbol{E}_6$. We also get the odd d for $\boldsymbol{E}_7$, respectively $\boldsymbol{E}_8$, by checking the compatibility from $\boldsymbol{E}_6$, respectively $\boldsymbol{E}_7$, thanks to Tables 1 and 2. The same argument works for ${}^2\boldsymbol{E}_6$ but when d' is even (we recall that d' is defined in Section 3.3). To finish $\boldsymbol{E}_7$ and $\boldsymbol{E}_8$, we need to look when d is even. In all these cases, the 1-series corresponding to the unipotent cuspidal representation of $\boldsymbol{D}_4$ is inside the $(d, 1)$-series containing the trivial representation. So we just have to check with Tables 1 and 2 the compatibility with $\boldsymbol{E}_6$ and $\boldsymbol{E}_7$. We are left with the last case of $\boldsymbol{F}_4$ and $d = 8$. But in this case Φ_8 does not appear in any of the polynomial orders of the 1-split-Levi, which concludes the proof. □

Lemma 3.7.2. *Let $\mathbf{M}$ be a 1-split Levi of $\mathbf{G}$ and $\mathcal{E} \subseteq \mathcal{E}(G, 1)$ a $(d, 1)$-series. Then $r_M^G(\mathcal{E})$ is a $(d, 1)$-set.*

Proof. Let $\sigma \in r_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E})$. There exists $\mathcal{E}'$ a unipotent $(d, 1)$-series in M such that $\sigma \in \mathcal{E}'$. We need to prove that $\mathcal{E}' \subseteq r_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E})$.

Since $\sigma \in r_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E})$, there exists $\pi \in \mathcal{E}$ such that $\langle \sigma, r_{\mathsf{M}}^{\mathsf{G}}(\pi)\rangle \neq 0$. By Frobenius reciprocity, $\langle i_{\mathsf{M}}^{\mathsf{G}}(\sigma), \pi\rangle \neq 0$, thus $\pi \in i_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E}')$. By Lemma 3.7.1, $i_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E}')$ is included in a $(d, 1)$-series, hence $i_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E}') \subseteq \mathcal{E}$. Again, by Frobenius reciprocity, we have that $\mathcal{E}' \subseteq r_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E})$ and the result follows. □

We have proved that the unipotent $(d, 1)$-series behave well with 1-induction. One may wonder if they also behave well with d-induction? This is what we are going to prove next. Actually, we will go further. We are going to check the compatibility with induction but from a $d\ell^a$-split Levi, for certain ℓ.

Lemma 3.7.3. *Assume that ℓ satisfies $(*)$ and let $\mathbf{M}$ be a $d\ell^a$-split Levi of $\mathbf{G}$ for some $a \geq 0$. Let $\mathcal{E} \subseteq \mathcal{E}(M, 1)$ be a $(d, 1)$-series. Then $\mathcal{R}_{\boldsymbol{M}}^{\boldsymbol{G}}(\mathcal{E})$ is included in a $(d, 1)$-series.*

Proof. By Propositions 3.2.3 and 3.2.4, we can assume that $\mathbf{G}$ is simple (notice that if b is an integer then $dl^a / \gcd(dl^a, b) = (d / \gcd(d, b))l^{a'}$, for some a' with $0 \leq a' \leq a$):

(1) If $\mathbf{G}$ is of type $\boldsymbol{A}_n$, then $\mathcal{E}(\mathsf{G}, 1)$ is a $(d, 1)$-series so we have the result.

(2) If $\mathbf{G}$ is of type $\boldsymbol{B}_n$, $\boldsymbol{C}_n$, $\boldsymbol{D}_n$ or ${}^2\boldsymbol{D}_n$. Then, as stated is the proof of [4, Theorem 3.2], the Levi $\mathbf{M}$ has type $\mathrm{GL}_{n_1}^{(dl^a)} \times \cdots \times \mathrm{GL}_{n_r}^{(dl^a)} \times \mathbf{H}$ where $\mathbf{H}$ as the same type as $\mathbf{G}$. Since $\mathcal{E}$ is a $(d, 1)$-series of M we know that $\mathcal{E} = \mathcal{E}(\mathrm{GL}_{n_1}(q^{dl^a}), 1) \times \cdots \times \mathcal{E}(\mathrm{GL}_{n_r}(q^{dl^a}), 1) \times \mathcal{E}_H$, where $\mathcal{E}_H$ is a $(d, 1)$-series of H.

Let us first assume that d is odd. Thus $\mathcal{E}_H$ is a 1-series in H by Proposition 3.4.2. Let $\pi = \pi_1 \otimes \cdots \otimes \pi_r \otimes \pi_H \in \mathcal{E}$. The representation π_H corresponds to a symbol of H. Now, $\mathcal{R}_{\mathbf{M}}^{\mathbf{G}}$ is the functor of $d\ell^a$-induction. Since $d\ell^a$ is odd, the proof of Theorem 3.2 of [4] shows that the symbols in $\mathcal{R}_{\mathbf{M}}^{\mathbf{G}}(\pi)$ are the symbols obtained from the symbol of π_H by adding $d\ell^a$-hooks. Thus all these symbols have the same 1-core which is the same as the 1-core of π_H. But $\mathcal{E}_{\mathsf{H}}$ is a 1-series, so all the representations have the same 1-core, hence this is also true for the representations in $\mathcal{R}_{\mathbf{M}}^{\mathbf{G}}(\mathcal{E})$. We have proved that $\mathcal{R}_{\mathbf{M}}^{\mathbf{G}}(\mathcal{E})$ is included in a 1-series and thus in a $(d, 1)$-series.

Now, let us prove the case where d is even. If $\mathbf{M} = \mathbf{G}$ there is nothing to do, so we can assume that $\mathbf{M}$ is proper in $\mathbf{G}$. The group $\mathbf{M}$ being a proper $d\ell^a$-split Levi of $\mathbf{G}$, none of the representations in $\mathcal{R}_{\mathbf{M}}^{\mathbf{G}}(\mathcal{E})$ are $d\ell^a$-cuspidal. Since $d\ell^a$ is even, by Proposition 3.4.6 we have that $\mathcal{R}_{\mathbf{M}}^{\mathbf{G}}(\mathcal{E}) \subseteq \mathcal{E}_1^{d\ell^a}(\mathsf{G})$, the $d\ell^a$-1-series of G containing the trivial representation. But $k(\mathsf{G}, d\ell^a) \leq k(\mathsf{G}, d)$. Hence, $\mathcal{E}_1^{d\ell^a}(\mathsf{G}) \subseteq \mathcal{E}_1^d(\mathsf{G})$ and we have the result.

(3) If $\mathbf{G}$ is of type ${}^2\boldsymbol{A}_n$, the proof is similar as in (2) using "Ennola"-duality and the parity of d' instead of d (notice that $(d\ell^a)' = (d')\ell^a$ since ℓ is odd).

(4) If $\mathbf{G}$ is of exceptional type, we will again use Tables 1 and 2.

Let us start with the case $a = 0$. So we are inducing $(d, 1)$-series from d-split Levis. If all the unipotent $(d, 1)$-series not containing the trivial representation are composed uniquely of d-cuspidal representations then we have the result. Tables 1 and 2 is written in terms of 1-series. However, we can look at Tables 1 and 2 from [4] to deduce the d-cuspidality. In these tables, the case where the d-split Levi is a torus is not written, but all the induced representations from a torus of the trivial representation will be in the $(d, 1)$-series containing the trivial. Hence, for a unipotent $(d, 1)$-series not containing the trivial representation, it is composed uniquely of d-cuspidal representations if none of the representations appears in Table 2 of [4]. This case deals with almost everyone except for $(\boldsymbol{E}_6, d = 3)$, $(\boldsymbol{E}_7, d = 2)$, $(\boldsymbol{E}_7, d = 3)$, $(\boldsymbol{E}_8, d = 2)$ and $(\boldsymbol{E}_8, d = 3)$. We can then check by hand the remaining case with Tables 1 and 2. Now, we need to do $a > 0$. There are only 8 cases which satisfies the hypotheses on ℓ, and such that Φ_d and $\Phi_{d\ell^a}$ divide the order of G. In all these cases, all the unipotent $(d, 1)$-series not containing the trivial representation are composed uniquely of $d\ell^a$-cuspidal representations, and so we have the result. □

Remark 3.7.4. We need the hypothesis on ℓ. For example, if $\ell = 3$, the group is ${}^3\boldsymbol{D}_4$, $d = 1$ and $a = 1$, then ${}^3\boldsymbol{D}_4[1]$ is in the induction of the trivial representation from the maximal 3-torus but is not in the same $(d, 1)$-series as the trivial.

We define, as in [6] $E_{q,\ell} := \{e, \ell \mid \phi_e(q)\} = \{d, d\ell, d\ell^2, \ldots, d\ell^a, \cdots\}$, where d is the order of q modulo ℓ. A $E_{q,\ell}$-torus is a F-stable torus of $\mathbf{G}$ such that its polynomial order is a product of cyclotomic polynomials in $\{\phi_e, e \in E_{q,\ell}\}$. A $E_{q,\ell}$-split Levi is then the centralizer of a $E_{q,\ell}$-torus.

For a F-stable Levi subgroup of $\mathbf{G}$, let us denote by $Z^\circ(\mathbf{M})$ the connected center of $\mathbf{M}$ and by $Z^\circ(\mathbf{M})_\ell^{\mathsf{F}}$ the subgroup of $Z^\circ(\mathbf{M})^{\mathsf{F}}$ of ℓ-elements.

Lemma 3.7.5. *Assume that ℓ satisfies $(*)$. Let $\mathbf{M}$ be a $E_{q,\ell}$-split Levi of $\mathbf{G}$ such that $\mathbf{M} = C_{\mathbf{G}}((Z^\circ(\mathbf{M})_\ell^{\mathsf{F}})^\circ$. Let $\mathcal{E}$ be a unipotent $(d, 1)$-series in M. Then $\mathcal{R}_{\mathbf{M}}^{\mathbf{G}}(\mathcal{E})$ is included in a $(d, 1)$-series.*

Proof. We will prove the result by induction on the semisimple rank of $\mathbf{G}$.

If $\mathbf{M} = \mathbf{G}$ nothing has to be done. Now, if $\mathbf{M}$ is a proper Levi in $\mathbf{G}$, then $Z^\circ(\mathbf{M})_\ell^{\mathsf{F}} \not\subseteq Z(\mathbf{G})$. Thus there exist some $a \geq 0$ such that $Z^\circ(\mathbf{M})_{\phi_{d\ell^a}} \not\subseteq Z(\mathbf{G})$, where $Z^\circ(\mathbf{M})_{\phi_{d\ell^a}}$ is the maximal $\Phi_{d\ell^a}$-subgroup of $Z^\circ(\mathbf{M})$. Let us denote by $\mathbf{L} := C_{\mathbf{G}}(Z^\circ(\mathbf{M})_{\phi_{d\ell^a}})$ which is then a proper $d\ell^a$-split Levi of $\mathbf{G}$ such that $\mathbf{M} \subseteq \mathbf{L}$. By Lemma 3.7.3, we know that $\mathcal{R}_{\mathbf{L}}^{\mathbf{G}}$ preserves the unipotent $(d, 1)$-series. By the induction hypothesis, $\mathcal{R}_{\mathbf{M}}^{\mathbf{L}}$ preserves the unipotent $(d, 1)$-series. Hence $\mathcal{R}_{\mathbf{M}}^{\mathbf{G}} = \mathcal{R}_{\mathbf{L}}^{\mathbf{G}} \circ \mathcal{R}_{\mathbf{M}}^{\mathbf{L}}$ preserves the unipotent $(d, 1)$-series. □

Remark 3.7.6. Let $\mathbf{M}$ be a $E_{q,\ell}$-split Levi of $\mathbf{G}$. If ℓ is good for $\mathbf{G}$ and $(Z(\mathbf{G})/Z^\circ(\mathbf{G}))^{\mathsf{F}}$ is of order prime to ℓ, then $\mathbf{M} = C_{\mathbf{G}}((Z^\circ(\mathbf{M})_\ell^{\mathsf{F}})^\circ$ by [6, Proposition 3.2].

Let $\mathcal{E}$ be a subset of $\mathcal{E}_\ell(\mathsf{G}, 1)$. We denote by $\bar{\mathcal{E}}$ the smallest $(d, 1)$-set containing $\mathcal{E}$. Thus Lemma 3.7.1 and 3.7.5 can be restated by $\overline{\mathcal{R}_{\mathbf{M}}^{\mathbf{G}}(\mathcal{E})}$ is a $(d, 1)$-series if $\mathbf{M}$ is a 1-split Levi or a $E_{q,\ell}$-split Levi (satisfying the conditions of Lemma 3.7.5) and $\mathcal{E}$ is a unipotent $(d, 1)$-series of M.

Lemma 3.7.7. *Let $\mathbf{M}, \mathbf{K}, \mathbf{L}, \mathbf{G}$ be groups such that $\mathbf{M}$ is a 1-split Levi of $\mathbf{K}$, $\mathbf{L}$ is a 1-split Levi of $\mathbf{G}$, $\mathbf{M}$ is a $E_{q,\ell}$-split Levi of $\mathbf{L}$ and $\mathbf{K}$ is a $E_{q,\ell}$-split Levi of $\mathbf{G}$. We also assume that ℓ satisfies $(*)$ and that the groups $\mathbf{M}$ and $\mathbf{K}$ satisfy the condition of Lemma 3.7.5. If $\mathcal{E}$ is a $(d, 1)$-series of M then $\overline{\mathcal{R}_{\mathbf{K}}^{\mathbf{G}}(\mathcal{R}_{\mathbf{M}}^{\mathbf{K}}(\mathcal{E}))} = \overline{\mathcal{R}_{\mathbf{L}}^{\mathbf{G}}(\mathcal{R}_{\mathbf{M}}^{\mathbf{L}}(\mathcal{E}))}$.*

Proof. Be Lemma 3.7.5 and Lemma 3.7.1, we know that $\mathcal{R}_{\mathbf{K}}^{\mathbf{G}}(\mathcal{R}_{\mathbf{M}}^{\mathbf{K}}(\mathcal{E}))$ is included in a $(d, 1)$-series and $\mathcal{R}_{\mathbf{L}}^{\mathbf{G}}(\mathcal{R}_{\mathbf{M}}^{\mathbf{L}}(\mathcal{E}))$ is included in a $(d, 1)$-series. Now, since $\mathcal{R}_{\mathbf{M}}^{\mathbf{G}} = \mathcal{R}_{\mathbf{K}}^{\mathbf{G}} \circ \mathcal{R}_{\mathbf{M}}^{\mathbf{K}} = \mathcal{R}_{\mathbf{L}}^{\mathbf{G}} \circ \mathcal{R}_{\mathbf{M}}^{\mathbf{L}}$, these two $(d, 1)$-series both contain $\mathcal{R}_{\mathbf{M}}^{\mathbf{G}}(\mathcal{E})$, hence they are equal. □

Remark 3.7.8. Note that this lemma does not follow directly from the transitivity of the Deligne–Lusztig induction. Indeed, for a set $\mathcal{E}$, the set $\mathcal{R}_{\mathbf{L}}^{\mathbf{G}}(\mathcal{R}_{\mathbf{M}}^{\mathbf{L}}(\mathcal{E}))$ might be larger that $\mathcal{R}_{\mathbf{M}}^{\mathbf{G}}(\mathcal{E})$.

Lemma 3.7.9. *Let ℓ be a good prime. Let $\mathbf{L}$ be a $E_{q,\ell}$-split Levi of $\mathbf{G}$ such that $\mathbf{L} = C_{\mathbf{G}}((Z^\circ(\mathbf{L})_\ell^{\mathsf{F}})^\circ$. Let $\mathbf{L}^*$ be a Levi in $\mathbf{G}^*$ in duality with $\mathbf{L}$. Then $\mathbf{L}^*$ is a $E_{q,\ell}$-split Levi of $\mathbf{G}^*$ such that $\mathbf{L}^* = C_{\mathbf{G}^*}((Z^\circ(\mathbf{L}^*)_\ell^{\mathsf{F}})^\circ$.*

Proof. We adapt the proof of [5, Proposition 1.4]. Let $\mathbf{L}^*$ be a Levi in $\mathbf{G}^*$ in duality with $\mathbf{L}$. Let $\mathbf{M}^* := C_{\mathbf{G}^*}((Z^\circ(\mathbf{L}^*)_\ell^{\mathsf{F}})^\circ$. We have that $\mathbf{L}^* \subseteq \mathbf{M}^*$, and since ℓ is good, $\mathbf{M}^*$ is a Levi subgroup by [5, Proposition 2.1(ii)]. We have that $Z^\circ(\mathbf{L}^*)_\ell^{\mathsf{F}} = Z^\circ(\mathbf{M}^*)_\ell^{\mathsf{F}}$.

Let $\mathbf{M}$ be a dual Levi such that $\mathbf{L} \subseteq \mathbf{M} \subseteq \mathbf{G}$. We have that $Z^\circ(\mathbf{M})_\ell^{\mathsf{F}} \subseteq Z^\circ(\mathbf{L})_\ell^{\mathsf{F}}$. But, by [8, Proposition 4.4.5], $|Z^\circ(\mathbf{M})^{\mathsf{F}}| = |Z^\circ(\mathbf{M}^*)^{\mathsf{F}}|$ and $|Z^\circ(\mathbf{L})^{\mathsf{F}}| = |Z^\circ(\mathbf{L}^*)^{\mathsf{F}}|$, thus $Z^\circ(\mathbf{M})_\ell^{\mathsf{F}} = Z^\circ(\mathbf{L})_\ell^{\mathsf{F}}$. So, $\mathbf{M} \subseteq C_{\mathbf{G}}((Z^\circ(\mathbf{L})_\ell^{\mathsf{F}})^\circ = \mathbf{L}$ and $\mathbf{M} = \mathbf{L}$. □

Let ℓ be a good prime for $\mathbf{G}$. Let $t \in \mathsf{G}^*$ a semisimple element of order a power of ℓ. Then $C_{\mathbf{G}^*}(t)^\circ$ is a Levi subgroup, and denote by $\mathbf{G}(t)$ a Levi in $\mathbf{G}$ dual to $C_{\mathbf{G}^*}(t)^\circ$.

Since t is a central element of $(C_{\mathbf{G}^*}(t)^\circ)^{\mathsf{F}}$, by [11, Proposition 13.30], there exist a linear character $\hat{t} \in \mathrm{Irr}(\mathsf{G}(t))$ such that the tensor product with $\hat{t}$ defines a bijection from $\mathcal{E}(\mathsf{G}(t), 1)$ to $\mathcal{E}(\mathsf{G}(t), t)$.

Let $\pi \in \mathcal{E}(\mathsf{G}, t)$. By the Jordan decomposition in the case of nonconnected center (defined in [23]) there exists $\pi_t \in \mathcal{E}(\mathsf{G}(t), 1)$ such that

$$\varepsilon_{\mathsf{G}}\varepsilon_{\mathbf{G}(t)}\mathcal{R}^{\mathsf{G}}_{\mathbf{G}(t)}(\hat{t}\pi_t) = \sum_{\pi' \in C\cdot\pi} \pi',$$

where π' runs over the orbit of π under the action of $C := C_{\mathbf{G}^*}(t)^{\mathsf{F}}/(C_{\mathbf{G}^*}(t)^\circ)^{\mathsf{F}}$, and ε_{G} and $\varepsilon_{\mathsf{G}(t)}$ are signs defined in [23, Proposition 5.1].

Remark 3.7.10. Let M be a 1-split Levi of G and $t \in \mathsf{M}^*$. Then there exists $\mathsf{M}(t)$ a Levi in M dual to $C_{\mathsf{M}^*}(t)^\circ$ which is a 1-split Levi of $\mathsf{G}(t)$ (the intersection of a 1-split Levi subgroup with a maximal rank subgroup is a 1-split Levi of the subgroup by [11, Proposition 2.2]).

Lemma 3.7.11. *Let $\boldsymbol{M}$ be a 1-split Levi subgroup of $\boldsymbol{G}$. Let t be a semisimple element of M^*, of order a power of ℓ, $\sigma \in \mathcal{E}(M, t)$, and $\pi \in \mathcal{E}(G, t)$ such that $\langle \pi, \mathcal{R}^{\boldsymbol{G}}_{\boldsymbol{M}}(\sigma)\rangle \neq 0$.*

Let $\sigma_t \in \mathcal{E}(M(t), 1)$ corresponding to σ by the Jordan decomposition. Then, there exists $\pi_t \in \mathcal{E}(G(t), 1)$, such that π_t corresponds to π by the Jordan decomposition and $\langle \pi_t, \mathcal{R}^{\boldsymbol{G}(t)}_{\boldsymbol{M}(t)}(\sigma_t)\rangle \neq 0$.

Proof. Let us write $\mathcal{R}^{\mathbf{G}(t)}_{\mathbf{M}(t)}(\hat{t}\sigma_t)$ as a sum of irreducible characters $\mathcal{R}^{\mathbf{G}(t)}_{\mathbf{M}(t)}(\hat{t}\sigma_t) = \sum_i n_i\pi_i$, with $n_i \in \mathbb{N}$ and π_i irreducible (note that since $\mathbf{M}(t)$ is a 1-split Levi subgroup of $\mathbf{G}(t)$, $\mathcal{R}^{\mathbf{G}(t)}_{\mathbf{M}(t)}$ is the usual Harish-Chandra induction, thus all the n_i are positive). Then we have that $\mathcal{R}^{\mathbf{G}}_{\mathbf{G}(t)}(\mathcal{R}^{\mathbf{G}(t)}_{\mathbf{M}(t)}(\hat{t}\sigma_t)) = \sum_i n_i\mathcal{R}^{\mathbf{G}}_{\mathbf{G}(t)}(\pi_i)$. By the "Jordan decomposition", each $\mathcal{R}^{\mathbf{G}}_{\mathbf{G}(t)}(\pi_i)$ is, up to a sign independent of π_i, a sum of irreducible characters of an orbit in $\mathcal{E}(\mathsf{G}, t)$ under the action of $C_{\mathbf{G}^*}(t)^{\mathsf{F}}/(C_{\mathbf{G}^*}(t)^\circ)^{\mathsf{F}}$. Hence, up to a sign, $\mathcal{R}^{\mathbf{G}}_{\mathbf{G}(t)}(\mathcal{R}^{\mathbf{G}(t)}_{\mathbf{M}(t)}(\hat{t}\sigma_t))$ is a sum with positive coefficients of irreducible characters of G.

Now, we have that $\mathcal{R}^{\mathbf{G}}_{\mathbf{G}(t)}(\mathcal{R}^{\mathbf{G}(t)}_{\mathbf{M}(t)}(\hat{t}\sigma_t)) = \mathcal{R}^{\mathbf{G}}_{\mathbf{M}(t)}(\hat{t}\sigma_t) = \mathcal{R}^{\mathbf{G}}_{\mathbf{M}}(\mathcal{R}^{\mathbf{M}}_{\mathbf{M}(t)}(\hat{t}\sigma_t))$.

We have that $\varepsilon_{\mathsf{M}}\varepsilon_{\mathsf{M}(t)}\mathcal{R}^{\mathbf{M}}_{\mathbf{M}(t)}(\hat{t}\sigma_t) = \sum_{\sigma' \in C\cdot\sigma} \sigma'$. Thus $\varepsilon_{\mathsf{M}}\varepsilon_{\mathsf{M}(t)}\mathcal{R}^{\mathbf{G}}_{\mathbf{M}}(\mathcal{R}^{\mathbf{M}}_{\mathbf{M}(t)}(\hat{t}\sigma_t)) = \sum_{\sigma' \in C\cdot\sigma} \mathcal{R}^{\mathbf{G}}_{\mathbf{M}}(\sigma')$. Like before, $\mathcal{R}^{\mathbf{G}}_{\mathbf{M}}$ is the usual Harish-Chandra induction, so it is a positive sum of characters. By hypothesis, $\langle \pi, \mathcal{R}^{\mathbf{G}}_{\mathbf{M}}(\sigma)\rangle \neq 0$, thus $\langle \pi, \mathcal{R}^{\mathbf{G}}_{\mathbf{M}(t)}(\hat{t}\sigma_t)\rangle \neq 0$.

Hence, there exists i_0 such that $n_{i_0} \neq 0$ and $\langle \pi, \mathcal{R}^{\mathbf{G}}_{\mathbf{G}(t)}(\pi_{i_0})\rangle \neq 0$. Take π_t, such that $\hat{t}\pi_t = \pi_{i_0}$. This π_t satisfies the conditions of the lemma. □

We remind the reader that for $\mathcal{E}$ a subset of $\mathcal{E}_\ell(\mathsf{G}, 1)$, the set $\bar{\mathcal{E}}$ denote the smallest $(d, 1)$-set containing $\mathcal{E}$.

Proposition 3.7.12. *We assume that ℓ satisfies $(*)$. Let $\boldsymbol{M}$ be a 1-split Levi of $\boldsymbol{G}$ and $\mathcal{E} \subseteq \mathcal{E}(M, 1)$ a $(d, 1)$-series. Then $i^G_M(\mathcal{E}_\ell) \subseteq \overline{i^G_M(\mathcal{E})}_\ell$.*

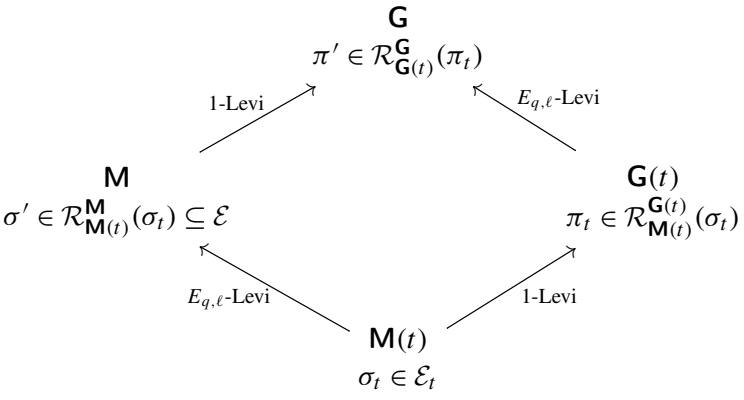
Proof. Let $\pi \in i^{\mathsf{G}}_{\mathsf{M}}(\mathcal{E}_\ell)$. By definition, there exists $\sigma \in \mathcal{E}_\ell$ such that $\langle \pi, i^{\mathsf{G}}_{\mathsf{M}}(\sigma)\rangle \neq 0$. Let $t \in \mathsf{M}^*$ be a semisimple element of order a power of ℓ, such that $\sigma \in \mathcal{E}(\mathsf{M}, t)$. We also have, that $\pi \in \mathcal{E}(\mathsf{G}, t)$.

By Lemma 3.7.11, we can take $\sigma_t \in \mathcal{E}(\mathsf{M}(t), 1)$ and $\pi_t \in \mathcal{E}(\mathsf{G}(t), 1)$, such that σ_t corresponds to σ by the Jordan decomposition, π_t corresponds to π by the Jordan decomposition and $\langle \pi_t, \mathcal{R}^{\mathbf{G}(t)}_{\mathbf{M}(t)}(\sigma_t)\rangle \neq 0$. Let σ' and π' be two irreducible characters in $\mathcal{E}(\mathsf{M}, 1)$ and $\mathcal{E}(\mathsf{G}, 1)$ respectively, such that $\langle \sigma', \mathcal{R}^{\mathbf{M}}_{\mathbf{M}(t)}(\sigma_t)\rangle \neq 0$ and $\langle \pi', \mathcal{R}^{\mathbf{G}}_{\mathbf{G}(t)}(\pi_t)\rangle \neq 0$.

By Theorem 3.1.3, σ' and σ are in the same ℓ-block, and π' and π are also in the same ℓ-block. Since, σ' and σ are in the same ℓ-block and $\sigma \in \mathcal{E}_\ell$, we have that $\sigma' \in \mathcal{E}$. In the same way, since π' and π are in the same ℓ-block, to prove that $\pi \in \overline{i_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E})}_\ell$ it is enough to prove that $\pi' \in \overline{i_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E})}$.

Let $\mathcal{E}_t$ be the $(d,1)$-series of $\mathsf{M}(t)$ containing σ_t. The Levi $\mathsf{G}(t)$ is the dual of $C_{\mathbf{G}^*}(t)^\circ$, hence by Lemma 3.7.9, it is a $E_{q,\ell}$-split Levi of G such that $\mathsf{G}(t) = C_{\mathsf{G}}((Z^\circ(\mathsf{G}(t))_\ell^{\mathsf{F}})^\circ$. We have the same result for the Levi $\mathsf{M}(t)$ of M. Now $\mathsf{M}(t)$ is a 1-split Levi of $\mathsf{G}(t)$ by Remark 3.7.10 and M is a 1-split Levi of G.

Let us summarize all the information about the Levis and the representations in a diagram:



We can apply Lemma 3.7.7 which says that

$$\overline{\mathcal{R}^{\mathsf{G}}_{\mathsf{G}(t)}(\mathcal{R}^{\mathsf{G}(t)}_{\mathsf{M}(t)}(\mathcal{E}_t))} = \overline{\mathcal{R}^{\mathsf{G}}_{\mathsf{M}}(\mathcal{R}^{\mathsf{M}}_{\mathsf{M}(t)}(\mathcal{E}_t))}.$$

Now, because $\langle \pi_t, \mathcal{R}^{\mathsf{G}(t)}_{\mathsf{M}(t)}(\sigma_t)\rangle \neq 0$, we have $\pi_t \in \mathcal{R}^{\mathsf{G}(t)}_{\mathsf{M}(t)}(\mathcal{E}_t)$ and $\langle \pi', \mathcal{R}^{\mathsf{G}}_{\mathsf{G}(t)}(\pi_t)\rangle \neq 0$, so $\pi' \in \overline{\mathcal{R}^{\mathsf{G}}_{\mathsf{G}(t)}(\mathcal{R}^{\mathsf{G}(t)}_{\mathsf{M}(t)}(\mathcal{E}_t))}$. Therefore, $\pi' \in \overline{\mathcal{R}^{\mathsf{G}}_{\mathsf{M}}(\mathcal{R}^{\mathsf{M}}_{\mathsf{M}(t)}(\mathcal{E}_t))}$ (note that the use of Lemma 3.7.7 is crucial here, as π' may not lie in $\mathcal{R}^{\mathsf{G}}_{\mathsf{M}(t)}(\mathcal{E}_t)$). Since, $\langle \sigma', \mathcal{R}^{\mathsf{M}}_{\mathsf{M}(t)}(\sigma_t)\rangle \neq 0$, $\sigma' \in \mathcal{R}^{\mathsf{M}}_{\mathsf{M}(t)}(\mathcal{E}_t)$, and thus $\overline{\mathcal{R}^{\mathsf{M}}_{\mathsf{M}(t)}(\mathcal{E}_t)} = \mathcal{E}$. Hence, $\pi' \in \overline{i_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E})}$, and we have the result. □

Proposition 3.7.13. *Let M be a 1-split Levi of G and $\mathcal{E} \subseteq \mathcal{E}(G,1)$ a $(d,1)$-set. Then if ℓ satisfies $(*)$, we have $r_M^G(\mathcal{E}_\ell) = r_M^G(\mathcal{E})_\ell$.*

Proof. Let $\sigma \in r_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E}_\ell)$. There exists $\pi \in \mathcal{E}_\ell$ such that $\langle \sigma, r_{\mathsf{M}}^{\mathsf{G}}(\pi)\rangle \neq 0$. Now, let $\mathcal{E}'$ be a $(d,1)$-series such that $\sigma \in \mathcal{E}'_\ell$. By Frobenius reciprocity, $\pi \in i_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E}'_\ell)$. By Proposition 3.7.12, $i_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E}'_\ell) \subseteq \overline{i_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E}')}_\ell$. Now, by Lemma 3.7.1, $\overline{i_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E}')}$ is a $(d,1)$-series, so $\overline{i_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E}')} = \mathcal{E}$. Thus $\mathcal{E}' \subseteq r_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E})$ and $\mathcal{E}'_\ell \subseteq r_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E})_\ell$. We have that $r_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E}_\ell) \subseteq r_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E})_\ell$.

Let us prove now the other inclusion. Let $\sigma \in r_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E})_\ell$. There exists $\mathcal{E}'$ a $(d,1)$-series such that $\mathcal{E}' \subseteq r_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E})$ and $\sigma \in \mathcal{E}'_\ell$. Now, $i_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E}') \subseteq \mathcal{E}$, so $\overline{i_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E}')} = \mathcal{E}$. By Proposition 3.7.12, $i_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E}'_\ell) \subseteq \overline{i_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E}')}_\ell = \mathcal{E}_\ell$. Hence, $\mathcal{E}'_\ell \subseteq r_{\mathsf{M}}^{\mathsf{G}}(\mathcal{E}_\ell)$, and we have the result. □

4. Blocks over $\bar{\mathbb{Z}}_\ell$

Now that we have introduced and studied the $(d, 1)$-series for finite reductive groups, we can come back to the study of G a reductive group over F. The purpose of this section is to explain how to find the unipotent ℓ-blocks of G. To do that, we will combine the results of sections 2 and 3. We will sum the 0-consistent systems of idempotents of Section 2, following what we have learnt from the $(d, 1)$-theory, so that the idempotents that we obtain have integer coefficients. This process will end up with ℓ-blocks in the case of a semisimple and simply connected group.

4.1. ***Unipotent ℓ-blocks.*** In Section 2.2, we explain how to get Bernstein blocks from 0-consistent systems constructed with unrefined depth zero types. In this section, we explain how to group those in order to get unipotent ℓ-blocks.

Let $\mathcal{T}^{\mathrm{un}}(G)$ be the subset of $\mathcal{T}(G)$ of pairs (σ, π) with π unipotent and $\mathcal{T}^{\mathrm{un}}_\ell(G)$ the subset of $\mathcal{T}(G)$ of pairs (σ, π) with $\pi \in \mathcal{E}_\ell(\bar{\mathsf{G}}_\sigma, 1)$. We thus have that

$$\mathrm{Rep}^{\mathrm{un}}_{\bar{\mathbb{Q}}_\ell}(G) = \prod_{[\mathfrak{t}]\in\mathcal{T}^{\mathrm{un}}(G)/\sim} \mathrm{Rep}^{[\mathfrak{t}]}_{\bar{\mathbb{Q}}_\ell}(G) \quad \text{and} \quad \mathrm{Rep}^{\mathrm{un}}_{\bar{\mathbb{Z}}_\ell}(G) \cap \mathrm{Rep}_{\bar{\mathbb{Q}}_\ell}(G) = \prod_{[\mathfrak{t}]\in\mathcal{T}^{\mathrm{un}}_\ell(G)/\sim} \mathrm{Rep}^{[\mathfrak{t}]}_{\bar{\mathbb{Q}}_\ell}(G).$$

Remark 4.1.1. Let G be a reductive group over a finite field and P be a parabolic subgroup of G with Levi component L. Then if L admits a unipotent cuspidal representation, then the association class of P is equal to its conjugation class; see for instance [22, (8.2.1)]. Hence, the equivalence relation $\sim$ is trivial on $\mathcal{T}^{\mathrm{un}}(G)$. In particular, $\mathrm{Rep}^{\mathrm{un}}_{\bar{\mathbb{Q}}_\ell}(G) = \prod_{\mathfrak{t}\in\mathcal{T}^{\mathrm{un}}(G)} \mathrm{Rep}^{\mathfrak{t}}_{\bar{\mathbb{Q}}_\ell}(G)$.

Let T be a subset of $\mathcal{T}^{\mathrm{un}}_\ell(G)$ which is $\sim$-stable. We can associate to T a system of idempotents e_T by $e_T := \sum_{[\mathfrak{t}]\in T/\sim} e_{[\mathfrak{t}]}$. We say that T is ℓ-integral if for all $\sigma \in \mathrm{BT}$, $e_{T,\sigma} = \sum_{[\mathfrak{t}]\in T/\sim} e_{[\mathfrak{t}],\sigma}$ is in $\bar{\mathbb{Z}}_\ell[\bar{\mathsf{G}}_\sigma]$. Thus, if T is ℓ-integral we can form a category $\mathrm{Rep}^{T}_{\bar{\mathbb{Z}}_\ell}(G)$.

If $[\mathfrak{t}] \in \mathcal{T}(G)/\sim$, we denote by $e^{[\mathfrak{t}]}$ the idempotent in the center of $\mathrm{Rep}_{\bar{\mathbb{Q}}_\ell}(G)$ associated to the category $\mathrm{Rep}^{[\mathfrak{t}]}_{\bar{\mathbb{Q}}_\ell}(G)$. We define also e^T by $e^T = \sum_{[\mathfrak{t}]\in T/\sim} e^{[\mathfrak{t}]}$.

Lemma 4.1.2. *The idempotent e^T is ℓ-integral if and only if T is ℓ-integral.*

Proof. It is clear that if T is ℓ-integral then e^T is ℓ-integral. Let us assume that e^T is ℓ-integral. Every ℓ-integral element in the center acts on smooth functions on G valued in $\bar{\mathbb{Z}}_\ell$ with compact support. In particular, for every $x \in \mathrm{BT}_0$, the function $e^T * e^+_x$ must be ℓ-integral. Let us prove that for $[\mathfrak{t}] \in \mathcal{T}(G)/\sim$ we have $e^{[\mathfrak{t}]} * e^+_x = e_{[\mathfrak{t}],x}$ which will end the proof.

Consider $V = \mathcal{C}^\infty_c(G, \bar{\mathbb{Q}}_\ell)e^+_x$. Since $e^+_x = \sum_{[\mathfrak{t}']\in\mathcal{T}(G)/\sim} e_{[\mathfrak{t}'],x}$ by Lemma 2.2.1, we have a decomposition $V = \oplus_{[\mathfrak{t}']\in\mathcal{T}(G)/\sim} V_{[\mathfrak{t}']}$ where $V_{[\mathfrak{t}']} = V e_{[\mathfrak{t}'],x}$. Now, $V_{[\mathfrak{t}]}$ is an object in $\mathrm{Rep}^{[\mathfrak{t}]}_{\bar{\mathbb{Q}}_\ell}(G)$ so $e^{[\mathfrak{t}]}$ acts as the identity on it, and if $[\mathfrak{t}'] \neq [\mathfrak{t}]$, $V_{[\mathfrak{t}']}$ is an object in $\mathrm{Rep}^{[\mathfrak{t}']}_{\bar{\mathbb{Q}}_\ell}(G)$ so is canceled by $e^{[\mathfrak{t}]}$ which finish the proof. □

Proposition 4.1.3. *If G is semisimple and simply connected the partition of $\mathcal{T}^{\mathrm{un}}_\ell(G)$ into minimal $\sim$-stable ℓ-integral subsets gives us the decomposition of $\mathrm{Rep}^{\mathrm{un}}_{\bar{\mathbb{Z}}_\ell}(G)$ into ℓ-blocks.*

Proof. Since G is semisimple and simply connected, Theorem 2.2.4 tells us that the idempotents $e^{[\mathfrak{t}]}$ are primitive idempotents in the center on $\bar{\mathbb{Q}}_\ell$. Thus, each ℓ-block of $\mathrm{Rep}^{\mathrm{un}}_{\bar{\mathbb{Z}}_\ell}(G)$ is associated to a $\sim$-stable

subset $T \subseteq \mathcal{T}_\ell^{\mathrm{un}}(G)$ such that e^T is ℓ-integral. Lemma 4.1.2 tells us that T is ℓ-integral. So the ℓ-block decomposition of $\mathrm{Rep}^{\mathrm{un}}_{\bar{\mathbb{Z}}_\ell}(G)$ gives us a partition of $\mathcal{T}_\ell^{\mathrm{un}}(G)$ into $\sim$-stable ℓ-integral subsets. But if T is $\sim$-stable ℓ-integral, we can construct a category from T, so these subsets must be minimal. □

Definition 4.1.4. Let ℓ be a prime number not dividing q. We will say that ℓ satisfies the condition $(**)$ if

$$\text{For all } \sigma \in \mathrm{BT},\ \ell \text{ satisfies } (*) \text{ for } \bar{\mathsf{G}}_\sigma. \tag{$**$}$$

In other words, ℓ satisfies $(**)$ if ℓ is an odd prime number not dividing q, such that $\ell \geq 5$ if a group of exceptional type (${}^3\boldsymbol{D}_4$, $\boldsymbol{G}_2$, $\boldsymbol{F}_4$, $\boldsymbol{E}_6$, ${}^2\boldsymbol{E}_6$, $\boldsymbol{E}_7$) is involved in a reductive quotient and $\ell \geq 7$ if $\boldsymbol{E}_8$ is involved in a reductive quotient.

Let ℓ be a prime number not dividing q, and d be the order of q mod ℓ. Let $\mathfrak{t}$ and $\mathfrak{t}'$ be two unrefined unipotent depth zero types.

Let $\omega \in \mathrm{BT}$. We define $\sim_{\ell,\omega}$, an equivalence relation on $\mathcal{T}^{\mathrm{un}}(G)$ by $\mathfrak{t} \sim_{\ell,\omega} \mathfrak{t}'$ if and only if $\mathfrak{t} = \mathfrak{t}'$ or there exist (σ, π) and (τ, π') such that $\mathfrak{t} = [\sigma, \pi]$, $\mathfrak{t}' = [\tau, \pi']$, $\omega \leq \sigma$, $\omega \leq \tau$, and $\mathrm{Irr}_{(\bar{\mathsf{G}}_\sigma,\pi)}(\bar{\mathsf{G}}_\omega) \cup \mathrm{Irr}_{(\bar{\mathsf{G}}_\tau,\pi')}(\bar{\mathsf{G}}_\omega)$ is contained in a $(d, 1)$-series.

Remark 4.1.5. (1) If $x \leq \omega$ and $\mathfrak{t}_1 \sim_{\ell,\omega} \mathfrak{t}_2$, then $\mathfrak{t}_1 \sim_{\ell,x} \mathfrak{t}_2$ by Lemma 3.7.1.

(2) If ℓ does not divides $|\bar{\mathsf{G}}_\omega|$, then the $(d, 1)$-series in $\bar{\mathsf{G}}_\omega$ are just the 1-series, so $\mathfrak{t} \sim_{\ell,\omega} \mathfrak{t}'$ if and only if $\mathfrak{t} = \mathfrak{t}'$.

(3) For $\mathfrak{t} \in \mathcal{T}^{\mathrm{un}}(G)$ and $\omega \in \mathrm{BT}$ fixed, the study of the $(d, 1)$-series summarized in Theorem 3.6.1 tells us exactly the set of $\mathfrak{t}'$ such that $\mathfrak{t} \sim_{\ell,\omega} \mathfrak{t}'$.

Proposition 4.1.6. *Assume that ℓ satisfies $(**)$. Let $\mathfrak{t}, \mathfrak{t}' \in \mathcal{T}^{\mathrm{un}}(G)$ and $\omega \in \mathrm{BT}$ such that $\mathfrak{t} \sim_{\ell,\omega} \mathfrak{t}'$. Then $\mathfrak{t}$ and $\mathfrak{t}'$ are contained in the same minimal $\sim$-stable ℓ-integral subset of $\mathcal{T}_\ell^{\mathrm{un}}(G)$.*

Proof. Let T be the minimal $\sim$-stable ℓ-integral subset of $\mathcal{T}_\ell^{\mathrm{un}}(G)$ containing $\mathfrak{t}$. We want to show that $\mathfrak{t}' \in T$. Since T is ℓ-integral, $e_{T,\omega} \in \bar{\mathbb{Z}}_\ell[\bar{\mathsf{G}}_\omega]$ and can be written as a sum of primitive central ℓ-integral idempotents. Since ℓ satisfies $(*)$ for $\bar{\mathsf{G}}_\omega$, we have a description of them by Theorem 3.1.2. In particular, if we denote by $\mathcal{E}$ the subset of $\mathrm{Irr}(\bar{\mathsf{G}}_\omega)$ cut out by $e_{T,\omega}$, we have that $\mathcal{E} \cap \mathcal{E}(\bar{\mathsf{G}}_\omega, 1)$ is a d-set. By construction of $e_{T,\omega}$, $\mathcal{E} \cap \mathcal{E}(\bar{\mathsf{G}}_\omega, 1)$ is also a 1-set so it is a $(d, 1)$-set. Let (σ, π) and (τ, π') such that $\mathfrak{t} = [\sigma, \pi]$, $\mathfrak{t}' = [\tau, \pi']$ and satisfying the conditions of $\mathfrak{t} \sim_{\ell,\omega} \mathfrak{t}'$. Since, $\mathfrak{t} \in T$, $\mathrm{Irr}_{(\bar{\mathsf{G}}_\sigma,\pi)}(\bar{\mathsf{G}}_\omega) \subseteq \mathcal{E} \cap \mathcal{E}(\bar{\mathsf{G}}_\omega, 1)$. But $\mathrm{Irr}_{(\bar{\mathsf{G}}_\sigma,\pi)}(\bar{\mathsf{G}}_\omega) \cup \mathrm{Irr}_{(\bar{\mathsf{G}}_\tau,\pi')}(\bar{\mathsf{G}}_\omega)$ is contained in a $(d, 1)$-series so $\mathrm{Irr}_{(\bar{\mathsf{G}}_\tau,\pi')}(\bar{\mathsf{G}}_\omega) \subseteq \mathcal{E} \cap \mathcal{E}(\bar{\mathsf{G}}_\omega, 1)$, and $\mathfrak{t}' \in T$. □

For G a finite reductive group, we denote by $\mathcal{E}(\mathsf{G}, \ell')$ the union of the Deligne–Lusztig series $\mathcal{E}(\mathsf{G}, s)$ with s of order prime to ℓ. Let $\mathcal{T}^{\ell'}(G)$ be the subset of $\mathcal{T}(G)$ of pairs (π, σ), such that $\sigma \in \mathcal{E}(\bar{\mathsf{G}}_\sigma, \ell')$.

Proposition 4.1.7. *If $T \subseteq \mathcal{T}(G)$ is $\sim$-stable ℓ-integral then $T \cap \mathcal{T}^{\ell'}(G) \neq \varnothing$.*

Proof. Let $\sigma \in \mathrm{BT}$ such that $e_{T,\sigma} \neq 0$. Since T is ℓ-integral, $e_{T,\sigma} \in \bar{\mathbb{Z}}_\ell[\bar{\mathsf{G}}_\sigma]$. So $e_{T,\sigma}$ is a sum of primitive central idempotents in $\bar{\mathbb{Z}}_\ell[\bar{\mathsf{G}}_\sigma]$. Let b be one of these primitive central idempotents. By [7, Theorem 9.12] there exists $\pi \in \mathcal{E}(\bar{\mathsf{G}}_\sigma, \ell')$ such that $b\pi \neq 0$. In particular, $e_{T,\sigma}\pi \neq 0$. There exist a Levi M of $\bar{\mathsf{G}}_\sigma$ and a cuspidal representation π' such that $\pi \in \mathrm{Irr}_{(M,\pi')}(\bar{\mathsf{G}}_\sigma)$ and $\pi' \in \mathcal{E}(\mathsf{M}, \ell')$. Thus there exists $\mathfrak{t} \in \mathcal{T}^{\ell'}(G)$ such

that $e_{[\mathfrak{t}],\sigma}\pi \neq 0$. Moreover, $e_{[\mathfrak{t}],\sigma}$ acts as the identity on π so $e_{T,\sigma}e_{[\mathfrak{t}],\sigma} \neq 0$. Now $e_{T,\sigma} = \sum_{[\mathfrak{t}']\in T/\sim} e_{[\mathfrak{t}'],\sigma}$, so $e_{T,\sigma}e_{[\mathfrak{t}],\sigma} = \sum_{[\mathfrak{t}']\in T/\sim} e_{[\mathfrak{t}'],\sigma}e_{[\mathfrak{t}],\sigma}$. Lemma 2.2.1 told us that if $[\mathfrak{t}] \neq [\mathfrak{t}']$ then $e_{[\mathfrak{t}'],\sigma}e_{[\mathfrak{t}],\sigma} = 0$, thus $\mathfrak{t} \in T$. □

Since we are interested in the unipotent blocks, we get the following corollary.

Corollary 4.1.8. *If $T \subseteq \mathcal{T}_\ell^{\mathrm{un}}(G)$ is $\sim$-stable ℓ-integral then $T \cap \mathcal{T}^{\mathrm{un}}(G) \neq \varnothing$.*

Proof. This is an immediate consequence of Proposition 4.1.7, since $\mathcal{T}^{\ell'}(G) \cap \mathcal{T}_\ell^{\mathrm{un}}(G) = \mathcal{T}^{\mathrm{un}}(G)$. □

Expressed in terms of ℓ-blocks of $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(G)$ this gives:

Corollary 4.1.9. *Assume that G is semisimple and simply connected. Let R be an ℓ-block of $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(G)$. Then R is characterized by the nonempty intersection $R \cap \mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Q}}_\ell}(G)$.*

Proof. Since G is semisimple and simply connected, by Proposition 4.1.3 R is defined by T a minimal $\sim$-stable ℓ-integral subset of $\mathcal{T}_\ell^{\mathrm{un}}(G)$. Now, the minimal $\sim$-stable ℓ-integral subsets form a partition of $\mathcal{T}_\ell^{\mathrm{un}}(G)$, so T is uniquely determined by any of its elements. Corollary 4.1.8 tells us that $T \cap \mathcal{T}^{\mathrm{un}}(G) \neq \varnothing$, so T is characterized by $T \cap \mathcal{T}^{\mathrm{un}}(G)$. □

4.2. *Decomposition of* $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(G)$. In this section, using the $(d, 1)$-theory for the reductive quotient in the Bruhat–Tits building, we will define an equivalence relation on $\mathcal{T}^{\mathrm{un}}(G)$. When G is semisimple and simply connected, an equivalence class will exactly correspond to $T \cap \mathcal{T}^{\mathrm{un}}(G)$, for T a minimal $\sim$-stable ℓ-integral set, and thus will give us a unipotent ℓ-block of G.

Let ℓ be a prime number which satisfies $(**)$, and d be the order of q modulo ℓ.

We define $\sim_\ell$, an equivalence relation on $\mathcal{T}^{\mathrm{un}}(G)$ by $\mathfrak{t} \sim_\ell \mathfrak{t}'$ if and only if there exist $\omega_1, \ldots, \omega_r \in \mathrm{BT}$ and $\mathfrak{t}_1, \ldots, \mathfrak{t}_{r-1} \in \mathcal{T}^{\mathrm{un}}(G)$ such that $\mathfrak{t} \sim_{\ell,\omega_1} \mathfrak{t}_1 \sim_{\ell,\omega_2} \mathfrak{t}_2 \cdots \sim_{\ell,\omega_r} \mathfrak{t}'$. We write $[\mathfrak{t}]_\ell$ for the equivalence class of $\mathfrak{t}$.

Remark 4.2.1. By Remark 4.1.5 (1), we can take in the definition $\omega_i \in \mathrm{BT}_0$.

Let $\mathfrak{t} \in \mathcal{T}^{\mathrm{un}}(G)$ and $\omega \in \mathrm{BT}$. We define $\mathcal{E}_{[\mathfrak{t}]_\ell,\omega}$ to be the subset of $\mathcal{E}(\bar{\mathsf{G}}_\omega, 1)$ cut out by $\sum_{\mathfrak{u}\in[\mathfrak{t}]_\ell} e_{\mathfrak{u},\omega}$.

Lemma 4.2.2. *The set $\mathcal{E}_{[\mathfrak{t}]_\ell,\omega}$ is a $(d, 1)$-set in $\bar{G}_\omega$.*

Proof. By definition $\mathcal{E}_{[\mathfrak{t}]_\ell,\omega}$ is a 1-set.

Let $(\sigma, \lambda) \in \mathcal{T}^{\mathrm{un}}(G)$ such that $\omega \leq \sigma$ and $\mathrm{Irr}_{(\bar{\mathsf{G}}_\sigma,\lambda)}(\bar{\mathsf{G}}_\omega) \subseteq \mathcal{E}_{[\mathfrak{t}]_\ell,\omega}$. By construction of $\mathcal{E}_{[\mathfrak{t}]_\ell,\omega}$, we have that $(\sigma, \lambda) \in [\mathfrak{t}]_\ell$.

Let $\mathcal{E}_{\sigma,\lambda}$ be the $(d, 1)$-series containing $\mathrm{Irr}_{(\bar{\mathsf{G}}_\sigma,\lambda)}(\bar{\mathsf{G}}_\omega)$. Let us prove that $\mathcal{E}_{\sigma,\lambda} \subseteq \mathcal{E}_{[\mathfrak{t}]_\ell,\omega}$. Let $(\sigma', \lambda') \in \mathcal{T}^{\mathrm{un}}(G)$ such that $\omega \leq \sigma'$ and $\mathrm{Irr}_{(\bar{\mathsf{G}}_{\sigma'},\lambda')}(\bar{\mathsf{G}}_\omega) \subseteq \mathcal{E}_{\sigma,\lambda}$. Then by definition, $(\sigma, \lambda) \sim_{\ell,\omega} (\sigma', \lambda')$. Thus, $(\sigma, \lambda) \sim_\ell (\sigma', \lambda')$ and $(\sigma', \lambda') \in [\mathfrak{t}]_\ell$. Therefore $\mathrm{Irr}_{(\bar{\mathsf{G}}_{\sigma'},\lambda')}(\bar{\mathsf{G}}_\omega) \subseteq \mathcal{E}_{[\mathfrak{t}]_\ell,\omega}$ and $\mathcal{E}_{\sigma,\lambda} \subseteq \mathcal{E}_{[\mathfrak{t}]_\ell,\omega}$.

Since, this is true for every $(\sigma, \lambda) \in \mathcal{T}^{\mathrm{un}}(G)$ such that $\omega \leq \sigma$ and $\mathrm{Irr}_{(\bar{\mathsf{G}}_\sigma,\lambda)}(\bar{\mathsf{G}}_\omega) \subseteq \mathcal{E}_{[\mathfrak{t}]_\ell,\omega}$, we get that $\mathcal{E}_{[\mathfrak{t}]_\ell,\omega}$ is a $(d, 1)$-set. □

By Lemma 4.2.2, $\mathcal{E}_{[\mathfrak{t}]_\ell,\omega}$ is a $(d, 1)$-set, so we can form $\mathcal{E}_{[\mathfrak{t}]_\ell,\omega,\ell}$, the ℓ-extension of $\mathcal{E}_{[\mathfrak{t}]_\ell,\omega}$ as in Section 3.2. Let $e_{[\mathfrak{t}]_\ell,\omega}$ be the idempotent in $\bar{\mathsf{G}}_\omega$ that cuts out $\mathcal{E}_{[\mathfrak{t}]_\ell,\omega,\ell}$. Since ℓ satisfies $(*)$ for $\bar{\mathsf{G}}_\omega$, Theorem 3.1.2 tells us that $e_{[\mathfrak{t}]_\ell,\omega}$ is ℓ-integral. Thus we just have defined $e_{[\mathfrak{t}]_\ell} = (e_{[\mathfrak{t}]_\ell,\omega})_{\omega\in\mathrm{BT}}$ an ℓ-integral system of idempotents.

Proposition 4.2.3. *The ℓ-integral system of idempotent $e_{[\mathfrak{t}]_\ell}$ is 0-consistent, thus defines $\mathrm{Rep}^{[\mathfrak{t}]_\ell}_{\overline{\mathbb{Z}}_\ell}(G)$ a subcategory of $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(G)$.*

Proof. Since the $\mathfrak{t} \in \mathcal{T}^{\mathrm{un}}(G)$ are G-conjugacy classes, $e_{[\mathfrak{t}]_\ell}$ is G-equivariant.

Let $\tau, \omega \in \mathrm{BT}$ such that $\omega \leq \tau$. It remains to prove that $e^+_\tau e_{[\mathfrak{t}]_\ell,\omega} = e_{[\mathfrak{t}]_\ell,\tau}$.

The idempotent $e_{[\mathfrak{t}]_\ell,\omega}$ is the idempotent that cuts out $\mathcal{E}_{[\mathfrak{t}]_\ell,\omega,\ell}$ and $e^+_\tau e_{[\mathfrak{t}]_\ell,\omega}$ is the idempotents that cuts out $r^{\bar{\mathsf{G}}_\omega}_{\bar{\mathsf{G}}_\tau}(\mathcal{E}_{[\mathfrak{t}]_\ell,\omega,\ell})$.

By Proposition 3.7.13, $r^{\bar{\mathsf{G}}_\omega}_{\bar{\mathsf{G}}_\tau}(\mathcal{E}_{[\mathfrak{t}]_\ell,\omega,\ell}) = r^{\bar{\mathsf{G}}_\omega}_{\bar{\mathsf{G}}_\tau}(\mathcal{E}_{[\mathfrak{t}]_\ell,\omega})_\ell$. But we know by definition of $\mathcal{E}_{[\mathfrak{t}]_\ell,\omega}$ that $r^{\bar{\mathsf{G}}_\omega}_{\bar{\mathsf{G}}_\tau}(\mathcal{E}_{[\mathfrak{t}]_\ell,\omega}) = \mathcal{E}_{[\mathfrak{t}]_\ell,\tau}$. Hence, we have $r^{\bar{\mathsf{G}}_\omega}_{\bar{\mathsf{G}}_\tau}(\mathcal{E}_{[\mathfrak{t}]_\ell,\omega,\ell}) = \mathcal{E}_{[\mathfrak{t}]_\ell,\tau,\ell}$. □

Remark 4.2.4. By Propositions 3.7.12 and 3.7.13, $\mathcal{E}_{[\mathfrak{t}]_\ell,\omega,\ell}$ is a union of Harish-Chandra series. Hence there exists a $\sim$-stable subset $T \subseteq \mathcal{T}^{\mathrm{un}}_\ell(G)$ such that $e_{[\mathfrak{t}]_\ell} = e_T$. Then Theorem 3.1.3 gives us a description of T in the following way. Let $(\sigma, \chi) \in \mathcal{T}^{\mathrm{un}}_\ell(G)$. Let t be a semisimple conjugacy class in $\bar{\mathsf{G}}^*_\sigma$ of order a power of ℓ, such that $\chi \in \mathcal{E}(\bar{\mathsf{G}}_\sigma, t)$. Let $\bar{\mathsf{G}}_\sigma(t)$ a Levi in $\bar{\mathsf{G}}_\sigma$ dual to $C_{\bar{\mathsf{G}}^*_\sigma}(t)^\circ$, with P as a parabolic subgroup, and $\chi_t \in \mathcal{E}(\bar{\mathsf{G}}_\sigma(t), 1)$ such that $\langle \chi, \mathcal{R}^{\bar{\mathsf{G}}_\sigma}_{\bar{\mathsf{G}}_\sigma(t)\subseteq \mathsf{P}}(\hat{t}\chi_t)\rangle \neq 0$. Let π be an irreducible component of $\mathcal{R}^{\bar{\mathsf{G}}_\sigma}_{\bar{\mathsf{G}}_\sigma(t)\subseteq \mathsf{P}}(\chi_t)$. Let $(\bar{\mathsf{G}}_\tau, \lambda)$ be the cuspidal support of π. Then (σ, χ) is in the subset T associated with $[(\tau, \lambda)]_\ell$.

Theorem 4.2.5. *Let ℓ be a prime number which satisfies $(**)$. Then we have a decomposition*

$$\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(G) = \prod_{[\mathfrak{t}]_\ell \in \mathcal{T}^{\mathrm{un}}(G)/\sim_\ell} \mathrm{Rep}^{[\mathfrak{t}]_\ell}_{\overline{\mathbb{Z}}_\ell}(G).$$

Proof. Let $e^\ell_1 = (e^\ell_{1,\sigma})_{\sigma\in \mathrm{BT}}$ be the 0-consistent system of idempotent that cuts out $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(G)$ (we have recalled the definition of e^ℓ_1 at the end of Section 2.1). Then the systems of idempotents $e_{[\mathfrak{t}]_\ell}$, for $[\mathfrak{t}]_\ell \in \mathcal{T}^{\mathrm{un}}(G)/\sim_\ell$ satisfy the following properties:

- For all $\sigma \in \mathrm{BT}$, $e^\ell_{1,\sigma} = \sum_{[\mathfrak{t}]_\ell \in \mathcal{T}^{\mathrm{un}}(G)/\sim_\ell} e_{[\mathfrak{t}]_\ell,\sigma}$.
- If $[\mathfrak{t}]_\ell$ and $[\mathfrak{t}']_\ell$ are two elements of $\mathcal{T}^{\mathrm{un}}(G)/\sim_\ell$ such that $[\mathfrak{t}]_\ell \neq [\mathfrak{t}']_\ell$, and if $\sigma \in \mathrm{BT}$, then $e_{[\mathfrak{t}]_\ell,\sigma} e_{[\mathfrak{t}']_\ell,\sigma} = 0$.

With these properties, the same proof as in [18, Proposition 2.3.5] shows the desired result. □

Remark 4.2.6. (1) From the construction of the system of idempotents $e_{[\mathfrak{t}]_\ell}$, we see that

$$\mathrm{Rep}^{[\mathfrak{t}]_\ell}_{\overline{\mathbb{Z}}_\ell}(G) \cap \mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Q}}_\ell}(G) = \prod_{\mathfrak{u}\in[\mathfrak{t}]_\ell} \mathrm{Rep}^{\mathfrak{u}}_{\overline{\mathbb{Q}}_\ell}(G).$$

(2) We also have a description of $\mathrm{Rep}^{[\mathfrak{t}]_\ell}_{\overline{\mathbb{Z}}_\ell}(G) \cap \mathrm{Rep}_{\overline{\mathbb{Q}}_\ell}(G)$ by Remark 4.2.4.

Theorem 4.2.7. *When G is semisimple and simply connected and ℓ satisfies $(**)$, the decomposition*

$$\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(G) = \prod_{[\mathfrak{t}]_\ell \in \mathcal{T}^{\mathrm{un}}(G)/\sim_\ell} \mathrm{Rep}^{[\mathfrak{t}]_\ell}_{\overline{\mathbb{Z}}_\ell}(G),$$

is the decomposition of $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(G)$ into ℓ-blocks.

Proof. Let $\mathfrak{t} \in \mathcal{T}^{\mathrm{un}}(G)$, we want to prove that $\mathrm{Rep}^{[\mathfrak{t}]_\ell}_{\overline{\mathbb{Z}}_\ell}(G)$ is an ℓ-block. Let T be the $\sim$-stable subset of $\mathcal{T}^{\mathrm{un}}_\ell(G)$ which defines $\mathrm{Rep}^{[\mathfrak{t}]_\ell}_{\overline{\mathbb{Z}}_\ell}(G)$. We need to prove that T is a minimal ℓ-integral set by Proposition 4.1.3.

We know that T is ℓ-integral. By Corollary 4.1.8, it is enough to prove that $T \cap \mathcal{T}^{\mathrm{un}}(G)$ is contained into a minimal ℓ-integral set. By construction, we have that $T \cap \mathcal{T}^{\mathrm{un}}(G) = \{\mathfrak{u} \in \mathcal{T}^{\mathrm{un}}(G), \mathfrak{u} \in [\mathfrak{t}]_\ell\}$.

Now, if $\mathfrak{u}$, $\mathfrak{u}'$ are two element of $\mathcal{T}^{\mathrm{un}}(G)$ such that $\mathfrak{u} \sim_{\ell,\omega} \mathfrak{u}'$, then by Proposition 4.1.6, $\mathfrak{u}$ and $\mathfrak{u}'$ are contained in the same minimal ℓ-integral set. Thus, if $\mathfrak{u} \sim_\ell \mathfrak{t}$, $\mathfrak{u}$ and $\mathfrak{t}$ are contained in the same minimal ℓ-integral set and we have the wanted result. □

4.3. ***Case $\ell = 2$ and groups of types A, B, C, D.*** In this section, we examine a case of a bad prime $\ell = 2$, but when the group is good, that is all the reductive quotients only involve types among $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$ and $\boldsymbol{D}$. We will prove that the unipotent category is a 2-block.

Theorem 4.3.1. *Let G be a semisimple and simply connected group such that all the reductive quotients only involve types among $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$ and $\boldsymbol{D}$, and $p \neq 2$. Then $\mathrm{Rep}^1_{\overline{\mathbb{Z}}_2}(G)$ is a 2-block.*

Proof. By Proposition 4.1.3, we want to prove that $\mathcal{T}^1_2(G)$ is a minimal $\sim$-stable 2-integral set. Let $T \subseteq \mathcal{T}^1_2(G)$ be a minimal $\sim$-stable 2-integral set. Let us prove that $\mathcal{T}^1_2(G) \subseteq T$.

Let $\sigma \in \mathrm{BT}$ such that $e_{T,\sigma} \neq 0$. Since T is 2-integral, $e_{T,\sigma}$ is a sum of 2-blocks. By [7, Theorem 21.14], the only unipotent 2-block of $\bar{\mathrm{G}}_\sigma$ is the idempotent cutting out $\mathcal{E}_2(\bar{\mathrm{G}}_\sigma, 1)$. Hence, $e_{T,\sigma}$ is this idempotent. Therefore, we get from the definition of $e_{T,\sigma}$ that for all $\mathfrak{t} = (\omega, \tau) \in \mathcal{T}^1_2(G)$, such that $\omega \leq \sigma$, we have that $\mathfrak{t} \in T$. In particular $(C, 1) \in T$, where C is a chamber. So, for all $\sigma \in \mathrm{BT}$, $e_{T,\sigma} \neq 0$ and $\mathcal{T}^1_2(G) \subseteq T$. □

5. Some examples

Section 4 describes the ℓ-blocks for a semisimple and simply connected group thanks to the equivalence relation $\sim_\ell$ on $\mathcal{T}^{\mathrm{un}}(G)$. In this section, we examine some examples and make $\sim_\ell$ explicit.

5.1. ***ℓ divides $q-1$.*** When ℓ divides $q-1$, hence $d = 1$, the $(d, 1)$-series are just the 1-series. In this case, $\sim_\ell$ is trivial on $\mathcal{T}^{\mathrm{un}}(G)$. Thus Theorem 4.2.7 gives us:

Proposition 5.1.1. *When G is semisimple and simply connected, ℓ satisfies $(**)$ and ℓ divides $q-1$, we have a decomposition into ℓ-blocks*

$$\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(G) = \prod_{\mathfrak{t} \in \mathcal{T}^{\mathrm{un}}(G)} \mathrm{Rep}^{\mathfrak{t}}_{\overline{\mathbb{Z}}_\ell}(G),$$

such that $\mathrm{Rep}^{\mathfrak{t}}_{\overline{\mathbb{Z}}_\ell}(G) \cap \mathrm{Rep}_{\overline{\mathbb{Q}}_\ell}(G) = \mathrm{Rep}^{\mathfrak{t}}_{\overline{\mathbb{Q}}_\ell}(G)$ is a single Bernstein block.

5.2. ***Blocks of $\mathbf{SL}_n$.*** Let us make the ℓ-blocks of SL_n explicit.

Theorem 5.2.1. *Let ℓ be prime not dividing q, then $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(\mathrm{SL}_n(F))$ is an ℓ-block.*

Proof. If $\ell \neq 2$, then we can apply Theorem 4.2.7. In this case, $\mathcal{T}^{\mathrm{un}}(G)$ is composed of only one element, the conjugacy class of $(C, 1)$ where C is a chamber. Hence $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(\mathrm{SL}_n(F))$ is an ℓ-block.

If $\ell = 2$, we can apply Theorem 4.3.1 and $\mathrm{Rep}^1_{\overline{\mathbb{Z}}_2}(\mathrm{SL}_n(F))$ is a 2-block. □

5.3. *Blocks of* $\mathbf{Sp_{2n}}$. In this section, we have a look at $G = \mathrm{Sp}_{2n}$. We assume in all this section that ℓ does not divide q.

If $\ell = 2$, Theorem 4.3.1 gives us the result. So we can assume that $\ell \neq 2$. Theorem 4.2.7 tells us that to know the ℓ-blocks of Sp_{2n} we need to understand $\mathcal{T}^{\mathrm{un}}(G)/\sim_\ell$. Let us start by describing $\mathcal{T}^{\mathrm{un}}(G)$. The group $\mathrm{Sp}_{2m}(k)$ has a unipotent cuspidal representation if and only if $m = s(s+1)$ for some integer s, and this representation is unique up to isomorphism. If $\sigma \in \mathrm{BT}$, then $\bar{\mathsf{G}}_\sigma \simeq \mathsf{H} \times \mathrm{Sp}_{2i}(k) \times \mathrm{Sp}_{2j}(k)$, where H is a product of $\mathrm{GL}_m(k)$, and $i + j \leq n$. Hence, we have a bijection between $\mathcal{T}^{\mathrm{un}}(G)$ and the set $\mathcal{S}^{\mathrm{un}}(G) := \{(s, s') \in \mathbb{N}^2, s(s+1) + s'(s'+1) \leq n\}$. For $(s, s') \in \mathcal{S}^{\mathrm{un}}(G)$ we will write $\mathfrak{t}(s, s') = (\sigma(s, s'), \pi(s, s'))$ for the corresponding element of $\mathcal{T}^{\mathrm{un}}(G)$.

Let d be the order of q modulo ℓ. The first case is when d is odd. Then Proposition 3.4.2 tells us that for $\sigma \in \mathrm{BT}$, the unipotent $(d, 1)$-series in $\bar{\mathsf{G}}_\sigma$ are the unipotent 1-series. Hence, $\sim_\ell$ is just the trivial equivalence relation on $\mathcal{T}^{\mathrm{un}}(G)$. Thus we get the decomposition of $\mathrm{Rep}^{\mathrm{un}}_{\bar{\mathbb{Z}}_\ell}(\mathrm{Sp}_{2n}(F))$ into ℓ-blocks

$$\mathrm{Rep}^{\mathrm{un}}_{\bar{\mathbb{Z}}_\ell}(\mathrm{Sp}_{2n}(F)) = \prod_{\mathfrak{t} \in \mathcal{T}^{\mathrm{un}}(G)} \mathrm{Rep}^{[\mathfrak{t}]_\ell}_{\bar{\mathbb{Z}}_\ell}(\mathrm{Sp}_{2n}(F)).$$

Now, we assume that d is even. We want to make the equivalence relation $\sim_\ell$ on $\mathcal{T}^{\mathrm{un}}(G)$ explicit.

Let us start by finding the $\mathfrak{t} \in \mathcal{T}^{\mathrm{un}}(G)$ such that $[\mathfrak{t}]_\ell = \{\mathfrak{t}\}$. Let $\mathcal{S}_c$ be the subset of $\mathcal{S}^{\mathrm{un}}(G)$ of couples (s, s') such that $[\mathfrak{t}(s, s')]_\ell = \{\mathfrak{t}(s, s')\}$. There are $n+1$ nonconjugate vertices in BT_0 that we denote $x_0, \dots, x_n$, such that $\bar{\mathsf{G}}_{x_i} \simeq \mathrm{Sp}_{2i}(k) \times \mathrm{Sp}_{2(n-i)}(k)$. Let $(s, s') \in \mathcal{S}^{\mathrm{un}}(G)$. We may assume that all the x_i and $\sigma(s, s')$ are in a same chamber. Then $x_i \leq \sigma(s, s')$ if and only if $s(s+1) \leq i$ and $s'(s'+1) \leq n - i$. Hence

$$\{x \in \mathrm{BT}_0, x \leq \sigma(s, s')\} = \{x_i, s(s+1) \leq i \leq n - s'(s'+1)\}.$$

We denote by Σ_s the symbol corresponding to the unipotent cuspidal representation of $\mathrm{Sp}_{2s(s+1)}$. That is

$$\Sigma_s = \begin{pmatrix} 0 & 1 & \cdots & 2s \\ & & & \end{pmatrix}.$$

Lemma 5.3.1. *We have*

$$\mathcal{S}_c = \left\{(s, s') \in \mathcal{S}^{\mathrm{un}}(G), \left\{ \begin{array}{l} s(s+1) + s'(s'-1) > n - d/2 \\ s'(s'+1) + s(s-1) > n - d/2 \end{array} \right\}\right\}.$$

Proof. By definition of $\sim_\ell$, we have that $\mathcal{S}_c$ is the subset of $\mathcal{S}^{\mathrm{un}}(G)$ of couples (s, s') such that for all $x_i \leq \sigma(s, s')$, either

$$\begin{cases} \ell \nmid |\mathrm{Sp}_{2i}(k)|, \\ \ell \nmid |\mathrm{Sp}_{2(n-i)}(k)|, \end{cases} \quad \text{or} \quad \begin{cases} \ell \nmid |\mathrm{Sp}_{2i}(k)|, \\ \ell \mid |\mathrm{Sp}_{2(n-i)}(k)|, \\ \mathrm{defect}(\Sigma_{s'}) > k(\mathrm{Sp}_{2(n-i)}(k), d), \end{cases} \quad \text{or}$$

$$\begin{cases} \ell \mid |\mathrm{Sp}_{2i}(k)|, \\ \mathrm{defect}(\Sigma_s) > k(\mathrm{Sp}_{2i}(k), d), \\ \ell \nmid |\mathrm{Sp}_{2(n-i)}(k)|, \end{cases} \quad \text{or} \quad \begin{cases} \ell \mid |\mathrm{Sp}_{2i}(k)|, \\ \mathrm{defect}(\Sigma_s) > k(\mathrm{Sp}_{2i}(k), d), \\ \ell \mid |\mathrm{Sp}_{2(n-i)}(k)|, \\ \mathrm{defect}(\Sigma_{s'}) > k(\mathrm{Sp}_{2(n-i)}(k), d). \end{cases}$$

We know that $|\mathrm{Sp}_{2i}(k)| = q^{n^2}\prod_{j=1}^{i}(q^{2j}-1)$ and d is the order of q modulo ℓ (with d even), hence $\ell \mid |\mathrm{Sp}_{2i}(k)|$ if and only if $d \leq 2i$. In the same way, $\ell \mid |\mathrm{Sp}_{2(n-i)}(k)|$ if and only if $d \leq 2(n-i)$.

By definition, $k(\mathrm{Sp}_{2i}(k), d) = \max\{k \geq 0, k \text{ odd}, (k^2-4k+3)/4 \leq i - d/2\}$. So $\mathrm{defect}(\Sigma_s) > k(\mathrm{Sp}_{2i}(k), d)$, if and only if $2s+1 > k(\mathrm{Sp}_{2i}(k), d)$ if and only if $((2s+1)^2-4(2s+1)+3)/4 > i-d/2$. But $((2s+1)^2-4(2s+1)+3)/4 = s(s-1)$. Hence $\mathrm{defect}(\Sigma_s) > k(\mathrm{Sp}_{2i}(k), d)$ if and only if $s(s-1) > i-d/2$ and $\mathrm{defect}(\Sigma_{s'}) > k(\mathrm{Sp}_{2(n-i)}(k), d)$ if and only if $s'(s'-1) > n-i-d/2$.

So, $\mathcal{S}_c$ is the set of $(s, s') \in \mathcal{S}^{\mathrm{un}}(G)$ such that for all $i \in \{s(s+1), \ldots, n-s'(s'+1)\}$ either

$$\begin{cases} d > 2i, \\ d > 2(n-i), \end{cases} \quad \text{or} \quad \begin{cases} d > 2i, \\ d \leq 2(n-i), \\ s'(s'-1) > n-i-d/2, \end{cases} \quad \text{or}$$

$$\begin{cases} d \leq 2i, \\ s(s-1) > i-d/2, \\ d > 2(n-i), \end{cases} \quad \text{or} \quad \begin{cases} d \leq 2i, \\ s(s-1) > i-d/2, \\ d \leq 2(n-i), \\ s'(s'-1) > n-i-d/2. \end{cases}$$

To make things clearer, let us rewrite these conditions on conditions on i

$$\begin{cases} i < d/2, \\ i > n-d/2, \end{cases} \quad \text{or} \quad \begin{cases} i < d/2, \\ i \leq n-d/2, \\ i > n-d/2-s'(s'-1), \end{cases} \quad \text{or}$$

$$\begin{cases} i \geq d/2, \\ i < s(s-1)+d/2, \\ i > n-d/2, \end{cases} \quad \text{or} \quad \begin{cases} i \geq d/2, \\ i < s(s-1)+d/2, \\ i \leq n-d/2, \\ i > n-d/2-s'(s'-1). \end{cases}$$

Now, since $s'(s'-1)$ is positive,the conditions

$$\begin{cases} i < d/2, \\ i > n-d/2, \end{cases} \quad \text{or} \quad \begin{cases} i < d/2, \\ i \leq n-d/2, \\ i > n-d/2-s'(s'-1), \end{cases}$$

are equivalent to

$$\begin{cases} i < d/2, \\ i > n-d/2-s'(s'-1). \end{cases}$$

We also have that the conditions

$$\begin{cases} i \geq d/2, \\ i < s(s-1)+d/2, \\ i > n-d/2, \end{cases} \quad \text{or} \quad \begin{cases} i \geq d/2, \\ i < s(s-1)+d/2, \\ i \leq n-d/2, \\ i > n-d/2-s'(s'-1), \end{cases}$$

are equivalent to

$$\begin{cases} i \geq d/2, \\ i < s(s-1) + d/2, \\ i > n - d/2 - s'(s'-1). \end{cases}$$

But now, since $s(s-1)$ is positive, the conditions

$$\begin{cases} i < d/2, \\ i > n - d/2 - s'(s'-1), \end{cases} \quad \text{or} \quad \begin{cases} i \geq d/2, \\ i < s(s-1) + d/2, \\ i > n - d/2 - s'(s'-1), \end{cases}$$

are equivalent to

$$\begin{cases} i < s(s-1) + d/2, \\ i > n - d/2 - s'(s'-1). \end{cases}$$

Finally, we have that $\mathcal{S}_c$ is the set of $(s, s') \in \mathcal{S}^{\mathrm{un}}(G)$ such that for all $i \in \{s(s+1), \dots, n - s'(s'+1)\}$, $i < s(s-1) + d/2$ and $i > n - d/2 - s'(s'-1)$, that is, it is the set of (s, s') such that $n - s'(s'+1) < s(s-1) + d/2$ and $s(s+1) > n - d/2 - s'(s'-1)$. □

We now want to prove that $[\mathfrak{t}(0,0)]_\ell = \{\mathfrak{t}(s, s'), (s, s') \notin \mathcal{S}_c\}$.

Proposition 5.3.2. *Let $(s, s') \in \mathcal{S}^{\mathrm{un}}(G) \setminus \mathcal{S}_c$. Then $\mathfrak{t}(s, s') \sim_\ell \mathfrak{t}(0, 0)$.*

Proof. By definition, since $(s, s') \notin \mathcal{S}_c$, there exists i such that

$$\begin{cases} \ell \mid |\mathrm{Sp}_{2i}(k)|, \\ \mathrm{defect}(\Sigma_s) \leq k(\mathrm{Sp}_{2i}(k), d), \end{cases} \quad \text{or} \quad \begin{cases} \ell \mid |\mathrm{Sp}_{2(n-i)}(k)|, \\ \mathrm{defect}(\Sigma_{s'}) \leq k(\mathrm{Sp}_{2(n-i)}(k), d). \end{cases}$$

Let us assume for example that

$$\begin{cases} \ell \mid |\mathrm{Sp}_{2(n-i)}(k)|, \\ \mathrm{defect}(\Sigma_{s'}) \leq k(\mathrm{Sp}_{2(n-i)}(k), d), \end{cases}$$

(the other case is similar). Since $\mathrm{defect}(\Sigma_{s'}) \leq k(\mathrm{Sp}_{2(n-i)}(k), d)$ Proposition 3.4.6 tells us that $\mathfrak{t}(s, s') \sim_{\ell, x_i} \mathfrak{t}(s, 0)$.

Let us have a look at x_n. First, since $s(s+1) \leq i \leq n$ then $x_n \leq \sigma(s, 0)$. Now since $\ell \mid |\mathrm{Sp}_{2(n-i)}(k)|$, $i \leq n - d/2$ (like in the proof of Lemma 5.3.1). Hence, $d/2 \leq n$ and $s(s-1) \leq s(s+1) \leq i \leq n - d/2$. This can be rewritten (like in the proof of Lemma 5.3.1) as $\ell \mid |\mathrm{Sp}_{2n}(k)|$ and $\mathrm{defect}(\Sigma_s) \leq k(\mathrm{Sp}_{2n}(k), d)$. Again, by Proposition 3.4.6, $\mathfrak{t}(s, 0) \sim_{\ell, x_n} \mathfrak{t}(0, 0)$.

Finally, $\mathfrak{t}(s, s') \sim_{\ell, x_i} \mathfrak{t}(s, 0) \sim_{\ell, x_n} \mathfrak{t}(0, 0)$, so $\mathfrak{t}(s, s') \sim_\ell \mathfrak{t}(0, 0)$. □

Bringing together everything that has been done so far, we get by Theorems 4.2.7 and 4.3.1.

Theorem 5.3.3. *Let ℓ be a prime not dividing q. Then we have the following decomposition of $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(\mathrm{Sp}_{2n}(F))$ into ℓ-blocks*:

(1) *If $\ell = 2$: $\mathrm{Rep}^{1}_{\overline{\mathbb{Z}}_2}(\mathrm{Sp}_{2n}(F))$ is a 2-block.*

(2) *If $\ell \neq 2$. Let d the order of q modulo ℓ*:

(a) *If d is odd*,

$$\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(\mathrm{Sp}_{2n}(F)) = \prod_{\mathfrak{t}\in\mathcal{T}^{\mathrm{un}}(G)} \mathrm{Rep}^{[\mathfrak{t}]_\ell}_{\overline{\mathbb{Z}}_\ell}(\mathrm{Sp}_{2n}(F)).$$

(b) *If d is even*,

$$\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Z}}_\ell}(\mathrm{Sp}_{2n}(F)) = \mathrm{Rep}^{[\mathfrak{t}(0,0)]_\ell}_{\overline{\mathbb{Z}}_\ell}(\mathrm{Sp}_{2n}(F)) \times \prod_{(s,s')\in\mathcal{S}_c} \mathrm{Rep}^{[\mathfrak{t}(s,s')]_\ell}_{\overline{\mathbb{Z}}_\ell}(\mathrm{Sp}_{2n}(F)).$$

Remark. In the case d odd, or d even and $(s,s')\in\mathcal{S}_c$, we see that the intersection of an ℓ-block with $\mathrm{Rep}^{\mathrm{un}}_{\overline{\mathbb{Q}}_\ell}(G)$ is a Bernstein block.

If $\ell > n$, in the case d even and $(s,s')\in\mathcal{S}_c$, we can say a bit more.

Lemma 5.3.4. *If $\ell > n$, d is even and $(s,s')\in\mathcal{S}_c$, then $\mathrm{Rep}^{[\mathfrak{t}(s,s')]_\ell}_{\overline{\mathbb{Z}}_\ell}(\mathrm{Sp}_{2n}(F)) \cap \mathrm{Rep}_{\overline{\mathbb{Q}}_\ell}(G)$ is a Bernstein block.*

Proof. First of all we have that $[\mathfrak{t}(s,s')]_\ell = \{\mathfrak{t}(s,s')\}$. Let $x\in \mathrm{BT}_0$ such that $x\preceq\sigma(s,s')$. From the definition of $\mathcal{S}_c$ and Proposition 3.4.6 we get that $\mathcal{E}_{\mathfrak{t}(s,s'),x}$ is composed uniquely of d-cuspidal representations. We use Theorem 3.1.3 to describe $\mathcal{E}_{\mathfrak{t}(s,s'),x,\ell}$. Let t be a semisimple conjugacy class in $\overline{\mathsf{G}}^*_x$ of order a power of ℓ. Let $\overline{\mathsf{G}}_x(t)$ a Levi in $\overline{\mathsf{G}}_x$ dual to $C_{\overline{\mathsf{G}}^*_x}(t)^\circ$. The Levi $\overline{\mathsf{G}}_x(t)$ is then a $E_{q,\ell}$-split Levi of $\overline{\mathsf{G}}_x$. But, if $\ell > n$, then ℓ is large for $\overline{\mathsf{G}}_x$ in the sense of [4, Definition 5.1] and therefore $E_{q,\ell} = \{d\}$ by [4, Proposition 5.2]. Thus $\overline{\mathsf{G}}_x(t)$ is a d-split Levi. Hence, if an irreducible constituent of $\mathcal{R}^{\mathsf{G}}_{\mathsf{G}(t)\subseteq\mathsf{P}}(\chi_t)$, for a unipotent character χ_t, is in $\mathcal{E}_{\mathfrak{t}(s,s'),x}$, then $\overline{\mathsf{G}}_x(t) = \overline{\mathsf{G}}_x$. Moreover, $\mathrm{Sp}_{2i}(k)$, doesn't have any nontrivial character, so Theorem 3.1.3 tells us that $\mathcal{E}_{\mathfrak{t}(s,s'),x,\ell} = \mathcal{E}_{\mathfrak{t}(s,s'),x}$. The system of idempotent $e_{\mathfrak{t}(s,s')}$ is therefore integral, and the proof is done. □

6. Stable ℓ-blocks for classical groups

In this section, we want to find the stable depth zero ℓ-blocks for classical unramified groups.

When G is a classical unramified group, we have the local Langlands correspondence [1; 13; 15; 17; 25]. The block decomposition is not compatible with the local Langlands correspondence, two irreducible representations may have the same Langlands parameter but not be in the same block. However, we can look for the "stable" blocks, which are the smallest direct factors subcategories stable by the local Langlands correspondence. These categories correspond to the primitive idempotents in the stable Bernstein center, as defined in [12]. In [19], there is a decomposition of the depth zero category

$$\mathrm{Rep}^0_{\overline{\mathbb{Q}}_\ell}(G) = \prod_{(\phi,\sigma)\in\widetilde{\Phi}_m(I_F^{\overline{\mathbb{Q}}_\ell},{}^L\boldsymbol{G})} \mathrm{Rep}^{(\phi,\sigma)}_{\overline{\mathbb{Q}}_\ell}(G)$$

indexed by the set $\widetilde{\Phi}_m(I_F^{\overline{\mathbb{Q}}_\ell},{}^L\boldsymbol{G})$ as defined in [19, Definition 4.4.2]. This decomposition satisfies the following theorem.

Theorem 6.0.1 [19, Theorem 4.7.5]. *Let G be an unramified classical group, $\Lambda = \overline{\mathbb{Q}}_\ell$ and $p \neq 2$. Then the decomposition*

$$\mathrm{Rep}^0_{\overline{\mathbb{Q}}_\ell}(G) = \prod_{(\phi,\sigma)\in\widetilde{\Phi}_m(I_F,{}^L\boldsymbol{G})} \mathrm{Rep}^{(\phi,\sigma)}_{\overline{\mathbb{Q}}_\ell}(G)$$

is the decomposition of $\mathrm{Rep}^0_{\overline{\mathbb{Q}}_\ell}(G)$ *into stable blocks.*

Over $\bar{\mathbb{Z}}_\ell$, an analogous decomposition is defined in [19]:

$$\mathrm{Rep}^0_{\bar{\mathbb{Z}}_\ell}(G) = \prod_{(\phi,\sigma)\in\widetilde{\Phi}_m(I_F^{\bar{\mathbb{Z}}_\ell},{}^L\boldsymbol{G})} \mathrm{Rep}^{(\phi,\sigma)}_{\overline{\mathbb{Q}}_\ell}(G).$$

We would like to prove that for unramified classical groups, this is the decomposition of the depth zero category into stable ℓ-blocks, that is that these categories correspond to primitive integral idempotents in the stable Bernstein center.

Let $(\phi,\sigma)\in\widetilde{\Phi}_m(I_F^{\overline{\mathbb{Q}}_\ell},{}^L\boldsymbol{G})$. The category $\mathrm{Rep}^{(\phi,\sigma)}_{\overline{\mathbb{Q}}_\ell}(G)$ is obtained by a consistent system of idempotents $e_{T_{(\phi,\sigma)}}$ associated to $T_{(\phi,\sigma)}\subseteq\mathcal{T}(G)$. These subsets $T_{(\phi,\sigma)}$ form a partition of $\mathcal{T}(G)$. A subset $T\subseteq\mathcal{T}(G)$ is said to be stable, if T is a union of $T_{(\phi,\sigma)}$ for $(\phi,\sigma)\in\widetilde{\Phi}_m(I_F^{\overline{\mathbb{Q}}_\ell},{}^L\boldsymbol{G})$.

Lemma 6.0.2. *If G is an unramified classical group and $p\neq 2$, the stable ℓ-blocks correspond to the minimal ℓ-integral stable subsets of $\mathcal{T}(G)$.*

Proof. By Theorem 6.0.1, the primitive idempotents in the stable Bernstein center correspond to the $T_{(\phi,\sigma)}$, hence every idempotent in the stable Bernstein center is associated with T a stable subset of $\mathcal{T}(G)$. Lemma 4.1.2 tells us that if the idempotent is integral then so is T. □

Let $(\phi,\sigma)\in\widetilde{\Phi}_m(I_F^{\overline{\mathbb{Q}}_\ell},{}^L\boldsymbol{G})$. Then [19, Proposition 4.4.6] defines a bijection

$$\Gamma : \widetilde{\Phi}_m(I_F^{\overline{\mathbb{Q}}_\ell},{}^L\boldsymbol{G}) \xrightarrow{\sim} \mathsf{G}^*_{ss}$$

where G^* is the dual of G over k and G^*_{ss} is the set of semisimple rational conjugacy classes in G^*.

Lemma 6.0.3. *Let $(\phi,\sigma)\in\widetilde{\Phi}_m(I_F^{\overline{\mathbb{Q}}_\ell},{}^L\boldsymbol{G})$. Then either $T_{(\phi,\sigma)}\subseteq\mathcal{T}^{\ell'}(G)$ (if $\Gamma(\phi,\sigma)$ is of order prime to ℓ) or $T_{(\phi,\sigma)}\cap\mathcal{T}^{\ell'}(G)=\varnothing$.*

Proof. To $(\phi,\sigma)\in\widetilde{\Phi}_m(I_F^{\overline{\mathbb{Q}}_\ell},{}^L\boldsymbol{G})$ is attached a system of conjugacy classes on the Bruhat–Tits building. By [19, Section 4.3], if $\Gamma(\phi,\sigma)$ is of order prime to ℓ, all of these conjugacy classes are of order prime to ℓ, and if $\Gamma(\phi,\sigma)$ is not of order prime to ℓ, then none of them are. Thus we get the result. □

Corollary 6.0.4. *If T is an ℓ-integral stable set such that $T\cap\mathcal{T}^{\ell'}(G)$ is a minimal stable set then T is a minimal stable ℓ-integral set.*

Proof. If T is an ℓ-integral stable set, then by Proposition 4.1.7 $T\cap\mathcal{T}^{\ell'}(G)\neq\varnothing$ and by Lemma 6.0.3 $T\cap\mathcal{T}^{\ell'}(G)$ is a stable set. Hence $T\cap\mathcal{T}^{\ell'}(G)$ is an nonempty stable set, and we get the result. □

Theorem 6.0.5. *Let G be an unramified classical group and $p \neq 2$. Then the decomposition*

$$\mathrm{Rep}^0_{\overline{\mathbb{Z}}_\ell}(G) = \prod_{(\phi,\sigma)\in\widetilde{\Phi}_m(I_F^{\overline{\mathbb{Z}}_\ell},{}^L\boldsymbol{G})} \mathrm{Rep}^{(\phi,\sigma)}_{\overline{\mathbb{Z}}_\ell}(G).$$

is the decomposition of $\mathrm{Rep}^0_{\overline{\mathbb{Z}}_\ell}(G)$ into stable ℓ-blocks.

Proof. Let $(\phi,\sigma) \in \widetilde{\Phi}_m(I_F^{\overline{\mathbb{Z}}_\ell},{}^L\boldsymbol{G})$. By construction, the category $\mathrm{Rep}^{(\phi,\sigma)}_{\overline{\mathbb{Z}}_\ell}(G)$ is associated with an ℓ-integral subset T of $\mathcal{T}(G)$. By [19, Proposition 4.5.1], $T = \cup_{(\phi',\sigma')} T_{(\phi',\sigma')}$, where the union is taken over the (ϕ',σ') that are sent to (ϕ,σ) by the natural map $\widetilde{\Phi}_m(I_F^{\overline{\mathbb{Q}}_\ell},{}^L\boldsymbol{G}) \to \widetilde{\Phi}_m(I_F^{\overline{\mathbb{Z}}_\ell},{}^L\boldsymbol{G})$, described in [19, Section 4.5] (obtained by restriction from $I_F^{\overline{\mathbb{Q}}_\ell}$ to $I_F^{\overline{\mathbb{Z}}_\ell}$). In particular, the set T is stable. So by Lemma 6.0.2, it remains to prove that T is minimal among the stable ℓ-integral sets.

By [19, Section 4.5], the inverse image of (ϕ,σ) by the map $\widetilde{\Phi}_m(I_F^{\overline{\mathbb{Q}}_\ell},{}^L\boldsymbol{G}) \to \widetilde{\Phi}_m(I_F^{\overline{\mathbb{Z}}_\ell},{}^L\boldsymbol{G})$ is all the (ϕ',σ') such that the ℓ-regular part of $\Gamma(\phi',\sigma')$ is given by $\Gamma(\phi,\sigma)$.

Hence exactly one (ϕ'_0,σ'_0) is such that $\Gamma(\phi'_0,\sigma'_0)$ is of order prime to ℓ. Hence by Lemma 6.0.3, $T \cap \mathcal{T}^{\ell'}(G) = T_{(\phi'_0,\sigma'_0)}$. Since T is an ℓ-integral stable set such that $T \cap \mathcal{T}^{\ell'}(G)$ is a minimal stable set, Corollary 6.0.4 tells us that T is a minimal stable ℓ-integral set, and that completes the proof. □

Acknowledgements

I would like to thank Jean-François Dat for the comments and remarks that made this article a better one.

References

[1] J. Arthur, *The endoscopic classification of representations: orthogonal and symplectic groups*, Amer. Math. Soc. Colloq. Publ. **61**, Amer. Math. Soc., Providence, RI, 2013. MR Zbl

[2] J. N. Bernstein, "Le 'centre' de Bernstein", pp. 1–32 in *Representations of reductive groups over a local field*, edited by P. Deligne, Hermann, Paris, 1984. MR Zbl

[3] C. Bonnafé and R. Rouquier, "Catégories dérivées et variétés de Deligne–Lusztig", *Publ. Math. Inst. Hautes Études Sci.* **97** (2003), 1–59. MR Zbl

[4] M. Broué, G. Malle, and J. Michel, "Generic blocks of finite reductive groups", pp. 7–92 in *Représentations unipotentes génériques et blocs des groupes réductifs finis*, Astérisque **212**, Soc. Math. France, Paris, 1993. MR Zbl

[5] M. Cabanes and M. Enguehard, "On unipotent blocks and their ordinary characters", *Invent. Math.* **117**:1 (1994), 149–164. MR Zbl

[6] M. Cabanes and M. Enguehard, "On blocks of finite reductive groups and twisted induction", *Adv. Math.* **145**:2 (1999), 189–229. MR Zbl

[7] M. Cabanes and M. Enguehard, *Representation theory of finite reductive groups*, New Math. Monogr. **1**, Cambridge Univ. Press, 2004. MR Zbl

[8] R. W. Carter, *Finite groups of Lie type*: *conjugacy classes and complex characters*, Wiley, New York, 1985. MR Zbl

[9] J.-F. Dat, "Equivalences of tame blocks for p-adic linear groups", *Math. Ann.* **371**:1-2 (2018), 565–613. MR Zbl

[10] P. Deligne and G. Lusztig, "Representations of reductive groups over finite fields", *Ann. of Math.* (2) **103**:1 (1976), 103–161. MR Zbl

[11] F. Digne and J. Michel, *Representations of finite groups of Lie type*, Lond. Math. Soc. Stud. Texts **21**, Cambridge Univ. Press, 1991. MR Zbl

[12] T. J. Haines, "The stable Bernstein center and test functions for Shimura varieties", pp. 118–186 in *Automorphic forms and Galois representations*, *II*, vol. Durham, UK, 2011, edited by F. Diamond et al., Lond. Math. Soc. Lect. Note Ser. **415**, Cambridge Univ. Press, 2014. MR Zbl

[13] M. Harris and R. Taylor, *The geometry and cohomology of some simple Shimura varieties*, Ann. of Math. Stud. **151**, Princeton Univ. Press, 2001. MR Zbl

[14] D. Helm, "The Bernstein center of the category of smooth $W(k)[\mathrm{GL}_n(F)]$-modules", *Forum Math. Sigma* **4** (2016), art. id. e11. MR Zbl

[15] G. Henniart, "Une preuve simple des conjectures de Langlands pour GL(n) sur un corps p-adique", *Invent. Math.* **139**:2 (2000), 439–455. MR Zbl

[16] G. James and A. Kerber, *The representation theory of the symmetric group*, Encycl. Math. Appl. **16**, Addison-Wesley, Reading, MA, 1981. MR Zbl

[17] T. Kaletha, A. Minguez, S. W. Shin, and P.-J. White, "Endoscopic classification of representations: inner forms of unitary groups", preprint, 2014. arXiv 1409.3731

[18] T. Lanard, "Sur les ℓ-blocs de niveau zéro des groupes p-adiques", *Compos. Math.* **154**:7 (2018), 1473–1507. MR Zbl

[19] T. Lanard, "Sur les ℓ-blocs de niveau zéro des groupes p-adiques, II", *Ann. Sci. École Norm. Sup.* (4) **54**:3 (2021), 683–750. MR Zbl

[20] P. Latham, "The unicity of types for depth-zero supercuspidal representations", *Represent. Theory* **21** (2017), 590–610. MR Zbl

[21] G. Lusztig, "Irreducible representations of finite classical groups", *Invent. Math.* **43**:2 (1977), 125–175. MR Zbl

[22] G. Lusztig, *Characters of reductive groups over a finite field*, Ann. of Math. Stud. **107**, Princeton Univ. Press, 1984. MR Zbl

[23] G. Lusztig, "On the representations of reductive groups with disconnected centre", pp. 157–166 in *Orbites unipotentes et représentations*, *I*, Astérisque **168**, Soc. Math. France, Paris, 1988. MR Zbl

[24] R. Meyer and M. Solleveld, "Resolutions for representations of reductive p-adic groups via their buildings", *J. Reine Angew. Math.* **647** (2010), 115–150. MR Zbl

[25] C. P. Mok, *Endoscopic classification of representations of quasi-split unitary groups*, Mem. Amer. Math. Soc. **1108**, Amer. Math. Soc., Providence, RI, 2015. MR Zbl

[26] L. Morris, "Level zero $\mathbb{G}$-types", *Compos. Math.* **118**:2 (1999), 135–157. MR Zbl

[27] V. Sécherre and S. Stevens, "Block decomposition of the category of ℓ-modular smooth representations of GL_n(F) and its inner forms", *Ann. Sci. École Norm. Sup.* (4) **49**:3 (2016), 669–709. MR Zbl

[28] M.-F. Vignéras, "Induced R-representations of p-adic reductive groups", *Selecta Math.* (*N.S.*) **4**:4 (1998), 549–623. MR Zbl

Communicated by Wee Teck Gan
Received 2021-07-26 Revised 2022-06-27 Accepted 2022-10-04

thomas.lanard@univie.ac.at *Faculty of Mathematics, University of Vienna, Vienna, Austria*

msp

ALGEBRA AND NUMBER THEORY 17:9 (2023)
https://doi.org/10.2140/ant.2023.17.1573

Isotriviality, integral points, and primitive primes in orbits in characteristic p

Alexander Carney, Wade Hindes and Thomas J. Tucker

We prove a characteristic p version of a theorem of Silverman on integral points in orbits over number fields and establish a primitive prime divisor theorem for polynomials in this setting. In characteristic p, the Thue–Siegel–Dyson–Roth theorem is false, so the proof requires new techniques from those used by Silverman. The problem is largely that isotriviality can arise in subtle ways, and we define and compare three different definitions of isotriviality for maps, sets, and curves. Using results of Favre and Rivera-Letelier on the structure of Julia sets, we prove that if φ is a nonisotrivial rational function and β is not exceptional for φ, then $\varphi^{-n}(\beta)$ is a nonisotrivial set for all sufficiently large n; we then apply diophantine results of Voloch and Wang that apply for all nonisotrivial sets. When φ is a polynomial, we use the nonisotriviality of $\varphi^{-n}(\beta)$ for large n along with a partial converse to a result of Grothendieck in descent theory to deduce the nonisotriviality of the curve $y^\ell = \varphi^n(x) - \beta$ for large n and small primes $\ell \neq p$ whenever β is not postcritical; this enables us to prove stronger results on Zsigmondy sets. We provide some applications of these results, including a finite index theorem for arboreal representations coming from quadratic polynomials over function fields of odd characteristic.

1. Introduction and Statement of Results

In [36, Theorem A], Silverman proved the following theorem.

Theorem 1.1 [36, Theorem A]. *Let $\varphi \in \mathbb{Q}(z)$ be rational function of degree at least 2, and let $\alpha \in \mathbb{P}^1(\mathbb{Q})$. If $\varphi^2 \notin \mathbb{Q}[z]$, then the set $\{\varphi^n(\alpha) \mid n \in \mathbb{Z}^+\}$ contains only finitely many points in $\mathbb{Z}$.*

We prove that the analogous theorem holds for nonisotrivial rational functions in $\mathbb{F}_p(t)$. Recall that a rational function $\varphi \in \mathbb{F}_p(t)(z)$ is said to be isotrivial if there is a $\sigma \in \overline{\mathbb{F}_p(t)}(z)$ of degree 1 such that $\sigma \circ \varphi \circ \sigma^{-1} \in \overline{\mathbb{F}}_p(z)$. We prove the following.

Theorem 1.2. *Let $\varphi \in \mathbb{F}_p(t)(z)$ be a nonisotrivial rational function of degree at least 2, and let $\alpha \in \mathbb{P}^1(\mathbb{F}_p(t))$. If $\varphi^2 \notin \mathbb{F}_p(t)[z]$, then $\{\varphi^n(\alpha) \mid n \in \mathbb{Z}^+\}$ contains only finitely many points in $\mathbb{F}_p[t]$.*

Silverman [36] also proves Theorem 1.1 over number fields; see [36, Theorem B]. Likewise, our most general form of Theorem 1.2 is stated in terms of S-integrality and isotriviality for rational functions defined over finite extensions of $\mathbb{F}_p(t)$. We will define S-integrality in the next section (see Definition 2.1). We give our more general definition of isotriviality for rational functions here.

MSC2020: primary 37P15; secondary 11G50, 11R32, 14G25, 37P05, 37P30.
Keywords: arithmetic dynamics, integral points, arboreal representations, Zsigmondy sets.

Definition 1.3. Let K be a finite extension of $\mathbb{F}_p(t)$ and let φ be a rational function in $K(z)$. We say that φ is an isotrivial rational function if there exists $\sigma \in \overline{K}(z)$ of degree 1 such that $\sigma \circ \varphi \circ \sigma^{-1} \in \overline{\mathbb{F}}_p(z)$.

Also recall that for a rational function $\varphi \in K(z)$, a point $\beta \in \mathbb{P}^1(K)$ is said to be *exceptional* for φ if its total orbit (both forward and backward) is finite. However, for the maps that we consider, this amounts to $\varphi^{-2}(\beta) = \{\beta\}$ by Riemann–Hurwitz. In particular, since totally inseparable maps are isotrivial (which may be seen by moving fixed points to 0 and ∞), we avoid the more exotic cases of exceptional points arising in positive characteristic; see, for instance, [38]. With this in place, we state our general form of Theorem 1.2.

Theorem 1.4. *Let K be a finite extension of $\mathbb{F}_p(t)$, let $\varphi \in K(z)$ be a nonisotrivial rational function with $\deg \varphi > 1$, let S be a finite set of places of K, and let $\alpha, \beta \in K$ where β is not exceptional for φ. Then $\{\varphi^n(\alpha) \mid n \in \mathbb{Z}^+\}$ contains only finitely many points that are S-integral relative to β.*

The main tools used in the proof of [36, Theorem A] are from diophantine approximation. Roughly, one takes an inverse image $\varphi^{-i}(\infty)$ that contains at least three points and applies Siegel's theorem on integral points for the projective line with at least three points deleted to conclude that there only finitely many n such that $\varphi^n(\alpha)$ are integral relative to $\varphi^{-i}(\infty)$ and thus only finitely many $n + i$ such that $\varphi^{n+i}(\alpha)$ is an integer. Over function fields in characteristic p, the problem is more complicated since Roth's theorem is false; in fact, no improvement on Liouville's theorem is possible in general. There is, however, a weaker version of Siegel's theorem, due to Wang [45, Theorem in $\mathbb{P}^1(K)$, page 337] and Voloch [44], which states that, for function fields in characteristic p, there are finitely many S-integral points on the projective line with a nonisotrivial set of points deleted. (Note that this is strictly weaker than Siegel's theorem, since any set of three points is automatically isotrivial, and there are isotrivial sets of every countable cardinality.) Basic functorial results on integral points thus imply that Theorem 1.4 will hold whenever $\varphi^{-n}(\beta)$ is a nonisotrivial set. In Theorem 3.1, we show that $\varphi^{-n}(\beta)$ is a nonisotrivial set for large n whenever φ is a nonisotrivial rational function and β is not exceptional, using results of Favre and Rivera-Letelier [14] on the structure of Julia sets at primes of genuinely bad reduction.

In the case where φ is a polynomial of separable degree greater than 1, we can prove a bit more than Theorem 1.4. To describe our result we need a bit of terminology. For a sequence $\{b_n\}_{n=1}^{\infty}$ of elements of a global field K, we say that a place $\mathfrak{p}$ of K is a *primitive divisor* of b_n if

$$v_{\mathfrak{p}}(b_n) > 0 \text{ and } v_{\mathfrak{p}}(b_m) \leq 0 \quad \text{for all } m < n.$$

For a positive integer ℓ, we say that $\mathfrak{p}$ is a *primitive ℓ-divisor* of b_n if

$$\mathfrak{p} \text{ is a primitive divisor of } b_n \text{ and } \ell \nmid v_{\mathfrak{p}}(b_n).$$

Given a rational function $\varphi \in K(x)$ and points $\alpha, \beta \in K$, we obtain a sequence $\{\varphi^n(\alpha) - \beta\}_{n=1}^{\infty}$. We define the Zsigmondy set $\mathcal{Z}(\varphi, \alpha, \beta)$ (see [3; 47]) for φ, α, and β as

$$\mathcal{Z}(\varphi, \alpha, \beta) = \{n \mid \varphi^n(\alpha) - \beta \text{ has no primitive divisors}\}.$$

Likewise, for a positive integer ℓ and α, β, and φ as above, we define the ℓ-Zsigmondy set $\mathcal{Z}(\varphi, \alpha, \beta, \ell)$ for φ, α, β, and ℓ as

$$\mathcal{Z}(\varphi, \alpha, \beta, \ell) = \{n \mid \varphi^n(\alpha) - \beta \text{ has no primitive } \ell\text{-divisors}\}.$$

We will also need a precise definition of critical points to state our next theorem. Let φ be a rational function in $K(z)$. We let $\deg_s \varphi$ denote the degree of the maximal separable extension of $K(\varphi(z))$ in $K(z)$ and let $\deg_i \varphi = (\deg \varphi)/(\deg_s \varphi)$; note that $\deg_i \varphi$ is also the largest power p^r of p such that φ can be written as $\varphi(z) = g(x^{p^r})$ for some rational function $g \in K(z)$. For $\gamma \in \mathbb{P}^1$, there are degree one rational functions $\sigma, \theta \in K(z)$ such that $\theta(0) = \gamma$ and $\sigma \circ \varphi \circ \theta(0) = 0$. We may then write $\sigma \circ \varphi \circ \theta(z) = z^e g(z)$ for some rational function g such that $g(z) \neq 0$. We call e the *ramification degree* of φ at γ denote it as $e_\varphi(\gamma/\varphi(\gamma))$. We say that γ is a *critical point* of φ if $e_\varphi(\gamma/\varphi(\gamma)) > \deg_i \varphi$.

We let $O_\varphi^+(\alpha)$ denote the set $\{\varphi^n(\alpha) \mid n \in \mathbb{Z}^+\}$, called the forward orbit of α with respect to ϕ. Moreover, we say that a point β is postcritical if there is a critical point γ of φ such that $\beta \in O^+(\gamma)$.

With this terminology, we have the following two theorems for polynomials.

Theorem 1.5. *Let K be a finite extension of $\mathbb{F}_p(t)$, let $f \in K[z]$ be a nonisotrivial polynomial with* $\deg f > 1$, *and let α and β be elements of K such that α is not preperiodic, β is not postcritical, and $\beta \notin O_f^+(\alpha)$. Then for any prime $\ell \neq p$, the Zsigmondy set $\mathcal{Z}(f, \alpha, \beta, \ell)$ is finite.*

Theorem 1.6. *Let K be a finite extension of $\mathbb{F}_p(t)$, let $f \in K[z]$ be a nonisotrivial polynomial with* $\deg f > 1$, *and let α and β be elements of K such that α is not preperiodic, β is not exceptional for f, and $\beta \notin O_f^+(\alpha)$. Then the Zsigmondy set $\mathcal{Z}(f, \alpha, \beta)$ is finite.*

Theorem 1.4 is not true in general for isotrivial rational functions, and Theorems 1.5 and 1.6 are not true not in general for isotrivial polynomials; see [30]. There are some results in the isotrivial case, however (see [21]), and some of the techniques here do work for a wide class of isotrivial rational functions. We may address these questions in a future paper.

Theorem 1.4 is proved by using two different notions of isotriviality. The first is our Definition 1.3 for functions. We now define an isotrivial set. Here we use a simple, if inelegant, definition rather than a slightly more technical one that generalizes to varieties other than $\mathbb{P}^1$. Below we regard an element of $\overline{K}(z)$ as a map from $\overline{K} \cup \infty$ to itself.

Definition 1.7. Let K be a finite extension of $\mathbb{F}_p(t)$ and let $\mathcal{S}$ be a finite subset of $\overline{K} \cup \infty$. We say that $\mathcal{S}$ is a isotrivial set if there exists $\sigma \in \overline{K}(z)$ of degree 1 such that $\sigma(\mathcal{S}) \subseteq \overline{\mathbb{F}}_p \cup \infty$.

We note that if φ is a nonisotrivial rational function the set $\varphi^{-1}(\beta)$ may still be an isotrivial set; for example any set of three or fewer elements is an isotrivial set, but there are nonisotrivial rational functions of degree 2 and 3.

Theorem 1.5 is proved using a third notion of isotriviality, this time for curves.

Definition 1.8. Let K be a finite extension of $\mathbb{F}_p(t)$ and let C be a curve defined over K. We say that C is an isotrivial curve if there is a curve C' defined over a finite extension k' of $K \cap \overline{\mathbb{F}}_p$ and a finite

extension K' of K such that

$$C \times_K K' \cong C' \times_{k'} K'.$$

An outline of the paper is as follows. Throughout this paper, K is a finite extension of $\mathbb{F}_p(t)$ as in Definitions 1.3 ,1.7, and 1.8. In Section 2, we introduce some basic facts about heights, integral points, and cross ratios that are used throughout the paper. Following that, we prove Theorem 3.1, which says that if φ is a nonisotrivial rational function of degree greater than 1 and β is not exceptional for φ, then $\varphi^{-n}(\beta)$ is a nonisotrivial set for all sufficiently large n. The proof uses work of Baker [1] and Favre and Rivera-Letelier [14] to produce elements in $\varphi^{-n}(\beta)$ whose v-adic cross ratio is not 1 at a place v of bad reduction. We then apply work of [45] (see also [44]) to give a quick proof of Theorem 1.4 in Section 4. In Section 5, we begin by proving Corollary 5.3, which states that if the roots of a polynomial F are distinct and form a nonisotrivial set, then the curve C given by $y^\ell = F(x)$ is a nonisotrivial curve when $\ell \neq p$ is a prime that is small relative to the degree of F. The techniques we use to do this build upon work in [19]; the idea is to use the adjunction formula to show that the projection map onto the x-coordinate is the unique map $\theta : C \to \mathbb{P}^1$ of degree ℓ up to change of coordinates on $\mathbb{P}^1$ (see Lemma 5.1). We then use Corollary 5.3 and Theorem 3.1 to show the nonisotriviality of curves associated to $\varphi^{-n}(\beta)$, where φ is a nonisotrivial rational function of degree greater than 1 and β is not exceptional for φ, in Theorem 5.5. In Section 6, we prove Proposition 6.1, which immediately implies Theorems 1.5 and 1.6; the proof uses Theorem 3.1 along with height bounds on nonisotrivial curves in characteristic p due to Szpiro [41] and Kim [25] (see Theorem 6.3). Finally, in Section 7, we present some applications of our results to other dynamical questions.

We note that the proof of Theorem 3.1 works the same for function fields in characteristic 0 as for function fields in characteristic p. Theorems 1.4, 1.5, and 1.6 all hold in stronger forms for function fields in characteristic 0, as proved in [16]; the main difference here is that Yamanoi [46] has proved the full Vojta conjecture for algebraic points on curves over function fields of characteristic 0 (see [43; 42]), whereas Theorem 6.3 is weaker than the full Vojta conjecture for algebraic points on curves over function fields of characteristic p. Analogs of Theorems 1.5 and 1.6 have not yet been proved over number fields, except in some very special cases (see [3; 47; 33; 31; 32]), but both theorems are implied by the *abc* conjecture (see [16]).

2. Preliminaries

In this section we will review some terminology and results on heights, integral points, and dynamics. For background on heights; see [20; 26; 6]. We set some notation below.

Throughout this paper, K will denote a finite extension of $\mathbb{F}_p(t)$ and k will denote the intersection $K \cap \overline{\mathbb{F}}_p$. Equivalently, K is the function field of a smooth, projective curve B defined over k.

2A. ***Places, heights, and reduction.*** Let M_K be the set of places of K, which corresponds to the set of closed points of B.

Since K is a function field, we choose a place $\mathfrak{p}_\infty$ of K, denote

$$\mathfrak{o}_K = \{z \in K \mid v_\mathfrak{p}(z) \geq 0 \text{ for all } \mathfrak{p} \neq \mathfrak{p}_\infty\},$$

and let $k_\mathfrak{p}$ be the residue field $\mathfrak{o}_K/\mathfrak{p}$. Also, define the local degree of $\mathfrak{p}$ to be

$$N_\mathfrak{p} = [k_\mathfrak{p} : k].$$

Likewise, for each $\mathfrak{p} \in M_K$ we let $|\cdot|_\mathfrak{p}$ be a normalized absolute value such that the product formula

$$\prod_{\mathfrak{p} \in M_K} |z|_\mathfrak{p} = 1$$

holds for all $z \in K^*$. Moreover, we define $K_\mathfrak{p}$ to be the completion of K with respect to $|\cdot|_\mathfrak{p}$ and define $\mathbb{C}_\mathfrak{p}$ to be the completion of the algebraic closure of $K_\mathfrak{p}$.

For $z \in K$, let $h(z)$ denote the logarithmic height of K. For $\varphi \in K(z)$ with $\deg \varphi = d \geq 2$, let $h_\varphi(z)$ denote the Call–Silverman canonical height of z relative to φ [13], defined by

$$h_\varphi(z) = \lim_{n\to\infty} \frac{h(\varphi^n(z))}{d^n}.$$

We will often write sums indexed by primes that satisfy some condition. These are taken to be primes of $\mathfrak{o}_K$. As an example of our indexing convention, observe that

$$\sum_{v_\mathfrak{p}(z)>0} v_\mathfrak{p}(z) N_\mathfrak{p} \leq h(z).$$

We say that a rational function $\varphi \in K(z)$ has *good reduction* at a place $\mathfrak{p}$ of K if the map it induces on $\mathbb{P}^1$ is nonconstant and well-defined modulo $\mathfrak{p}$. More precisely, we write $\varphi(x) = f/g$, where all the coefficients of f and g are in $(\mathfrak{o}_K)_\mathfrak{p}$, and either f or g has at least one coefficient in $(\mathfrak{o}_K)_\mathfrak{p}^*$. We let $f_\mathfrak{p}$ and $g_\mathfrak{p}$ denote the reductions of f and g at $\mathfrak{p}$. We say that φ has good reduction at $\mathfrak{p}$ if $f_\mathfrak{p}$ and $g_\mathfrak{p}$ have no common root in the algebraic closure of the residue field of $\mathfrak{p}$ and $\deg(f_\mathfrak{p}/g_\mathfrak{p}) = \deg \varphi$. We say that φ has *bad reduction* at $\mathfrak{p}$ if it does not have good reduction at $\mathfrak{p}$. This notion is dependent on our choice of coordinates. We say that φ has *potentially good reduction* at $\mathfrak{p}$ if there is a finite extension K' of K, a prime $\mathfrak{q}$ of K' lying over $\mathfrak{p}$, and a degree one rational function $\sigma \in K'(z)$ such that $\sigma \circ \varphi \circ \sigma^{-1}$ has good reduction at $\mathfrak{q}$. We say that φ has *genuinely bad reduction* at $\mathfrak{p}$ if φ does not have potentially good reduction at $\mathfrak{p}$.

2B. ***Integral points.*** Let S be a nonempty finite subset of M_K. The ring of S-integers in K is defined to be

$$\mathfrak{o}_{K,S} := \{z \in K : |z|_\mathfrak{p} \leq 1 \text{ for all } \mathfrak{p} \notin S\}.$$

Given a place $\mathfrak{p}$ of K and two points $\alpha = [x_1 : y_1]$ and $\beta = [x_2, y_2]$ in $\mathbb{P}^1(\mathbb{C}_\mathfrak{p})$, define the $\mathfrak{p}$-*adic chordal metric* $\delta_\mathfrak{p}$ by

$$\delta_\mathfrak{p}(\alpha, \beta) = \frac{|x_1 y_2 - y_1 x_2|_\mathfrak{p}}{\max\{|x_1|_\mathfrak{p}, |y_1|_\mathfrak{p}\} \cdot \max\{|x_2|_\mathfrak{p}, |y_2|_\mathfrak{p}\}}.$$

Note that we always have $0 \leq \delta_{\mathfrak{p}}(\alpha, \beta) \leq 1$, and that $\delta_{\mathfrak{p}}(\alpha, \beta) = 0$ if and only if $\alpha = \beta$. Then the ring $\mathfrak{o}_{K,S}$ is equivalent to the set which is maximally distant from ∞ outside of S, i.e., the set of $z \in K$ such that

$$\delta_{\mathfrak{p}}(z, \infty) = \delta_{\mathfrak{p}}([z : 1], [1, 0]) = 1$$

for all $\mathfrak{p} \notin S$.

We can now extend our definition of S-integrality to any divisor D on $\mathbb{P}^1$ that is defined over K.

Definition 2.1. Fix a nonempty finite set of places $S \subset M_K$. Let D be an effective divisor on $\mathbb{P}^1$ that is defined over K. Then $\alpha \in \mathbb{P}^1(K)$ is S-integral relative to D provided that for all places $\mathfrak{p} \notin S$, all $\tau \in \mathrm{Gal}(\overline{K}/K)$, and all $\beta \in \mathrm{Supp}\, D$, we have

$$\delta_{\mathfrak{p}}(\alpha, \tau(\beta)) = 1.$$

For affine coordinates $[\alpha : 1] \in \mathbb{P}^1(K)$ and a divisor D defined over K that does not contain the point at infinity in its support, the statement that $[\alpha : 1]$ is S-integral relative to D is equivalent to

$$\begin{aligned} |\alpha - \tau(\beta)|_{\mathfrak{p}} &\geq 1 \quad \text{if } |\tau(\beta)|_{\mathfrak{p}} \leq 1, \text{ and} \\ |\alpha|_{\mathfrak{p}} &\leq 1 \quad \text{if } |\tau(\beta)|_{\mathfrak{p}} > 1 \end{aligned}$$

for all $\mathfrak{p} \notin S$, all $\tau \in \mathrm{Gal}(\overline{K}/K)$, and all $[1 : \beta] \in \mathrm{Supp}\, D$.

Let θ be a linear fractional change of coordinate on $\mathbb{P}^1(\overline{K})$. Then α is S-integral relative to β if and only if $\theta(\alpha)$ is S-integral relative to $\theta(\beta)$ provided we allow an enlargement of S depending only on θ. We prove a variant of this statement for any $\theta \in K[x]$ later in the paper. The following is a simple and standard consequence of our definition of S-integrality (see [39, Corollary 2.4], for example). Recall that for a point $\alpha \in \mathbb{P}^1(K)$, the divisor $\varphi^*(\alpha)$ is defined as $\sum_{\varphi(\beta)=\alpha} e_\varphi(\beta/\alpha)\beta$.

Lemma 2.2. *Let $\varphi \in K(x)$ and S be a set of primes containing all the primes of bad reduction for φ. Then, for any $\alpha, \gamma \in \mathbb{P}^1(K)$, we have that $\varphi(\gamma)$ is S-integral relative to α if and only if γ is S-integral relative to $\varphi^*(\alpha)$.*

2C. ***The cross ratio.*** Let $|\cdot|$ be a non-Archimedean absolute value on a field L. For any distinct $x_1, x_2, y_1, y_2 \in L$ we define

$$(x_1, x_2; y_1, y_2) = \frac{|x_1 - y_2||x_2 - y_1|}{|x_1 - y_1||x_2 - y_2|}.$$

We may extend this to points in $x_1, x_2, y_1, y_2 \in L \cup \infty$ by eliminating the terms involving ∞; for example,

$$(\infty, x_2; y_1, y_2) = \frac{|x_2 - y_1|}{|x_2 - y_2|}.$$

Importantly, for $\sigma \in \mathrm{PGL}_2(L)$, we have $(z_1, z_2; z_3, z_4) = (\sigma z_1, \sigma z_2; \sigma z_3, \sigma z_4)$. This is easily seen by noting that an element of $\mathrm{PGL}_2(L)$ is a composition of translations, scaling maps, and the map sending every element to its multiplicative inverse, and that $(z_1, z_2; z_3, z_4)$ is invariant under all these types of maps.

We will use the following two lemmas for points $x_1, x_2, y_1, y_2 \in L$. The first lemma is immediate.

Lemma 2.3. *Suppose that* $|x_1| < |y_1| < |x_2| < |y_2|$. *Then*

$$(x_1, x_2; y_1, y_2) = \frac{|y_2||x_2|}{|y_1||y_2|} > 1.$$

Lemma 2.4. *Suppose that there are points* $a_1, a_2 \in L$ *such that* $|x_1 - a_1|, |y_1 - a_1| < |a_1 - a_2|$ *and* $|x_2 - a_2|, |y_2 - a_2| < |a_1 - a_2|$. *Then*

$$(x_1, x_2; y_1, y_2) > 1.$$

Proof. After a translation, we may assume that $a_1 = 0$. Then $|x_1|, |y_1| < |a_2|$ and $|x_2|, |y_2| = |a_2|$. Thus, we have

$$(x_1, x_2; y_1, y_2) = \frac{|a_2||a_2|}{|x_1 - y_1||x_2 - y_2|} > 1. \qquad \square$$

Remark 2.5. The cross ratio of x_1, x_2, y_1, y_2 is often defined without taking absolute values, i.e., as

$$\frac{(x_1 - y_2)(x_2 - y_1)}{(x_1 - y_1)(x_2 - y_2)}.$$

The advantage of the definition we use is that it extends to points in Berkovich space; see [14]. While we do not use this extension, it can be used to give a quick proof of our Proposition 3.2. We give a slightly longer proof that we think may be more accessible for some readers.

3. Nonisotriviality of inverse images

In this section, we will prove the following theorem.

Theorem 3.1. *Let* $\varphi \in K(z)$ *have* $\deg \varphi > 1$. *Suppose that* φ *is not isotrivial and that* β *is not exceptional for* φ. *Then for all sufficiently large* n *the set* $\varphi^{-n}(\beta)$ *is not an isotrivial set.*

We will derive Theorem 3.1 from the following proposition.

Proposition 3.2. *Suppose* $\varphi \in K(z)$ *has genuinely bad reduction at the prime* $\mathfrak{p}$. *Let* $|\cdot|$ *be an extension of* $|\cdot|_{\mathfrak{p}}$ *to* $\mathbb{C}_{\mathfrak{p}}$. *Then for any nonexceptional* $\alpha \in K$, *and for all sufficiently large* n, *there are elements* $z_1, z_2, z_3, z_4 \in \varphi^{-n}(\alpha)$ *such that*

$$(z_1, z_2; z_3, z_4) > 1.$$

Proof. We work over the non-Archimedean complete field $\mathbb{C}_{\mathfrak{p}}$, and consider the dynamical system induced by φ on the Berkovich projective line $\mathbb{P}^{1,an}$. We will use some basic facts about the topology of the Berkovich projective line, including the classification of points as Type I, II, III, or IV; see [2] or [4] for a detailed description of the topology of the Berkovich projective line.

By [14, Théorème E] (see also [4, Theorem 8.15]), bad reduction implies that the equilibrium measure ρ_φ is nonatomic. Thus, there are four or more points all of the same type (I, II, III, or IV) in the support of ρ_φ.

Since ρ_φ is nonatomic and the inverse images of a nonexceptional point equidistribute with respect to ρ_φ we have the following fact.

Fact 3.3. For any γ in the support of ρ_φ, any open subset U containing γ, and any positive integer m, there is an N such that $U \cap \varphi^{-n}(\beta)$ contains m or more points for all $n \geq N$.

We also have the following basic facts about the topology of $\mathbb{P}^{1,an}$.

Fact 3.4. Let $\xi(a, r)$, where $a \in K$ and $r > 0$, be a point of Type II or Type III corresponding to the disc $\{x \in K \mid |x-a| \leq r\}$. Then for any $\epsilon > 0$, there is an open set $U \subset \mathbb{P}^{1,an}$ with $\xi(a, r) \in U$ such that every point x of Type I in U satisfies $r - \epsilon < |x - a| < r + \epsilon$.

Fact 3.5. Let a_1 and a_2 be any two points of the same type in $\mathbb{P}^{1,an}$, which are not concentric Type II or III points. Then there exist open sets U_1 and U_2 with $a_1 \in U_1$ and $a_2 \in U_2$ such that $U_1 \cap \mathbb{P}^1(\mathbb{C}_\mathfrak{p})$ and $U_2 \cap \mathbb{P}^1(\mathbb{C}_\mathfrak{p})$ are disjoint open discs.

Proof. Since a_1 and a_2 are not concentric, $a_1 \wedge a_2$, the unique point such that $[a_1, \infty] \cap [a_2, \infty] = [a_1 \wedge a_2, \infty]$, is not equal to a_1 or a_2; see [14]. Now let D_i be the open disc corresponding to any Type II point in the open interval $(a_i, a_1 \wedge a_2)$, for $i = 1, 2$. Then there are open sets U_i such that $U_i \cap \mathbb{P}^1(\mathbb{C}_\mathfrak{p}) = D_i$. □

Now suppose that the support of ρ_φ contains two nonconcentric points z_1, z_2 of the same type. Then, by Facts 3.3 and 3.5, for all sufficiently large n there must be open discs $D(a_1, r_1)$ and $D(a_2, r_2)$ with $|a_1 - a_2| > \max\{r_1, r_2\}$ and points $x_1, x_2, y_1, y_2 \in \varphi^{-n}(\beta)$ with $x_1, y_1 \in D(a_1, r_1)$ and $x_2, y_2 \in D(a_2, r_2)$. By Lemma 2.4, we have

$$(x_1, x_2; y_1, y_2) > 1,$$

proving the proposition.

Now suppose that ρ_φ contains four concentric points of Type II or Type III, corresponding to closed discs $\bar{D}(a, r_i)$, for $i = 1, 2, 3, 4$, for some fixed a. We suppose that $r_1 < r_2 < r_3 < r_4$, and after an affine change of coordinates, we may suppose that $a = 0$. By Facts 3.3 and 3.4, for any $\epsilon > 0$, there must be an n such that $\varphi^{-n}(\beta)$ contains points z_1, z_2, z_3, z_4 with $|z_i|$ within ϵ of r_i for each i. Choosing ϵ appropriately, we will then have $|z_1| < |z_2| < |z_3| < |z_4|$. Then $(z_1, z_3; z_2, z_4) > 1$ by Lemma 2.3. □

Proof of Theorem 3.1. By [1, Theorem 1.9], since φ is nonisotrivial, it must have genuine bad reduction over some prime $\mathfrak{p}$. Then we may apply Proposition 3.2 to obtain four points in $\varphi^{-n}(\beta)$ with cross ratio greater than one for any sufficiently large n. Since the cross ratio of four points in $\bar{\mathbb{F}}_p \cup \infty$ is always 1 and the cross ratio is invariant under change of coordinate, we see then that $\varphi^{-n}(\beta)$ is a nonisotrivial set for all sufficiently large n. □

4. Proof of Theorem 1.4

We will use the following theorem due to Wang [45, Theorem in $\mathbb{P}^1(K)$, page 337] and Voloch [44].

Theorem 4.1. *Let D be an effective divisor on $\mathbb{P}^1$ that is defined over K. If the points in* Supp D *form a nonisotrivial set, then the set of points in $\mathbb{P}^1(K)$ that are S-integral relative to D is finite.*

The corollary below follows easily.

Corollary 4.2. *Let $\varphi \in K(z)$, let $\beta \in K$. Suppose that there is some i such that $\varphi^{-i}(\beta)$ is not an isotrivial set. Then for any $\alpha \in K$, the forward orbit $O_\varphi^+(\alpha)$ contains only finitely many points that are S-integral relative to β.*

Proof. We may extend S to contain all the primes of bad reduction for φ. The set of iterates $\varphi^{n-i}(\alpha)$ that are S-integral relative to $(\varphi^i)^*(\beta)$ is finite by Theorem 4.1, so by Lemma 2.2, the set of points $\varphi^n(\alpha)$ that are S-integral relative to β must be finite. □

The proof of Theorem 1.4 is now easy.

Proof of Theorem 1.4. By Theorem 3.1, there is some i such that $\varphi^{-i}(\beta)$ is not an isotrivial set. Applying Corollary 4.2 then gives the desired conclusion. □

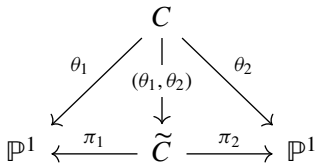
5. Nonisotriviality of certain curves

Let $\pi : C \to \mathbb{P}^1$ be a separable nonconstant morphism defined over K. We define the *ramification locus* of π to be the support of $\pi(R_\pi)$, where R_π is the ramification divisor of π. If the ramification locus of π is an isotrivial set, then it follows from descent theory (see [34], for example) that C must be isotrivial. On the other hand, given any finite subset $\mathcal{U}$ of $\mathbb{P}^1$, one can use interpolation to construct a nonconstant separable morphism $f : \mathbb{P}^1 \to \mathbb{P}^1$ such that the ramification locus of f contains $\mathcal{U}$; thus, there are isotrivial curves that admit nonconstant separable morphisms $\pi : C \to \mathbb{P}^1$ such that the ramification locus of π is a nonisotrivial set. We can show, however, that if the degree of $\pi : C \to \mathbb{P}^1$ is a prime $\ell \neq p$ that is small relative to the genus of C and the ramification locus of π is a nonisotrivial set, then C must indeed be a nonisotrivial curve. This enables us to prove Theorem 5.5, which gives rise to diophantine estimates used in the proofs of Theorems 1.5 and 1.6. The technique here is similar to that of [19]. We begin with a lemma about uniqueness of low prime degree maps on curves of high genus.

Lemma 5.1. *Let C be a curve of genus g over K and let ℓ be a prime such that $(\ell-1)^2 < g$ and $\ell \neq p$. Suppose there is morphism $\theta_1 : C \to \mathbb{P}^1$ of degree ℓ. Then for any morphism $\theta_2 : C \to \mathbb{P}^1$ of degree ℓ, there is an automorphism $\lambda : \mathbb{P}^1 \to \mathbb{P}^1$ such that $\theta_2 = \lambda \circ \theta_1$.*

Proof. Suppose that $g > (\ell-1)^2$ and that $\theta_2 : C \to \mathbb{P}^1$ is another map of degree ℓ on C. Then we have a map $(\theta_1, \theta_2) : C \to \mathbb{P}^1 \times \mathbb{P}^1$; let $\widetilde{C}$ be the image of this map. If (θ_1, θ_2) is injective, then $\widetilde{C}$ also has genus g; see [17, Theorem II.8.19]. On the other hand, $\widetilde{C}$ is a curve of bidegree (d_1, d_2) in $\mathbb{P}^1 \times \mathbb{P}^1$ for some $d_i \leq \ell$. Hence, the Adjunction Formula implies that $g \leq (d_1-1)(d_2-1) \leq (\ell-1)^2$, a contradiction; see

[17, Example V.1.5.2]. Therefore, (θ_1, θ_2) is not an injection. However, we have a commutative diagram



where the π_i are the restrictions of the natural projections $\pi_i : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1$ to $\widetilde{C}$. Therefore,

$$\deg(\pi_1) \cdot \deg((\theta_1, \theta_2)) = \deg(\theta_1) = \ell = \deg(\theta_2) = \deg(\pi_2) \cdot \deg((\theta_1, \theta_2)).$$

However, (θ_1, θ_2) is not injective, so that $\deg((\theta_1, \theta_2)) > 1$. Therefore, $\deg((\theta_1, \theta_2)) = \ell$, since ℓ is prime. Hence, $\deg(\pi_1) = 1 = \deg(\pi_2)$, and both π_i are isomorphisms [35, Corollary 2.4.1]. In particular, $\pi_2 \circ \pi_1^{-1} = \lambda$ is a linear fractional transformation, and $\theta_2 = \lambda \circ \theta_1$ as claimed. □

Theorem 5.2. *Let C be a curve of genus g over K and let ℓ be a prime such that $(\ell-1)^2 < g$ and $\ell \neq p$. Suppose there is morphism $\theta : C \to \mathbb{P}^1$ of degree ℓ such that the ramification locus of θ is a nonisotrivial set. Then C is a nonisotrivial curve.*

Proof. Suppose that C is isotrivial; we will prove that this implies that the ramification locus of θ must be isotrivial. Then for some finite extensions K' of K and k' of k there is a model $\mathcal{C}$ for $C \times_K K'$ over the k'-curve X corresponding to the function field K' such that for any place $t \in X(\overline{k'})$, the curve $\mathcal{C}_t \times_{k(t)} L$ is isomorphic to $C \times_K L$, where $k(t)$ is the field of definition of t and $L = K' \cdot k(t)$. Let $\mathcal{P}$ be a model for $\mathbb{P}^1$ over X. Then, for all but finitely many places $t \in X(\overline{k'})$, the morphism θ specializes to a degree ℓ morphism $\theta_t : \mathcal{C}_t \to \mathbb{P}^1_{k(t)}$ defined over $k(t)$. Let $\theta_2 = \theta_t \times_{k(t)} L$. Since $\theta_2 : C \to \mathbb{P}^1$ has degree ℓ, and $(\ell-1)^2 < g$, there is a $\lambda \in \mathrm{PGL}_2(\overline{K})$ such that $\theta_2 = \lambda \circ \theta$, by Lemma 5.1. But λ must take the ramification locus of θ to the ramification locus of θ_2, which is defined over k'. Hence, the ramification locus of θ must be isotrivial. □

Corollary 5.3. *Let F be a polynomial over K without repeated roots such that the roots of F form a nonisotrivial set. Let ℓ be a prime number such that $\ell \neq p$ and $\ell - 1 < \deg F/2 - 1$. Then the curve C given by $y^\ell = F(x)$ is not isotrivial.*

Proof. Let $\theta : C \to \mathbb{P}^1$ be the map coming from projection onto the x-coordinate. Then $\deg \theta = \ell$. Since the genus of C is at least $(\ell-1)\deg F/2 - (\ell-1)$ by Riemann–Hurwitz and the ramification locus of θ includes the roots of F (note: it will be larger than that if θ also ramifies over the point at infinity), applying Theorem 5.2 shows that C is not isotrivial. □

As mentioned above, there are obvious examples of maps $\pi : C \to \mathbb{P}^1$, where C is isotrivial but the ramification locus of π is not, but we have not found examples of isotrivial curves of the specific form $y^m = F(x)$, for F a polynomial with distinct roots that form a nonisotrivial set and m is an integer greater than 1 that is not a power of p.

Question 5.4. Does there exist an isotrivial curve of the form $y^m = F(x)$, where F is a polynomial with distinct roots that form a nonisotrivial set and m is an integer greater than 1 that is not a power of p?

Corollary 5.3 and the techniques of [18] can be used to show that when p is odd and m is even, the answer to Question 5.4 is "no"; we cannot however rule out examples where m is odd or $p = 2$.

We are now ready to prove a theorem guaranteeing the nonisotriviality of certain curves obtained by taking inverse images of points under iterates of a nonisotrivial rational function.

Theorem 5.5. *Let $\varphi \in K(x)$ be a nonisotrivial rational function. Let $\beta \in K$ be nonexceptional for φ. Then for any prime $\ell \neq p$, there is an n such that the curve given by*

$$y^\ell = \prod_{\substack{\gamma \in \overline{K} \\ \varphi^n(\gamma) = \beta}} (x - \gamma)$$

(*where the product $\prod_{\substack{\gamma \in \overline{K} \\ \varphi^n(\gamma) = \beta}} (x - \gamma)$ is taken without multiplicities*) *is not an isotrivial curve.*

Proof. If $\infty \notin \varphi^{-n}(\beta)$ for any n, then this is immediate from Corollary 5.3 and Theorem 3.1. Otherwise, since $\deg_s \varphi > 1$ (because purely inseparable rational functions are isotrivial) and β is not exceptional for φ, there is some m such that $\varphi^{-m}(\beta)$ contains at least three points. Thus, there is some point $\beta' \in \varphi^{-m}(\beta)$ such that $\infty \notin \varphi^{-n}(\beta')$ for any n. Then there is some m' such that $\varphi^{-m'}(\beta')$ is not isotrivial by Theorem 3.1, and since the set of points other than ∞ in $\varphi^{-(m+m')}(\beta)$ contains $\varphi^{-m'}(\beta')$, this set is nonisotrivial as well, so the curve given by

$$y^\ell = \prod_{\substack{\gamma \in \overline{K} \\ \varphi^{m+m'}(\gamma) = \beta}} (x - \gamma)$$

is not an isotrivial curve for all m large enough so that $\varphi^{-(m+m')}(\beta)$ contains more than $2\ell + 1$ points, by Corollary 5.3. □

Hindes conjectured [18, Conjecture 3.1] that when φ is a nonisotrivial polynomial of degree prime to p and β is not postcritical for φ, then for some n and some ℓ prime to p, the curve

$$y^\ell = \prod_{\substack{\gamma \in \overline{K} \\ \varphi^n(\gamma) = \beta}} (x - \gamma)$$

is not isotrivial. Theorem 5.5 answers this with many of the hypotheses removed. Note that by taking the product without multiplicities, we essentially remove the issue of β being postcritical. We note that Ferraguti and Pagano have proved Theorem 5.5 in the special case where φ is a quadratic polynomial, $\ell = 2$, and $p \neq 2$; see [15, Theorem 2.4].

6. Proof of Theorems 1.5 and 1.6

Theorems 1.5 and 1.6 will both follow from the following more general statement.

Proposition 6.1. *Let $f \in K[x]$ be nonisotrivial with* $\deg f > 1$ *and let $\ell \neq p$ be a prime number. Let $\alpha, \beta \in K$ where $\beta \notin O_\varphi^+(\alpha)$ and α is not preperiodic. Suppose that for some r, there is a $\gamma \in f^{-r}(\beta)$ such that γ is neither postcritical nor periodic and such that $e_{f^r}(\gamma/\beta)$ is prime to ℓ. Then $\mathcal{Z}(f, \alpha, \beta, \ell)$ is finite.*

We will prove Proposition 6.1 by combining effective forms of the Mordell Conjecture over function fields (see 6.3) with Theorem 5.5 and the following lemma from [10, Lemma 5.2]; see also [16, Proposition 5.1]. Note that while this lemma is stated in characteristic 0 in [10], the proof is the same word-for-word for finite extensions of $\mathbb{F}_p(t)$.

Lemma 6.2. *Let $f \in K[x]$ with $d = \deg(f) \geq 2$. Let $\alpha \in K$ with $h_f(\alpha) > 0$. Let $\gamma_1, \gamma_2 \in K$ such that $\gamma_2 \notin \mathcal{O}_f(\gamma_1)$ and $\gamma_1 \notin O_f(\alpha)$. For $n > 0$, let $\mathcal{X}(n)$ denote the set of primes $\mathfrak{p}$ of $\mathfrak{o}_K$ such that*

$$\min(v_\mathfrak{p}(f^m(\alpha) - \gamma_1), v_\mathfrak{p}(f^n(\alpha) - \gamma_2)) > 0$$

for some $0 < m < n$. Then for any $\epsilon > 0$, we have

$$\sum_{\mathfrak{p} \in \mathcal{X}(n)} N_\mathfrak{p} \leq \epsilon d^n h_f(\alpha) + O_\epsilon(1).$$

for all n.

The next result we use follows from (any of the) effective forms of the Mordell Conjecture over function fields [25; 27; 41]. To make this precise, we need some terminology. Let C be a curve over K and let $P \in C$ be a point on C defined over some finite extension $K(P)/K$. Then we let $h_{\mathcal{K}_C}(P)$ denote the logarithmic height of P with respect to the canonical divisor $\mathcal{K}_C$ of C and let

$$d_K(P) = \frac{2g(K(P)) - 2}{[K(P) : K]}$$

denote the logarithmic discriminant of P; here $g(K(P))$ is the genus of $K(P)$. Then we have the following height bounds for rational points on nonisotrivial curves due to Szpiro [41] and Kim [25].

Theorem 6.3. *Let C be a nonisotrivial curve of genus at least two over a finite extension K of $\mathbb{F}_p(t)$. Then there are constants $B_1 > 0$ and B_2 (depending only on C) such that*

$$h_{\mathcal{K}_C}(P) \leq B_1 d_K(P) + B_2 \tag{6.3.1}$$

holds for all $P \in C$.

Remark 6.4. The first of these bounds (with explicit B_1 and B_2 in the semistable case) are due to Szpiro [41, Section 3], and the best possible bounds (i.e., with smallest possible B_1) are due to Kim [25]. Strictly speaking, the bound in [41, Section 3] is stated for semistable curves. However, one may always pass to a finite extension L/K over which C is semistable [41, Section 1] and thus obtain bounds of the form in (6.3.1). Likewise, the bound in [25] is stated for curves with nonzero Kodaira–Spencer class. However, the general nonisotrivial case follows from this one as follows. Assuming that C/K is nonisotrivial and $\mathrm{char}(K) = p$, there is an inseparability degree $r = p^e$ and a separable extension L/K such that C is

defined over L^r and that the Kodaira–Spencer class of C over L^r is nonzero; see [41, pages 51–53]. Now apply Kim's theorem to C/L^r. In either case, Castelnuovo's inequality [40, Theorem 3.11.3] applied to the composite extensions $L(P) = LK(P)$ or $L^r(P) = L^rK(P)$ may be used to appropriately alter B_1 and B_2 to go from bounds with d_L or d_{L^r} back to those with d_K.

Before we apply the height bounds for points on curves from Theorem 6.3 to dynamics, we need the following elementary observation about valuations and powers.

Lemma 6.5. *Let $K/\mathbb{F}_p(t)$ be finite extension and let $\ell \neq p$ be a prime. Then there is a finite extension L of K such that if u is any element of K with the property that $\ell \mid v_{\mathfrak{p}}(u)$ for all primes $\mathfrak{p}$ of K, then u is an ℓ-th power in L.*

Proof. Suppose that $u \in K$ is such that $\ell \mid v_{\mathfrak{p}}(u)$ for all primes $\mathfrak{p}$ of K. Then the divisor $(u) = \ell D_u$ for some divisor $D_u \in \mathrm{Div}^0(K)$ of degree 0. Hence, the linear equivalence class of D_u is an ℓ-torsion class in $\mathrm{Cl}^0(K)$, the group of divisor classes of degree 0. In particular, there are only finitely many possible linear equivalence classes for D_u by [40, Proposition 5.1.3]. Thus, there is a finite set $\mathcal{S}$ of $u \in K$, each satisfying $(u) = \ell D_u$ for some $D_u \in \mathrm{Div}^0(K)$, such that for any $u' \in K$ with $(u') = \ell D_{u'}$ for a divisor $D_u \in \mathrm{Div}^0(K)$, the divisor $D_{u'}$ is linearly equivalent to D_u for some $u \in \mathcal{S}$. Let L' be the finite extension of K generated by the ℓ-th roots of the elements of $\mathcal{S}$. Now if u and u' are two such elements of K as above such that D_u and $D_{u'}$ are linearly equivalent, then $D_u - D_{u'} = (w_{u,u'})$ for some $w_{u,u'} \in K$. Hence, $u/u' = c_{u,u'} w_{u,u'}^{\ell}$ for some $c_{u,u'}$ in the field of constants of K. In particular, there are only finitely many possible such $c_{u,u'}$ since the field of constants of K is finite. Adjoining the ℓ-th roots of these $c_{u,u'}$ to L' gives a finite extension L of K. □

Lemma 6.6. *Let $\mathcal{S}$ be a finite set of primes of K, let $F \in \mathfrak{o}_{K,\mathcal{S}}[z]$ be a polynomial without repeated roots and let $\ell \neq p$ be a prime such that $C : y^\ell = F(x)$ is a nonisotrivial curve of genus $g(C) > 1$. Then there are constants $r_1 > 0$ and r_2 (depending on F, ℓ, K, and $\mathcal{S}$) such that*

$$\sum_{\substack{v_{\mathfrak{p}}(F(a))>0 \\ \ell \nmid v_{\mathfrak{p}}(F(a))}} N_{\mathfrak{p}} \geq r_1 h(a) + r_2 \tag{6.6.1}$$

holds for all $a \in \mathfrak{o}_{K,\mathcal{S}}$.

Proof. Suppose that $C : y^\ell = F(x)$ is a nonisotrivial curve of genus $g(C) > 1$. Then given $a \in \mathfrak{o}_{K,\mathcal{S}}$, we let $u_a := F(a)$ and choose a corresponding point $P_a = (a, \sqrt[\ell]{u_a})$ on C. From here, we proceed in cases.

Suppose first that $\ell \mid v_{\mathfrak{p}}(u_a)$ for all primes $\mathfrak{p}$ of K. Then by Lemma 6.5 there exists a finite extension L/K (independent of a) such that u_a is an ℓ-th power in L. In particular, since we may assume that L contains a primitive ℓ-th root of unity, $K(P_a) \subseteq L$. Therefore, (6.3.1) implies that $h_{\mathcal{K}_C}(P_a)$ is absolutely bounded. However, the canonical divisor class is ample in genus at least 2, so that the set of possible points P_a is finite in this case. Therefore, $h(a)$ is bounded and (6.6.1) holds trivially (take $r_1 = 1$ and choose r_2 to be sufficiently negative).

Now suppose that there exists a prime $\mathfrak{p}$ of K such that $\ell \nmid v_{\mathfrak{p}}(u_a)$. Then we may apply the genus formula in [40, Corollary 3.7.4] to deduce that

$$\begin{aligned} d_K(P_a) &= 2g(K) - 2 + \tfrac{1}{\ell}\sum_{\mathfrak{p}} (\ell - \gcd(\ell, v_{\mathfrak{p}}(u_a)))N_{\mathfrak{p}} \\ &= 2g(K) - 2 + \left(\frac{\ell-1}{\ell}\right) \sum_{\substack{v_{\mathfrak{p}}(u_a)>0 \\ \ell \nmid v_{\mathfrak{p}}(u_a)}} N_{\mathfrak{p}} + \left(\frac{\ell-1}{\ell}\right) \sum_{\substack{v_{\mathfrak{p}}(u_a)<0 \\ \ell \nmid v_{\mathfrak{p}}(u_a)}} N_{\mathfrak{p}} \\ &\leq 2g(K) - 2 + \left(\frac{\ell-1}{\ell}\right) \sum_{\substack{v_{\mathfrak{p}}(u_a)>0 \\ \ell \nmid v_{\mathfrak{p}}(u_a)}} N_{\mathfrak{p}} + \left(\frac{\ell-1}{\ell}\right) \sum_{\mathfrak{p} \in \mathcal{S}} N_{\mathfrak{p}}, \end{aligned} \tag{6.6.2}$$

since the only way that $u_a := F(a)$ can have negative valuation at $\mathfrak{p}$ is if $\mathfrak{p} \in \mathcal{S}$. However, this is a finite set of primes. Therefore, (6.6.2) implies that

$$d_K(P_a) \leq \left(\frac{\ell-1}{\ell}\right) \sum_{\substack{v_{\mathfrak{p}}(F(a))>0 \\ \ell \nmid v_{\mathfrak{p}}(F(a))}} N_{\mathfrak{p}} + O_{K,\mathcal{S}}(1). \tag{6.6.3}$$

On the other hand, if $\pi : C \to \mathbb{P}^1$ is the map given by projection onto the x-coordinate, then π pulls back a degree one divisor on $\mathbb{P}^1$ (yielding the Weil height on $\mathbb{P}^1$) to a degree ℓ divisor on C. Hence, the algebraic equivalence of divisors and [37, Theorem III.10.2] (see also [26, Section 4.3]) together imply that

$$\lim_{h_{\mathcal{K}_C}(P)\to\infty} \frac{h(\pi(P))}{h_{\mathcal{K}_C}(P)} = \frac{\ell}{2g(C)-2}.$$

In particular, we may deduce that

$$h(a) \leq \frac{(1+\epsilon)\ell}{(2g(C)-2)} h_{\mathcal{K}_C}(P_a) + O_{K,F,\ell,\epsilon}(1) \tag{6.6.4}$$

for all $\epsilon > 0$ and all $a \in K$ (not just $a \in \mathfrak{o}_{K,S}$). Finally, by choosing $\epsilon = 1$ and combining (6.3.1), (6.6.3), and (6.6.4), we see that there are constants $r_1 > 0$ and r_2 (depending on F, ℓ, K, and $\mathcal{S}$) such that

$$\sum_{\substack{v_{\mathfrak{p}}(F(a))>0 \\ \ell \nmid v_{\mathfrak{p}}(F(a))}} N_{\mathfrak{p}} \geq r_1 h(a) + r_2$$

holds for all $a \in \mathfrak{o}_{K,\mathcal{S}}$. In particular, after replacing r_1 and r_2 with the minimum of the corresponding constants from the first and second cases above, we prove Lemma 6.6. □

Lemma 6.7. *Let $f \in K[z]$ be a nonisotrivial polynomial with* $\deg f = d > 1$ *and let $\alpha, \gamma \in K$ where γ is not postcritical. Then for any prime $\ell \neq p$, there is a $\delta > 0$ such that for all sufficiently large n, we have*

$$\sum_{\substack{v_{\mathfrak{p}}(f^n(\alpha)-\gamma)>0 \\ \ell \nmid v_{\mathfrak{p}}(f^n(\alpha)-\gamma)}} N_{\mathfrak{p}} \geq \delta d^n h_f(\alpha). \tag{6.7.1}$$

Proof. Let $\mathcal{S}$ be finite set of primes such that α, γ, and all the coefficients of f are in $\mathfrak{o}_{K,\mathcal{S}}$. Then $f^n(\alpha) \in \mathfrak{o}_{K,\mathcal{S}}$ for all m. By Theorem 5.5, there is an m such that the curve given by

$$y^\ell = \prod_{\substack{\beta \in \overline{K} \\ f^m(\beta)=\gamma}} (x-\beta)$$

is not an isotrivial curve. There is an $\omega \in K$ (the leading term of $f^m(z)-\gamma$) and an e (coming from the degree of inseparability of f^ℓ) such that

$$f^m(z) - \gamma = \omega \prod_{\substack{\beta \in \overline{K} \\ f^m(\beta)=\gamma}} (z-\beta)^{p^e}.$$

Let

$$F(z) = \prod_{\substack{\beta \in \overline{K} \\ f^m(\beta)=\gamma}} (z-\beta).$$

Applying Lemma 6.6 with $a = f^{n-m}(\alpha)$ we see that since $\ell \neq p$, we have constants r_1, r_2 such that

$$\sum_{\substack{v_\mathfrak{p}(f^n(\alpha)-\gamma)>0 \\ \ell \nmid v_\mathfrak{p}(f^n(\alpha)-\gamma)}} N_\mathfrak{p} \geq \left(\sum_{\substack{v_\mathfrak{p}(F(a))>0 \\ \ell \nmid v_\mathfrak{p}(F(a))}} N_\mathfrak{p} \right) - h(\omega) \geq r_1 h(f^{n-m}(\alpha)) + r_2 - h(\omega).$$

Since $|h_f - h| \leq O(1)$ and $h_f(f^{n-m}(\alpha)) = d^{n-m} h_f(\alpha)$, we see that there is a constant r_3 such that

$$\sum_{\substack{v_\mathfrak{p}(f^n(\alpha)-\gamma)>0 \\ \ell \nmid v_\mathfrak{p}(f^n(\alpha)-\gamma)}} N_\mathfrak{p} \geq r_1 d^{n-m} h_f(\alpha) + r_3$$

for all n. Choosing a δ such that $0 < \delta < r_1/d^m$ then gives

$$\sum_{\substack{v_\mathfrak{p}(f^n(\alpha)-\gamma)>0 \\ \ell \nmid v_\mathfrak{p}(f^n(\alpha)-\gamma)}} N_\mathfrak{p} \geq \delta d^n h_f(\alpha)$$

for all sufficiently large n, as desired. □

We are now ready to prove Proposition 6.1.

Proof of Proposition 6.1. We first note it suffices to prove this after passing to a finite extension of K since $\ell \neq p$. To see this, let L be a finite extension of K, let L^s denote the separable closure of K in L, and let $\mathfrak{q}$ be a prime in L lying over a prime $\mathfrak{p}$ of K. Then $v_\mathfrak{q}(f^n(\alpha)-\beta) = [L : L^s] v_\mathfrak{p}(f^n(\alpha)-\beta)$ unless $\mathfrak{p}$ is in the finite set of primes of K that ramify in L^s. We also note that $h_f(\alpha) > 0$ since α is not preperiodic and f is not isotrivial, by [1, Corollary 1.8].

We change coordinates so that $\beta = 0$. Let r be the smallest positive integer such that $f^r(\gamma) = 0$. After passing to a finite extension we may assume that all the roots of $f^r(z)$ are in K. Let $e = e_{f^r}(\gamma/\beta)$ and write

$$f^r(z) = (z-\gamma)^e g(z).$$

Then for all but finitely many primes $\mathfrak{p}$ of K we have

$$v_{\mathfrak{p}}(f^{n+r}(\alpha)) = e v_{\mathfrak{p}}(f^n(\alpha) - \gamma) \tag{6.7.2}$$

for all n.

Since γ is not postcritical, by Lemma 6.7, there exists $\delta > 0$ such that for all sufficiently large n, we have

$$\sum_{\substack{v_{\mathfrak{p}}(f^n(\alpha)-\gamma)>0 \\ \ell \nmid v_{\mathfrak{p}}(f^n(\alpha)-\gamma)}} N_{\mathfrak{p}} \geq \delta d^n h_f(\alpha). \tag{6.7.3}$$

Let $\mathcal{W}$ be the roots of $f^r(z)$ that are not roots of $f^{r'}(z)$ for any $r' < r$. Let $\mathcal{S}_1$ be the set of primes of bad reduction for f and let $\mathcal{S}_2$ be the set of primes such that $v_{\mathfrak{p}}(f^{r'}(w)) > 0$ for some $r' < r$ and some $w \in \mathcal{W} \cup \{\alpha\}$. Now, for each n, let $\mathcal{Y}(n)$ be the set of primes $\mathfrak{p}$ such that $v_{\mathfrak{p}}(f^n(\alpha) - \gamma) > 0$ and $v_{\mathfrak{p}}(f^{n'}(\alpha)) > 0$ for some $n' < n + r$. If $\mathfrak{p} \notin \mathcal{S}_1 \cup \mathcal{S}_2$ for $\mathfrak{p} \in \mathcal{Y}(n)$, then $v_{\mathfrak{p}}(f^m(\alpha)) - \gamma') > 0$ for some $\gamma' \in \mathcal{W}$ and some $m < n$; this follows from the fact that if $s \geq r$ is the smallest integer such that $v_{\mathfrak{p}}(f^s(\alpha)) > 0$, then $v_{\mathfrak{p}}(f^{s-r}(\alpha) - \gamma') > 0$ for some $\gamma' \in \mathcal{W}$. Thus, since γ is not in the forward orbit of α (since $\beta \notin O_\varphi^+(\alpha)$ by assumption) or of any element of $\mathcal{W}$ (since it is not periodic) and the sets $\mathcal{W}$, $\mathcal{S}_1$, and $\mathcal{S}_2$ are all finite, we may apply Lemma 6.2 to each element of $\mathcal{W}$. We obtain

$$\sum_{\mathfrak{p} \in \mathcal{Y}(n)} N_{\mathfrak{p}} \leq \frac{\delta}{2} d^n h_f(\alpha) \tag{6.7.4}$$

for all sufficiently large n. Combining (6.7.4) with (6.7.2) and (6.7.3), we see that for all sufficiently large n, there is a prime $\mathfrak{p}$ such that

- $v_{\mathfrak{p}}(f^n(\alpha) - \gamma) > 0$;
- $\ell \nmid v_{\mathfrak{p}}(f^n(\alpha) - \gamma)$;
- $v_{\mathfrak{p}}(f^{n'}(\alpha)) = 0$ for all $0 < n' < n$; and
- $v_{\mathfrak{p}}(f^{n+r}(\alpha)) = e v_{\mathfrak{p}}(f^n(\alpha) - \gamma)$.

Since e is prime to ℓ, it follows that the Zsigmondy set $\mathcal{Z}(f, \alpha, \beta, \ell)$ is finite. □

7. Applications

The original Zsigmondy theorem [3; 47] had to do with orders of algebraic numbers modulo primes. We can treat a related dynamical problem; here we will not assume nonisotriviality. We begin with some notation and terminology. If $\alpha \in K$ is an integer at a prime $\mathfrak{p}$, we let $\alpha_{\mathfrak{p}} \in k_{\mathfrak{p}}$ be its reduction at $\mathfrak{p}$. If $f \in K[x]$, and all of the coefficients of f are integers at $\mathfrak{p}$, we let $f_{\mathfrak{p}} \in k_{\mathfrak{p}}[x]$ be the reduction of f at $\mathfrak{p}$ obtained by reducing each coefficient of f at $\mathfrak{p}$. If $g : \mathcal{U} \to \mathcal{U}$ is any map from a set to itself and $u \in \mathcal{U}$ is periodic under g, then the *prime period* of u for g is the smallest positive integer m such that $g^m(u) = u$. We say that a polynomial $f \in K[x]$ is additive if $f(\alpha + \beta) = f(\alpha) + f(\beta)$ for all $\alpha, \beta \in \overline{K}$.

Theorem 7.1. *Let f be a polynomial of degree greater than 1 and let $\alpha \in K$ be a point that is not preperiodic for f. If f is not both isotrivial and additive, then for all but finitely many positive integers n, there is a prime $\mathfrak{p}$ such that the prime period of $\alpha_\mathfrak{p}$ for $f_\mathfrak{p}$ is equal to n. If f is isotrivial and additive, then for all but finitely many positive integers n that are not a power of p, there is a $\mathfrak{p}$ such that the prime period of $\alpha_\mathfrak{p}$ for $f_\mathfrak{p}$ is equal to n.*

Proof. If f is not isotrivial, this follows immediately from Theorem 1.6 by letting $\alpha = \beta$. If f is isotrivial, then after a change of coordinates, we may assume that $f \in k[x]$ and $\alpha \in K \setminus k$ for some finite extension k of $\mathbb{F}_p$. If f is not additive then for all but finitely many positive integers n, there exists $\beta_n \in \bar{k}$ having prime period n for f, by [30, Theorem]. For each such β_n, there exists $\mathfrak{p}_n$ such that $\alpha_{\mathfrak{p}_n} = \beta_n$, so we see that for all but all but finitely many positive integers n, there exists $\mathfrak{p}$ such that the prime period of $\alpha_\mathfrak{p}$ for $f_\mathfrak{p}$ is equal to n. If f is additive, then for all but finitely many positive integers n that are not a power of p, there exists $\beta_n \in \bar{k}$ having prime period n for f, by [30, Theorem]. Then, as in the nonadditive case, we may choose $\mathfrak{p}_n$ such that $\alpha_{\mathfrak{p}_n} = \beta_n$. □

Theorem 1.4 allows one to prove characteristic p analogs of various results that rely on the results of [36]. For example, the proofs of Theorems 4 and 5 of [5] extend easily to the case of nonisotrivial rational functions over a function field in characteristic p, using Theorem 1.4. Similarly, one can use Theorem 1.4 to prove Theorem 4 of [11] with the additional hypothesis that at least one of the wandering critical points of φ has a ramification degree that is not a power of p.

We will now prove a few results about unicritical polynomials that rely on Theorem 1.5, which is not available over number fields.

The following lemma is very similar to [9, Proposition 3.1]; we include the proof for a sake of completeness.

Lemma 7.2. *Let $f(x) = x^d + c$ where d is an integer greater than 1 that is not divisible by p, let $\beta \in K$, and let n be a positive integer. Let $\mathfrak{p}$ be any prime of K such that*

(i) $|c|_\mathfrak{p} \leq 1$;

(ii) $|\beta|_\mathfrak{p} \leq 1$; *and*

(iii) $|f^m(0) - \beta|_\mathfrak{p} = 1$ *for all* $0 \leq m \leq n$.

Then $\mathfrak{p}$ does not ramify in $K(f^{-n}(\beta))$.

Proof. We proceed by induction. The case where $n = 1$ follows immediately from taking the discriminant of $x^d + (c - \beta)$. Now, let $\mathfrak{p}$ be a prime satisfying (i)–(iii) for some $n \geq 2$. Then it also satisfies them for $n - 1$, so by the inductive hypothesis, the prime $\mathfrak{p}$ does not ramify in $K(f^{-(n-1)}(\beta))$. Now, $K(f^{-n}(\beta))$ is obtained from $K(f^{-(n-1)}(\beta))$ by adjoining elements of the form $\sqrt[d]{\gamma_i - c}$ for $f^{n-1}(\gamma_i) = \beta$. For any prime $\mathfrak{q}$ in $K(f^{-(n-1)}(\beta))$ lying over $\mathfrak{p}$, we see that $|\gamma_i|_\mathfrak{q} \leq 1$ by (i) and (ii). We also have $|\gamma_i|_\mathfrak{q} \geq 1$ since otherwise γ would be in the same residue class as 0, which contradicts (iii). Thus, each $\mathfrak{q}$ in $K(f^{-(n-1)}(\beta))$ lying over $\mathfrak{p}$ does not ramify in any $K(f^{-(n-1)}(\beta))(\sqrt[d]{\gamma_i - c}) = K(f^{-n}(\beta))$. Since each

such $\mathfrak{q}$ does not ramify over $\mathfrak{p}$ by the inductive hypothesis, it follows that $\mathfrak{p}$ does not ramify in $K(f^{-n}(\beta))$, as desired. □

The next lemma follows a proof that is similar to that of [9, Proposition 3.2] and [11, Theorem 5].

Lemma 7.3. *Let $f(x) = x^d + c$ where $c \in K \setminus k$ where d is an integer greater than 1 that is not divisible by p. Let $\beta \in K$, let $\ell \neq p$ be a prime number, and let e be a positive integer such that ℓ^e divides d. Suppose that $\mathfrak{p}$ is a primitive ℓ-divisor of $f^n(0) - \beta$ such that $|c|_\mathfrak{p} = |\beta|_\mathfrak{p} = 1$. Then for any prime $\mathfrak{p}'$ in $K(f^{-(n-1)}(\beta))$ that lies over $\mathfrak{p}$, there is a prime $\mathfrak{q}$ in $K(f^{-n}(\beta))$ such that ℓ^e divides $e(\mathfrak{q}/\mathfrak{p}')$.*

Proof. Let $\mathfrak{p}'$ be a prime in $K(f^{-(n-1)}(\beta))$ lying over $\mathfrak{p}$. By Lemma 7.2, the prime $\mathfrak{p}$ does not ramify in $K(f^{-(n-1)}(\beta))$, so $v_{\mathfrak{p}'}(z) = v_\mathfrak{p}(z)$ for all $z \in K$. Since $f^n(0) - \beta = \prod_{f^{n-1}(\gamma)=\beta}(f(0) - \gamma)$, we see that there is some $\gamma \in f^{-(n-1)}(\beta)$ such that $\ell \nmid v_{\mathfrak{p}'}(c - \gamma)$. Thus, if $\mathfrak{q}$ is a prime of $K(f^{-(n-1)}(\beta))(\sqrt[d]{c-\gamma})$ lying over $\mathfrak{p}'$, we see that $\ell^e \mid e(\mathfrak{q}/\mathfrak{p}')$. □

Using the Lemmas above, we can prove a result for separable nonisotrivial polynomials of the form $x^d + c$ that is a special case of a characteristic p analog of [9, Theorem 1.1]. Note that if $f(x) = x^d + c$ and d is not divisible by p, then f is isotrivial if and only if $c \in \overline{\mathbb{F}}_p$. To see this, note that $h_f(0) = \frac{h(c)}{d} > 0$ when $c \notin \overline{\mathbb{F}}_p$, as can be seen by simply considering the orbit of f at the places v where $|c|_v > 1$. Therefore, if $c \notin \overline{\mathbb{F}}_p$, then f has a critical point that is not preperiodic, and hence f cannot be isotrivial. We note also that a polynomial of the form $x^d + c$ is separable if and only if $p \nmid d$.

Theorem 7.4. *Let $f(x) = x^d + c$ be a separable nonisotrivial polynomial of degree $d > 1$. Let $\beta \in K$. Then for all sufficiently large n, there is a prime $\mathfrak{p}$ of K such that $\mathfrak{p}$ ramifies in $K(f^{-n}(\beta))$ but not in $K(f^{-(n-1)}(\beta))$.*

Proof. Since 0 is not periodic and every point in K other than $\beta = c$ has $d > 1$ distinct preimages under f, we see that for any $\beta \neq c$, there is a $\gamma \in f^{-1}(\beta)$ meeting the conditions of Proposition 6.1. Furthermore, we note that if $\beta = c$, then $f^{-n}(\beta) = f^{-(n-1)}(0)$ for all $n > 0$, so it suffices to prove the result for $\beta = 0$; thus, we need only treat the case where $\beta \neq c$.

Let $\ell \neq p$ be a prime dividing d. By Proposition 6.1, for all sufficiently large n, there is a prime $\mathfrak{p}$ such that $v_\mathfrak{p}(f^n(0) - \beta) > 0$ with $\ell \nmid v_\mathfrak{p}(f^n(0) - \beta)$ and $v_\mathfrak{p}(f^m(0) - \beta) = 0$ for all $0 < m < n$. Since $|c|_\mathfrak{p} = |\beta|_\mathfrak{p} = 1$ for all but finitely many $\mathfrak{p}$ we may also suppose that $|c|_\mathfrak{p} = |\beta|_\mathfrak{p} = 1$. Then, by Lemma 7.2, the prime $\mathfrak{p}$ does not ramify in $K(f^{-(n-1)}(\beta))$. By Lemma 7.3, it does ramify in $K(f^{-n}(\beta))$. □

The next result is a characteristic p analog of a theorem of Pagano [29, Theorem 1.3] for number fields (see also [8] for a similar result); the growth condition here is stronger than what Pagano obtains over number fields.

Theorem 7.5. *Let $f(x) = x^d + c$ be a separable nonisotrivial polynomial of degree $d > 1$. Let $\beta \in K$. Then there is a constant $C(n, \beta) > 0$ such that $[K(f^{-n}(\beta)) : K] > C(n, \beta)d^n$ for all positive integers n.*

Proof. It will suffice to show that d divides $[K(f^{-n}(\beta)) : K(f^{-(n-1)}(\beta))]$ for all sufficiently large n. Let ℓ be a prime such that $\ell^e \mid d$ for some $e > 0$. Applying Proposition 6.1 as in Theorem 7.4, we see that for

all sufficiently large n, there is a prime $\mathfrak{p}$ with the property $|c|_\mathfrak{p} = |\beta|_\mathfrak{p} = 1$ such that $v_\mathfrak{p}(f^n(0) - \beta) > 0$ with $\ell \nmid v_\mathfrak{p}(f^n(0) - \beta)$ and $v_\mathfrak{p}(f^m(0) - \beta) = 0$ for all $0 < m < n$. Then Lemma 7.3 implies that for any prime $\mathfrak{p}'$ in $K(f^{-(n-1)}(\beta))$ that lies over $\mathfrak{p}$, there is a prime $\mathfrak{q}$ in $K(f^{-n}(\beta))$ such that ℓ^e divides $e(\mathfrak{q}/\mathfrak{p}')$. Hence $\ell^e \mid [K(f^{-n}(\beta)) : K(f^{-(n-1)}(\beta))]$. Since this holds for any prime $\ell \neq p$ such that $\ell^e \mid d$ for some $e > 0$, it follows that $d \mid [K(f^{-n}(\beta)) : K(f^{-(n-1)}(\beta))]$ for all sufficiently large n, and our proof is complete. □

We can now prove a finite index result for iterated monodromy groups of quadratic polynomials. We need a little terminology to state our result.

Let L be a field, let f be a quadratic polynomial, and let $\beta \in \bar{L}$. For $n \in \mathbb{N}$, let $L_n(f, \beta) = L(f^{-n}(\beta))$ be the field obtained by adjoining the n-th preimages of β under f to $L(\beta)$, and let $L_\infty(f, \beta) = \bigcup_{n=1}^{\infty} L_n(f, \beta)$. We let $G_\infty(\beta) = \mathrm{Gal}(L_\infty(f, \beta)/L)$. The group $G_\infty(\beta)$ embeds into $\mathrm{Aut}(T_\infty^2)$, the automorphism group of an infinite 2-ary rooted tree T_∞^2 (note that all of the definitions here generalize to rational functions of any degree — see [28] or [23], for example). Boston and Jones [7] asked if $G_\infty(\beta)$ had finite index in $\mathrm{Aut}(T_\infty^2)$ whenever f is not postcritically finite in the case where L is a number field. It was later shown [24] that this is true if the pair (f, β) is eventually stable (see below), assuming the *abc* conjecture. This was also shown to be true unconditionally for nonisotrivial quadratic polynomials over function fields of characteristic 0 in [12].

For $\beta \in \bar{L}$ and a polynomial $f \in L[x]$, the pair (f, β) is said to be *eventually stable* if the number of irreducible factors of $f^n(x) - \beta$ over $L(\beta)$ is bounded independently of n as $n \to \infty$ (stability and eventual stability can also be defined for rational functions as in [22]). We will prove a finite index result for nonisotrivial quadratic polynomials over function fields of odd positive characteristic under an eventual stability assumption.

The technique we use is the same as that used in [12]; see also [24; 10; 19]. We make use of [12, Proposition 7.7], which is stated in characteristic 0 but is true with no changes in the proof in characteristic p provided that $K(f^{-n}(\beta))$ is separable over K for all n, which is automatic here when $p > 2$; the following result is a strengthening of [18, Corollary 1].

Theorem 7.6. *Let f be a nonisotrivial quadratic polynomial defined over a field K that is a finite extension of $\mathbb{F}_p(t)$. Suppose that $p > 2$ and that β is not postcritical or periodic for f. Suppose furthermore that the pair (f, β) is eventually stable. Then $G_\infty(\beta)$ has finite index in* $\mathrm{Aut}(T_\infty^2)$.

Proof. As in [12], it will suffice to show that for all sufficiently large N, we have

$$\mathrm{Gal}(K_N/K_{N-1}) \cong C_2^{2^N},$$

where C_2 is the cyclic group with two elements. After a change of variables, we may assume that $f(x) = x^2 + c$ for some $c \in K \setminus k$.

Since (f, β) is eventually stable, there is an m such that $f^m(x) - \beta = (x - \gamma_1) \cdots (x - \gamma_{2^m})$ for γ_i with the property that $f^n(x) - \gamma_i$ is irreducible over $K(\gamma_i)$ for all n for $i = 1, \ldots, 2^m$, by [10, Proposition 4.2]. Let $L = K(\gamma_1, \ldots, \gamma_{2^m})$. It follows from [12, Proposition 7.7] and Lemma 7.3 (see Remark 7.7) that we

must have $\mathrm{Gal}(K_{n+m}/K_{n+m-1}) \cong [C_2]^{2^{m+n}}$ whenever there are primes $\mathfrak{p}_i$ of L, for $i = 1, \dots, 2^m$, such that

(i) $v_{\mathfrak{p}_i}(c) = v_{\mathfrak{p}_i}(\gamma_j) = 0$ for $j = 1, \dots, 2^m$;

(ii) $2 \nmid v_{\mathfrak{p}_i}(f^n(0) - \gamma_i)$;

(iii) $v_{\mathfrak{p}_i}(f^{n'}(0) - \gamma_i) = 0$ for all $n' < n$;

(iv) $v_{\mathfrak{p}_i}(f^{n'}(0) - \gamma_j) = 0$ for all $n' \leq n$ and $j \neq i$; and

(v) $\mathfrak{p}_i$ does not ramify over $\mathfrak{p}_i \cap K$.

Note that conditions (i) clearly holds for all but finitely many primes $\mathfrak{p}_i$. Likewise, (v) holds for all but finitely many primes due to the separability of L over K, which follows from the fact that f is quadratics and $p \neq 2$. Hence, we will be done if we can show that for all sufficiently large n, there are $\mathfrak{p}_i$, for $i = 1, \dots, 2^m$, that satisfy conditions (ii), (iii), and (iv).

Now, fix a γ_i. By Lemma 6.7, there exists $\delta > 0$ such that for all sufficiently large n, we have

$$\sum_{\substack{v_{\mathfrak{p}}(f^n(0)-\gamma_i)>0 \\ 2 \nmid v_{\mathfrak{p}}(f^n(0)-\gamma_i)}} N_{\mathfrak{p}} \geq \delta d^n h_f(0). \tag{7.6.1}$$

For any n, let $\mathcal{X}(n)$ be the set of primes $\mathfrak{p}$ such that $v_{\mathfrak{p}}(f^n(0) - \gamma_i) > 0$ and $v_{\mathfrak{p}}(f^{n'}(0) - \gamma_i) > 0$ for some $n' < n$. Since γ_i is neither periodic nor postcritical and $h_f(0) > 0$, we may apply Lemma 6.2. We see then that for all sufficiently large n, we have

$$\sum_{\mathfrak{p} \in \mathcal{X}(n)} N_{\mathfrak{p}} \leq \frac{\delta}{3} d^n h_f(0). \tag{7.6.2}$$

For any n and $j \neq i$, we let $\mathcal{Y}_j(n)$ be the set of primes $v_{\mathfrak{p}}(f^n(0) - \gamma_i) > 0$ and $v_{\mathfrak{p}}(f^{n'}(0) - \gamma_j) > 0$ for some $n' \leq n$. Since $f^{n'}(\gamma_j) \neq \gamma_i$ for all n' and $i \neq j$, we may apply Lemma 6.2 again. Since in addition we have $v_{\mathfrak{p}}(\gamma_i - \gamma_j) \neq 0$ for all but finitely many $\mathfrak{p}$ when $i \neq j$, we see that for all sufficiently large n, we have

$$\sum_{j \neq i} \sum_{\mathfrak{p} \in \mathcal{Y}_j(n)} N_{\mathfrak{p}} \leq \frac{\delta}{3} d^n h_f(0). \tag{7.6.3}$$

Since $\delta h_f(0) > 0$, Equations (7.6.1), (7.6.2), and (7.6.3) imply that for any sufficiently large n, there is a prime $\mathfrak{p}_i$ satisfying conditions (ii), (iii), and (iv), and our proof is complete. □

Remark 7.7. We note that while conditions (i) and (ii) above are weaker as stated than Condition R from [12, Definition 7.2], they do imply that the prime $\mathfrak{p}_i$ ramifies in $K(f^{-n}(\gamma_i))$ (by Lemma 7.3), which is what [12, Proposition 7.7] requires.

It should also be possible to prove a finite index result along the lines of Theorem 7.6 more generally for nonisotrivial polynomials of the form $x^d + c$, where $d > 2$ and $p \nmid d$ by modifying techniques in [12] and combining them with our argument for Theorem 7.5 above.

Acknowledgements

Benedetto, Dragos Ghioca, Minhyong Kim, Carlo Pagano, Joe Silverman, Dinesh Thakur, Felipe Voloch, and Julie Wang for many helpful conversations. We give special thanks to Juan Rivera-Letelier, who provided us with the argument for Proposition 3.2 and without whose help this paper likely would not have been possible. Finally, we thank the anonymous referee for their many helpful suggestions.

References

[1] M. Baker, "A finiteness theorem for canonical heights attached to rational maps over function fields", *J. Reine Angew. Math.* **626** (2009), 205–233. MR Zbl

[2] M. Baker and R. Rumely, *Potential theory and dynamics on the Berkovich projective line*, Math. Surv. Monogr. **159**, Amer. Math. Soc., Providence, RI, 2010. MR Zbl

[3] A. S. Bang, "Taltheoretiske Undersøgelser", *Tidsskrift Mat.* **4**:5 (1886), 70–80, 130–137.

[4] R. L. Benedetto, *Dynamics in one non-archimedean variable*, Grad. Stud. in Math. **198**, Amer. Math. Soc., Providence, RI, 2019. MR Zbl

[5] R. L. Benedetto, D. Ghioca, B. Hutz, P. Kurlberg, T. Scanlon, and T. J. Tucker, "Periods of rational maps modulo primes", *Math. Ann.* **355**:2 (2013), 637–660. MR Zbl

[6] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Math. Monogr. **4**, Cambridge Univ. Press, 2006. MR Zbl

[7] N. Boston and R. Jones, "Arboreal Galois representations", *Geom. Dedicata* **124** (2007), 27–35. MR Zbl

[8] G. Boxall, G. Jones, and H. Schmidt, "Rational values of transcendental functions and arithmetic dynamics", *J. Eur. Math. Soc.* **24**:5 (2022), 1567–1592. MR Zbl

[9] A. Bridy and T. J. Tucker, "ABC implies a Zsigmondy principle for ramification", *J. Number Theory* **182** (2018), 296–310. MR Zbl

[10] A. Bridy and T. J. Tucker, "Finite index theorems for iterated Galois groups of cubic polynomials", *Math. Ann.* **373**:1-2 (2019), 37–72. MR Zbl

[11] A. Bridy, P. Ingram, R. Jones, J. Juul, A. Levy, M. Manes, S. Rubinstein-Salzedo, and J. H. Silverman, "Finite ramification for preimage fields of post-critically finite morphisms", *Math. Res. Lett.* **24**:6 (2017), 1633–1647. MR Zbl

[12] A. Bridy, J. R. Doyle, D. Ghioca, L.-C. Hsia, and T. J. Tucker, "Finite index theorems for iterated Galois groups of unicritical polynomials", *Trans. Amer. Math. Soc.* **374**:1 (2021), 733–752. MR Zbl

[13] G. S. Call and J. H. Silverman, "Canonical heights on varieties with morphisms", *Compos. Math.* **89**:2 (1993), 163–205. MR Zbl

[14] C. Favre and J. Rivera-Letelier, "Théorie ergodique des fractions rationnelles sur un corps ultramétrique", *Proc. Lond. Math. Soc.* (3) **100**:1 (2010), 116–154. MR Zbl

[15] A. Ferraguti and C. Pagano, "Constraining images of quadratic arboreal representations", *Int. Math. Res. Not.* **2020**:22 (2020), 8486–8510. MR Zbl

[16] C. Gratton, K. Nguyen, and T. J. Tucker, "ABC implies primitive prime divisors in arithmetic dynamics", *Bull. Lond. Math. Soc.* **45**:6 (2013), 1194–1208. MR Zbl

[17] R. Hartshorne, *Algebraic geometry*, Grad. Texts in Math. **52**, Springer, 1977. MR Zbl

[18] W. Hindes, "Prime divisors in polynomial orbits over function fields", *Bull. Lond. Math. Soc.* **48**:6 (2016), 1029–1036. MR Zbl

[19] W. Hindes and R. Jones, "Riccati equations and polynomial dynamics over function fields", *Trans. Amer. Math. Soc.* **373**:3 (2020), 1555–1575. MR Zbl

[20] M. Hindry and J. H. Silverman, *Diophantine geometry: an introduction*, Grad. Texts in Math. **201**, Springer, 2000. MR Zbl

[21] H.-L. Huang, C.-L. Sun, and J. T.-Y. Wang, "Integral orbits over function fields", *Int. J. Number Theory* **10**:8 (2014), 2187–2204. MR Zbl

[22] R. Jones and A. Levy, "Eventually stable rational functions", *Int. J. Number Theory* **13**:9 (2017), 2299–2318. MR Zbl
[23] J. Juul, P. Kurlberg, K. Madhu, and T. J. Tucker, "Wreath products and proportions of periodic points", *Int. Math. Res. Not.* **2016**:13 (2016), 3944–3969. MR Zbl
[24] J. Juul, H. Krieger, N. Looper, M. Manes, B. Thompson, and L. Walton, "Arboreal representations for rational maps with few critical points", pp. 133–151 in *Research directions in number theory* (Banff, AB, 2017), edited by J. S. Balakrishnan et al., Assoc. Women Math. Ser. **19**, Springer, 2019. MR Zbl
[25] M. Kim, "Geometric height inequalities and the Kodaira–Spencer map", *Compos. Math.* **105**:1 (1997), 43–54. MR Zbl
[26] S. Lang, *Fundamentals of Diophantine geometry*, Springer, 1983. MR Zbl
[27] A. Moriwaki, "Height inequality of nonisotrivial curves over function fields", *J. Algebraic Geom.* **3**:2 (1994), 249–263. MR Zbl
[28] R. W. K. Odoni, "The Galois theory of iterates and composites of polynomials", *Proc. Lond. Math. Soc.* (3) **51**:3 (1985), 385–414. MR Zbl
[29] C. Pagano, "The size of arboreal images, I: Exponential lower bounds for PCF and unicritical polynomials", preprint, 2021. arXiv 2104.11175
[30] T. Pezda, "Cycles of polynomials in algebraically closed fields of positive characteristic", *Colloq. Math.* **67**:2 (1994), 187–195. MR Zbl
[31] L. P. Postnikova and A. Schinzel, "Primitive divisors of the expression $a^n - b^n$ in algebraic number fields", *Mat. Sb.* (*N.S.*) **75 (117)** (1968), 171–177. In Russian; translated in *Math. USSR-Sb.* **4**:2 (1968), 153–159. MR
[32] B. Rice, "Primitive prime divisors in polynomial arithmetic dynamics", *Integers* **7** (2007), art. id. A26. MR Zbl
[33] A. Schinzel, "Primitive divisors of the expression $A^n - B^n$ in algebraic number fields", *J. Reine Angew. Math.* **268/269** (1974), 27–33. MR Zbl
[34] A. Grothendieck, *Revêtements étales et groupe fondamental, Fasc. II: Exposés VI, VIII–XI* (Séminaire de Géométrie Algébrique du Bois Marie 1960–1961), Inst. des Hautes Études Sci., Paris, 1963. MR
[35] J. H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts in Math. **106**, Springer, 1986. MR Zbl
[36] J. H. Silverman, "Integer points, Diophantine approximation, and iteration of rational maps", *Duke Math. J.* **71**:3 (1993), 793–829. MR Zbl
[37] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math. **151**, Springer, 1994. MR Zbl
[38] J. H. Silverman, "Rational functions with a polynomial iterate", *J. Algebra* **180**:1 (1996), 102–110. MR Zbl
[39] V. A. Sookdeo, "Integer points in backward orbits", *J. Number Theory* **131**:7 (2011), 1229–1239. MR Zbl
[40] H. Stichtenoth, *Algebraic function fields and codes*, 2nd ed., Grad. Texts in Math. **254**, Springer, 2009. MR Zbl
[41] L. Szpiro, "Propriétés numériques du faisceau dualisant relatif", pp. 44–78 in *Séminaire sur les pinceaux de courbes de genre au moins deux*, Astérisque **86**, Soc. Math. France, Paris, 1981. MR Zbl
[42] P. Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Math. **1239**, Springer, 1987. MR Zbl
[43] P. Vojta, "A more general *abc* conjecture", *Int. Math. Res. Not.* **1998**:21 (1998), 1103–1116. MR Zbl
[44] J. F. Voloch, "Diophantine approximation in characteristic p", *Monatsh. Math.* **119**:4 (1995), 321–325. MR Zbl
[45] J. T.-Y. Wang, "Integral points of projective spaces omitting hyperplanes over function fields of positive characteristic", *J. Number Theory* **77**:2 (1999), 336–346. MR Zbl
[46] K. Yamanoi, "The second main theorem for small functions and related problems", *Acta Math.* **192**:2 (2004), 225–294. MR Zbl
[47] K. Zsigmondy, "Zur Theorie der Potenzreste", *Monatsh. Math. Phys.* **3**:1 (1892), 265–284. MR Zbl

Communicated by Jason P. Bell
Received 2021-12-31 Revised 2022-09-02 Accepted 2022-10-04

alexanderjcarney@gmail.com *Department of Mathematics, University of Rochester, Rochester, NY, United States*
wmh33@txstate.edu *Department of Mathematics, Texas State University, San Marcos, TX, United States*
thomas.tucker@rochester.edu *Department of Mathematics, University of Rochester, Rochester, NY, United States*

ALGEBRA AND NUMBER THEORY 17:9 (2023)
https://doi.org/10.2140/ant.2023.17.1595

Operations in connective K-theory

Alexander Merkurjev and Alexander Vishik

We classify additive operations in connective K-theory with various torsion-free coefficients. We discover that the answer for the integral case requires understanding of the $\hat{\mathbb{Z}}$ case. Moreover, although integral additive operations are topologically generated by Adams operations, these are not reduced to infinite linear combinations of the latter ones. We describe a topological basis for stable operations and relate it to a basis of stable operations in graded K-theory. We classify multiplicative operations in both theories and show that homogeneous additive stable operations with $\hat{\mathbb{Z}}$-coefficients are topologically generated by stable multiplicative operations. This is not true for integral operations.

1. Introduction

Let k be a field of characteristic 0. An *oriented cohomology theory* A^* over k is a functor from the category $\mathbf{Sm}_k^{op}$ of smooth quasiprojective varieties over k to the category of $\mathbb{Z}$-graded commutative rings equipped with a push-forward structure and satisfying certain axioms. In this article, we study the, so-called, *small theories*. For these, the appropriate choice is [Vishik 2019, Definition 2.1], which employs a strong form of the localization axiom and is some breed of the axioms of Panin and Smirnov [Panin 2004, Definition 1.1.7] and that of Levine and Morel [2007, Definition 1.1.2]. In particular, every oriented cohomology theory A^* admits a theory of Chern classes c_n^A of vector bundles. Among such theories there is the universal one — the algebraic cobordism of Levine and Morel Ω^* [2007]. We will work with the *free* theories, i.e., theories obtained from Ω^* by a change of coefficients. These are exactly the theories of *rational type* for which the results of Vishik [2019] apply.

Examples of free oriented cohomology theories are:

- *Chow theory* CH^* that assigns to a smooth variety X over k the Chow ring $\mathrm{CH}^*(X)$;
- *Graded K-theory* K^*_{gr} that takes X to the Laurent polynomial ring $K_0(X)[t,t^{-1}]$ (graded by the powers of the *Bott element* t of degree -1) over the Grothendieck ring $K_0(X)$;
- *Connective K-theory* that takes a smooth variety X to the ring $\mathrm{CK}^*(X)$ of X (see [Cai 2008; Dai and Levine 2014]).

Merkurjev was supported by the NSF grant DMS #1801530.
MSC2020: 19L20, 19L41, 55S25.
Keywords: connective K-theory, additive operations, oriented cohomology theories.

The connective K-theory is the "smallest" oriented cohomology theory "living" above Chow theory and graded K-theory: there are natural graded morphisms

$$\begin{array}{ccc} & \mathrm{CK}^*(X) & \\ \swarrow & & \searrow \\ \mathrm{CH}^*(X) & & K^*_{\mathrm{gr}}(X) \end{array}$$

that yield graded isomorphisms

$$\mathrm{CK}^*(X)/t\,\mathrm{CK}^{*+1}(X) \xrightarrow{\sim} \mathrm{CH}^*(X) \quad \text{and} \quad \mathrm{CK}^*(X)[t^{-1}] \xrightarrow{\sim} K^*_{\mathrm{gr}}(X).$$

Moreover, multiplication $\mathrm{CK}^{n+1}(X) \xrightarrow{t} \mathrm{CK}^n(X)$ by the Bott element $t \in \mathrm{CK}^{-1}(k)$ is an isomorphism if $n < 0$. The map $\mathrm{CK}^0(X) \to K^0_{\mathrm{gr}}(X) = K_0(X)$ is also an isomorphism, so we can identify $\mathrm{CK}^n(X)$ with $K_0(X)$ for all $n \leqslant 0$.

For any $n \geqslant 0$, the image of $\mathrm{CK}^n(X) \xrightarrow{t^n} \mathrm{CK}^0(X) = K_0(X)$ is the subgroup $K_0^{(n)}(X) \subset K_0(X)$ generated by the classes of coherent $\mathcal{O}_X$-modules with codimension of support at least n. Note that the map t^n may not be injective in general if $n > 1$.

Let A^* and B^* be two oriented cohomology theories. An *additive operation* $G : A^* \to B^*$ is a morphism between functors A^* and B^* considered as contravariant functors from $\mathbf{Sm}_k$ to the category of abelian groups. Examples of additive operations are Adams operations in algebraic K-theory and Steenrod operations in the Chow groups modulo a prime integer.

If A^* is an oriented cohomology theory and R is a commutative ring, we write $A^n_R(X)$ for $A^n(X) \otimes_{\mathbb{Z}} R$ and $\mathbf{OP}^{n,m}_R(A)$ for the R-module of R-linear operations $A^n_R \to A^m_R$.

It is proved in [Vishik 2019, §6.3] that every free oriented cohomology theory A^* admits the *Adams operations* $\Psi^A_m \in \mathbf{OP}^{n,n}_R(A)$ for all n and m. The operation Ψ^A_m in $\mathbf{OP}^{1,1}_R(A)$ satisfies

$$\Psi^A_m(c^A_1(L)) = c^A_1(L^{\otimes m})$$

for a line bundle L. Moreover, there is an R-linear map

$$\mathrm{Ad}_n : R[\![x]\!] \to \mathbf{OP}^{n,n}_R(A)$$

taking the power series $(1-x)^m$ to the Adams operation Ψ^A_m for all $m \in \mathbb{Z}$.

In general, the map Ad_n is neither injective nor surjective — see below. But it is shown in [Vishik 2019, §6.1] that Ad_n is an isomorphism if A^* is the graded K-theory, thus,

$$\mathbf{OP}^{n,n}_R(K_{\mathrm{gr}}) \simeq R[\![x]\!].$$

Since the power series $(1-x)^m$ generate $R[\![x]\!]$ as a topological R-module in the x-adic topology, we can say that the R-module $\mathbf{OP}^{n,n}_R(K_{\mathrm{gr}})$ is topologically generated by the Adams operations in the graded K-theory. Moreover, since multiplication by the Bott element is an isomorphism in K^*_{gr}, we have $\mathbf{OP}^{n,m}_R(K_{\mathrm{gr}}) = R[\![x]\!] \cdot t^{n-m}$.

In the present paper, we study the groups $\mathbf{OP}^{n,m}_R := \mathbf{OP}^{n,m}_R(\mathrm{CK})$ of operations in the connective K-theory over R. We write, for simplicity, $\mathbf{OP}^{n,m}$ for $\mathbf{OP}^{n,m}_{\mathbb{Z}}$.

The groups $\mathrm{CK}^n(X)$ for $n \leqslant 0$ are identified with $K_0(X)$, hence translating the above result on the operations in graded K-theory, we see that $\mathrm{Ad}_n : R[\![x]\!] \to \mathbf{OP}^{n,n}_R$ is an isomorphism for $n \leqslant 0$.

The Adams operation Ψ_0 is trivial on CK^n_R for $n \geqslant 1$, i.e., $\mathrm{Ad}_n(1) = 0$, so we consider the restriction $\mathrm{Ad}'_n : xR[\![x]\!] \to \mathbf{OP}^{n,n}_R$ of the map Ad_n. The R-module $\mathrm{CK}^1_R(X)$ is a canonical direct summand via multiplication by t of $\mathrm{CK}^0_R(X) = K_0(X)_R$ with the complement $R \cdot 1$. This leads to a ring isomorphism $\mathbf{OP}^{0,0}_R \simeq R \times \mathbf{OP}^{1,1}_R$. Moreover, the map $\mathrm{Ad}'_1 : xR[\![x]\!] \to \mathbf{OP}^{1,1}_R$ is an isomorphism.

The structure of the groups $\mathbf{OP}^{n,n}_R$, with $n > 1$, is much more delicate and depends on the base ring R. The homomorphisms $\mathrm{Ad}'_n : xR[\![x]\!] \to \mathbf{OP}^{n,n}_R$ for $n \geqslant 2$ are not surjective in general.

It came as a surprise to us that the structure of $\mathbf{OP}^{n,n}_R$ is very simple over the ring of *profinite integers* $\hat{\mathbb{Z}} = \lim(\mathbb{Z}/n\mathbb{Z})$:

Theorem. *The map* $\mathrm{Ad}'_n : x\hat{\mathbb{Z}}[\![x]\!] \to \mathbf{OP}^{n,n}_{\hat{\mathbb{Z}}}$ *is an isomorphism if* $n \geqslant 1$. *In particular, the* $\hat{\mathbb{Z}}$*-module* $\mathbf{OP}^{n,n}_{\hat{\mathbb{Z}}}$ *is topologically generated by the Adams operations.*

Over $\mathbb{Z}$, the map Ad'_n is not surjective if $n \geqslant 2$.

Theorem. *The group* $\mathbf{OP}^{n,n}$ *of integral operations is isomorphic, canonically, to a subgroup of* $\mathbf{OP}^{n,n}_{\hat{\mathbb{Z}}}$. *Moreover, there is an exact sequence*

$$0 \to x\mathbb{Z}[\![x]\!] \xrightarrow{\mathrm{Ad}'_n} \mathbf{OP}^{n,n} \to (\hat{\mathbb{Z}}/\mathbb{Z})^{n-1} \to 0$$

if $n \geqslant 1$.

Thus, the group $\hat{\mathbb{Z}}$ also shows up in the computation of $\mathbf{OP}^{n,n}$ over $\mathbb{Z}$. For example, $\mathbf{OP}^{2,2}$ as a subgroup of $\mathbf{OP}^{2,2}_{\hat{\mathbb{Z}}} = x\hat{\mathbb{Z}}[\![x]\!]$ is generated by $x\mathbb{Z}[\![x]\!]$ and the power series $\sum_{i>0}((c-c_i)/i)x^i$ for all $c \in \hat{\mathbb{Z}}$ and integers c_i such that $c - c_i$ is divisible by i for all $i > 0$, i.e., c_i in $\mathbb{Z}$ represents congruence class of c modulo i.

We prove that the rings $\mathbf{OP}^{n,n}$ and $\mathbf{OP}^{n,n}_{\hat{\mathbb{Z}}}$ are commutative. Moreover, the rings $\mathbf{OP}^{n,n}$ are "almost" integral domains: the only zero divisors are the multiples of $\Psi_1 \pm \Psi_{-1}$.

An operation $G : A^* \to B^*$ is called *multiplicative* if G is a morphism of functors $\mathbf{Sm}_k \to$ Rings. Examples are *twisted* Adams operations Ψ^c_b, defined as follows: Let $b \in \hat{\mathbb{Z}}$ and $c \in \hat{\mathbb{Z}}^\times$. Then the operation Ψ^c_b is homogeneous and equal to $c^{-n} \cdot \Psi_{bc}$ on $\mathrm{CK}^n_{\hat{\mathbb{Z}}}$, where Ψ_{bc} is the (generalized) Adams operation with the power series $(1-x)^{bc}$. We classify all multiplicative operations on $\mathrm{CK}^*_{\hat{\mathbb{Z}}}$ in Section 5.

The notion of "stability" in topology can be considered in an algebraic setting as follows (see [Vishik 2019, §3.1]): Let **SmOp** be a category whose objects are pairs (X, U), where $X \in \mathbf{Sm}_k$ and U is an open subvariety of X. Any theory A^* extends from $\mathbf{Sm}_k$ to **SmOp** by the rule

$$A^*((X, U)) := \mathrm{Ker}(A^*(X) \to A^*(U)),$$

and every additive operation $A^* \to B^*$ on $\mathbf{Sm}_k$ extends uniquely to an operation on **SmOp**. There is an identification

$$\sigma^A_T : A^*((X, U)) \xrightarrow{\cong} A^{*+1}(\Sigma_T(X, U)),$$

where $\Sigma_T(X, U) := (X, U) \wedge (\mathbb{P}^1, \mathbb{P}^1 \backslash 0) = \big(X \times \mathbb{P}^1, X \times (\mathbb{P}^1 \backslash 0) \cup U \times \mathbb{P}^1\big)$.

For any additive operation $G : A^* \to B^*$, we define its *desuspension* as the unique operation $\Sigma^{-1}G : A^* \to B^*$ such that

$$G \circ \sigma_T^A = \sigma_T^B \circ \Sigma^{-1}G.$$

A *stable* additive operation $G : A^* \to B^*$ is the collection $\{G^{(n)} \mid n \geqslant 0\}$ of operations $A^* \to B^*$ such that $G^{(n)} = \Sigma^{-1}G^{(n+1)}$.

In Section 6, we classify stable operations in connective K-theory over $\hat{\mathbb{Z}}$. We prove that under the identification

$$\mathbf{OP}_{\hat{\mathbb{Z}}}^{n,n} = \begin{cases} \hat{\mathbb{Z}}[\![x]\!], & \text{if } n \leqslant 0, \\ x\hat{\mathbb{Z}}[\![x]\!], & \text{if } n \geqslant 1, \end{cases}$$

the desuspension map is given by the formula

$$\Sigma^{-1}(G) = \begin{cases} \Phi(G), & \text{if } n \leqslant 1, \\ \Phi(G) - \Phi(G)(0), & \text{if } n > 1, \end{cases}$$

where $G \in \mathbf{OP}_{\hat{\mathbb{Z}}}^{n,n}$ and $\Phi(G) = (x-1)(dG/dx)$. Thus, the desuspension map Σ^{-1} yields a tower of injective maps

$$\hat{\mathbb{Z}}[\![x]\!] = \mathbf{OP}_{\hat{\mathbb{Z}}}^{0,0} \hookleftarrow \mathbf{OP}_{\hat{\mathbb{Z}}}^{1,1} \hookleftarrow \cdots \hookleftarrow \mathbf{OP}_{\hat{\mathbb{Z}}}^{n,n} \hookleftarrow \cdots .$$

The group of homogeneous degree 0 stable operations $\mathrm{CK}_{\hat{\mathbb{Z}}}^* \to \mathrm{CK}_{\hat{\mathbb{Z}}}^*$ is canonically isomorphic to the group

$$S := \bigcap_n \mathrm{Im}(\Phi^n) \subset \hat{\mathbb{Z}}[\![x]\!].$$

We identify this group in Section 6. In particular, we prove that S is the closure in the x-adic topology of $\hat{\mathbb{Z}}[\![x]\!]$ of the set of all (finite) $\hat{\mathbb{Z}}$-linear combinations of the Adams power series A_r, for $r \in \hat{\mathbb{Z}}^\times$. The $\hat{\mathbb{Z}}$-module S and its integral version S_0 appear to be of an uncountable rank. We describe a topological basis for them.

We call a multiplicative operation G *stable* if the constant sequence $(G, G, G, \dots)$ is stable. We prove that stable multiplicative operations $\mathrm{CK}_{\hat{\mathbb{Z}}}^* \to \mathrm{CK}_{\hat{\mathbb{Z}}}^*$ are exactly operations Ψ_1^c, for $c \in \hat{\mathbb{Z}}^\times$. Thus, we obtain:

Theorem. *Homogeneous degree* 0 *stable additive operations on* $\mathrm{CK}_{\hat{\mathbb{Z}}}^*$ *are topologically generated by the stable multiplicative operations on it.*

Similarly, stable multiplicative operations on CK^* are $\Psi_1^{\pm 1}$. This time though, they don't generate the group of stable additive operations which is of uncountable rank.

Recall that additive operations in (graded) K-theory were determined in [Vishik 2019, §6.1]. In the present paper, we determine stable and multiplicative operations in K_{gr}. We describe a basis of the group of stable K_{gr}-operations and relate it to the basis of stable CK-operations. The ring of stable operations is dual to the Hopf algebra of co-operations defined over $\mathbb{Z}$, and therefore, has the structure of a (topological) Hopf algebra. The Hopf algebra of co-operations coincides with $K_0(K)$ in topology and has been studied in [Adams and Clarke 1977; Adams et al. 1971; Clarke et al. 2001; Johnson 1984; Strong and Whitehouse 2010]. The case of CK was investigated, in particular, in [Kane 1981].

The main tool used in our proofs is the general result of Vishik [2019, Theorem 6.2] that asserts, when applied to the connective K-theory, that an operation $G \in \mathbf{OP}_R^{n,m}$ for $n \geqslant 1$ is given by a sequence of symmetric power series $G_l \in R[\![x_1, \dots, x_l]\!]$ for all $l \geqslant n$ satisfying certain conditions. In particular, G_l divisible by $x_1 \cdots x_l$ and $-G_{l+1} = \partial(G_l)$, the *partial derivative* of G_l (see Definition 2.1) for all $l \geqslant n$, i.e., all power series G_l are determined by G_n. We show that if R is torsion free, then G_n can be integrated over $K = R \otimes \mathbb{Q}$: there is a unique power series $H \in xK[\![x]\!]$ such that $G_n = \partial^{n-1}(H)$. Thus, the operation G is determined by a power series H in one variable over K such that $\partial^{n-1}(H) \in R[\![x_1, \dots, x_n]\!]$.

The article is organized as follows: In Section 2, we prove general results which will permit us to integrate the multivariate symmetric power series and reduce the classification of operations to the description of power series in one variable with certain integrality properties. These properties are then studied and the respective power series are classified in Section 3. In Section 4, we apply the obtained results in combination with [Vishik 2019, Theorem 6.2] to produce a description of additive operations in CK with integral and $\hat{\mathbb{Z}}$-coefficients. We describe the ring structure on the set of homogeneous operations. The description of operations in K_{gr} comes as an easy by-product. In the latter case, we also describe the dual bialgebra of co-operations. Multiplicative operations in CK and K_{gr} are studied in Section 5. Finally, Section 6 is devoted to the computation of stable operations.

2. Symmetric power series

2A. ***Partial derivatives.*** Let $F(x, y)$ be a (commutative) formal group law over a commutative ring R. We write $x * y := F(x, y)$.

Let $G(x_1, \dots, x_n) \in R[\![x_1, \dots, x_n]\!]$ be a power series in $n \geqslant 1$ variables.

Definition 2.1. The *partial derivative* of G (with respect to F) is the power series

$$(\partial G)(x_1, x_2, \dots, x_{n+1}) = G(x_1 * x_2, x_3, \dots, x_{n+1}) - G(x_1, x_3, \dots, x_{n+1}) - G(x_2, x_3, \dots, x_{n+1}) + G(0, x_3, \dots, x_{n+1}),$$

which lies in $R[\![x_1, \dots, x_{n+1}]\!]$.

Note that the partial derivative is always taken with respect to the first variable (in this case x_1) in the list of variables. Write ∂^m for the iterated partial derivative. We also set $(\partial^0 G)(x_1, \dots, x_n) = G(x_1, \dots, x_n) - G(0, x_2, \dots, x_n)$.

For a subset $I \subset [1, m+1] := \{1, \dots, m+1\}$, write x_I for the $*$-sum of all x_i with $i \in I$. In particular, $x_\varnothing = 0$. Then

$$(\partial^m G)(x_1, \dots, x_{m+n}) = \sum (-1)^{|I|} G(x_I, x_{m+2}, \dots, x_{m+n}) \in R[\![x_1, x_2, \dots, x_{m+n}]\!], \tag{2.2}$$

where the sum is taken over all 2^{m+1} subsets $I \subset [1, m+1]$. In particular, $\partial^m G$ is symmetric with respect to the first $m+1$ variables.

Observation 2.3. If $G \in R[\![x_1, \dots, x_n]\!]$ is such that ∂G is a symmetric power series, then $\partial^m G$ is symmetric for all $m \geqslant 1$.

Indeed, since ∂G is symmetric, $\partial^m G = \partial^{m-1}(\partial G)$ is symmetric with respect to the last n variables. But $\partial^m G$ is symmetric with respect to the first $m+1$ variables, hence it is symmetric.

Notation 2.4. For any commutative $\mathbb{Q}$-algebra K, write

$$\lg_1(x) := \log(1-x) = -\sum_{i\geqslant 1} \frac{x^i}{i} \in K[\![x]\!]$$

and for any $n \geqslant 0$,

$$\lg_n(x) := \frac{1}{n!}\big(\lg_1(x)\big)^n \in K[\![x]\!].$$

In particular, $\lg_0(x) = 1$.

For the rest of this section, $*$ denotes the multiplicative formal group law, i.e., $x*y = x + y - xy$.

The power series $\lg_1(x)$ belongs to the kernel of ∂. Moreover, we have the following statement:

Proposition 2.5. *For any commutative $\mathbb{Q}$-algebra K and any $n > 0$, the kernel of $\partial^{n-1} : K[\![x]\!] \to K[\![x_1, \dots, x_n]\!]$ is equal to*

$$\sum_{0\leqslant r<n} K \cdot \lg_r(x).$$

Proof. We make the following change of variables:

$$y_i = \lg_1(x_i) = \log(1-x_i),$$

where $x_1 = x$. The multiplicative group law $*$ translates to the additive one. In the new variables, the partial derivative is homogeneous and lowers the degree in y_1 by 1. Therefore, the kernel of ∂^n is spanned by $1, y_1, \dots, y_1^{n-1}$. □

The following formula is very useful:

Proposition 2.6. *Let K be a $\mathbb{Q}$-algebra, $G \in K[\![x]\!]$ and n a positive integer. Then*

$$(\partial^n G)(x_1, x_2, \dots x_{n+1}) = \sum_{k=1}^{\infty} \frac{1}{k!}\,\partial^{n-1}\left((1-x)^k \frac{d^k G}{dx^k}\right)(x_1, x_2, \dots, x_n)\cdot x_{n+1}^k.$$

Proof. Note that both sides don't contain monomials $\bar{x}^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_{n+1}^{\alpha_{n+1}}$ if at least one α_i is zero. We prove that for every multiindex α with $\alpha_i > 0$ for all i, the $\bar{x}^\alpha$- coefficients of both sides are equal. Set $k = \alpha_{n+1}$.

By (2.2), the $\bar{x}^\alpha$-coefficient of the left-hand side is the same as the $\bar{x}^\alpha$-coefficient of $G(x_1 * x_2 * \cdots * x_{n+1})$. To determine this coefficient, we differentiate (in the standard way) k times the series $G(x_1 * x_2 * \cdots * x_{n+1})$ by x_{n+1}, plug in $x_{n+1} = 0$ and divide by $k!$. Since our formal group law is multiplicative, we have $1 - x * y = (1-x)(1-y)$, and so,

$$\frac{d}{dx_{n+1}}(x_1 * x_2 * \cdots * x_{n+1}) = (1-x_1)(1-x_2)\cdots(1-x_n).$$

It follows that the $\underline{x}^\alpha$-coefficient in the left-hand side is equal to the $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$-coefficient of

$$\frac{1}{k!}(1-x_1)^k(1-x_2)^k\cdots(1-x_n)^k \frac{d^k G}{dx^k}(x_1 * x_2 * \cdots * x_n).$$

On the other hand, the $\underline{x}^{\alpha}$-coefficient of the right-hand side is equal to the $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$-coefficient of $(1/k!)\partial^{n-1}\big((1-x)^k(d^kG/dx^k)\big)(x_1, x_2, \ldots, x_n)$. This is the same as the $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$-coefficient of

$$\frac{1}{k!}(1 - x_1 * x_2 * \cdots * x_n)^k G^{(k)}(x_1 * x_2 * \cdots * x_n)$$
$$= \frac{1}{k!}(1-x_1)^k(1-x_2)^k\cdots(1-x_n)^k\frac{d^kG}{dx^k}(x_1 * x_2 * \cdots * x_n). \quad \square$$

For a nonzero power series $H \in R[\![x_1, \ldots, x_n]\!]$, denote by $v(H)$ the smallest degree of monomials in H. Set also $v(0) = \infty$.

Observation 2.7. Suppose that a commutative ring R is torsion free. A direct calculation shows that for positive integers n and m, we have $v(\partial^{n-1}(x^m)) = m$ if $m \geqslant n$. It follows that $v(\partial^{n-1}(G)) = v(G)$ for every $G \in R[\![x]\!]$ such that $v(G) \geqslant n$.

2B. *Integration of symmetric power series.*

Definition 2.8. A power series $G \in R[\![x_1, \ldots, x_n]\!]$ is called *double-symmetric* if G itself and ∂G are both symmetric.

In the following proposition, we prove that double-symmetric power series can be symmetrically integrated over any commutative $\mathbb{Q}$-algebra:

Proposition 2.9. *Let K be a commutative $\mathbb{Q}$-algebra and $G \in K[\![x_1, \ldots, x_n]\!]$, with $n \geqslant 2$, be a symmetric power series divisible by $x_1 \cdots x_n$. The following are equivalent*:

(1) *G is double-symmetric.*

(2) *All derivatives $\partial^m(G)$, where $m \geqslant 0$, are symmetric power series.*

(3) *There is a power series $L \in K[\![x]\!]$ such that $G = \partial^{n-1}(L)$.*

(4) *There is $H \in K[\![x_1, \ldots, x_{n-1}]\!]$ such that $\partial(H) = G$.*

(5) *There is a unique symmetric $H \in K[\![x_1, \ldots, x_{n-1}]\!]$, divisible by $x_1 \cdots x_{n-1}$, with zero coefficient at $x_1 \cdots x_{n-1}$ and such that $\partial(H) = G$.*

Proof. Note that (1) $\Longleftrightarrow$ (2) by Observation 2.3. We will prove the equivalence of all statements by induction on n. The implication (3) $\Longrightarrow$ (2) is clear, and the implications (2) $\Longrightarrow$ (1) and (3) $\Longrightarrow$ (4) are trivial.

(5) $\Longrightarrow$ (3): Follows by induction applied to H.

(1) or (4) $\Longrightarrow$ (5): Over a commutative $\mathbb{Q}$-algebra every formal group law is isomorphic to the additive one. So we may assume that the group law is additive, i.e., the derivative is defined by

$$(\partial G)(x, y, \bar{t}\,) = G(x + y, \bar{t}\,) - G(x, \bar{t}\,) - G(y, \bar{t}\,) + G(0, \bar{t}\,).$$

We first prove uniqueness. Indeed if $\partial H = 0$, then H is linear in x_1, and since H is symmetric and divisible by $x_1 \cdots x_{n-1}$, we must have $H = 0$.

Case $n = 2$: The implication (4) $\Longrightarrow$ (5) is obvious. We prove (1) $\Longrightarrow$ (5). We may assume that G is a homogeneous polynomial of degree $d > 1$. The symmetry of the derivative of $G(x, y)$ results in the following cocycle condition:

$$G(x + y, z) + G(x, y) = G(x + z, y) + G(x, z).$$

In particular, we have the following equalities:

$$G(x + y, x + y) + G(x, y) = G(2x + y, y) + G(x, x + y),$$
$$G(2x + y, y) + G(2x, y) = G(2x, 2y) + G(y, y),$$
$$G(x, x + y) + G(x, y) = G(2x, y) + G(x, x).$$

It follows that

$$\begin{aligned}\partial(G(x, x))(x, y) &= G(x + y, x + y) - G(x, x) - G(y, y)\\ &= G(2x, 2y) - 2G(x, y)\\ &= (2^d - 2)(G(x, y)),\end{aligned}$$

hence $G(x, y) = \partial(H)$, where $H(x) = G(x, x)/(2^d - 2)$.

Case $n = 3$: Write $G(x, y, z) = \sum_{i\geqslant 1} G_i(x, y)z^i$. By the very definition, if G satisfies (1), respectively (4), then all $G_i(x, y)$ also satisfy (1), respectively (4). By induction, they satisfy (5). Integrating each $G_i(x, y)$, we get a power series $H = \sum_{i,j\geqslant 1} a_{i,j}x^i y^j$ in two variables such that $\partial H = G$.

Note that we can change H by any series $\sum_i c_i xy^i$ without changing ∂H. This way, we can make $H = \sum_{i,j\geqslant 1} a_{i,j}x^i y^j$ with $a_{i,1} = a_{1,i}$ and $a_{1,1} = 0$. We claim that H is symmetric. Indeed, from the symmetry of ∂H, we have

$$\binom{i+k}{i} a_{i+k,j} = \binom{j+k}{j} a_{j+k,i},$$

for any $i, j, k \geqslant 1$. This implies that

$$\frac{1}{i+l}\binom{i+l}{i} a_{i+l-1,1} = a_{l,i},$$

and so, $a_{i,l} = a_{l,i}$, for any $i, l \geqslant 2$. This shows that H is symmetric. Observe that such symmetric integration is unique provided $a_{1,1} = 0$.

Case $n > 3$: Write $G = \sum_{i\geqslant 1} G_i \cdot x_n^i$ with $G_i \in K[\![x_1, \dots, x_{n-1}]\!]$. Again, by the very definition, the slices G_i of G are double-symmetric. By the inductive assumption, these can be uniquely integrated to symmetric power series $H_i \in K[\![x_1, \dots, x_{n-2}]\!]$ as in (5). Putting these power series together, we obtain

$$H = \sum_{i\geqslant 1} H_i \cdot x_{n-1}^i \in K[\![x_1, \dots, x_{n-1}]\!]$$

such that $\partial H = G$. Write

$$H = \sum_{i_1,\dots,i_{n-1}} a_{i_1,\dots,i_{n-1}} x_1^{i_1} \cdots x_{n-1}^{i_{n-1}}.$$

Modifying H by $x_1 \cdots x_{n-1}L(x_{n-1})$ for an appropriate power series L, we may assume $a_{i,1,\dots,1} = a_{1,1,\dots,i}$ for all i.

We claim that H is symmetric. The $x_1^{i_1}\cdots x_n^{i_n}$-coefficient of $G=\partial H$ is equal to $\binom{i_1+i_2}{i_1}a_{i_1+i_2,i_3,\dots,i_n}$. Therefore, since G is symmetric, H is symmetric with respect to $x_2,\dots,x_{n-1}$, if $i_1>1$. Recall that H is also symmetric in $x_1,\dots,x_{n-2}$. Therefore, it suffices to show that the coefficient $a_{1,i_2,\dots,i_{n-1}}$ does not change if we interchange i_{n-1} with i_k for some $k=2,\dots,n-2$.

Suppose all indices $i_1,\dots,i_{n-1}$ but one are equal to 1. Then the statement follows from the equality $a_{1,1,\dots,i}=a_{i,1,\dots,1}=a_{1,i,\dots,1}$ for all i. Otherwise, at least two indices, say $i_k=u$ and $i_l=v$ with $k<l$ are greater than 1.

If $l<n-1$, set $w=i_{n-1}$. We have (here and below, we indicate only the indices which are permuted, hidden indices remain unchanged):

$$a_{1,u,v,w}=a_{v,u,1,w}=a_{v,w,1,u}=a_{1,w,v,u},$$

so we interchanged i_k and i_{n-1}. If $l=n-1$, we can write

$$a_{1,u,v}=a_{u,1,v}=a_{u,v,1}=a_{v,u,1}=a_{v,1,u}=a_{1,v,u},$$

i.e., we again interchanged i_k and i_{n-1}. □

3. The groups $\mathcal{Q}_R^n$

The formal group law is multiplicative in this section. Let R be a commutative ring and $K=R\otimes_{\mathbb{Z}}\mathbb{Q}$. We assume that R is torsion free (as an abelian group), i.e., R can be identified with a subring of K.

Definition 3.1. For any integer $n\geqslant 1$, let us denote by $\mathcal{Q}_R^n$ the R-module of the power series G in $xK[\![x]\!]$, for which $\partial^{n-1}(G)\in R[\![x_1,\dots,x_n]\!]$. For example, $\mathcal{Q}_R^1=xR[\![x]\!]$. We also set $\mathcal{Q}_R^n=R[\![x]\!]$ if $n\leqslant 0$.

Note that, in view of Proposition 2.5, $xR[\![x]\!]$ and $\sum_{0<r<n}K\cdot \lg_r(x)$ are contained in $\mathcal{Q}_R^n$. In Theorem 4.12 below, we will see that the quotient of $\mathcal{Q}_R^n$ by the second of these subspaces can be identified with the space of additive operations on CK_R^n.

Lemma 3.2. *Suppose R has no nontrivial $\mathbb{Z}$-divisible elements. Then*

$$xR[\![x]\!]\cap\left(\sum_{0<r<n}K\cdot\lg_r(x)\right)=0.$$

Proof. Consider the operator Φ on $K[\![x]\!]$ mapping $R[\![x]\!]$ to itself:

$$\Phi(F(x)):=(x-1)\cdot\frac{d}{dx}(F(x)).$$

Observe that $\Phi(\lg_r(x))=\lg_{r-1}(x)$. Suppose $\sum_{0<r<n}q_r\cdot\lg_r(x)\in xR[\![x]\!]$, where $q_r\in K$, and let r be the largest index such that $q_r\neq 0$. Applying Φ^{r-1} to the sum, we see that $q_{r-1}+q_r\lg_1(x)\in R[\![x]\!]$. Let $n\in\mathbb{N}$ be such that $nq_{r-1}\in R$ and $nq_r\in R$. It follows that $nq_r\in iR$ for every integer $i>0$, i.e., nq_r is a nonzero $\mathbb{Z}$-divisible element in R, a contradiction. □

Definition 3.3. Let n and m be integers. If $n>0$, denote by $\mathcal{Q}_R^{n,m}$ the submodule of $\mathcal{Q}_R^n$ consisting of all power series G such that $v(\partial^{n-1}G)\geqslant m$. If $n\leqslant 0$, set $\mathcal{Q}_R^{n,m}=x^{\max(0,m)}\cdot R[\![x]\!]$.

Theorem 4.12 permits us to describe the R-module of operations $\mathbf{OP}_R^{n,m}$ in terms of the modules $\mathcal{Q}_R^{n,m}$.

Since $v(\partial^{n-1}G) \geqslant n$ for every $G \in \mathcal{Q}_R^n$ with $n > 0$, we have $\mathcal{Q}_R^{n,m} = \mathcal{Q}_R^{n,n} = \mathcal{Q}_R^n$ if $n \geqslant m$. Note also that $\mathcal{Q}_R^{1,m} = x^{\max(1,m)} \cdot R[\![x]\!]$.

3A. ***The groups*** $\mathcal{Q}_{\hat{\mathbb{Z}}}^n$**.** In this section, we determine the structure of the modules $\mathcal{Q}_{\hat{\mathbb{Z}}}^n$ over the ring $\hat{\mathbb{Z}} = \lim(\mathbb{Z}/n\mathbb{Z})$. We write $\hat{\mathbb{Q}}$ for $\hat{\mathbb{Z}} \otimes \mathbb{Q}$. Note that $\hat{\mathbb{Q}} = \hat{\mathbb{Z}} + \mathbb{Q}$ and $\mathbb{Z} = \hat{\mathbb{Z}} \cap \mathbb{Q}$ in $\hat{\mathbb{Q}}$.

Lemma 3.4. *Let $b_1, b_2, \dots, b_m \in \hat{\mathbb{Z}}$ be such that $b_i \equiv b_j \pmod{j}$ for every i divisible by j. Then there is $b \in \mathbb{Z}$ such that $b \equiv b_i \pmod{i}$ for all $i = 1, \dots, m$.*

Proof. Let $p_1, p_2, \dots, p_s$ be all primes that are $\leq m$. For every k, let $q_k = p_k^{r_k}$ be the largest power of p_k such that $q_k \leqslant m$. By the Chinese remainder theorem, we can find $b \in \mathbb{Z}$ such that $b \equiv b_{q_k} \pmod{q_k}$ for all k. We claim that b works. Take any $i \leqslant m$. We prove that $b \equiv b_i \pmod{i}$. Write i as the product $i = \prod q_k'$, where q_k' is a power of p_k. Clearly, q_k' divides q_k. We have

$$\begin{aligned} b_{q_k'} &\equiv b_i \pmod{q_k'}, \quad \text{by assumption,} \\ b_{q_k} &\equiv b_{q_k'} \pmod{q_k'}, \quad \text{by assumption,} \\ b &\equiv b_{q_k} \pmod{q_k}, \quad \text{by construction.} \end{aligned}$$

It follows that $b \equiv b_i \pmod{q_k'}$ for all k, hence $b \equiv b_i \pmod{i}$. □

Let $G(x) = \sum_{i=1}^{\infty} a_i x^i$, with $a_i \in \hat{\mathbb{Q}}$.

Lemma 3.5. *For positive integers $j \leqslant s$, the $x^j y^s$-coefficient of ∂G is equal to*

$$\sum_{i=0}^{j} (-1)^{j-i} \binom{s+i}{s} \binom{s}{j-i} a_{s+i}.$$

Proof. We have

$$\frac{1}{s!} \frac{d^s G}{dx^s} = \sum_{i=0}^{\infty} \binom{s+i}{s} a_{s+i} x^i.$$

The statement follows from Proposition 2.6. □

Set $b_i = i a_i$ for all $i \geqslant 1$.

Corollary 3.6. *If $\partial G \in \hat{\mathbb{Z}}[\![x, y]\!]$, then $b_i - b_1 \in \hat{\mathbb{Z}}$ for all $i \geqslant 1$. In particular, if $a_1 \in \hat{\mathbb{Z}}$, then all b_i are in $\hat{\mathbb{Z}}$.*

Proof. The xy^j-coefficient of ∂G is equal to $b_{j+1} - b_j$. □

Proposition 3.7. *Let $G \in \mathcal{Q}_{\hat{\mathbb{Z}}}^2$, and let $n > 1$ be an integer such that $a_i \in \hat{\mathbb{Z}}$ for all $i < n$. Let $p^t < n$ be a power of a prime integer p such that p^t divides n. Then p^t divides b_n.*

Proof. Take $j = p^t$ and $s = n - p^t \geqslant p^t$. By Lemma 3.5, the $x^j y^s$-coefficient of ∂G is equal to

$$\sum_{i=0}^{j} (-1)^{j-i} \binom{s+i}{s} \binom{s}{j-i} a_{s+i} \in \hat{\mathbb{Z}}.$$

By assumption, all terms in the sum but the last one belong to $\hat{\mathbb{Z}}$, hence so does the last one: $\binom{n}{p^t} a_n \in \hat{\mathbb{Z}}$. But $\binom{n}{p^t} a_n = \binom{n-1}{p^t-1} b_n / p^t$, hence $\binom{n-1}{p^t-1} b_n$ is divisible by p^t. As $\binom{n-1}{p^t-1}$ is prime to p, the coefficient b_n

is divisible by p^t (recall that $\binom{a+b}{a}$ is relatively prime to p if and only if there is no shift of digits in the long addition of a and b written in the p-base). □

Proposition 3.8. *We have*

$$\mathcal{Q}^2_{\hat{\mathbb{Z}}} = \hat{\mathbb{Q}} \cdot \lg_1(x) \oplus x\hat{\mathbb{Z}}[\![x]\!].$$

Proof. Let $G(x) = \sum_{i=1}^{\infty} a_i x^i \in \mathcal{Q}^2_{\hat{\mathbb{Z}}}$, and set $b_i = ia_i$, as before. Adding $a_1 \lg_1(x)$ to $G(x)$, we may assume that $a_1 = 0$. By Corollary 3.6, we have $b_i \in \hat{\mathbb{Z}}$ for all i.

We claim that for every positive integer $i < n$ such that i divides n, we have $b_n \equiv b_i$ modulo i. We prove this by induction on n. By Lemma 3.4 applied to $m = n-1$, there is $b \in \mathbb{Z}$ such that $b \equiv b_i$ modulo i for all $i < n$. Subtracting $b \lg_1(x)$ from $G(x)$, we may assume that b_i is divisible by i for all $i < n$, or equivalently, $a_i \in \hat{\mathbb{Z}}$ for all $i < n$. We prove that b_n is divisible by i, for every $i < n$ dividing n.

Case 1: Assume $n = p^k$ is a power of a prime p. Then $i = p^t$ is a smaller power of p. By Proposition 3.7, we have that i divides b_n.

Case 2: Assume n is not power of a prime. Write n as a product of powers of distinct primes: $n = q_1 q_2 \cdots q_s$. By Proposition 3.7, q_k divides b_n for every k, hence n divides b_n. In particular, i divides b_n. The claim is proved.

Let $b \in \hat{\mathbb{Z}}$ be such that $b \equiv b_n \pmod{n}$ for all n. We have

$$G = b \lg_1(x) + \sum_{n \geqslant 1} \frac{b_n - b}{n} x^n \in \hat{\mathbb{Z}} \cdot \lg_1(x) + x\hat{\mathbb{Z}}[\![x]\!]. \qquad \square$$

Corollary 3.9. *Let $G(x) = ax + \cdots \in \mathcal{Q}^2_{\hat{\mathbb{Z}}}$ be a power series with $a \in \hat{\mathbb{Z}}$. Then $G(x) \in \hat{\mathbb{Z}} \cdot \lg_1(x) + x\hat{\mathbb{Z}}[\![x]\!]$.*

In analogy with partial derivative with respect to the first variable, Definition 2.1, we may define the partial derivative with respect to any other variable. In the next statement, we will use such partial derivatives for $H(x, y)$. In particular,

$$(\partial_y H)(x, y, z) = H(x, y * z) - H(x, y) - H(x, z) + H(x, 0).$$

Lemma 3.10. *Let $H(x, y) = \sum_{i,j \geqslant 1} a_{i,j} x^i y^j \in \hat{\mathbb{Q}}[\![x, y]\!]$ be a power series such that both ∂-partial derivatives of H have coefficients in $\hat{\mathbb{Z}}$ and $a_{i,1}$, as well as $a_{1,i}$, are in $\hat{\mathbb{Z}}$, for all i. Then $H(x, y) \in \hat{\mathbb{Z}}[\![x, y]\!]$.*

Proof. Consider some j-th row of H: $y^j \cdot \sum_{i \geqslant 1} a_{i,j} x^i$. We know that $\sum_{i \geqslant 1} a_{i,j} x^i \in \mathcal{Q}^2_{\hat{\mathbb{Z}}}$. By Corollary 3.9, we have that $\sum_{i \geqslant 1} a_{i,j} x^i$ is equal to $c_j \cdot \lg_1(x)$ modulo $x\hat{\mathbb{Z}}[\![x]\!]$ for some $c_j \in \hat{\mathbb{Z}}$. Hence, $c_j / i \equiv a_{i,j} \pmod{\hat{\mathbb{Z}}}$ for all i. Applying the same considerations to the i-th column $x^i \cdot \sum_{j \geqslant 1} a_{i,j} y^j$, we obtain

$$\frac{c_j}{i} \equiv \frac{d_i}{j} \pmod{\hat{\mathbb{Z}}},$$

for certain $d_i \in \hat{\mathbb{Z}}$. Let us show that all c_i (and d_j) are zeros. Indeed, we have

$$jc_j \equiv id_i \pmod{ij}.$$

Hence, jc_j is divisible by i, for any i and, hence $c_j = 0$. This implies that $a_{i,j} \in \hat{\mathbb{Z}}$ for any i, j. □

Lemma 3.11. *Suppose*

$$H(x_1, \dots, x_n) = \sum_{i_1, \dots, i_n > 0} a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n} \in \hat{\mathbb{Q}}[\![x_1, \dots, x_n]\!]$$

is such a power series that all ∂-partial derivatives of H with respect to all variables have coefficients in $\hat{\mathbb{Z}}$ and $a_{i_1, \dots, i_n} \in \hat{\mathbb{Z}}$ as long as all i_j but one are equal to 1. *Then H has coefficients in $\hat{\mathbb{Z}}$.*

Proof. Induction on n. For $n = 1$, there is nothing to prove. For $n = 2$, this is Lemma 3.10. We can assume that $n \geqslant 3$. Suppose we know the statement for $r < n$. Let $L \subset [1, n]$ be some subset. Consider the sum of monomials of H with $i_j = 1$, for every $j \in L$. Plugging $x_j = 1$ for all $j \in L$, we obtain the power series in variables $x_j, j \notin L$ which we will call the L-cell H_L of H. Similarly, considering the sum of the monomials of H with the given i_1 and plugging $x_1 = 1$ into it, we get the power series $H_{i_1}(x_2, \dots, x_n)$, which we call the hyperslice of H. Note, that all the cells of H satisfy the conditions of the lemma. By our assumption, these have all coefficients in $\hat{\mathbb{Z}}$. That is, $a_{i_1, \dots, i_n} \in \hat{\mathbb{Z}}$ provided, at least, one of the i_j is 1. The hyperslice H_{i_1} satisfies the conditions of the lemma too (note that $n \geqslant 3$). Thus, H_{i_1} has coefficients in $\hat{\mathbb{Z}}$ and so does H. □

The following theorem is a generalization of Proposition 3.8:

Theorem 3.12. *For every $n \geqslant 1$,*

$$\mathcal{Q}^n_{\hat{\mathbb{Z}}} = \coprod_{0 < r < n} \hat{\mathbb{Q}} \cdot \lg_r(x) \oplus x\hat{\mathbb{Z}}[\![x]\!].$$

Proof. The statement is clear if $n \leqslant 0$. Now assume that $n \geqslant 1$. It follows from Lemma 3.2 that $\coprod_{0<r<n} \hat{\mathbb{Q}} \cdot \lg_r(x) \cap \hat{\mathbb{Z}}[\![x]\!] = 0$.

We prove the rest by induction on n. For $n = 1$, this follows by definition, and for $n = 2$, this is given by Proposition 3.8.

($n \Rightarrow n + 1$): Let $G \in \mathcal{Q}^{n+1}_{\hat{\mathbb{Z}}}$. Consider the power series $H(x_1, \dots, x_n) = \partial^{n-1}(G)$. Let

$$H(x_1, \dots, x_n) = \sum_{i_1, \dots, i_n \geqslant 1} a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n}.$$

Note that the degreewise smallest term of $\partial^{n-1}(\lg_n(x))$ is $(-1)^n x_1 \cdots x_n$. By subtracting an appropriate $\hat{\mathbb{Q}}$-multiple of $\lg_n(x)$ from G, we may assume that $a_{1, \dots, 1} = 0$.

As $\partial(H)$ has coefficients in $\hat{\mathbb{Z}}$, the "ray" $\sum_{i \geqslant 1} a_{i,1,\dots,1} x_1^i$ is a power series with terms of degree $\geqslant 2$ whose ∂-derivative is integral. By Corollary 3.9, up to a power series in $\hat{\mathbb{Z}}[\![x_1]\!]$, it is equal to $c \cdot \lg_1(x_1)$, for some $c \in \hat{\mathbb{Z}}$.

Since

$$\partial^{n-1}(\lg_n)(x_1, \dots, x_n) = \lg_1(x_1) \cdots \lg_1(x_n),$$

subtracting from $G(x)$ an appropriate multiple of $\lg_n(x)$, we may assume that the coefficients $a_{i,1,\dots,1}$ are in $\hat{\mathbb{Z}}$, for all $i \geqslant 1$. Since H is symmetric, by Lemma 3.11, all coefficients of the power series H are in $\hat{\mathbb{Z}}$. By the induction hypothesis, $G(x) \in \mathcal{Q}^n = \coprod_{0<r<n} \hat{\mathbb{Q}} \cdot \lg_r(x) + x\hat{\mathbb{Z}}[\![x]\!]$. □

3B. ***The groups $\mathcal{Q}^n$.*** Write $\mathcal{Q}^n$ for $\mathcal{Q}^n_{\mathbb{Z}} \subset \mathcal{Q}^n_{\hat{\mathbb{Z}}}$.

We define a homomorphism

$$\rho_n : \mathcal{Q}^n \to \hat{\mathbb{Q}}^{n-1}$$

for $n \geqslant 1$ as the composition (see Theorem 3.12)

$$\mathcal{Q}^n \hookrightarrow \mathcal{Q}^n_{\hat{\mathbb{Z}}} = \coprod_{0<r<n} \hat{\mathbb{Q}} \cdot \mathrm{lg}_r(x) \oplus x\hat{\mathbb{Z}}[\![x]\!] \xrightarrow{\text{proj}} \coprod_{0<r<n} \hat{\mathbb{Q}} \cdot \mathrm{lg}_r(x) \simeq \hat{\mathbb{Q}}^{n-1}.$$

We will show that the map ρ_n is surjective.

Consider the power series

$$\widetilde{\mathrm{lg}}_r(x) = (-1)^r \sum_{0<i_1<\cdots<i_r} \frac{x^{i_r}}{i_1 \cdots i_r} \equiv (-1)^r \frac{x^r}{r!} \pmod{x^{r+1}}.$$

For a sequence $a = (a_i)_{i\geqslant 1}$ in $\hat{\mathbb{Z}}$, let us denote by $a \cdot \widetilde{\mathrm{lg}}_r(x) \in \hat{\mathbb{Q}}[\![x]\!]$ the power series

$$(-1)^r \sum_{0<i_1<\cdots<i_r} \frac{a_{i_1} \cdot x^{i_r}}{i_1 \cdots i_r} \equiv (-1)^r \frac{a_1}{r!} x^r \pmod{x^{r+1}}.$$

If all $a_i \in \mathbb{Z}$, we have $a \cdot \widetilde{\mathrm{lg}}_r(x) \in \mathbb{Q}[\![x]\!]$.

Lemma 3.13. *For every sequence a, we have*

$$(x-1) \cdot \frac{d}{dx}(a \cdot \widetilde{\mathrm{lg}}_r(x)) = a \cdot \widetilde{\mathrm{lg}}_{r-1}(x).$$

Proof. Write $(-1)^r a \cdot \widetilde{\mathrm{lg}}_r(x) = \sum b_i x^i$ and $(-1)^{r-1} a \cdot \widetilde{\mathrm{lg}}_{r-1}(x) = \sum c_i x^i$. We need to prove that $(m+1)b_{m+1} - mb_m = c_m$ for every m. We have

$$(m+1)b_{m+1} = \sum_{0<i_1<\cdots<i_{r-1}<m+1} \frac{a_{i_1}}{i_1 \cdots i_{r-1}}.$$

The sum of the terms with $i_{r-1} < m$ is equal to mb_m. The sum of the terms with $i_{r-1} = m$ coincides with c_m. □

In particular, $\Phi(\widetilde{\mathrm{lg}}_r(x)) = \widetilde{\mathrm{lg}}_{r-1}(x)$. Note that we also have $\Phi(\mathrm{lg}_r(x)) = \mathrm{lg}_{r-1}(x)$ and series $\widetilde{\mathrm{lg}}_r(x)$ and $\mathrm{lg}_r(x)$ have no constant terms for $r \geqslant 1$. Since the kernel of Φ consists of constants only and $\widetilde{\mathrm{lg}}_1(x) = \mathrm{lg}_1(x)$, by definition, it follows by induction on r that $\widetilde{\mathrm{lg}}_r(x) = \mathrm{lg}_r(x)$, for all r. In particular, we can define the product $a \cdot \mathrm{lg}_r(x)$ as above.

Lemma 3.14. *For every $c \in \hat{\mathbb{Z}}$ and every integer $r > 0$, there is a sequence $\tilde{c} = (c_i)_{i\geqslant 1}$ of integers $c_i \in \mathbb{Z}$ such that $c_i \equiv c \pmod{i}$ for all i and*

$$(c - \tilde{c}) \cdot \mathrm{lg}_i(x) \in \hat{\mathbb{Z}}[\![x]\!]$$

for all $i = 1, \ldots, r$, where $c - \tilde{c}$ is the sequence $(c - c_i)_{i\geqslant 1}$.

Proof. Take any collection $\tilde{c} = (c_i)_{i\geqslant 1}$ of integers. Note that for every $i \geqslant 1$ and $k = 1, \dots, r$, the x^{i+k-1}-coefficient of $\tilde{c} \cdot \lg_k(x)$ is a linear combination of $c_1, \dots, c_i$ with rational coefficients where the c_i-coefficient is equal to $(-1)^k/(i(i+1)\cdots(i+k-1))$.

We will modify $c_1, c_2, \dots$ inductively to make all coefficients of the power series

$$G_k = (c - \tilde{c}) \cdot \lg_k(x)$$

integral for all $k = 1, \dots, r$. Let c_1 be an integer congruent to c modulo $r!$, so the x^k-coefficient of G_k is integer for every $k = 1, \dots, r$. Suppose we have modified $c_1, \dots c_n$ so that the x^j-coefficient of G_k is integral for all $k = 1, \dots, r$ and $j \leqslant n + k - 1$.

By induction on $k = 1, \dots, r$, we will modify c_{n+1} to make integral the x^{n+k}-coefficient of G_k. Note that the integral x^j-coefficients of G_k for $j \leqslant n + k - 1$ will not change. If $k = 1$, we don't modify c_{n+1}: the power series G_1 is already integral.

$k \Rightarrow k + 1$: By Lemma 3.13,

$$(x - 1) \cdot \frac{\mathrm{d}G_{k+1}}{\mathrm{d}x} = G_k.$$

Hence, if $G_k = \sum_{i\geqslant k} b_i x^i$ and $G_{k+1} = \sum_{i\geqslant k+1} a_i x^i$, then

$$a_{n+l+1} = \frac{-1}{n+l+1}(b_k + \ldots + b_{n+l})$$

for all l.

By induction, $b_k, \dots, b_{n+k}$ are integral. Recall that these are linear combinations of the c_i', where $c_i' = c - c_i$ and c_{n+1}' appear only in b_{n+k}. We modify c_{n+1} by adding the integer $t(n+1)(n+2)\cdots(n+k)$ to c_{n+1} with some $t \in \mathbb{Z}$. Note that $b_k, \dots, b_{n+k-1}$ remain unchanged and b_{n+k} changes to $b_{n+k} + t$, so it stays integral. Choose t to make a_{n+k+1} integral.

Note that c_{n+1}' comes with coefficient $(-1)^l/((n+1)\cdots(n+l))$ in the x^{n+l}-coefficient of G_l. Since $(n+1)\cdots(n+l)$ divides $(n+1)\cdots(n+k)$ when $l \leqslant k$, the x^{n+l}-coefficient of G_l remains integral for $l \leqslant k$. □

Now we prove that the map $\rho_n : \mathcal{Q}^n \to \hat{\mathbb{Q}}^{n-1}$ is surjective. Since $q \cdot \lg_r \in \mathcal{Q}^n$ for all $q \in \mathbb{Q}$ and $r = 1, \dots, n-1$, we have $\mathbb{Q}^{n-1} \subset \mathrm{Im}(\rho_n)$. It suffices to show that $\hat{\mathbb{Z}}^{n-1} \subset \mathrm{Im}(\rho_n)$. Choose $c_r \in \hat{\mathbb{Z}}$ for $r = 1, \dots, n-1$. By Lemma 3.14, there are sequences of integers $\tilde{c}_r$ such that $(c_r - \tilde{c}_r) \cdot \lg_r(x) \in \hat{\mathbb{Z}}[\![x]\!]$.

As

$$\tilde{c}_r \cdot \lg_r(x) = c_r \cdot \lg_r(x) - (c_r - \tilde{c}_r) \cdot \lg_r(x),$$

we have $\rho_n\big(\sum_{0<r<n} \tilde{c}_r \cdot \lg_r(x)\big) = (c_r)_{r=1,\dots,n-1}$, proving that ρ_n is surjective.

Note that the kernel of ρ_n is equal to $x\hat{\mathbb{Z}}[\![x]\!] \cap \mathbb{Q}[\![x]\!] = x\mathbb{Z}[\![x]\!]$. Thus, we have an exact sequence

$$0 \to x\mathbb{Z}[\![x]\!] \to \mathcal{Q}^n \xrightarrow{\rho_n} \hat{\mathbb{Q}}^{n-1} \to 0. \tag{3.15}$$

We have proved that if $n \geqslant 1$, the group $\mathcal{Q}^n$ is generated by $x\mathbb{Z}[\![x]\!]$ and the power series $(c - \tilde{c}) \cdot \lg_r(x)$, as in Lemma 3.14, where $c \in \hat{\mathbb{Z}}$ and $r = 1, \dots, n-1$.

The power series in $\mathcal{Q}^n$ can be approximated by polynomials as follows:

Lemma 3.16. *For every $m > 0$ and n, we have*

$$\mathcal{Q}^n \subset \mathbb{Z}[x]_{\leqslant m-1} + \sum_{0<r<n} \mathbb{Q} \cdot \lg_r(x) + x^m \mathbb{Q}[\![x]\!],$$

where $\mathbb{Z}[x]_{\leqslant m-1}$ is the group of integral polynomials of degree at most $m-1$.

Proof. We may assume that $n > 1$. In view of (3.15), the group $\mathcal{Q}^n$ modulo

$$x\mathbb{Z}[\![x]\!] + \sum_{0<r<n} \mathbb{Q} \cdot \lg_r(x)$$

is generated by power series of the form $\tilde{c} \cdot \lg_r(x)$, where $r = 1, \dots, n-1$ and $\tilde{c}$ is the collection of integers such that $c_i \equiv c \pmod{i}$ for all i for an element $c \in \hat{\mathbb{Z}}$ as in Lemma 3.14.

Let d be an integer congruent to c modulo the least common multiple of the denominators of the x^i-coefficients of $\lg_r(x)$ for all $i = 1, \dots, m-1$. Then the x^m-truncation F of $(\tilde{c}-d) \cdot \lg_r(x)$ is contained in $\mathbb{Z}[x]_{\leqslant m-1}$ and $\tilde{c} \cdot \lg_r(x)$ is congruent to F modulo $\mathbb{Z} \cdot \lg_r(x) + x^m \mathbb{Q}[\![x]\!]$. □

4. Operations

Let k be a field of characteristic 0, and write $\mathbf{Sm}_k$ for the category of smooth quasiprojective varieties over k. An *oriented cohomology theory* A^* over k is a functor from $\mathbf{Sm}_k^{op}$ to the category of $\mathbb{Z}$-graded commutative rings equipped with a push-forward structure and satisfying certain axioms (see [Vishik 2019, Definition 2.1]). We write

$$A^*(X) = \coprod_{n \in \mathbb{Z}} A^n(X)$$

for a variety X in $\mathbf{Sm}_k$, and let $A^*(k)$ denote the *coefficient ring* $A^*(\operatorname{Spec} k)$.

Let A^* be an oriented cohomology theory. There is a (unique) associated formal group law

$$F_A(x, y) = \sum_{i,j \geqslant 0} a_{i,j}^A x^i y^j = x + y + a_{1,1} \cdot xy + \text{higher terms} \in A^*(k)[\![x, y]\!]$$

that computes the first Chern class of the tensor product of two line bundles L and L' (see, for example, [Panin 2003, p. 3 and Section 3.9], [Panin 2004, Section 2.7], [Levine and Morel 2007, §1.1] or [Vishik 2019, §2.3]):

$$c_1^A(L \otimes L') = F_A\big(c_1^A(L), c_1^A(L')\big).$$

Example 4.1. The *Chow theory* CH^* takes a smooth variety X to the Chow ring $\mathrm{CH}^*(X)$ of X. We have $\mathrm{CH}^*(k) = \mathbb{Z}$ and $F_{\mathrm{CH}}(x, y) = x + y$ is the *additive* group law.

Example 4.2 (see [Levine and Morel 2007, Example 1.15]). The *graded K-theory* K_{gr}^* takes X to the Laurent polynomial ring $K_0(X)[t, t^{-1}]$, graded by the powers of the *Bott element* t of degree -1, over the Grothendieck ring $K_0(X)$ of X. We have $K_{\mathrm{gr}}^*(k) = \mathbb{Z}[t, t^{-1}]$ and $F_{K_{\mathrm{gr}}}(x, y) = x + y - txy$ is the *multiplicative* group law.

Example 4.3 (see [Cai 2008; Dai and Levine 2014]). The *connective K-theory* takes X to the ring $\mathrm{CK}^*(X)$ of X. We have $\mathrm{CK}^*(k) = \mathbb{Z}[t]$ and $F_{CK}(x, y) = x + y - txy$.

All cohomology theories in these examples are of *rational type* (see [Vishik 2019, §4.1] and [Levine and Morel 2007]).

If A^* is an oriented cohomology theory and R a commutative ring, the functor A^*_R defined by $A^*_R(X) = A^*(X) \otimes_{\mathbb{Z}} R$ is also an oriented cohomology theory with values in the category of graded R-algebras.

Definition 4.4. Let A^* and B^* be two oriented cohomology theories. An *R-linear operation* $G : A^*_R \to B^*_R$ is a morphism between functors A^*_R and B^*_R considered as contravariant functors from $\mathbf{Sm}_k$ to the category of R-modules (cf. [Vishik 2019, Definition 3.3]). Note that G may not respect the gradings on A^*_R and B^*_R.

Let $n, m \in \mathbb{Z}$. A morphism $G : A^n_R \to B^m_R$ between contravariant functors from $\mathbf{Sm}_k$ to the category of R-modules can be viewed as an R-linear operation via the obvious composition $A^*_R \twoheadrightarrow A^n_R \to B^m_R \hookrightarrow B^*_R$. All such operations form an R-module $\mathbf{OP}^{n,m}_R(A^*, B^*)$. The composition of operations yields an R-linear pairing

$$\mathbf{OP}^{n,m}_R(A^*, B^*) \otimes_R \mathbf{OP}^{m,r}_R(B^*, C^*) \to \mathbf{OP}^{n,r}_R(A^*, C^*).$$

In particular, $\mathbf{OP}^{n,n}_R(A^*) := \mathbf{OP}^{n,n}_R(A^*, A^*)$ has a structure of an R-algebra.

Example 4.5 (see [Cai 2008; Dai and Levine 2014]). Multiplication by t yields an operation $\mathrm{CK}^{n+1}_R \to \mathrm{CK}^n_R$ that is an isomorphism if $n < 0$. There are graded R-linear operations

$$\mathrm{CK}^*_R \to \mathrm{CH}^*_R \quad \text{and} \quad \mathrm{CK}^*_R \to (K^*_{\mathrm{gr}})_R.$$

The sequence

$$\mathrm{CK}^{n+1}(X) \xrightarrow{t} \mathrm{CK}^n(X) \to \mathrm{CH}^n(X) \to 0$$

is exact for every n and X.

If $n \geqslant 0$, the image of the homomorphism

$$\mathrm{CK}^n(X) \to K^n_{\mathrm{gr}}(X) = K_0(X)t^{-n} \simeq K_0(X)$$

is generated by the classes of coherent $\mathcal{O}_X$-modules with codimension of support at least n. If $n \leqslant 0$, this map is an isomorphism.

The following fundamental theorem was proved in [Vishik 2019, Theorem 6.2]:

Theorem 4.6. *Let A^* be a cohomology theory of rational type and B^* be any oriented cohomology theory over k. Let R be a commutative ring. Then there is an R-isomorphism between the set $\mathbf{OP}^{n,m}_R(A^*, B^*)$ of R-linear operations $G : A^n_R \to B^m_R$ and the set consisting of the following data $\{G_l, l \in \mathbb{Z}_{\geqslant 0}\}$:*

$$G_l \in \mathrm{Hom}_R\big(A^{n-l}(k) \otimes R,\, B^*(k)[\![x_1, \dots, x_l]\!]_{(m)} \otimes R\big)$$

satisfying

(1) *$G_l(\alpha)$ is a symmetric power series for all l and $\alpha \in A^{n-l}(k) \otimes R$,*

(2) *$G_l(\alpha)$ is divisible by $x_1 \cdots x_l$ for all l and α,*

(3) $G_l(\alpha)(y +_B z, x_2, \dots, x_l) = \sum_{i,j} G_{i+j+l-1}(\alpha \cdot a^A_{i,j})(y^{\times i}, z^{\times j}, x_2, \dots, x_l)$, *for* $l > 0$, *where* $a^A_{i,j}$ *are the coefficients of the formal group law of* A^* *and the sum* $y +_B z$ *is taken with respect to the formal group law of* B^* (*here*, $t^{\times i}$ *denotes* i *copies of* t).

Here, $B^*(k)[\![x_1, \dots, x_n]\!]_{(m)}$ is the subgroup in $B^*(k)[\![x_1, \dots, x_n]\!]$ consisting of all homogeneous degree m power series (all the x_i have degree 1).

The functions G_l are determined by the operation G as follows (see [Vishik 2019, §5]): Write L_i for the pull-back of the canonical line bundle on $\mathbb{P}^\infty$ with respect to the i-th projection $(\mathbb{P}^\infty)^l \to \mathbb{P}^\infty$. Then

$$G_l(\alpha)\big(c^B_1(L_1), \dots, c^B_1(L_l)\big) = G\big(\alpha \cdot c^A_1(L_1) \cdot \ldots \cdot c^A_1(L_l)\big), \tag{4.7}$$

where c_1 is the first Chern class.

Remark 4.8. Theorem 4.6 was proved in [Vishik 2019, Theorem 6.2] in the case $R = \mathbb{Z}$. The general case readily follows. Indeed, multiplication by an element $r \in R$ yields operations $r : A^n_R \to A^n_R$ and $r : B^m_R \to B^m_R$. An additive operation $G : A^n_R \to B^m_R$ is R-linear if and only if $G \circ r = r \circ G$ for all $r \in R$. The latter is equivalent to the equality $G_l \circ r = r \circ G_l$ for all l, i.e., that all G_l are R-linear.

Example 4.9 (see [Vishik 2019, §6.3]). Let A^* be a cohomology theory of rational type and $m \in \mathbb{Z}$. Consider the power series $[m](x) := x +_A \cdots +_A x \in A^*(k)[\![x]\!]$ (m times). The *Adams operation* $\Psi^A_m \in \mathbf{OP}^{*,*}_R$ is determined by $(G_l)_{l \geqslant 0}$, where G_l is multiplication by the power series $[m](x_1) \cdots [m](x_l)$ (l factors), in particular, G_0 is the identity. The Adams operations satisfy the relations

$$\Psi^A_k \circ \Psi^A_m = \Psi^A_{km} = \Psi^A_m \circ \Psi^A_k$$

for all k and m.

4A. ***Operations in connective K-theory.*** We would like to determine the R-module $\mathbf{OP}^{n,m}_R$ of all R-linear operations $G : \mathrm{CK}^n_R \to \mathrm{CK}^m_R$ for any pair of integers n and m. By Theorem 4.6, G is given by a collection of power series $G_l(\alpha) \in R[t][\![x_1, \dots, x_n]\!]_{(m)}$, where $\alpha \in \mathrm{CK}^{n-l}_R(k)$ and $l \geqslant 0$, satisfying the conditions of the theorem. The group $\mathrm{CK}^{n-l}_R(k)$ is trivial if $l < n$ and $\mathrm{CK}^{n-l}_R(k) = R \cdot t^{l-n}$ otherwise. (Recall that t has degree -1.) In the first case, $G_l(\alpha) = 0$, and in the latter case, the power series $G_l(\alpha)$ are uniquely determined by $G_l(t^{l-n})$. We will simply write G_l for $G_l(t^{l-n})$.

If $l \geqslant \max(1, n)$, Theorem 4.6 (3) reads as follows (here $\bar{z}$ denotes $z_2, \dots, z_l$):

$$G_l(x + y - txy, \bar{z}) = G_l(x, \bar{z}) + G_l(y, \bar{z}) - G_{l+1}(x, y, \bar{z}).$$

In other words,

$$G_{l+1} = -\partial_t G_l, \tag{4.10}$$

where the derivative ∂_t is taken with respect to $F_{\mathrm{CK}}(x, y) = x + y - txy$. Thus, G_{l+1} is uniquely determined by G_l.

If $n > 0$, then the operation G yields the double-symmetric power series $G_n \in R[t][\![x_1, \dots, x_n]\!]_{(m)}$ that is divisible by $x_1 \cdots x_n$. Conversely, if we have that $H \in R[t][\![x_1, \dots, x_n]\!]_{(m)}$ is a double-symmetric

power series divisible by $x_1 \cdots x_n$, then setting $G_{n+i} := (-1)^i \partial_t^i(H)$ for all $i \geqslant 0$, we get a sequence of power series that determines an R-linear operation G (see Observation 2.3).

If $n \leqslant 0$, then the operation G is determined by $G_0 \in R[t]_m$ and the power series $G_1 \in R[t][\![x]\!]_m$ that is uniquely determined by $(G_1)|_{t=1} \in x^{\max(1,m)} R[\![x]\!]$. If $m > 0$, then $G_0 = 0$, otherwise $G_0 \in R \cdot t^{-m}$ and we can combine G_0 and G_1 together into the power series $H = (G_0 - G_1)|_{t=1} \in R[\![x]\!]$.

If $L \in R[t][\![x_1, \dots, x_n]\!]_{(m)}$, then $v(L|_{t=1}) \geqslant m$. Conversely, for every $J \in R[\![x_1, \dots, x_n]\!]$ with $v(J) \geqslant m$, there is a unique homogeneous power series $L \in R[t][\![x_1, \dots, x_n]\!]$ of degree m such that $L|_{t=1} = J$. If L is double-symmetric and divisible by $x_1 \cdots x_n$, then so is $L|_{t=1}$ (with respect to the derivative ∂ given by the formal group law $x + y - xy$) and conversely.

We have proved the following statement:

Proposition 4.11. *Let R be a commutative ring, and let n and m be two integers. An R-linear operation $G : \mathrm{CK}_R^n \to \mathrm{CK}_R^m$ is determined by*:

(1) *A power series $H \in x^{\max(0,m)} R[\![x]\!]$, if $n \leqslant 0$. In this case, $G_0 = H(0) \cdot t^{-m}$ and $G_1 \in xR[t][\![x]\!]_{(m)}$ is a unique homogeneous power series such that $H = (G_0 - G_1)|_{t=1}$ and $G_l = (-1)^{l-1} \partial_t^{l-1}(G_1)$ for $l > 1$,*

(2) *A double-symmetric power series $J \in R[\![x_1, \dots, x_n]\!]$ divisible by $x_1 \cdots x_n$ such that $v(J) \geqslant m$, if $n > 0$. In this case $G_l = 0$ for $l = 0, \dots, n-1$ and $G_n \in R[t][\![x_1, \dots, x_n]\!]_{(m)}$ is a unique homogeneous power series such that $G_n|_{t=1} = J$ and $G_l = (-1)^{l-n} \partial_t^{l-n}(G_n)$ for $l > n$.*

Let R be a commutative ring that is torsion free as an abelian group. Define an R-module homomorphism

$$\lambda_{n,m} : \mathcal{Q}_R^{n,m} \to \mathbf{OP}_R^{n,m},$$

see Definition 3.3, as follows: If $n \leqslant 0$, then $\lambda_{n,m}(H)$ for $H \in \mathcal{Q}^{n,m} = x^{\max(0,m)} \cdot R[\![x]\!]$ is the operation given by Proposition 4.11 (1). If $n > 0$, then $\lambda_{n,m}(H)$ for $H \in \mathcal{Q}^{n,m}$ is the operation given by the polynomial $J = (-1)^n \partial^{n-1}(H)$ as in Proposition 4.11 (2).

The following theorem determines the R-module of operations $\mathbf{OP}_R^{n,m}$ in terms of the modules $\mathcal{Q}_R^{n,m}$ of power series in one variable:

Theorem 4.12. *Let R be a commutative ring that is torsion free as an abelian group and $K = R \otimes \mathbb{Q}$. The homomorphisms $\lambda_{n,m}$ yield an R-linear isomorphism between $\mathbf{OP}_R^{n,m}$ and the factor module of $\mathcal{Q}_R^{n,m}$ by the K-subspace spanned by $\lg_i(x)$, where $i = 1, \dots, n-1$. In particular, $\mathbf{OP}_R^{n,m} \simeq x^{\max(0,m)} \cdot R[\![x]\!]$, if $n \leqslant 0$, and $\mathbf{OP}_R^{1,m} \simeq x^{\max(1,m)} \cdot R[\![x]\!]$.*

Proof. The surjectivity of $\lambda_{n,m}$ follows from Propositions 2.9 and 4.11. The kernel of $\lambda_{n,m}$ is determined in Proposition 2.5. □

Corollary 4.13. *The map $\lambda_{n,m}$ yields an isomorphism (see Definition 3.1)*

$$\mathcal{Q}_R^n \cap x^{\max(0,n,m)} \cdot K[\![x]\!] \xrightarrow{\sim} \mathbf{OP}_R^{n,m}.$$

Proof. The case $m \leqslant n$ follows from the theorem. Otherwise, by Observation 2.7, $v(\partial^{n-1} x^i) = i$ for all $i \geqslant n$. □

Let $n, m \in \mathbb{Z}$ and i, j be nonnegative integers. We define an R-linear homomorphism

$$\mathcal{Q}_R^{n,m} \to \mathcal{Q}_R^{n+i,m-j}$$

as follows: If $n \leqslant 0$, $m \leqslant 0$ and $n + i > 0$, the map

$$\mathcal{Q}_R^{n,m} = R[\![x]\!] \to xR[\![x]\!] \hookrightarrow \mathcal{Q}_R^{n+i,m-j}$$

takes H to $\partial^0(H) = H - H(0)$. Otherwise, $\mathcal{Q}_R^{n,m} \subset \mathcal{Q}_R^{n+i,m-j}$, and the map we define is the inclusion.

Multiplication by t^k yields an operation $\mathrm{CK}_R^{*+k} \to \mathrm{CK}_R^*$ and, therefore, yields the homomorphisms $\mathbf{OP}_R^{n,m} \to \mathbf{OP}_R^{n+i,m-j}$ for all i, $j \geqslant 0$.

Proposition 4.14. *The diagram*

$$\begin{array}{ccc} \mathcal{Q}_R^{n,m} & \longrightarrow & \mathcal{Q}_R^{n+i,m-j} \\ {\scriptstyle \lambda_{n,m}}\downarrow & & \downarrow{\scriptstyle \lambda_{n+i,m-j}} \\ \mathbf{OP}_R^{n,m} & \longrightarrow & \mathbf{OP}_R^{n+i,m-j}, \end{array}$$

is commutative.

Proof. The case $i = 0$ follows directly from the definition. It remains to consider the case $i = 1$ and $j = 0$.

Suppose first that $n > 0$. Let $H \in \mathcal{Q}_R^{n,m} \subset \mathcal{Q}_R^{n+i,m-j}$ and $G = \lambda_{n,m}(H) \in \mathbf{OP}_R^{n,m}$. In particular, $G_n|_{t=1} = (-1)^{n-1}\partial^{n-1}(H)$. Denote by G' the image of G in $\mathbf{OP}_R^{n+1,m}$. Write L_i for the pull-back of the canonical line bundle on $\mathbb{P}^\infty$ with respect to the i-th projection $(\mathbb{P}^\infty)^{n+1} \to \mathbb{P}^\infty$. The power series G'_{n+1} is determined by, see (4.7), the equality

$$\begin{aligned} G'_{n+1}\big(c_1(L_1), \ldots, c_1(L_{n+1})\big) &= G'\big(c_1(L_1) \cdots c_1(L_{n+1})\big) \\ &= G\big(tc_1(L_1) \cdots c_1(L_{n+1})\big) \\ &= G_{n+1}(t)\big(c_1(L_1), \ldots, c_1(L_{n+1})\big) \\ &= G_{n+1}\big(c_1(L_1), \ldots, c_1(L_{n+1})\big), \end{aligned}$$

hence $G'_{n+1} = G_{n+1}$. It follows from (4.10) that

$$\begin{aligned} G'_{n+1}|_{t=1} = G_{n+1}|_{t=1} = -(\partial_t G_n)|_{t=1} &= -\partial(G_n|_{t=1}) \\ &= -\partial((-1)^n\partial^{n-1}(H)) = (-1)^{n+1}\partial^n(H), \end{aligned}$$

and therefore, $G' = \lambda_{n+1,m}(H)$.

If $n < 0$ or if $n = 0$ and $m > 0$, we have $\mathcal{Q}_R^{n,m} \subset \mathcal{Q}_R^{n+1,m}$ and the statement follows immediately from the definitions. It remains to consider the case $n = 0$ and $m \leqslant 0$. Let $H \in \mathcal{Q}_R^{0,m} = R[\![x]\!]$ and $G = \lambda_{0,m}(H) \in \mathbf{OP}_R^{0,m}$. In particular, $H = (G_0 - G_1)|_{t=1}$. Denote by G' the image of G in $\mathbf{OP}_R^{1,m}$. A computation, as above, shows that $G'_1 = G_1$. Hence,

$$G'_1|_{t=1} = G_1|_{t=1} = -(H - H(0)).$$

Therefore, $G' = \lambda_{1,m}(H - H(0))$ and $H - H(0)$ is the image of H in $\mathcal{Q}_R^{1,m}$. □

Corollary 4.13 and Proposition 4.14 yield:

Corollary 4.15. *If $m \leqslant n$ then the map $\mathbf{OP}_R^{n,n} \to \mathbf{OP}_R^{n,m}$ is an isomorphism.*

In particular, there is a canonical ring homomorphism

$$\mathbf{OP}_R^{n,n} \to \mathbf{OP}_R^{n+1,n} \xrightarrow{\sim} \mathbf{OP}_R^{n+1,n+1}.$$

Example 4.16. Note that the identification $\mathbf{OP}_R^{0,0} = R[\![x]\!]$ is not a ring isomorphism. The corresponding ring structure on $R[\![x]\!]$ will be described in Section 4E. The natural surjective homomorphism

$$R[\![x]\!] = \mathbf{OP}_R^{0,0} \to \mathbf{OP}_R^{1,1} = xR[\![x]\!]$$

takes a power series $G(x)$ to $G(x) - G(0)$. Its kernel is generated by 1. The complementary operation $G(x) \mapsto G(0)$ on $\mathrm{CK}^0 = K_0$ is an idempotent that takes the class of a vector bundle E to $\mathrm{rank}(E) \cdot 1$, where 1 is the identity in K_0. In particular, we get a natural R-algebra isomorphism $\mathbf{OP}_R^{0,0} \simeq R \times \mathbf{OP}_R^{1,1}$.

4B. ***Adams operations.*** Let R be a torsion free ring. We define the composition

$$\mathrm{Ad}_n : R[\![x]\!] \to \mathcal{Q}_R^n \xrightarrow{\lambda_{n,n}} \mathbf{OP}_R^{n,n},$$

where the first map is the identity if $n \leqslant 0$ and it is the composition of the projection $\partial^0 : R[\![x]\!] \to xR[\![x]\!]$ and the inclusion of $xR[\![x]\!]$ into $\mathcal{Q}_R^n$. The image of Ad_n is denoted $\mathbf{OP}_{R,\mathrm{cl}}^{n,n}$ and called the submodule of *classical operations*.

If $n \leqslant 0$, we have $\mathbf{OP}_{R,\mathrm{cl}}^{n,n} = \mathbf{OP}_R^{n,n} = R[\![x]\!]$. If $n \geqslant 1$, it follows from Lemma 3.2 and Theorem 4.12 that in the case R has no nontrivial $\mathbb{Z}$-divisible elements (for example, $R = \mathbb{Z}$ or $\hat{\mathbb{Z}}$), the restriction of Ad_n on $xR[\![x]\!]$ is injective and, therefore, $\mathbf{OP}_{R,\mathrm{cl}}^{n,n} \simeq xR[\![x]\!]$.

Let m be an integer. In the notation of the Example 4.9, $[m](x) = (1 - (1 - tx)^m)/t$. In view of Proposition 4.11, the Adams operations $\Psi_m \in \mathbf{OP}_{R,\mathrm{cl}}^{n,n}$ are defined by

$$\Psi_m = \mathrm{Ad}_n((1-x)^m). \tag{4.17}$$

Since the power series $(1-x)^m$ generate $R[\![x]\!]$ as topological R-module in the x-adic topology, the group of classical operations $\mathbf{OP}_{R,\mathrm{cl}}^{n,n}$ is topologically generated by the Adams operations.

By Proposition 4.14, we have that the operations Ψ_k are compatible with the canonical homomorphisms $\mathbf{OP}_R^{n,n} \to \mathbf{OP}_R^{n+1,n+1}$.

For every $k \geqslant 0$, consider the additive operations $\Upsilon_k = \sum_{i=0}^{k} (-1)^i \binom{k}{i} \Psi_i$. Then $\Upsilon_k = \lambda_{n,n}(x^k)$ if $k \geqslant 0$. Recall that $\Upsilon_0 = 0$ if $n \geqslant 1$. It follows that the R-module $\mathbf{OP}_{R,\mathrm{cl}}^{n,n}$ consists of all linear combinations $\sum_{k \geqslant 0} \alpha_k \cdot \Upsilon_k$ with $\alpha_k \in R$ (cf. [Vishik 2019, Theorem 6.8]). If R has no nontrivial $\mathbb{Z}$-divisible elements, the coefficients α_k, (where $k \geqslant 0$ if $n \leqslant 0$ and $k \geqslant 1$ if $n \geqslant 1$) are uniquely determined by the operation.

4C. ***Operations over $\hat{\mathbb{Z}}$.*** In Section 3, we determined the modules $\mathcal{Q}_R^n$ over the ring $R = \hat{\mathbb{Z}}$. Theorems 3.12 and 4.12 yield:

Theorem 4.18. *There are canonical isomorphisms*

$$\mathbf{OP}^{n,n}_{\hat{\mathbb{Z}}} = \mathbf{OP}^{n,n}_{\hat{\mathbb{Z}},cl} \simeq \begin{cases} \hat{\mathbb{Z}}[\![x]\!], & \text{if } n \leqslant 0, \\ x\hat{\mathbb{Z}}[\![x]\!], & \text{if } n \geqslant 1. \end{cases}$$

In particular, the natural map $\mathbf{OP}^{n,n}_{\hat{\mathbb{Z}}} \to \mathbf{OP}^{n+1,n+1}_{\hat{\mathbb{Z}}}$ is an isomorphism for all $n \geqslant 1$. It follows from Theorem 4.12 that for any two integers n and m,

$$\mathbf{OP}^{n,m}_{\hat{\mathbb{Z}}} \simeq \begin{cases} x^{\max(0,m)} \cdot \hat{\mathbb{Z}}[\![x]\!], & \text{if } n \leqslant 0, \\ \{G \in x\hat{\mathbb{Z}}[\![x]\!] \mid v(\partial^{n-1}(G)) \geqslant m\}, & \text{if } n \geqslant 1. \end{cases}$$

4D. ***Operations over*** $\mathbb{Z}$**.** Now we turn to the case $R = \mathbb{Z}$ and, for simplicity, write $\mathbf{OP}^{n,m}$ for $\mathbf{OP}^{n,m}_{\mathbb{Z}}$.

Corollary 4.13 implies that the natural homomorphism $\mathbf{OP}^{n,m} \to \mathbf{OP}^{n,m}_{\hat{\mathbb{Z}}}$ is injective. In particular, we can identify $\mathbf{OP}^{n,n}$ with a subgroup of $\mathbf{OP}^{n,n}_{\hat{\mathbb{Z}}} = x\hat{\mathbb{Z}}[\![x]\!]$ for all $n \geqslant 1$, so we have a sequence of subgroups

$$\mathbf{OP}^{1,1} \subset \mathbf{OP}^{2,2} \subset \cdots \subset \mathbf{OP}^{n,n} \subset \cdots \subset x\hat{\mathbb{Z}}[\![x]\!].$$

Recall (Theorem 4.12) that $\mathbf{OP}^{n,m} \simeq x^{\max(0,m)} \cdot \mathbb{Z}[\![x]\!]$ if $n \leqslant 0$ and $\mathbf{OP}^{n,m} \simeq \mathbf{OP}^{n,n}$ if $m \leqslant n$ by Corollary 4.15.

Let $m \geqslant n \geqslant 1$. By Theorem 4.12, we can identify $\mathbf{OP}^{n,m}$ with the factor group of $\mathcal{Q}^{n,m}$ by the subgroup $\sum_{r=1}^{n-1} \mathbb{Q} \cdot \lg_r(x)$. It follows that the map ρ_n in (3.15) yields a homomorphism

$$\mathbf{OP}^{n,m} \to (\hat{\mathbb{Q}}/\mathbb{Q})^{n-1} = (\hat{\mathbb{Z}}/\mathbb{Z})^{n-1}.$$

By the proof of Lemma 3.16, this map is surjective. Its kernel is denoted $\mathbf{OP}^{n,m}_{\mathrm{cl}}$ and called the subgroup of *classical operations*. In the case $n = m$, this group coincides with the group of classical operation defined earlier. In view of Corollary 4.13, $\mathbf{OP}^{n,m}_{\mathrm{cl}}$ is identified with the group $\big(\coprod_{r=1}^{n-1} \mathbb{Q} \cdot \lg_r(x) + x\mathbb{Z}[\![x]\!]\big) \cap x^m\mathbb{Q}[\![x]\!]$.

We view the group $x\mathbb{Z}[x]_{\leqslant m-1}$ of integral polynomials of degree at most $m-1$ as a lattice in the $\mathbb{Q}$-space $x\mathbb{Q}[\![x]\!]/(x^m)$. Denote by $\mathcal{L}^{n,m}$ the intersection of $x\mathbb{Z}[x]_{\leqslant m-1}$ with the image in $x\mathbb{Q}[\![x]\!]/(x^m)$ of the space $\coprod_{r=1}^{n-1} \mathbb{Q} \cdot \lg_r(x)$. Then $\mathcal{L}^{n,m}$ is a subgroup of $x\mathbb{Z}[x]_{\leqslant m-1}$ of rank $n-1$.

We get the following description of the group of classical operations:

$$\mathbf{OP}^{n,m}_{\mathrm{cl}} = \mathcal{L}^{n,m} \oplus x^m\mathbb{Z}[\![x]\!].$$

If $m = n \geqslant 1$, the map of $\mathbb{Q}$-spaces is an isomorphism and $\mathcal{L}^{n,n} = x\mathbb{Z}[x]_{\leqslant n-1}$. It follows that

$$\mathbf{OP}^{n,n}_{\mathrm{cl}} = x\mathbb{Z}[\![x]\!].$$

Recall that $\mathbf{OP}^{n,n}_{\mathrm{cl}} = \mathbf{OP}^{n,n} = \mathbb{Z}[\![x]\!]$ if $n \leqslant 0$ and $\mathbf{OP}^{n,m} = \mathbf{OP}^{n,n}$ if $m \leqslant n$.

We summarize our results in the following statement:

Theorem 4.19. *The natural homomorphism* $\mathbf{OP}^{n,m} \to \mathbf{OP}^{n,m}_{\hat{\mathbb{Z}}}$ *is injective. For any integers* $m \geqslant n \geqslant 1$, *there is an exact sequence*

$$0 \to \mathbf{OP}^{n,m}_{\mathrm{cl}} \to \mathbf{OP}^{n,m} \to (\hat{\mathbb{Z}}/\mathbb{Z})^{n-1} \to 0,$$

where $\mathbf{OP}^{n,m}_{\mathrm{cl}} = \mathcal{L}^{n,m} \oplus x^m\mathbb{Z}[\![x]\!]$. *Moreover*, $\mathbf{OP}^{n,n}_{\mathrm{cl}} = x\mathbb{Z}[\![x]\!]$.

Remark 4.20. Similar arguments yield the following formula for $m \geqslant n \geqslant 1$:

$$\mathbf{OP}^{n,m}_{\hat{\mathbb{Z}}} = \mathcal{L}^{n,m}_{\hat{\mathbb{Z}}} \oplus x^m \hat{\mathbb{Z}}[\![x]\!],$$

where $\mathcal{L}^{n,m}_{\hat{\mathbb{Z}}} = \mathcal{L}^{n,m} \otimes \hat{\mathbb{Z}}$.

4E. *Composition.* The R-module homomorphism $\mathrm{Ad}_n : R[\![x]\!] \to \mathbf{OP}^{n,n}_R$ is not a ring homomorphism. In this section we introduce a new product on $R[\![x]\!]$ so that Ad_n becomes an R-algebra homomorphism.

Let $H, H' \in R[\![x]\!]$, write $H' = \sum_{i \geqslant 0} a_i x^i$ and define the *composition* in H and H' by the formula

$$H \circ H' = a_0 \cdot H(0) + \sum_{i \geqslant 1} (-1)^i a_i \cdot (\partial^{i-1} H)(x^{\times i}).$$

The composition $\circ$ is distributive in H and H' with respect to addition. (Note that the usual substitution of power series is only one-sided distributive.) The polynomial $1 - x$ is the identity for the composition $(1 - x) \circ H = H = H \circ (1 - x)$ for all H. We view $R[\![x]\!]$ as an R-algebra with product given by the composition.

Lemma 4.21. *The maps* $\mathrm{Ad}_n : R[\![x]\!] \to \mathbf{OP}^{n,n}_R$ *are R-algebra homomorphisms.*

Proof. In view of Proposition 4.14, it suffices to consider the case $n = 0$. Let $H, H' \in R[\![x]\!]$ and write $H' = \sum_{i \geqslant 0} a_i x^i$. If $G_0, G_1, \ldots \in R[t][\![x]\!]$ is the sequence of power series corresponding to $\mathrm{Ad}_0(H)$ (see Proposition 4.11), then $G_0 = H(0) \in R$, $H = (G_0 - G_1)|_{t=1}$ and $G_i = (-1)^{i-1} \partial_t^{i-1}(G_1)$ for $i > 1$. Note that $G_1(t, x) = -H(tx) + H(0)$.

Write L for the canonical line bundle on $\mathbb{P}^\infty$. By (4.7) and (4.10),

$$\mathrm{Ad}_0(H)(c_1(L)^i) = G_i(c_1(L)^{\times i}) = (-1)^{i-1}(\partial_t^{i-1} G_1)(c_1(L)^{\times i}) = (-1)^i (\partial^{i-1} H)(t c_1(L)^{\times i}).$$

Therefore, we have

$$\begin{aligned}\big(\mathrm{Ad}_0(H) \circ \mathrm{Ad}_0(H')\big)(c_1(L)) &= -\mathrm{Ad}_0(H)\Big(\sum_{i \geqslant 1} a_i c_1(L)^i\Big) = -\sum_{i \geqslant 1} a_i (\mathrm{Ad}_0(H))(c_1(L)^i) \\ &= \sum_{i \geqslant 1} (-1)^{i-1} a_i \cdot (\partial^{i-1} H)\big(t c_1(L)^{\times i}\big).\end{aligned}$$

On the other hand, write $H \circ H' = (G_0'' - G_1'')|_{t=1}$, where $G_0'' = a_0 \cdot H(0)$ and

$$G_1'' = \sum_{i \geqslant 1} (-1)^{i-1} a_i \cdot (\partial^{i-1} H)(t x^{\times i}).$$

It follows that

$$\mathrm{Ad}_0(H \circ H')(c_1(L)) = G_1''(c_1(L)) = \sum_{i \geqslant 1} (-1)^{i-1} a_i \cdot (\partial^{i-1} H)(t c_1(L)^{\times i}) = (\mathrm{Ad}_0(H) \circ \mathrm{Ad}_0(H'))(c_1(L)).$$

If $r \in R = \mathrm{CK}^0_R(k)$, then

$$\mathrm{Ad}_0(H \circ H')(r) = G_0'' \cdot r = a_0 \cdot H(0) \cdot r = \mathrm{Ad}_0(H)(a_0 \cdot r) = (\mathrm{Ad}_0(H) \circ \mathrm{Ad}_0(H'))(r).$$

Overall, $\mathrm{Ad}_0(H \circ H') = \mathrm{Ad}_0(H) \circ \mathrm{Ad}_0(H')$. □

The polynomials $A_m := (1-x)^m$ satisfy $\mathrm{Ad}_n(A_m) = \Psi_m$ in $\mathbf{OP}_R^{n,n}$. It follows from Lemma 4.21 and Example 4.9 that

$$A_k \circ A_m = A_{km} = A_m \circ A_k$$

for all k and m.

Proposition 4.22. *Let R be a commutative ring and K a $\mathbb{Q}$-algebra. Then*

(1) *The composition $\circ$ in $R[\![x]\!]$ is commutative.*

(2) *The power series $\lg_r(x) \in K[\![x]\!]$, $r \geqslant 0$, are orthogonal idempotents that partition the identity, that is, $\lg_n(x) \circ \lg_m(x) = \delta_{n,m} \cdot \lg_n(x)$ and $1 - x = \sum_{r \geqslant 0} \lg_r(x)$.*

Proof. (1) It follows from the definition that the power series $x^n \circ G$ and $G \circ x^n$ are contained in $x^n R[\![x]\!]$ for all n and G. Let $H, G \in R[\![x]\!]$. Fix an integer $n > 0$ and write $H = H_1 + H_2$ and $G = G_1 + G_2$, where H_1 and G_1 are linear combinations of the Adams polynomials A_i and $H_2, G_2 \in x^n R[\![x]\!]$. As H_1 and G_1 commute, the remark above yields $H \circ G - G \circ H \in x^n R[\![x]\!]$. Since this holds for all n, we have $H \circ G = G \circ H$.

(2) The iterated derivative $\partial^i(\lg_n(x))$ is zero if $i \geqslant n$ and

$$(\partial^{n-1} \lg_n)(x_1, \ldots, x_n) = \prod_{i=1}^{n} \log(1 - x_i).$$

It follows that $\lg_n(x) \circ x^m = 0$ if $m > n$ and

$$\lg_n(x) \circ x^n = (-1)^n (\partial^{n-1} \lg_n)(x^{\times n}) = (-1)^n (\log(1-x))^n = (-1)^n n! \lg_n(x).$$

This calculation together with the first part of the proposition and the fact that the lowest term of $\lg_r(x)$ is $x^r/r!$ show that the power series $\lg_r(x)$ are orthogonal idempotents.

Finally, $\sum_{n \geqslant 1} \lg_n(x) = e^{\lg_1(x)} = (1-x)$. □

Since $\lg_r(x)$ are orthogonal idempotents which form a topological basis of the power series ring, from the continuity and distributivity of $\circ$, we obtain that our composition is associative.

Theorems 4.18 and 4.19 together with Proposition 4.22 yield the following corollary:

Corollary 4.23. *The rings $\mathbf{OP}_{\hat{\mathbb{Z}}}^{n,n}$ and $\mathbf{OP}^{n,n}$ are commutative.*

Let K be a $\mathbb{Q}$-algebra. We view $K[\![x]\!]$ as a ring with respect to addition and composition. Let $G \in K[\![x]\!]$ and write $G = \sum_{i \geqslant 0} a_i \lg_i$ for (unique) $a_i \in K$. Denote as $K^{[n,\infty)}$ the ring of K-sequences, parametrized by integers $\geqslant n$ under pointwise operations. It follows from Proposition 4.22 that the map

$$b : K[\![x]\!] \to K^{[0,\infty)}, \tag{4.24}$$

taking G to the sequence $(a_i)_{i \geqslant 0}$, is a ring isomorphism. It takes $x^n K[\![x]\!]$ onto $K^{[n,\infty)}$ for every n.

Example 4.25. The image of the polynomial $A_m(x) = (1-x)^m$ is equal to $(1, m, m^2, \ldots)$. Indeed, by substituting $y = \log(1-x)$ into the equality $e^{my} = \sum_{i \geqslant 0} m^i y^i / i!$, we get $A_m(x) = \sum_{i \geqslant 0} m^i \lg_i(x)$.

4F. ***Topology.*** In this section, we introduce three topologies on $\hat{\mathbb{Z}}[\![x]\!]$.

Proposition 4.26. *Let $G \in \mathbf{OP}_R^{n,n}$ and $m \geqslant n$. The following conditions are equivalent*:

(1) $G \in \mathrm{Im}(\mathbf{OP}_R^{n,m} \to \mathbf{OP}_R^{n,n})$;

(2) *G is zero on every smooth variety of dimension $< m$.*

Proof. (1) $\Longrightarrow$ (2): Since $\mathrm{CK}_R^m(X) = 0$, for any variety X of dimension $< m$, the operation G is zero on X.

(2) $\Longrightarrow$ (1): Let $n \geqslant 1$. By Proposition 4.11 (2), the operation G is given by a double-symmetric power series $H(x_1, \dots, x_n) \in R[\![x_1, \dots, x_n]\!]_{(n)}$ such that $H = (G_n)|_{t=1}$. We need to prove that $v(H) \geqslant m$. We will show that any monomial $\bar{x}^{\bar{r}} = x_1^{r_1} \cdots x_n^{r_n}$ of H with $\sum_i r_i < m$ is zero.

Consider $X_{\bar{r}} := \prod_i \mathbb{P}^{r_i}$. This is a variety of dimension $< m$. Write x_i for the first Chern class in $\mathrm{CK}_R^1(X_{\bar{r}})$ of the pull-back of the canonical line bundle on $\mathbb{P}^{r_i}$ with respect to the i-th projection $X_{\bar{r}} \to \mathbb{P}^{r_i}$. By (4.7),

$$0 = G(x_1 \cdots x_n) = G_n(x_1, \dots, x_n) \in \mathrm{CK}_R^n(X_{\bar{r}}).$$

By the projective bundle theorem,

$$\mathrm{CK}_R^n(X_{\bar{r}}) = R[\![x_1, \dots, x_n]\!]/(x_1^{r_1+1}, \dots, x_n^{r_n+1}).$$

Therefore, the monomial $\bar{x}^{\bar{r}}$ of H is trivial.

The case $n \leqslant 0$ follows similarly (and easier) from Proposition 4.11 (1). □

Corollary 4.27. *Let $d \geqslant 0$ be an integer and $G \in \mathbf{OP}^{n,n}$. Then there is a $\mathbb{Z}$-linear combination $G' \in \mathbf{OP}^{n,n}$ of the Adams operations Ψ_k with $k = 0, \dots, d$ such that G and G' agree on $\mathrm{CK}^n(X)$ for all smooth varieties X of dimension $\leqslant d$.*

Proof. By Lemma 3.16 applied to $m = d + 1$, there is a polynomial $G' \in \mathbb{Z}[x]$ of degree at most d such that $G - G' \in \sum_{0<r<n} \mathbb{Q} \cdot \lg_r(x) + x^{d+1}\mathbb{Q}[\![x]\!]$. Let X be a smooth variety of dimension $\leqslant d$. As $v(\partial^{n-1}(G - G')) \geqslant d + 1$, in view of Theorem 4.12, we have $G - G' \in \mathrm{Im}(\mathbf{OP}^{n,m} \to \mathbf{OP}^{n,n})$. Therefore, by Proposition 4.26, it follows that $G - G'$ is trivial on X. Finally, G' is a linear combination of the Adams polynomials A_k with $k = 0, \dots, d$. □

Definition 4.28. We introduce three topologies on $\hat{\mathbb{Z}}[\![x]\!]$:

- τ_s is generated by the neighborhoods of zero U_m consisting of power series divisible by x^m, for some $m \geqslant 0$, i.e., τ_s is the x-adic topology.
- τ_w is generated by the neighborhoods of zero $U_m + V_N$, where V_N consists of all power series divisible by some $N \in \mathbb{N}$.
- τ_o is generated by the neighborhoods of zero W_m consisting of power series, where the respective operation acts trivially on varieties of dimension $< m$.

Recall, that a topology φ is *coarser* than the topology ψ, denoted $\varphi \leqslant \psi$, if any set open with respect to φ is also open with respect to ψ.

Proposition 4.29. $\tau_w \leqslant \tau_o \leqslant \tau_s$.

Proof. The inequality $v(G(x)) \geqslant m$ implies $v(\partial^{n-1}G(x)) \geqslant m$, and therefore, by Theorem 4.12, $G \in \mathrm{Im}(\mathbf{OP}^{n,m}_{\hat{\mathbb{Z}}} \to \mathbf{OP}^{n,n}_{\hat{\mathbb{Z}}})$. Therefore, it follows from Proposition 4.26 that $\tau_o \leqslant \tau_s$.

Note that the topology τ_w is generated by the neighborhoods of zero $U_{N,m} = (N, x^m) \subset \hat{\mathbb{Z}}[\![x]\!]$, and the topology τ_o is generated by the neighborhoods of zero $W_k = \{G \in \hat{\mathbb{Z}}[\![x]\!] \mid v(\partial^{n-1}(G)) \geqslant k\}$ by Proposition 4.26. We need to show that for every N and m there is k with $W_k \subset U_{N,m}$.

We have similar compact (Hausdorff) topology τ_w on $\hat{\mathbb{Z}}[\![x_1, \ldots, x_n]\!]$ so that the map ∂^{n-1} is continuous in τ_w. Note that the map $\partial^{n-1} : \hat{\mathbb{Z}}[\![x]\!] \to \hat{\mathbb{Z}}[\![x_1, \ldots, x_n]\!]$ is injective and the induced map from $\hat{\mathbb{Z}}[\![x]\!]$ to the image of ∂^{n-1} is a homeomorphism (since the image of every closed subset is closed as $\hat{\mathbb{Z}}[\![x]\!]$ is compact and the target is Hausdorff). In particular, if $G_k \in \hat{\mathbb{Z}}[\![x]\!]$ is a sequence such that the sequence $\partial^{n-1}(G_k)$ converges to 0, then the sequence G_k converges to 0 in $\hat{\mathbb{Z}}[\![x]\!]$.

Now we prove that for every N and m there is k with $W_k \subset U_{N,m}$. Assume on the contrary that for every k we can find $G_k \in W_k$, but $G_k \notin U_{N,m}$. Then $\partial^{n-1}(G_k)$ converges to 0, but G_k does not converge to 0 in $\hat{\mathbb{Z}}[\![x]\!]$, a contradiction. □

Observation 4.30. (1) For $n = 1$, we have $\tau_o = \tau_s$.

(2) For $n > 1$, we have $\tau_w \neq \tau_o \neq \tau_s$.

Proof. (1) This follows from Proposition 4.26, since $n = 1$.

(2) For $n > 1$, W_m contains, in particular, all power series $\sum_i a_i x^i \in \hat{\mathbb{Z}}[\![x]\!]$, where $a_1 = ia_i$, for all $0 < i < m$, which is not contained in any U_l, for $l > 1$. Thus, $\tau_o \neq \tau_s$.

For $m > n \geqslant 1$, W_m/U_m is a free $\hat{\mathbb{Z}}$-module of rank $(n-1)$, while $(U_m + V_N)/U_m$ is a free $\hat{\mathbb{Z}}$-module of rank $(m-1)$. Hence, $\tau_w \neq \tau_o$. □

We view $\mathbf{OP}^{n,n}$ and $\mathbf{OP}^{n,n}_{\hat{\mathbb{Z}}}$ as the topological rings for the topologies τ_w, τ_o and τ_s, respectively, via the inclusions $\mathbf{OP}^{n,n} \hookrightarrow \mathbf{OP}^{n,n}_{\hat{\mathbb{Z}}} \hookrightarrow \hat{\mathbb{Z}}[\![x]\!]$.

Note that the x-adic topology τ_s can be defined on $R[\![x]\!]$ for every R.

Consider the restriction $b : R[\![x]\!] \to K^{[0,\infty)}$ of the map (4.24). We view $K^{[0,\infty)}$ as a topological ring with the basis of neighborhoods of zero given by the ideals $K^{[n,\infty)}$ for all $n > 0$, so that the map is continuous.

Proposition 4.31. *The image of the map $b : R[\![x]\!] \to K^{[0,\infty)}$ is contained in $R^{[0,\infty)}$.*

Proof. By Example 4.25, the image of the Adams polynomial A_m under the map (4.24) is contained in $R^{[0,\infty)}$. But the set of all linear combinations of Adams polynomials is dense in $R[\![x]\!]$ in the topology τ_s. The statement follows since $R^{[0,\infty)}$ is closed in $K^{[0,\infty)}$. □

Proposition 4.31 identifies the ring $\mathbf{OP}^{n,n}_{\hat{\mathbb{Z}}} \subset \hat{\mathbb{Z}}[\![x]\!]$ with a subring of $\hat{\mathbb{Z}}^{[n,\infty)}$ and $\mathbf{OP}^{n,n}$ with a subring of $\mathbb{Z}^{[n,\infty)}$ if $n \geqslant 0$. Indeed, if $n \geqslant 1$, the kernel of the composition

$$\mathcal{Q}^n_{\hat{\mathbb{Z}}} \xrightarrow{\lambda_{n,n}} \mathbf{OP}^{n,n}_{\hat{\mathbb{Z}}} \xrightarrow{b} \hat{\mathbb{Z}}^{[0,\infty)} \to \hat{\mathbb{Z}}^{[n,\infty)}$$

is generated by $\lg_r$, with $0 < r < n$, and all these logarithms are contained in the kernel of $\lambda_{n,n}$.

The ring $\mathbf{OP}^{n,n}$ is not a domain: we have $(\Psi_1 + \Psi_{-1})(\Psi_1 - \Psi_{-1}) = 0$. Let

$$e_\pm = \tfrac{1}{2}(\Psi_1 \pm \Psi_{-1}) \in \mathbf{OP}^{n,n}\big[\tfrac{1}{2}\big],$$

so e_+ and e_- are orthogonal idempotents and $e_+ + e_- = 1$. There is an embedding

$$\mathbf{OP}^{n,n} \hookrightarrow \mathbf{OP}^{n,n}\big[\tfrac{1}{2}\big] = \mathbf{OP}^{n,n}\big[\tfrac{1}{2}\big]e_+ \times \mathbf{OP}^{n,n}\big[\tfrac{1}{2}\big]e_-.$$

Proposition 4.32. *If $n \geqslant 1$, the rings $\mathbf{OP}^{n,n}\big[\frac{1}{2}\big]e_\pm$ are domains.*

Proof. Recall that there is an injective ring homomorphism

$$b : \mathbf{OP}^{n,n} \hookrightarrow \mathbb{Z}^{[1,\infty)}$$

such that $b(\Psi_m) = (m, m^2, m^3, \dots)$ for all m. In particular,

$$b(e_+) = (0, 1, 0, 1, \dots) \quad \text{and} \quad b(e_-) = (1, 0, 1, 0, \dots).$$

Lemma 4.33. *Let $(a_1, a_2, \dots) \in \mathrm{Im}(b)$. Then for any prime integer p, we have that $a_i \equiv a_j$ modulo p if $i \equiv j$ modulo $p - 1$.*

Proof. It suffices to prove the statement for $b(\Psi_m)$. We have $a_i - a_j = m^i - m^j = m^j(m^{i-j} - 1)$. If m is not divisible by p, then $m^{i-j} - 1$ is divisible by p. □

Let $G \cdot H = 0$ in $\mathbf{OP}^{n,n}$. Set $(a_1, a_2, \dots) = b(G)$ and $(b_1, b_2, \dots) = b(H)$. We have $a_i b_i = 0$ for all i. To prove the statement, it suffices to show that if $a_i \neq 0$ for some i, then $b_j = 0$ for all $j \equiv i$ modulo 2.

Choose an odd prime p that does not divide a_i. By Lemma 4.33, a_j is not divisible by p for all j such that $i \equiv j$ modulo $p - 1$. In particular, $a_j \neq 0$, hence $b_j = 0$. Thus, we have proved that $b_j = 0$ for all $j \equiv i$ modulo $p - 1$.

Lemma 4.34. *There are infinitely many primes q such that* $\gcd(q - 1, p - 1) = 2$.

Proof. Let c be the odd part of $p - 1$ (that is, $(p - 1)/c$ is a 2-power). By Dirichlet, there are infinitely many primes q such that $q \equiv 3$ modulo 4 and $q \equiv 2$ modulo c. Clearly, $\gcd(q - 1, p - 1) = 2$ for such q. □

Let j be such that $j \equiv i$ modulo 2. We need to prove that $b_j = 0$. Take any prime q as in Lemma 4.34. There are positive integers k and m such that

$$t := i + (p - 1)k = j + (q - 1)m.$$

We have proved that $b_t = 0$ since $t \equiv i$ modulo $p - 1$. By Lemma 4.33, $0 = b_t \equiv b_j$ modulo q, i.e., b_j is divisible by q. We have proved that b_j is divisible by infinitely many primes q, hence $b_j = 0$. □

4G. ***Operations in graded K-theory.*** In this section, we will determine the R-module of all R-linear operations $G : K^n_{\mathrm{gr}R} \to K^m_{\mathrm{gr}R}$ for any pair of integers n and m denoted by $\mathbf{OP}^{n,m}_R(K^*_{\mathrm{gr}})$. Recall that $K^n_{\mathrm{gr}R} = K^0_{\mathrm{gr}R} \cdot t^{-n} = \mathrm{CK}^0_R \cdot t^{-n}$, hence by Theorem 4.12, we get:

Corollary 4.35. $\mathbf{OP}^{n,m}_R(K^*_{\mathrm{gr}}) = \mathbf{OP}^{0,0}_R(K^*_{\mathrm{gr}}) \cdot t^{m-n} = \mathbf{OP}^{0,0}_R(\mathrm{CK}^*) \cdot t^{m-n} = R[\![x]\!] \cdot t^{m-n}$.

Recall that the product operation in the ring $\mathbf{OP}^{n,m}_R(K^*_{\mathrm{gr}}) = R[\![x]\!]$ is the composition $\circ$ (see Section 4E). Moreover, $R[\![x]\!]$ is a (topological) bialgebra over R with coproduct defined by the rule

$$(1-x)^n \to (1-x)^n \otimes (1-x)^n$$

for all $n \geqslant 0$ that reads $\Psi \mapsto \Psi \otimes \Psi$ in the language of operations.

Let us describe the dual bialgebra A (over $\mathbb{Z}$) of *co-operations* as follows: Let A be the subring of the polynomial ring $\mathbb{Q}[s]$ consisting of all polynomials f such that $f(a) \in \mathbb{Z}$ for all $a \in \mathbb{Z}$. In particular, $\mathbb{Z}[s] \subset A$. The polynomials

$$e_n := \frac{1}{n!}\,(-s)(1-s)\cdots(n-1-s) = (-1)^n \binom{s}{n} \in A$$

for all $n \geqslant 0$ form a basis of A as an abelian group. Consider a pairing

$$A \otimes R[\![x]\!] \to R, \quad a \otimes G \mapsto \langle a, G\rangle \in R,$$

such that $\langle e_n, x^m\rangle = \delta_{n,m}$. This pairing identifies $R[\![x]\!]$ with the dual coalgebra for A via the isomorphism

$$\mathrm{Hom}_{\mathbb{Z}}(A, R) \xrightarrow{\sim} R[\![x]\!],$$

taking a homomorphism $\alpha : A \to R$ to the power series $\sum_{n\geqslant 0} \alpha(e_n)x^n$.

Lemma 4.36. *For every polynomial $f \in A$, we have $\langle f, (1-x)^m\rangle = f(m)$.*

Proof. We may assume that $f = e_n$ for some n. Then

$$\langle f, (1-x)^m\rangle = \langle e_n, (1-x)^m\rangle = (-1)^n \binom{m}{n} = e_n(m) = f(m). \qquad \square$$

The lemma shows that a co-operation f evaluated at the Adams operation Ψ_m is equal to $f(m)$.

It follows from Lemma 4.36 that

$$\langle s^n, (1-x)^{km}\rangle = (km)^n = k^n \cdot m^n = \langle s^n, (1-x)^k\rangle \cdot \langle s^n, (1-x)^m\rangle.$$

As the composition in $R[\![x]\!]$ satisfies $(1-x)^k \circ (1-x)^m = (1-x)^{km}$, the composition in $R[\![x]\!]$ is dual to the coproduct of A taking s^n to $s^n \otimes s^n$ in $A \otimes A$.

The equality

$$\langle s^{i+j}, (1-x)^m\rangle = m^{i+j} = m^i \cdot m^j = \langle s^i, (1-x)^m\rangle \cdot \langle s^j, (1-x)^m\rangle$$

shows that the product in A is dual to the coproduct in $R[\![x]\!]$. Thus, the bialgebra $R[\![x]\!]$ of operations is dual to the bialgebra A of co-operations.

Remark 4.37. The polynomial ring $\mathbb{Z}[s]$ is a bialgebra with respect to the coproduct $s \to s \otimes s$. The dual bialgebra over R is $R^{[0,\infty)}$. The dual of the embedding $\mathbb{Z}[s] \to A$ is the homomorphism $b : R[\![x]\!] \to R^{[0,\infty)}$ defined in Proposition 4.31, since by Lemma 4.36,

$$\langle s^n, (1-x)^m \rangle = m^n = \big\langle s^n, b((1-x)^m) \big\rangle$$

as $b((1-x)^m) = (1, m, \dots, m^n, \dots)$.

5. Multiplicative operations

Definition 5.1. A *multiplicative operation* $G : A^* \to B^*$ is a morphism of functors from $\mathbf{Sm}_k$ to the category of rings. That is, the ring structure is respected. (We don't assume that G is a graded ring homomorphism.)

As was noticed in topology and then in the algebrogeometric context in [Panin 2004, §2.7.5] there is a functor from the category of oriented cohomology theories and their multiplicative operations to the category of formal group laws. Let us briefly describe this functor.

If A^* and B^* are oriented cohomology theories over k, to any multiplicative operation $G : A^* \to B^*$ one can assign the morphism

$$(\varphi_G, \gamma_G) : (A^*(k), F_A) \to (B^*(k), F_B)$$

of the respective formal group laws, where $\varphi_G : A^*(k) \to B^*(k)$ is the restriction of G to $\mathrm{Spec}(k)$ and $\gamma_G(x) \in xB^*(k)[\![x]\!]$ is defined by the condition

$$G\big(c_1^A(O(1))\big) = \gamma_G\big(c_1^B(O(1))\big) \in B^*(\mathbb{P}^\infty) = B^*(k)[\![x]\!].$$

In the algebrogeometric context, the power series $\gamma_G(x)/x$ was introduced in this generality in [Panin 2004, Definition 2.5.1] and [Smirnov 2006] in order to state and prove Riemann–Roch type theorems [Panin 2004, Theorems 2.5.3 and 2.5.4] for a multiplicative operation G. This series is called the *inverse Todd genus* of G.

The following theorem permits us to reduce the classification of multiplicative operations to algebra.

Theorem 5.2 [Vishik 2019, Theorem 6.9]. *Let A^* be a theory of rational type and B^* be any oriented cohomology theory. Then the assignment $G \mapsto (\varphi_G, \gamma_G)$ is a bijection between the set of multiplicative operations $G : A^* \to B^*$ and the set of morphisms of formal group laws.*

Example 5.3. Let R be either $\mathbb{Z}$, $\mathbb{Z}_p$ or $\hat{\mathbb{Z}}$ and $b \in R$. The Adams operation $\Psi_b : \mathrm{CK}_R^* \to \mathrm{CK}_R^*$ is homogeneous and multiplicative. The corresponding map φ is the identity and $\gamma = (1-(1-tx)^b)/t$. If $c \in R^\times$, write Ψ_b^c for the homogeneous multiplicative *twisted* Adams operation with $\varphi(t) = ct$ and $\gamma = (1-(1-tx)^{bc})/ct$ (in particular, $\Psi_b^1 = \Psi_b$). It follows from the equality

$$\Psi_b^c(tx) = \Psi_b^c(t)\Psi_b^c(x) = ct \cdot \gamma(x) = 1-(1-tx)^{bc}$$

that on CK^n_R the operation Ψ^c_b is equal to $c^{-n}\cdot\Psi_{bc}$. For any $c\in R$, let Ψ^c_0 be the homogeneous multiplicative operation with $\varphi(t)=ct$ and $\gamma=0$. This operation is zero in positive degrees and is equal to $c^n\cdot\mathrm{rank}$ on $\mathrm{CK}^{-n}_R=(K_0)_R$ for $n\geqslant 0$.

Write Θ for the multiplicative operation $\mathrm{CK}^*_R\to\mathrm{CK}^*_R$ which is the identity on CK^0_R, multiplication by $t^n:\mathrm{CK}^n_R\to\mathrm{CK}^0_R$ if $n\geqslant 0$ and the canonical isomorphism $\mathrm{CK}^n_R\to\mathrm{CK}^0_R$ (inverse to multiplication by t^{-n}) if $n\leqslant 0$. This operation is not homogeneous and its image is CK^0_R. Set $\widetilde{\Psi}^c_b:=\Theta\circ\Psi^c_b$. This is a multiplicative operation with image in CK^0_R. The corresponding function $\varphi(t)=c$ and $\gamma=(1-(1-tx)^{bc})/c$.

The introduced operations satisfy the following relations (use Theorem 5.2): $\Psi^0_0=\widetilde{\Psi}^0_0$ and

$$\Psi^c_b\circ\Psi^e_d=\Psi^{ce}_{bd},\quad \Psi^c_b\circ\widetilde{\Psi}^e_d=\widetilde{\Psi}^e_{cbd},\quad \widetilde{\Psi}^c_b\circ\Psi^e_d=\widetilde{\Psi}^{ce}_{bd},\quad \widetilde{\Psi}^c_b\circ\widetilde{\Psi}^e_d=\widetilde{\Psi}^e_{cbd}.$$

Over $\mathbb{Q}$, every formal group law is isomorphic to the additive one. Hence, for every theory C^*, we have isomorphisms of formal group laws.

$$(\mathrm{id},\exp_C):(C^*\otimes_{\mathbb{Z}}\mathbb{Q},F_C)\rightleftarrows(C^*\otimes_{\mathbb{Z}}\mathbb{Q},F_{\mathrm{add}}):(\mathrm{id},\log_C)$$

Suppose that (in the context of Definition 5.1) the coefficient ring $B^*(k)$ of the target theory has no torsion. Then the composition $(\mathrm{id},\exp_B)\circ(\varphi_G,\gamma_G)\circ(\mathrm{id},\log_A)$ identifies the set of multiplicative operations $A^*\to B^*$ with a subset of morphisms of formal group laws

$$(A^*\otimes_{\mathbb{Z}}\mathbb{Q},F_{\mathrm{add}})\to(B^*\otimes_{\mathbb{Z}}\mathbb{Q},F_{\mathrm{add}}).$$

The latter morphism is defined by (ψ,γ), where, in our case, $\psi=\varphi\otimes_{\mathbb{Z}}\mathbb{Q}$, for some ring homomorphism $\varphi=\varphi_G:A^*(k)\to B^*(k)$ and $\gamma(x)=b\cdot x$, for some $b\in B^*(k)$. In other words,

$$(\varphi_G,\gamma_G)=(\mathrm{id},\log_B)\circ(\varphi_G,\gamma)\circ(\mathrm{id},\exp_A).$$

Then

$$\gamma_G(x)=\varphi_G(\exp_A)(b\cdot\log_B(x)).$$

5A. ***Multiplicative operations in*** **CK.** For $A^*=B^*=\mathrm{CK}^*_{\hat{\mathbb{Z}}}$, we have $A=B=\hat{\mathbb{Z}}[t]$, $F_A=F_B=x+y-txy$ and

$$\log_{\mathrm{CK}}(x)=\frac{\log(1-tx)}{t},\quad \exp_{\mathrm{CK}}(z)=\frac{1-e^{zt}}{t}.$$

Note that a ring homomorphism φ from $\hat{\mathbb{Z}}[t]$ to a ring T such that $\bigcap_{n>0}nT=0$ is uniquely determined by $\varphi(t)$ in T (such a choice is realized by a homomorphism, if $\hat{\mathbb{Z}}$ can be mapped to T). Indeed, suppose that φ and ψ satisfy $\varphi(t)=\psi(t)$. For any $f\in\hat{\mathbb{Z}}[t]$ and $n>0$, write $f=g+nh$ for some $g\in\mathbb{Z}[t]$ and $h\in\hat{\mathbb{Z}}[t]$. Then $\varphi(g)=\psi(g)$ and hence $\varphi(f)-\psi(f)\in nT$. Since this holds for all $n>0$, we have $\varphi(f)-\psi(f)=0$ for all f.

Thus, the map $\varphi_G:\hat{\mathbb{Z}}[t]\to\hat{\mathbb{Z}}[t]$ is determined by $\varphi_G(t)=c(t)\in\hat{\mathbb{Z}}[t]$. Let $b=b(t)\in\hat{\mathbb{Z}}[t]$. Note that any choice of $b(t)$ and $c(t)$ gives a morphism of rational formal group laws and so, a multiplicative

operation $G : \mathrm{CK}^*_{\hat{\mathbb{Z}}} \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathrm{CK}^*_{\hat{\mathbb{Z}}} \otimes_{\mathbb{Z}} \mathbb{Q}$ with

$$\gamma_G(t,x) = \frac{1-(1-tx)^{b(t)c(t)/t}}{c(t)} = \sum_{n\geqslant 1}(-1)^{n-1}(tx)^n \frac{\binom{b(t)c(t)/t}{n}}{c(t)},$$

which lifts to an operation $\mathrm{CK}^*_{\hat{\mathbb{Z}}} \to \mathrm{CK}^*_{\hat{\mathbb{Z}}}$ if and only if the coefficients of our power series belong to $\hat{\mathbb{Z}}$. The coefficient at x^n is

$$a_n = (-1)^{n-1}\frac{b(t)\prod_{k=1}^{n-1}\big(b(t)c(t)-kt\big)}{n!}. \tag{5.4}$$

Denote by $b_p(t)$ and $c_p(t)$ the $\mathbb{Z}_p$-components of our polynomials. If we have $\deg(b_p(t)c_p(t)) > 1$ for some p, the leading term of our t-polynomial will be clearly nonintegral (for some n). Similarly, if for some p, the constant term of $b_p(t)c_p(t)$ is nonzero, then the smallest term of the p-component of our t-polynomial will be nonintegral, for some n. Hence, the polynomial $b(t)c(t)$ is linear. Then, for a given prime p, either $b_p(t) = b_p$ and $c_p(t) = c_p t$, or $b_p(t) = b_p t$ and $c_p(t) = c_p$, for some $b_p, c_p \in \mathbb{Z}_p$. Then the $\mathbb{Z}_p$- component of our coefficient is:

$$(a_n)_p = (-1)^{n-1}t^m b_p \frac{\binom{b_p c_p - 1}{n-1}}{n}, \quad \text{where } m = n-1 \text{ or } m = n.$$

If $b_p \neq 0$, then this will be integral for all n if and only if $c_p \in \mathbb{Z}_p^\times$, while if $b_p = 0$, then c_p can be an arbitrary element from $\mathbb{Z}_p$. Let us denote the ($\mathbb{Z}_p$-components of) operations with $m = n-1$ as $\Psi^{c_p}_{b_p}$, while the ones with $m = n$ as $\widetilde{\Psi}^{c_p}_{b_p}$ (see Example 5.3; we suppress p from notations). Here, $\Psi^{c_p}_{b_p}$ respects the grading on $\mathrm{CK}^*_{\mathbb{Z}_p}$, while $\widetilde{\Psi}^{c_p}_{b_p}$ maps $\mathrm{CK}^*_{\mathbb{Z}_p}$ to $\mathrm{CK}^0_{\mathbb{Z}_p}$. The pairs (b_p, c_p) run over the set $(\mathbb{Z}_p\backslash 0) \times \mathbb{Z}_p^\times \cup \{0\} \times \mathbb{Z}_p$ and, in addition, we have that $\Psi^0_0 = \widetilde{\Psi}^0_0$.

Thus, any multiplicative operation G on $\mathrm{CK}^*_{\hat{\mathbb{Z}}}$ splits into the product $\times_p G_{(p)}$ of operations on $\mathrm{CK}^*_{\mathbb{Z}_p}$, where each $G_{(p)}$ is one of the $\Psi^{c_p}_{b_p}$ or $\widetilde{\Psi}^{c_p}_{b_p}$. Let $\mathcal{P}$ be the set of prime numbers and $J \subset \mathcal{P}$ be the subset of those primes, for which $(b_p, c_p) \neq (0,0)$ and $G_{(p)}$ is $\widetilde{\Psi}$. Then the data (J, b, c), where the p-components of $b, c \in \hat{\mathbb{Z}}$ are b_p and c_p, determines our operation G. Let us call it ${}^J\Psi^c_b$. Here, (J, b, c) runs over all possible triples satisfying (1) $b_p \neq 0 \Longrightarrow c_p \in \mathbb{Z}_p^\times$ and (2) $(b_p, c_p) = (0,0) \Longrightarrow p \notin J$.

The operations ${}^\varnothing\Psi^1_b$ are (nontwisted) Adams operations with $\varphi_G = \mathrm{id}$, which naturally form a ring isomorphic to $\hat{\mathbb{Z}}$. These operations commute with every other operation. The operations ${}^\varnothing\Psi^c_1$ are invertible and form a group isomorphic to $\hat{\mathbb{Z}}^\times$. Below we will suppress $J = \varnothing$ from the notation and will denote the respective operations simply as Ψ^c_b.

The formulas in Example 5.3 show that the monoid of multiplicative operations is noncommutative.

5B. ***Multiplicative operations in K_{gr} over $\mathbb{Z}$.*** For $A^* = B^* = K^*_{\mathrm{gr}}$, we have $A = B = \mathbb{Z}[t, t^{-1}]$ and $F_A = F_B = x + y - txy$. Similar calculations, as in the previous section, show that the coefficient a_n in (5.4) will belong to $\mathbb{Z}[t, t^{-1}]$ for every n if and only if $b(t)c(t)$ is linear in t. Thus, $c(t) = ct^l$, for $c = \pm 1$ and $l \in \mathbb{Z}$, and $b(t) = bt^{1-l}$, for some $b \in \mathbb{Z}$.

Then the coefficient a_n is

$$(-1)^{n-1}t^{n-l}\frac{\binom{bc}{n}}{c}.$$

Denote this operation as ${}^l\Psi^c_b$. It scales the grading on K^*_{gr} by the coefficient l. So, only the operations ${}^1\Psi^c_b$ are homogeneous.

The case $c(t) = t$ and $b(t) = b$, that is, ${}^1\Psi^1_b$ corresponds to the Adams operation Ψ_b, see [Vishik 2019, §6.3]. In this case, $\varphi_G = \mathrm{id}$. The operation ${}^{-1}\Psi^1_1$ is an automorphism of order 2 acting identically on K^0_{gr} and mapping t to t^{-1}.

We will omit l and c from the notation ${}^l\Psi^c_b$ when these will be equal to 1.

6. Stable operations

The purpose of this section is to describe stable operations in CK and K_{gr} with integral and $\hat{\mathbb{Z}}$-coefficients. The spaces of such operations appear to have countable topological bases, which we describe in Theorems 6.25 and 6.34. We also describe stable multiplicative operations and show that these generate additive ones only in the case of $\hat{\mathbb{Z}}$-coefficients.

To be able to discuss stability of operations, we need the notion of a suspension. Following Voevodsky, Panin [2003] and Smirnov [2006] we can introduce the category of pairs **SmOp** whose objects are pairs (X, U), where $X \in \mathbf{Sm}_k$ and U is an open subvariety of X, see [Vishik 2019, Definition 3.1], with the smash product

$$(X, U) \wedge (Y, V) := (X \times Y, X \times V \cup U \times Y)$$

and the natural functor $\mathbf{Sm}_k \to \mathbf{SmOp}$ given by $X \mapsto (X, \varnothing)$. Then suspension can be defined as

$$\Sigma_T(X, U) := (X, U) \wedge (\mathbb{P}^1, \mathbb{P}^1 \backslash 0).$$

Any theory A^* extends from $\mathbf{Sm}_k$ to **SmOp** by the rule

$$A^*((X, U)) := \mathrm{Ker}(A^*(X) \to A^*(U)).$$

Any additive operation $A^* \to B^*$ on $\mathbf{Sm}_k$ extends uniquely to an operation on **SmOp**.

An element $\varepsilon^A = c^A_1(O(1)) \in A^*((\mathbb{P}^1, \mathbb{P}^1 \backslash 0))$ defines an identification

$$\sigma^A_T : A^*((X, U)) \xrightarrow{\cong} A^{*+1}(\Sigma_T(X, U)),$$

given by $x \mapsto x \wedge \varepsilon^A$.

Definition 6.1. For any additive operation $G : A^* \to B^*$, we define its *desuspension* as the unique operation $\Sigma^{-1}G : A^* \to B^*$ such that

$$G \circ \sigma^A_T = \sigma^B_T \circ \Sigma^{-1}G.$$

Definition 6.2. A *stable* additive operation $G : A^* \to B^*$ is the collection $\{G^{(n)} \mid n \geqslant 0\}$ of operations $A^* \to B^*$ such that $G^{(n)} = \Sigma^{-1}G^{(n+1)}$.

Proposition 6.3. *Suppose that $G : A^* \to B^*$ is a multiplicative operation with $\gamma_G(x) \equiv bx$ modulo x^2 for some $b \in B^*(k)$. Then $\Sigma^{-1}G = b \cdot G$.*

Proof. We have

$$G(\sigma_T^A(u)) = G(u \wedge \varepsilon^A) = G(u) \wedge G(\varepsilon^A) = G(u) \wedge (b \cdot \varepsilon^B) = \sigma_T^B(b \cdot G(u)). \qquad \square$$

We call a multiplicative operation G *stable* if the constant sequence $(G, G, G, \dots)$ is stable. By Proposition 6.3, G is stable if and only if the linear coefficient of γ_G is equal to 1 (see [Vishik 2019, Proposition 3.8]).

For a commutative ring R, define the operator

$$\Phi = \Phi_R : R[\![x]\!] \to R[\![x]\!], \quad \Phi(G) = (x-1)\frac{\mathrm{d}G}{\mathrm{d}x},$$

6A. ***Stable operations in* CK *over* $\hat{\mathbb{Z}}$.** Recall that when $A^* = B^* = \mathrm{CK}^*_{\hat{\mathbb{Z}}}$, the group of additive operations $\mathbf{OP}^{n,n}_{\hat{\mathbb{Z}}}$, for $n \leqslant 0$ and $n \geqslant 1$, can be identified with $\hat{\mathbb{Z}}[\![x]\!]$, respectively, $x\hat{\mathbb{Z}}[\![x]\!]$.

Proposition 6.4. *The desuspension operator $\Sigma^{-1} : \mathbf{OP}^{n,n}_{\hat{\mathbb{Z}}} \to \mathbf{OP}^{n-1,n-1}_{\hat{\mathbb{Z}}}$ is given by the rule*

$$\Sigma^{-1}(G) = \begin{cases} \Phi(G), & \text{if } n \leqslant 1, \\ \partial^0(\Phi(G)) = \Phi(G) - \Phi(G)(0), & \text{if } n > 1. \end{cases}$$

Proof. The Adams operation Ψ_k is identified with the power series $A_k(x) = (1-x)^k$ if $n \leqslant 0$ and with $(1-x)^k - 1$ if $n > 0$. By Proposition 6.3, we have $\Sigma^{-1}\Psi_k = k\Psi_k$, so the formula holds for $G = \Psi_k$.

The map Σ^{-1} is continuous in τ_o, and the map Φ is continuous in τ_s. Hence, both maps are continuous as the maps $\tau_s \to \tau_o$. Since τ_o is Hausdorff (as τ_w is), it follows that the set of power series, where Σ^{-1} and Φ coincide, is closed in τ_s. But the set of linear combinations of Adams operations is everywhere dense in τ_s. $\square$

It follows from Proposition 6.4 that the desuspension map Σ^{-1} is injective and yields a tower of injective maps in the other direction:

$$\hat{\mathbb{Z}}[\![x]\!] = \mathbf{OP}^{0,0}_{\hat{\mathbb{Z}}} \xleftarrow{\Sigma^{-1}} \mathbf{OP}^{1,1}_{\hat{\mathbb{Z}}} \xleftarrow{\Sigma^{-1}} \cdots \xleftarrow{\Sigma^{-1}} \mathbf{OP}^{n,n}_{\hat{\mathbb{Z}}} \xleftarrow{\Sigma^{-1}} \cdots . \tag{6.5}$$

Moreover, the group $\mathbf{OP}^{\mathrm{st}}_{\hat{\mathbb{Z}}}$ of homogeneous degree 0 stable operations $\mathrm{CK}^*_{\hat{\mathbb{Z}}} \to \mathrm{CK}^*_{\hat{\mathbb{Z}}}$ that is the limit of the sequence (6.5) is naturally isomorphic to the group

$$S := \cap_n \operatorname{Im}(\Phi^n) = \cap_n \operatorname{Im}((\Sigma^{-1})^n) \subset \hat{\mathbb{Z}}[\![x]\!].$$

Indeed, if $\{G^{(n)} \mid n \geqslant 0\}$ is a stable operation, then $G^{(0)} = \Phi^n(G^{(n)})$ for every n, hence $G^{(0)} \in S$. Conversely, given $G \in S$, write $G = \Phi^n(H^{(n)})$ for every n. Since $\operatorname{Ker}(\Phi^n)$ consists of constant power series only, the sequence $G^{(n)} = \Phi(H^{(n+1)})$ is a stable operation.

Lemma 6.6. *Let $G \in x\hat{\mathbb{Z}}[\![x]\!]$ and $n \geqslant 1$. Then*

(1) *$\partial^n(G)$ has coefficients in $\mathbb{Z}$ if and only if $\partial^{n-1}(\Phi(G))$ has coefficients in $\mathbb{Z}$.*

(2) *$v(\partial^n(G)) \geqslant m$ for some m if and only if $v(\partial^{n-1}(\Phi(G))) \geqslant m - 1$.*

Proof. ($\Rightarrow$): Follows from Proposition 2.6 for both (1) and (2).

($\Leftarrow$): Simply write H_k for $(x-1)^k(\mathrm{d}^k G/\mathrm{d}x^k)$. We claim that $\partial^{n-1}(H_k)$ has coefficients in $\mathbb{Z}$ in case (1) and $v(\partial^{n-1}(H_k)) \geqslant m-k$ in case (2) for every $k \geqslant 1$. We prove the statements by induction on k. To show ($k \Rightarrow k+1$): We have $H_{k+1} = \Phi(H_k) - kH_k$, hence

$$\partial^{n-1}(H_{k+1}) = \partial^{n-1}\big(\Phi(H_k)\big) - k\partial^{n-1}(H_k).$$

Then $k\partial^{n-1}(H_k)$ has coefficients in $\mathbb{Z}$ in case (1) and $v(k\partial^{n-1}(H_k)) \geqslant m-k$ in case (2) by the induction hypothesis. As the derivative $\partial^n(H_k)$ has coefficients in $\mathbb{Z}$ in case (1) and $v(\partial^n(H_k)) \geqslant m-k$ in case (2), it follows from Proposition 2.6, applied to the power series H_k, that $\partial^{n-1}(\Phi(H_k))$ also has coefficients in $\mathbb{Z}$ in case (1) and $v\big(\partial^{n-1}(\Phi(H_k))\big) \geqslant m-k-1$ in case (2). It follows that $\partial^{n-1}(H_{k+1})$ has coefficients in $\mathbb{Z}$ in case (1) and $v(\partial^{n-1}(H_{k+1})) \geqslant m-k-1$ in case (2). The claim is proved.

Note that all coefficients of H_k are divisible by $k!$ in $\hat{\mathbb{Z}}$. It follows that the power series $(1/k!)\partial^{n-1}(H_k)$ have coefficients in $\mathbb{Z}$ in case (1). By Proposition 2.6, $\partial^n(G)$ has coefficients in $\mathbb{Z}$ in case (1) and $v(\partial^n(G)) \geqslant m$ in case (2). □

In particular, we can describe the integral operations $\mathbf{OP}^{n,m}$ as follows:

Proposition 6.7. *Let $G \in x\hat{\mathbb{Z}}[\![x]\!]$ and $m \geqslant n \geqslant 1$. Then $G \in \mathbf{OP}^{n,m}$ if and only if $\Phi^n(G) \in \mathbb{Z}[\![x]\!]$ and $v(\Phi^n(G)) \geqslant m-n$.*

Proof. Theorem 4.12 and iterated applications of Lemma 6.6 show that $G \in \mathbf{OP}^{n,m}$ if and only if $\partial^0(\Phi^{n-1}(G)) \in \mathbb{Z}[\![x]\!]$ and $v(\partial^0(\Phi^{n-1}(G))) \geqslant m-n+1$. Thus, it suffices to prove the following for a power series $H \in \hat{\mathbb{Z}}[\![x]\!]$ and integer $k \geqslant 0$:

(1) $\partial^0(H) \in \mathbb{Z}[\![x]\!] \iff \Phi(H) \in \mathbb{Z}[\![x]\!]$,

(2) $v(\partial^0(H)) \geqslant k+1 \iff v(\Phi(H)) \geqslant k$.

If $\partial^0(H) \in \mathbb{Z}[\![x]\!]$, then clearly $\Phi(H) \in \mathbb{Z}[\![x]\!]$. Conversely, if $\Phi(H) \in \mathbb{Z}[\![x]\!]$, then

$$\partial^0(H) \in \mathbb{Q}[\![x]\!] \cap \hat{\mathbb{Z}}[\![x]\!] = \mathbb{Z}[\![x]\!].$$

The second statement follows from the obvious equality $v(\partial^0(H)) = v(\Phi(H)) + 1$. □

Let m a positive integer. It follows from Lemma 6.6 (2) that there is a tower of inclusions as in (6.5):

$$x^m\hat{\mathbb{Z}}[\![x]\!] = \mathbf{OP}^{0,m}_{\hat{\mathbb{Z}}} \hookleftarrow \mathbf{OP}^{1,m+1}_{\hat{\mathbb{Z}}} \hookleftarrow \cdots \hookleftarrow \mathbf{OP}^{n,n+m}_{\hat{\mathbb{Z}}} \hookleftarrow \cdots . \tag{6.8}$$

Additionally, for every n, we have $\mathbf{OP}^{n,n+m}_{\hat{\mathbb{Z}}} \cap \mathbf{OP}^{n+1,n+1}_{\hat{\mathbb{Z}}}$ in $\mathbf{OP}^{n,n}_{\hat{\mathbb{Z}}}$ coincides with $\mathbf{OP}^{n+1,n+m+1}_{\hat{\mathbb{Z}}}$. Therefore, we obtain:

Proposition 6.9. *The group of homogeneous degree m stable operations $\mathrm{CK}^*_{\hat{\mathbb{Z}}} \to \mathrm{CK}^{*+m}_{\hat{\mathbb{Z}}}$ is naturally isomorphic to the intersection $x^{\max(0,m)}\hat{\mathbb{Z}}[\![x]\!] \cap S$.*

The map $\Phi : \hat{\mathbb{Z}}[\![x]\!] \to \hat{\mathbb{Z}}[\![x]\!]$ is continuous in τ_w, and the space $\hat{\mathbb{Z}}[\![x]\!]$ is compact Hausdorff. Hence, $\mathrm{Im}(\Phi^n)$ is closed in $\hat{\mathbb{Z}}[\![x]\!]$ for any n. It follows that the set S is also closed in $\hat{\mathbb{Z}}[\![x]\!]$ in the topology τ_w, and hence in τ_o and τ_s.

It follow from Proposition 4.26 and Lemma 6.6 that the topology on $\mathbf{OP}^{\mathrm{st}}_{\hat{\mathbb{Z}}}$ induced by τ_o is generated by the neighborhoods of zero W_m consisting of all collections $\{G^{(n)} \mid n \geqslant 0\}$ such that $G^{(n)}$ acts trivially on varieties of dimension $< n+m$. We still denote this topology by τ_o.

Let $A_r(x) = (1-x)^r \in \hat{\mathbb{Z}}[\![x]\!]$ for $r \in \hat{\mathbb{Z}}$. Note that $\Phi(A_r) = r \cdot A_r$. In particular, if r is invertible in $\hat{\mathbb{Z}}$, then $A_r \in S$.

We can describe the set S via divisibility conditions on the coefficients of the power series.

Theorem 6.10. *The set $S = \cap_r \mathrm{Im}(\Phi^r) \subset \hat{\mathbb{Z}}[\![x]\!]$ consists of all power series $G = \sum_{i \geqslant 0} a_i x^i$ satisfying the following property: for every prime p and every positive integers n and m such that m is divisible by p^n, for every nonnegative $j < m$ divisible by p, the sum $\sum_{i=j}^{m-1} \binom{i}{j} a_i$ is divisible by p^n.*

Proof. Let n be a positive integer, $G \in S$ and write $G = \Phi^n(H)$ for some $H \in \hat{\mathbb{Z}}[\![x]\!]$. Consider the ideal $I = (p^n, x^m) \subset \hat{\mathbb{Z}}[\![x]\!]$, where m is divisible by p^n. Note that $\Phi(I) \subset I$ since p^n divides m.

Let G' be the x^m-truncation of G and H' the x^m-truncation of H. As $G - G' \in I$ and $H - H' \in I$, we have $G' - \Phi^n(H') \in I$. Since G' and $\Phi^n(H')$ are polynomials of degree less than m, we conclude that G' and $\Phi^n(H')$ are congruent modulo p^n.

We write G' and H' as polynomials in $y = x - 1$. Since $\Phi^n(y^i) = i^n y^i$, the y^i-coefficients of $\Phi^n(H')$ are divisible by p^n for all i divisible by p. It follows that the same property holds for G'. As

$$G' = \sum_{i=0}^{m-1} a_i x^i = \sum_{i=0}^{m-1} a_i (y+1)^i = \sum_{i=0}^{m-1} a_i \sum_{j=0}^{i} \binom{i}{j} y^j = \sum_{j=0}^{m-1} y^j \sum_{i=j}^{m-1} \binom{i}{j} a_i,$$

the divisibility condition holds.

Conversely, as $\hat{\mathbb{Z}} = \prod \mathbb{Z}_p$, it suffices to prove the statement over $\mathbb{Z}_p$. Let $G \in \mathbb{Z}_p[\![x]\!]$ satisfy the divisibility condition in the theorem. Choose n and m such that m is divisible by p^n and set $I = (p^n, x^m) \subset \mathbb{Z}_p[\![x]\!]$ as above. Recall that $\Phi(I) \subset I$. Let F be the x^m-truncation of G. By assumption, we can write $F \equiv \sum b_i y^i$ modulo p^n, where the sum is taken over $i < m$ that are prime to p. In particular, $G \equiv \sum b_i y^i$ modulo I.

Choose $r > 0$ and set $F' = \sum (b_i / i^r) y^i$. Then $\Phi^r(F') = \sum b_i y^i \equiv G$ modulo I, i.e., G is in the image of Φ^r modulo I. As $\mathrm{Im}(\Phi^r)$ is closed in $\mathbb{Z}_p[\![x]\!]$ in the topology τ_w, we have $G \in \mathrm{Im}(\Phi^r)$ for all r, i.e., $G \in S$. □

6B. ***Stable operations in* CK *over* $\mathbb{Z}$.** Now we turn to the study of stable operations over $\mathbb{Z}$.

Proposition 6.11. *The preimage of $\mathbf{OP}^{n,n}$ under $\Sigma^{-1} : \mathbf{OP}^{n+1,n+1}_{\hat{\mathbb{Z}}} \to \mathbf{OP}^{n,n}_{\hat{\mathbb{Z}}}$ is equal to $\mathbf{OP}^{n+1,n+1}$ for every $n \geqslant 0$.*

Proof. As $\Sigma^{-1} = \partial^0 \circ \Phi$, for $n \geqslant 1$, and $\Sigma^{-1} = \Phi$, for $n = 0$, this follows from Proposition 6.7. □

Thus, we have a tower

$$\mathbb{Z}[\![x]\!] = \mathbf{OP}^{0,0} \hookleftarrow \mathbf{OP}^{1,1} \hookleftarrow \cdots \hookleftarrow \mathbf{OP}^{n,n} \hookleftarrow \cdots,$$

given by the desuspension and the group $\mathbf{OP}^{\mathrm{st}}$ of stable homogeneous degree 0 integral operations is identified with $S_0 := S \cap \mathbb{Z}[\![x]\!]$, where S is described by Theorem 6.10. Applying Proposition 6.7 again, we get:

Proposition 6.12. *The group of homogeneous degree m stable operations $\mathrm{CK}^* \to \mathrm{CK}^{*+m}$ is naturally isomorphic to the intersection $x^{\max(0,m)}\mathbb{Z}[\![x]\!] \cap S_0$.*

We would like to determine the structure of S_0.

Lemma 6.13. *For every $n \geqslant 0$, there is a positive integer d such that $dx^n \in S + x^{n+1}\hat{\mathbb{Z}}[\![x]\!]$.*

Proof. Choose distinct elements $r_0, \ldots, r_n \in \hat{\mathbb{Z}}^\times$ such that $r_i - r_j \in \mathbb{Z}$ for all i and j. The x^i-coefficients with $i = 0, 1, \ldots, n$ of the power series $A_{r_j}(x) = (1-x)^{r_j} \in S$ form an $(n+1) \times (n+1)$ Van der Monde type matrix $\left[(-1)^i \binom{r_j}{i}\right]$. Its determinant d is a nonzero integer since all $r_i - r_j$ are integers. It follows that there is a $\hat{\mathbb{Z}}$-linear combination of the A_{r_j} that is equal to dx^n modulo x^{n+1}. □

Note that any ideal in $\hat{\mathbb{Z}}$ that contains a nonzero integer is generated by a positive integer (the smallest positive integer in the ideal). It follows from Lemma 6.13 that for every $n \geqslant 0$, there exists a unique positive integer d_n such that the ideal of all $a \in \hat{\mathbb{Z}}$ with the property $ax^n \in S + x^{n+1}\hat{\mathbb{Z}}[\![x]\!]$ is generated by d_n. We will determine the integers d_n below.

For every $n \geqslant 0$, choose a power series $G_n \in S$ such that $G_n \equiv d_n x^n$ modulo x^{n+1}.

Lemma 6.14. *Let $G = \sum_{i \geqslant 0} a_i x^i \in S$ be such that $a_0, \ldots, a_{n-1} \in \mathbb{Z}$. Then there exist $b_i \in \hat{\mathbb{Z}}$ for all $i \geqslant n$ such that $G - \sum_{i \geqslant n} b_i G_i \in S_0$.*

Proof. Find an integer a_n' such that $a_n - a_n'$ is divisible by d_n, thus, $a_n = a_n' + d_n b_n$ for some $b_n \in \hat{\mathbb{Z}}$. Then the x^i-coefficients of $G - b_n G_n$ are integer for $i = 0, \ldots, n$. Continuing this procedure, we determine all b_i for $i \geqslant n$, so that all coefficients of $G - \sum_{i \geqslant n} b_i G_i$ are integers. □

Theorem 6.15. *For all $n \geqslant 0$, there are power series $F_n \in S_0$ such that $F_n \equiv d_n x^n$ modulo x^{n+1}. Moreover*:

(1) *The group S_0 consists of all infinite linear combinations $\sum_{n \geqslant 0} a_n F_n$ with $a_n \in \mathbb{Z}$.*

(2) *The group of homogeneous degree m stable operations $\mathrm{CK}^* \to \mathrm{CK}^{*+m}$ is naturally isomorphic to the group of all infinite linear combinations $\sum_{n \geqslant \max(0,m)} a_n F_n$ with $a_n \in \mathbb{Z}$.*

Proof. Fix $n \geqslant 0$. The coefficient d_n of G_n is an integer. Applying Lemma 6.14, we find $b_i \in \hat{\mathbb{Z}}$ for $i \geqslant n+1$ such that $F_n := G_n - \sum_{i \geqslant n+1} b_i G_i \in S_0$. Statements (1) and (2) are clear. □

6C. *The integers d_n.* Our next goal is to determine the integers d_n. Let $n > 0$ be an integer. For an integer r write L_r for the n-tuple of binomial coefficients

$$\left(\binom{r}{0}, \binom{r}{1}, \ldots, \binom{r}{n-1}\right) = (1, r, \ldots) \in \mathbb{Z}^n.$$

For an n-sequence $\bar{a} = (a_1, \dots, a_n)$ of positive integers, let $d(\bar{a})$ be the determinant of the $n \times n$ matrix with columns $L_{a_1}, L_{a_2}, \dots, L_{a_n}$. We have

$$d(\bar{a}) = \Big(\prod_{s>t}(a_s - a_t)\Big) \Big/ \prod_{k=1}^{n-1} k! \in \mathbb{Z}. \tag{6.16}$$

Let p be a prime integer. An n-sequence $\bar{a}$ is called *p-prime* if all its terms are prime to p. Let $\bar{a}^{(n)}_{\min}$ be the "smallest" strictly increasing p-prime n-sequence

$$(1, 2, \dots, p-1, p+1, \dots).$$

Lemma 6.17. *Let $\bar{a}$ be a p-prime n-sequence that differs from $\bar{a}^{(n)}_{\min}$ at one term only. Then $d(\bar{a}^{(n)}_{\min})$ divides $d(\bar{a})$ in the ring of p-adic integers $\mathbb{Z}_p$.*

Proof. Suppose $\bar{a}$ is obtained from $\bar{a}^{(n)}_{\min}$ by replacing a term a by b. It follows from (6.16) that

$$\frac{d(\bar{a})}{d(\bar{a}^{(n)}_{\min})} = \frac{\prod(b - a')}{\prod(a - a')},$$

where the products are taken over all terms a' of $\bar{a}_{\min}$, except a. Since a is prime to p, the product $\prod(a - a')$ generates the same ideal in $\mathbb{Z}_p$ as $a!(c-a)!$, where c is the last term of $\bar{a}_{\min}$. Similarly, as b is prime to p, the product $\prod(b - a')$ generates the same ideal in $\mathbb{Z}_p$ as

$$b(b-1)\cdots(b-a+1)\cdot(b-a-1)\cdots(b-c+1)(b-c) = (-1)^{c-a}a!(c-a)!\binom{b}{a}\binom{c-b}{c-a}. \qquad \square$$

Corollary 6.18. *The integer $d(\bar{a}^{(n)}_{\min})$ divides $d(\bar{a}^{(n+1)}_{\min})$ in $\mathbb{Z}_p$.*

Proof. In the cofactor expansion (Laplace's formula) of the determinant $d(\bar{a}^{(n+1)}_{\min})$ along the last row, all minors are divisible by $d(\bar{a}^{(n)}_{\min})$ in view of Lemma 6.17. $\square$

Let M_n be the $\mathbb{Z}_p$-submodule of $(\mathbb{Z}_p)^n$ that is generated by the tuples $L_{a_1}, L_{a_2}, \dots, L_{a_n}$, where $(a_1, a_2, \dots, a_n) = \bar{a}^{(n)}_{\min}$.

Lemma 6.19. *Let b be an integer prime to p. Then the n-tuple L_b is contained in M_n. In others words, the $\mathbb{Z}_p$-submodule of $(\mathbb{Z}_p)^n$ generated by L_b for all integers $b > 0$ prime to p coincides with M_n.*

Proof. By Cramer's rule, the solutions of the equation $L_b = x_1 L_{a_1} + \cdots + x_n L_{a_n}$ are given by the formula $x_i = d(\bar{a}_{(i)})/d(\bar{a}^{(n)}_{\min})$, where the sequence $\bar{a}_{(i)}$ is obtained from $\bar{a}^{(n)}_{\min}$ by replacing the i-th term with b. By Lemma 6.17, we have $x_i \in \mathbb{Z}_p$. $\square$

The following statement is a generalization of Lemma 6.17:

Corollary 6.20. *Let $\bar{a}$ be any p-prime n-sequence. Then $d(\bar{a}^{(n)}_{\min})$ divides $d(\bar{a})$ in $\mathbb{Z}_p$.*

Set

$$d_n = d_n^{(p)} := \frac{d(\bar{a}^{(n+1)}_{\min})}{d(\bar{a}^{(n)}_{\min})}.$$

By Corollary 6.18, we have $d_n \in \mathbb{Z}_p$.

Write n in the form $n = (p-1)k + i$, where $i = 0, 1 \ldots, p-2$ and $k = \lfloor n/(p-1) \rfloor$. Then it follows from (6.16) that

$$d_n \mathbb{Z}_p = \frac{p^k \cdot k!}{n!} \mathbb{Z}_p, \quad \text{or, equivalently,} \quad v_p(d_n) = k + v_p(k!) - v_p(n!), \tag{6.21}$$

where v_p is the p-adic discrete valuation.

Note that $v_p((n+k)!) = v_p((pk+i)!) = v_p((pk)!) = k + v_p(k!)$, hence $d_n \mathbb{Z}_p = (n+k)!/n! \mathbb{Z}_p$. Observe that the function $n \mapsto v_p(d_n)$ is not monotonic.

Proposition 6.22. *An $(n+1)$-tuple $(0, 0, \ldots, 0, d)$ is contained in M_{n+1} if and only if d is divisible by d_n in $\mathbb{Z}_p$.*

Proof. As in the proof of Lemma 6.19, $(0, 0, \ldots, 0, d) \in M_{n+1}$ if and only if $d \cdot d(\bar{a}_{(i)})$ is divisible by $d(\bar{a}^{(n+1)}_{\min})$ in $\mathbb{Z}_p$ for all i, where the sequence $\bar{a}_{(i)}$ is obtained from $\bar{a}^{(n)}_{\min}$ by deleting the i-th term in $\bar{a}^{(n+1)}_{\min}$. We have $d(\bar{a}_{(i)}) = d(\bar{a}^{(n)}_{\min})$ if $i = n+1$, and by Corollary 6.20, all $d(\bar{a}_{(i)})$ are divisible by $d(\bar{a}^{(n)}_{\min})$, whence the result. □

For an integer r, let as before $A_r(x) = (1-x)^r$. Note that the n-tuple L_r is the tuple of coefficients (after appropriate change of signs) of the x^n-truncation of the polynomial A_r. Denote by $N^{(p)}$ the $\mathbb{Z}_p$-submodule of $\mathbb{Z}_p[x]$ generated by A_r for all integers $r > 0$ prime to p. We get an immediate corollary from Lemma 6.19 and Proposition 6.22.

Proposition 6.23. *Let $d \in \mathbb{Z}_p$ and $n \geqslant 0$. Then $dx^n \in N^{(p)} + x^{n+1}\mathbb{Z}_p[x]$ if and only if d is divisible by d_n. Moreover, there is a $\mathbb{Z}_p$-linear combination G_n of the Adams polynomials $A_{a_1}, A_{a_2}, \ldots, A_{a_{n+1}}$, where $(a_1, a_2, \ldots, a_{n+1}) = \bar{a}^{(n+1)}_{\min}$, such that $G_n \equiv d_n x^n \pmod{x^{n+1}}$.*

Proposition 6.24. *The set $S_{\mathbb{Z}_p} = \bigcap_r \operatorname{Im}(\Phi^r_{\mathbb{Z}_p})$ contains a power series $\equiv dx^n \pmod{x^{n+1}}$ if and only if d is divisible by d_n in $\mathbb{Z}_p$.*

Proof. Suppose that $G \in S_{\mathbb{Z}_p}$ and $G \equiv dx^n$ modulo x^{n+1}. Choose integers $k > 0$ such that p^k is divisible by $d(\bar{a}^{(n+1)}_{\min})$ and $m > n$ is divisible by p^k, and consider the ideal $I = (p^k, x^m) \subset \mathbb{Z}_p[\![x]\!]$. We have $G = \Phi^k(G')$ for some $G' \in \mathbb{Z}_p[\![x]\!]$ and write

$$G' = \sum_{i=0}^{m-1} b_i A_i \quad \text{modulo } x^m \mathbb{Z}_p[\![x]\!]$$

for some $b_i \in \mathbb{Z}_p$. Applying Φ^k and taking into account $\Phi^k(A_i) = i^k A_i$, we get $G = \Phi^k(G') \in N^{(p)} + I$. Taking the x^{n+1}-truncations, we see that

$$dx^n \in N^{(p)} + x^{n+1}\mathbb{Z}_p[x] + p^k \mathbb{Z}_p[x].$$

As p^k is divisible by $d(\bar{a}^{(n+1)}_{\min})$, we conclude that $p^k \mathbb{Z}_p[x] \subset N^{(p)} + x^{n+1}\mathbb{Z}_p[x]$. Therefore, we have $dx^n \in N^{(p)} + x^{n+1}\mathbb{Z}_p[x]$. By Proposition 6.23, d is divisible by d_n. □

Now we turn to the ring $\hat{\mathbb{Z}}$. The integers d_n defined before Lemma 6.14 are the products of primary parts of $d_n = d_n^{(p)}$ determined as above for every prime p. In view of (6.21), we have

$$v_p(d_n) = \Big\lfloor \frac{n}{p-1} \Big\rfloor + v_p\Big(\Big\lfloor \frac{n}{p-1} \Big\rfloor !\Big) - v_p(n!)$$

for every prime p. For example, $d_0 = 1$, $d_1 = 2$, $d_2 = 2^2 \cdot 3$, $d_3 = 2^3$, $d_4 = 2^4 \cdot 3 \cdot 5$, $d_5 = 2^5 \cdot 3$, $d_6 = 2^6 \cdot 3^2 \cdot 7$ and $d_7 = 2^7 \cdot 3^2$.

Propositions 6.23 and 6.24 yield:

Theorem 6.25. *Let $n \geqslant 0$ be an integer. Then*:

(1) *There exists a $\hat{\mathbb{Z}}$-linear combination G_n of the Adams polynomials $A_{a_1}, A_{a_2}, \dots, A_{a_{n+1}}$ for some $a_1, a_2, \dots, a_{n+1} \in \hat{\mathbb{Z}}^\times$ such that $G_n \equiv d_n x^n$ modulo x^{n+1}.*

(2) *The set $S = \bigcap_r \operatorname{Im}(\Phi^r_{\hat{\mathbb{Z}}})$ contains a power series $\equiv dx^n \pmod{x^{n+1}}$ if and only if d is divisible by d_n in $\hat{\mathbb{Z}}$. It consists of all (infinite) linear combinations of G_n.*

Remark 6.26. It follows from Proposition 6.23 that $a_1, a_2, \dots, a_{n+1} \in \hat{\mathbb{Z}}^\times$ can be chosen so that for every prime p, we have $((a_1)_p, (a_2)_p, \dots, (a_{n+1})_p) = \bar{a}_{\min}^{(n+1)}$ with respect to p. In particular, $a_1 = 1$.

Proposition 6.27. *The set $S = \cap_r \operatorname{Im}(\Phi^r)$ is the closure in the topology τ_s, and hence, in the topologies τ_o and τ_w of the set of all (finite) $\hat{\mathbb{Z}}$-linear combinations of the power series A_r for $r \in \hat{\mathbb{Z}}^\times$.*

Proof. Denote as T_s, T_w, T_o the closures of the mentioned set of linear combinations in our three topologies. As S is closed in τ_w, we have $T_s \subset T_o \subset T_w \subset S$.

Let $G \in x^k \hat{\mathbb{Z}}[\![x]\!] \cap S$. Then by Theorem 6.25, $G \equiv dx^k \pmod{x^{k+1}}$, where $d = d_k \cdot c$, for some $c \in \hat{\mathbb{Z}}$. We know that there exists a $\hat{\mathbb{Z}}$-linear combination G_k of the power series $A_{a_1}, A_{a_2}, \dots, A_{a_k}$ (with invertible a_i) such that $G_k \equiv d_k x^k \pmod{x^{k+1}}$. Hence, $G - c \cdot G_k \in x^{k+1} \hat{\mathbb{Z}}[\![x]\!] \cap S$. Applying this inductively, we obtain that, for any $G \in S$ and any positive integer m, there exists a finite $\hat{\mathbb{Z}}$-linear combination H of invertible A_r, such that $G - H \in x^m \hat{\mathbb{Z}}[\![x]\!] \cap S$. Therefore, $T_s = S$, and hence $T_s = T_o = T_w = S$. □

6D. *Stable operations in K_{gr}.* In Section 4G, we defined the bialgebra A of co-operations in K_{gr} with a canonical element $s \in A$. Recall that for a commutative ring R, the bialgebra of operations $\mathbf{OP}_R^{n,n}(K_{\mathrm{gr}}) = \mathbf{OP}_R^{0,0}(\mathrm{CK}) = R[\![x]\!]$ is dual to A. The same proof as in Proposition 6.4 shows that the desuspension operator

$$\Sigma^{-1} : R[\![x]\!] = \mathbf{OP}_R^{n,n}(K_{\mathrm{gr}}) \to \mathbf{OP}_R^{n-1,n-1}(K_{\mathrm{gr}}) = R[\![x]\!]$$

coincides with Φ. It follows that

$$\mathbf{OP}_R^{\mathrm{st}}(K_{\mathrm{gr}}) = \lim(R[\![x]\!] \xleftarrow{\Phi} R[\![x]\!] \xleftarrow{\Phi} R[\![x]\!] \xleftarrow{\Phi} \cdots).$$

Lemma 6.28. *The desuspension operator Φ is dual to the multiplication by s in A.*

Proof. As $\Phi((1-x)^m) = m(1-x)^m$, in view of Lemma 4.36, we have

$$\big\langle e_n, \Phi((1-x)^m) \big\rangle = \langle e_n, m(1-x)^m \rangle = m \cdot e_n(m) = \langle s e_n, (1-x)^m \rangle.$$ □

The localization $A[1/s]$ can be identified with $\operatorname{colim}(A \xrightarrow{s} A \xrightarrow{s} \cdots)$. Therefore,

$$\mathbf{OP}_R^{\mathrm{st}}(K_{\mathrm{gr}}) \simeq \operatorname{Hom}\Big(A\Big[\frac{1}{s}\Big], R\Big),$$

i.e., the bialgebra $\mathbf{OP}_R^{\mathrm{st}}(K_{\mathrm{gr}})$ of stable operations is dual to $A[1/s]$.

The bialgebra $A[1/s]$ coincides with the algebra of degree 0 stable operations $K_0(K)$ in topology (see [Johnson 1984, Proposition 3] and [Adams et al. 1971]). Moreover, $A[1/s]$ is a free abelian group of countable rank [Adams and Clarke 1977, Theorem 2.2] and can be described as the set of all Laurent polynomials $f \in \mathbb{Q}[s, s^{-1}]$ such that $f(a/b) \in \mathbb{Z}[1/(ab)]$ for all integers a and $b \neq 0$.

It follows that the bialgebra $A[1/s]$ admits an antipode $s \mapsto s^{-1}$ that makes $A[1/s]$ a Hopf algebra. It follows that $\mathbf{OP}_R^{\mathrm{st}}(K_{\mathrm{gr}})$ is a (topological) Hopf algebra.

Remark 6.29. We have a diagram of homomorphisms of bialgebras and its dual:

$$\begin{array}{ccc} \mathbb{Z}[s] & \longrightarrow & A \\ \downarrow & & \downarrow \\ \mathbb{Z}[s, s^{-1}] & \longrightarrow & A\big[\frac{1}{s}\big] \end{array} \qquad\qquad \begin{array}{ccc} R^{[0,\infty)} & \xleftarrow{\ b\ } & R[\![x]\!] \\ \uparrow & & \uparrow \\ R^{\mathbb{Z}} & \longleftarrow & \mathbf{OP}_R^{\mathrm{st}}(K_{\mathrm{gr}}) \end{array}$$

The bottom maps are homomorphisms of Hopf algebras. The antipode of $R^{\mathbb{Z}}$ takes a sequence r_i to r_{-i}.

The group of degree 0 stable operations $\mathbf{OP}_{\hat{\mathbb{Z}}}^{\mathrm{st}}(K_{\mathrm{gr}})$ coincides with $\mathbf{OP}_{\hat{\mathbb{Z}}}^{\mathrm{st}}(\mathrm{CK}) = S$, whose structure was described in Theorem 6.25. Our nearest goal is to determine the structure of $\mathbf{OP}_{\mathbb{Z}}^{\mathrm{st}}(K_{\mathrm{gr}})$. We remark that this group is different from $\mathbf{OP}_{\mathbb{Z}}^{\mathrm{st}}(\mathrm{CK}) = S \cap \mathbb{Z}[\![x]\!]$.

Let R be one of the following rings: $\mathbb{Z}$, $\mathbb{Z}_p$ or $\hat{\mathbb{Z}}$. Recall that we have an injective homomorphism $b_R : R[\![x]\!] \to R^{[0,\infty)}$ taking $(1-x)^m$ to the sequence $(1, m, m^2, \dots)$. The operation Φ on $R[\![x]\!]$ corresponds to the shift operation Π on $R^{[0,\infty)}$ defined by $\Pi(a)_i = a_{i+1}$.

An *n-interval* of a sequence a in $R^{[0,\infty)}$ or $R^{\mathbb{Z}}$ is the n-tuple $(a_i, a_{i+1}, \dots, a_{i+n-1})$ for some i. We say that this interval *starts at* i.

For every $n \geqslant 1$, let M_n be the R-submodule of R^n generated by the n-tuples $\bar{r} := (1, r, r^2, \dots, r^{n-1})$ for all integers $r > 0$. Note that M_n is of finite index in R^n.

Lemma 6.30. *A sequence $a \in R^{[0,\infty)}$ belongs to the image of b_R if and only if for every $n > 0$, the n-interval of a starting at 0 is contained in M_n.*

Proof. ($\Rightarrow$): This is clear.

($\Leftarrow$): Note that by assumption a is contained in the closure of $\operatorname{Im}(b_R)$. On the other hand, if $R = \mathbb{Z}_p$ or $\hat{\mathbb{Z}}$, the space $R[\![x]\!]$ is compact in τ_w and $R^{[0,\infty)}$ is Hausdorff, hence $\operatorname{Im}(b_R)$ is closed, i.e., $a \in \operatorname{Im}(b_R)$. If $R = \mathbb{Z}$, it follows from the case $R = \hat{\mathbb{Z}}$ that $a = b_{\hat{\mathbb{Z}}}(G)$ for some $G \in \hat{\mathbb{Z}}[\![x]\!]$. Since at the same time $G \in \mathbb{Q}[\![x]\!]$, we have $G \in \mathbb{Z}[\![x]\!]$. □

Let $T_R \subset R^{\mathbb{Z}}$ be the R-submodule of all sequences $a \in R^{\mathbb{Z}}$ such that every n-interval of a is contained in M_n for all $n \geqslant 1$. If $a \in T_R$, by Lemma 6.30, for every $n \geqslant 0$, there is $G_n \in R[\![x]\!]$ such that $b_R(G_n) = (a_{-n}, a_{-n+1}, \dots)$. Since $\Phi(G_{n+1}) = G_n$, the sequence $(G_n)_{n \geqslant 0}$ determines an element in $\mathbf{OP}_R^{\mathrm{st}}(K_{\mathrm{gr}})$. This construction establishes an isomorphism $\mathbf{OP}_R^{\mathrm{st}}(K_{\mathrm{gr}}) \simeq T_R$. Note that $T_{\hat{\mathbb{Z}}} = \mathbf{OP}_{\hat{\mathbb{Z}}}^{\mathrm{st}}(\mathrm{CK}) = S = \bigcap_r \operatorname{Im}(\Phi^r)$.

For every $n \geqslant 1$, let N_n be the R-submodule of R^n generated by the n-tuples $\bar{r}$ for all $r \in R^\times$. Then N_n is of finite index in R^n if $R = \mathbb{Z}_p$ or $\hat{\mathbb{Z}}$.

Note that every n-tuple $\bar{r}$, with $r \in R^\times$, extends to the sequence a with $a_i = r^i$ that is contained in T_R.

Lemma 6.31. *The module $N_n \subset M_n$ for all $n \geqslant 1$.*

Proof. It suffices to consider the case $R = \mathbb{Z}_p$. Choose an integer $m > 0$ such that $p^m \cdot \mathbb{Z}_p^n \subset M_n$. Let $r \in \mathbb{Z}_p^\times$. Find an integer $r' > 0$ congruent to r modulo p^m. Then the tuple $\bar{r} = (1, r, r^2, \dots, r^{n-1})$ is congruent to $\bar{r}'$ modulo p^m. Hence, $\bar{r} = \bar{r}' + (\bar{r} - \bar{r}') \in M_n + p^m \mathbb{Z}_p^n \subset M_n$. □

It follows from Lemma 6.31 that every element in N_n is an n-interval of a sequence in T_R.

Proposition 6.32. *If $R = \mathbb{Z}_p$ or $\hat{\mathbb{Z}}$, the R-module T_R consists of all sequences $a \in R^{\mathbb{Z}}$ such that every n-interval of a is contained in N_n for all $n \geqslant 1$.*

Proof. We may assume that $R = \mathbb{Z}_p$. Let $a \in T_R$. In view of Lemma 6.31, it suffices to show that every n-interval v of a starting at i is contained in N_n for all $n \geqslant 1$. Take an integer $m > 0$ and consider the $(n+m)$-interval w of $\Pi^{-m}(a)$ starting at i, so that v is the part of w on the right. Write w as a (finite) linear combination $\sum t_r \bar{r}$ over positive integers r, where $t_r \in \mathbb{Z}_p$ and $\bar{r} = (1, r, r^2, \dots, r^{n+m-1}) \in M_{n+m}$. Applying Π^m to $\Pi^{-m}(a)$, we see that $v = \sum t_r r^m \hat{r}$, where $\hat{r} = (1, r, r^2, \dots, r^{n-1}) \in M_n$. As r^m is divisible by p^m if r is divisible by p, it follows from the definition of N_n that $v \in N_n + p^m M_n$. Since N_n is of finite index in M_n, we can choose m such that $p^m M_n \subset N_n$, hence $a \in N_n$. □

Denote by $\theta : R^{\mathbb{Z}} \to R^{\mathbb{Z}}$ the reflection operation taking a sequence a to the sequence $\theta(a)_i = a_{-i}$.

Corollary 6.33. *The module T_R is invariant under θ.*

Proof. In the case $R = \mathbb{Z}_p$ or $\hat{\mathbb{Z}}$, it suffice to notice that if $r \in \mathbb{R}^\times$, the symmetric n-tuple

$$(r^{n-1}, r^{n-2}, \dots, r, 1) = r^{n-1}\big(1, r^{-1}, (r^{-1})^2, \dots, (r^{-1})^{n-1}\big)$$

is contained in N_n. If $R = \mathbb{Z}$, the statement follows from the equality $T_{\mathbb{Z}} = T_{\hat{\mathbb{Z}}} \cap \mathbb{Z}^{\mathbb{Z}}$. □

Now let $R = \hat{\mathbb{Z}}$ and $n \geqslant 0$. The ideal of all $t \in \hat{\mathbb{Z}}$ such that $(0, \dots, 0, t) \in N_n$ is generated by a (unique) positive integer $\tilde{d}_n = n! \cdot d_n$, where the integers d_n were introduced in Section 6C. We know that

$$v_p(\tilde{d}_n) = v_p((n + k_p)!)$$

for all primes p, where $k_p = \lfloor n/(p-1) \rfloor$. By Theorem 6.15, there are power series $F_n \in S_0 = S \cap \mathbb{Z}[\![x]\!]$ such that $F_n \equiv d_n x^n$ modulo x^{n+1}.

Let $f^{(n)} \in T_{\hat{\mathbb{Z}}}$ be the image of F_n under the map $S = \mathbf{OP}^{\mathrm{st}}_{\hat{\mathbb{Z}}}(K_{\mathrm{gr}}) \to \hat{\mathbb{Z}}^{\mathbb{Z}}$. Thus, $(0, \dots, 0, \tilde{d}_n)$ is the n-interval of $f^{(n)}$ starting at 0. For example, we can choose

$$f^{(0)} = (\dots, 1, 1, 1, 1, \dots),$$
$$f^{(1)} = (\dots, 0, 2, 0, 2, \dots).$$

As in the proof of Theorem 6.15, modifying $f^{(n)}$ by adding multiples of the shifts of $f^{(m)}$ for $m > n$ and their reflections, we can obtain $f^{(n)} \in \mathbb{Z}^{\mathbb{Z}}$ for all n.

Theorem 6.34. *Every sequence $a \in T_{\mathbb{Z}} \simeq \mathbf{OP}^{\mathrm{st}}_{\mathbb{Z}}(K_{\mathrm{gr}})$ can be written in the form*

$$a = \sum_{i=0}^{\infty} \left[b_{2i} \Pi^{-i} \theta(f^{(2i)}) + b_{2i+1} \Pi^{i}(f^{(2i+1)}) \right]$$

for unique $b_0, b_1, \ldots \in \mathbb{Z}$.

Proof. We determine the integers $b_0, b_1, \ldots$ inductively so that for every $m \geqslant 0$ the sum $\sum_{i=0}^{m}$ of the terms in the right-hand side and the sequence a have the same $(2m+2)$-intervals starting at $-m$. □

Remark 6.35. Observe that $\{\Pi^{-i}\theta(f^{(2i)}),\ \Pi^{i}(f^{(2i+1)}) \mid i \in \mathbb{Z}_{\geqslant 0}\}$ is also a topological basis of $\mathbf{OP}^{\mathrm{st}}_{\hat{\mathbb{Z}}}(K_{\mathrm{gr}})$. Note that, at the same time, $\{f^{(j)} \mid j \in \mathbb{Z}_{\geqslant 0}\}$ forms a topological basis for $\mathbf{OP}^{\mathrm{st}}_{\mathbb{Z}}(\mathrm{CK})$ and $\mathbf{OP}^{\mathrm{st}}_{\hat{\mathbb{Z}}}(\mathrm{CK})$. This shows the relation between operations in CK and those in K_{gr}. In particular, there are substantially more operations in the former theory.

6E. ***Stable multiplicative operations.*** We first consider stable multiplicative operations on $\mathrm{CK}^*_{\hat{\mathbb{Z}}}$. From Proposition 6.3, we obtain:

Proposition 6.36. *Stable multiplicative operations $\mathrm{CK}^*_{\hat{\mathbb{Z}}} \to \mathrm{CK}^*_{\hat{\mathbb{Z}}}$ are exactly operations Ψ^c_1, for $c \in \hat{\mathbb{Z}}^\times$. These operations are invertible and form a group isomorphic to $\hat{\mathbb{Z}}^\times$. Similarly, stable multiplicative operations on CK^* form a group isomorphic to $\mathbb{Z}^\times$.*

Restricted to $\mathrm{CK}^0_{\hat{\mathbb{Z}}}$, the operation Ψ^c_1 is given by $G_0 = 1$ (as it is multiplicative and so, maps 1 to 1), while $G(tx) = G(t)G(x) = ct \cdot \gamma_G(x) = 1 - (1-tx)^c$ and so, our operation corresponds to the power series $A_c = (1-x)^c$. In other words, on $\mathrm{CK}^0_{\hat{\mathbb{Z}}}$, the operation Ψ^c_1 coincides with the Adams operation Ψ_c. Then on $\mathrm{CK}^n_{\hat{\mathbb{Z}}}$, it is equal to $c^{-n} \cdot \Psi_c$.

Proposition 6.27 gives:

Corollary 6.37. *The set of homogeneous stable additive operations on $\mathrm{CK}^*_{\hat{\mathbb{Z}}}$ is the closure in the topology τ_o of the set of (finite) $\hat{\mathbb{Z}}$-linear combinations of stable multiplicative operations.*

Remark 6.38. Note that the respective statement for $\mathbb{Z}$-coefficients is not true, as there are only two stable multiplicative operations on CK^*, namely, Ψ^1_1 and Ψ^{-1}_1, while the group of stable additive operations there has infinite (uncountable) rank.

Now we consider stable multiplicative operations on K^*_{gr} over $\mathbb{Z}$.

Proposition 6.39. *Stable multiplicative operations $K^*_{\mathrm{gr}} \to K^*_{\mathrm{gr}}$ are exactly operations Ψ^c_1, for $c = \pm 1$. These are invertible and form a group isomorphic to $\mathbb{Z}^\times \cong \mathbb{Z}/2\mathbb{Z}$.*

Proof. The linear coefficient of γ_G for the operation ${}^l\Psi^c_b$ is $t^{1-l}b$, see Section 5B. This will be equal to 1 exactly when $l = 1$ and $b = 1$. □

As above, the operation Ψ^c_1 corresponds to the power series $A_c = (1-x)^c$. On K^n_{gr} it coincides with $c^{-n} \cdot \Psi^1_c$.

References

[Adams and Clarke 1977] J. F. Adams and F. W. Clarke, "Stable operations on complex K-theory", *Illinois J. Math.* **21**:4 (1977), 826–829. MR Zbl

[Adams et al. 1971] J. F. Adams, A. S. Harris, and R. M. Switzer, "Hopf algebras of cooperations for real and complex K-theory", *Proc. Lond. Math. Soc.* (3) **23** (1971), 385–408. MR Zbl

[Cai 2008] S. Cai, "Algebraic connective K-theory and the niveau filtration", *J. Pure Appl. Algebra* **212**:7 (2008), 1695–1715. MR Zbl

[Clarke et al. 2001] F. Clarke, M. D. Crossley, and S. Whitehouse, "Bases for cooperations in K-theory", *K-Theory* **23**:3 (2001), 237–250. MR Zbl

[Dai and Levine 2014] S. Dai and M. Levine, "Connective algebraic K-theory", *J. K-Theory* **13**:1 (2014), 9–56. MR Zbl

[Johnson 1984] K. Johnson, "The action of the stable operations of complex K-theory on coefficient groups", *Illinois J. Math.* **28**:1 (1984), 57–63. MR Zbl

[Kane 1981] R. M. Kane, *Operations in connective K-theory*, Mem. Amer. Math. Soc. **254**, Amer. Math. Soc., Providence, RI, 1981. MR Zbl

[Levine and Morel 2007] M. Levine and F. Morel, *Algebraic cobordism*, Springer, 2007. MR Zbl

[Panin 2003] I. Panin, "Oriented cohomology theories of algebraic varieties", *K-Theory* **30**:3 (2003), 265–314. MR Zbl

[Panin 2004] I. Panin, "Riemann–Roch theorems for oriented cohomology", pp. 261–333 in *Axiomatic, enriched and motivic homotopy theory* (Cambridge, 2002), edited by J. P. C. Greenlees, NATO Sci. Ser. II Math. Phys. Chem. **131**, Kluwer Acad., Dordrecht, 2004. MR Zbl

[Smirnov 2006] A. L. Smirnov, "Orientations and transfers in the cohomology of algebraic varieties", *Algebra i Analiz* **18**:2 (2006), 167–224. In Russian; translated in *St. Petersburg Math. J.* **18**:2 (2007), 305–346. MR

[Strong and Whitehouse 2010] M.-J. Strong and S. Whitehouse, "Integer-valued polynomials and K-theory operations", *Proc. Amer. Math. Soc.* **138**:6 (2010), 2221–2233. MR Zbl

[Vishik 2019] A. Vishik, "Stable and unstable operations in algebraic cobordism", *Ann. Sci. École Norm. Sup.* (4) **52**:3 (2019), 561–630. MR Zbl

Communicated by Raman Parimala
Received 2022-01-26 Revised 2022-08-17 Accepted 2022-10-04

merkurev@math.ucla.edu *Department of Mathematics, University of California, Los Angeles, CA, United States*

alexander.vishik@nottingham.ac.uk *School of Mathematical Sciences, University of Nottingham, Nottingham, United Kingdom*

ALGEBRA AND NUMBER THEORY 17:9 (2023)
https://doi.org/10.2140/ant.2023.17.1637

The structure of Frobenius kernels for automorphism group schemes

Stefan Schröer and Nikolaos Tziolas

We establish structure results for Frobenius kernels of automorphism group schemes for surfaces of general type in positive characteristic. It turns out that there are surprisingly few possibilities. This relies on properties of the famous Witt algebra, which is a simple Lie algebra without finite-dimensional counterpart over the complex numbers, together with its twisted forms. The result actually holds true for arbitrary proper integral schemes under the assumption that the Frobenius kernel has large isotropy group at the generic point. This property is measured by a new numerical invariant called the foliation rank.

Introduction

Let k be an algebraically closed ground field of characteristic $p \geq 0$ and X be a proper scheme. Then the *automorphism group scheme* $\mathrm{Aut}_{X/k}$ is locally of finite type, and the connected component $\mathrm{Aut}^0_{X/k}$ is of finite type. The corresponding Lie algebra $\mathfrak{h} = H^0(X, \Theta_{X/k})$ is the space of global vector fields.

MSC2020: 14L15, 14J50, 14G17, 14J29, 17B50, 13N15.
Keywords: automorphism group schemes, restricted lie algebras, surfaces of general type, foliations.

If X is smooth and of general type, then the group $\mathrm{Aut}(X)$ is actually finite, according to a general result of Martin-Deschamps and Lewin-Ménégaux [1978].

Throughout this paper, we are mainly interested in characteristic $p > 0$. Then the group scheme $\mathrm{Aut}_{X/k}$ comes with a relative Frobenius map, and the resulting Frobenius kernel $H = \mathrm{Aut}_{X/k}[F]$ is a *height-one group scheme*. The group of rational points is trivial, but the coordinate ring may contain nilpotent elements. The Lie algebra $\mathfrak{h} = H^0(X, \Theta_{X/k})$ remains the space of global vector fields or, equivalently, the space of k-linear derivations $D : \mathscr{O}_X \to \mathscr{O}_X$. The p-fold composition in the associative ring of k-linear differential operators endows the Lie algebra with an additional structure, the so-called *p-map* $D \mapsto D^{[p]}$, which turns $\mathfrak{h}$ into a *restricted Lie algebra*. By the *Demazure–Gabriel correspondence*, height-one group schemes and restricted Lie algebras determine each other.

Our goal is to uncover the *structural properties* of the height-one group scheme $H = \mathrm{Aut}_{X/k}[F]$ or, equivalently, the restricted Lie algebra $\mathfrak{h} = H^0(X, \Theta_{X/k})$, and our initial motivation was to understand the case of surfaces of general type. Such surfaces with $\mathfrak{h} \neq 0$ were first constructed by Russell [1984] and Lang [1983]. These constructions rely on Tango curves [1972], and come with a purely inseparable covering by a ruled surface. By a similar construction with abelian surfaces, Shepherd-Barron [1996, Theorem 5.3] produced examples in characteristic $p = 2$ that are non-uniruled. Ekedahl [1987, pp. 145–146] already had examples with rational double points for arbitrary $p > 0$; the vector fields, however, do not extend to a resolution of singularities. Recently, Martin [2022a; 2022b] studied infinitesimal automorphism group schemes of elliptic and quasielliptic surfaces.

However, almost nothing seems to be known about the general structure of the height-one group schemes $H = \mathrm{Aut}_{X/k}[F]$, and one would expect little restrictions in this respect. The main result of this paper asserts that under certain assumptions, quite the opposite is true:

Theorem 12.1. *Let X be a proper integral scheme with foliation rank $r \leq 1$. Then the Frobenius kernel $H = \mathrm{Aut}_{X/k}[F]$ is isomorphic to the Frobenius kernel of one of the following three basic types of group schemes*:

$$\mathrm{SL}_2, \quad \mathbb{G}_a^{\oplus n} \quad \textit{or} \quad \mathbb{G}_a^{\oplus n} \rtimes \mathbb{G}_m,$$

for some integer $n \geq 0$.

In the latter two cases, the respective Frobenius kernels are $\alpha_p^{\oplus n}$ and the semidirect product $\alpha_p^{\oplus n} \rtimes \mu_p$. The *foliation rank* is a new invariant that can be defined as follows: Forming the quotient $Y = X/H$ by the Frobenius kernel of the automorphism group scheme, the canonical map $X \to Y$ induces a height-one extension $E = k(Y) \subset k(X) = F$ of function fields, and the foliation rank $r \geq 0$ is given by $[F : E] = p^r$. Via the Jacobson correspondence, this can also be expressed in terms of the *inertia subgroup scheme* for the induced action of the base-change H_F on $F \otimes_E F$. This geometric interpretation of the Jacobson correspondence seems to be of independent interest (see Section 5).

If X is a proper normal surface with $h^0(\omega_X^\vee) = 0$, for example, a surface of general type or a properly elliptic surface, the foliation rank is automatically $r \leq 1$, and the above result applies (see Corollary 12.2). Indeed, our initial motivation was to find restrictions on the Frobenius kernels for surfaces of general type.

The key idea in the proof is to relate our geometric problem to algebraic properties of the famous *Witt algebra* $\mathfrak{g}_0 = \mathrm{Der}_E(F_0)$, formed with the truncated polynomial ring $F_0 = E[t]/(t^p)$ over certain function fields E. This algebra was indeed introduced by Ernst Witt, see the discussion in [Strade 1993]. It is one of the simple algebras in odd characteristic $p > 0$ having no finite-dimensional counterpart over the complex numbers. Note that it has nothing to do with the ring of Witt vectors, or Witt groups for quadratic forms.

The foliation rank is $r = 1$ if and only if $\deg(X/Y) = p$. This situation is paradoxical, because it may hold even with large Frobenius kernels. We now compare $H = \mathrm{Aut}_{X/k}[F]$ with the generic fiber of the relative group scheme $G = \mathrm{Aut}_{X/Y}$. In other words, we relate the restricted Lie algebra $\mathfrak{h} = H^0(X, \Theta_{X/k})$ over k with the restricted Lie algebra $\mathfrak{g} = \mathrm{Der}_E(F)$ over the function field $E = k(Y)$. The latter is a *twisted form* of the Witt algebra $\mathfrak{g}_0 = \mathrm{Der}_E(F_0)$. The classification of its subalgebras due to Premet and Stewart [2019] is one key ingredient for our proof. Among other surprising features, $\mathfrak{g}_0$ contains Cartan algebras of different dimensions. A crucial observations is that *the bigger Cartan algebras disappear after passing to twisted forms like* $\mathfrak{g}$, *leaving few possibilities for subalgebras*. This is an algebraic incarnation for the fact that the reduced part of a group scheme may not be a subgroup scheme, and if it is, it may not be normal.

The semidirect products $\alpha_p^{\oplus n} \rtimes \mu_p$, indeed, occur as Frobenius kernels of automorphism group schemes. In Section 14, we construct examples of surfaces as coverings $X \to \mathbb{P}^2$ of degree p or divisors $X \subset \mathbb{P}^3$ of degree $2p + 1$, such that $\mathfrak{h} = k^n \rtimes \mathfrak{gl}_1(k)$, for certain integers $n \geq 0$. So far, we do not know if $\mathfrak{h} = \mathfrak{sl}_2(k)$ may also occur. In our examples, the minimal resolutions are surfaces S of general type, and X are their canonical models.

Such X are also called *canonically polarized surface*. They come with two *Chern numbers* $c_1^2 = c_1^2(L^\bullet_{X/k}) = K_X^2$ and $c_2 = c_2(L^\bullet_{X/k})$. This was introduced by Ekedahl, Hyland and Shepherd-Barron [Ekedahl et al. 2012] for general proper surfaces whose local rings are complete intersections, such that the cotangent complex is perfect. Using Noether's inequality and results from Ekedahl [1988], we show with more classical methods:

Theorem 13.2. *Let X be a canonically polarized surface, with Chern numbers c_1^2 and c_2. Then the Lie algebra $\mathfrak{h} = H^0(X, \Theta_{X/k})$ for the Frobenius kernel $H = \mathrm{Aut}_{X/k}[F]$ has the property* $\dim(\mathfrak{h}) \leq \Phi(c_1^2, c_2)$ *for the polynomial*

$$\Phi(x, y) = \begin{cases} \frac{1}{144}(73x + y)^2 - 1, & \text{if } c_1^2 \geq 2, \\ \frac{1}{144}(121x + y)^2 - 1, & \text{if } c_1^2 = 1. \end{cases}$$

With Noether's inequality, this also gives the weaker bound $\dim(\mathfrak{h}) \leq \Psi(c_1^2)$ with the polynomial

$$\Psi(x) = \begin{cases} \frac{169}{4}x^2 + 39x + 8, & \text{if } c_1^2 \geq 2, \\ \frac{441}{4}x^2 + 63x + 8, & \text{if } c_1^2 = 1. \end{cases}$$

Note that Xiao [1995] proved $|\mathrm{Aut}(X)| \leq 1764c_1^2$ over the complex numbers.

The paper is organized as follows: Section 1 contains general facts on restricted Lie algebras and their semidirect products. In Section 2, we examine multiplicative and additive vectors and the toral rank. In Section 3, we collect general facts on automorphism group schemes for proper schemes and the quotient by height-one group schemes, and we discuss twisted forms of some relevant restricted Lie algebras. Section 5 contains a geometric interpretation of the Jacobson correspondence, in terms of inertia group schemes at generic points. We introduce the foliation rank and establish its basic properties in Section 6. In Section 7, we analyze the removal of subvector spaces under certain twists. Then we make a detailed analysis of the automorphism group scheme for radical extensions of prime degree in Section 8, followed by an examination of the corresponding Witt algebras in Section 9. In Section 10, we show how structural properties of restricted Lie algebras over different fields are inherited. Our main result on the structure of the Frobenius kernel for automorphism groups is contained in Section 11. Section 13 contains the bound for surfaces of general type. In the final Section 14, we construct examples.

1. Restricted Lie algebras

In this section, we review some standard results on restricted Lie algebras and height-one group schemes that are relevant for the applications we have in mind. Let k be a ground field of characteristic $p > 0$. For each ring R, not necessarily commutative or associative, the vector space $\mathrm{Der}_k(R)$ of k-derivations $D : R \to R$ is closed under forming commutators $[D, D']$ and p-fold compositions D^p in the associative ring $\mathrm{End}_k(R)$. One now views $\mathrm{Der}_k(R)$ as a *Lie algebra*, endowed with the map $D \mapsto D^p$ as an additional structure.

This leads to the following abstraction: A *restricted Lie algebra* is a Lie algebra $\mathfrak{g}$, together with a map $\mathfrak{g} \to \mathfrak{g}$, $x \mapsto x^{[p]}$, called the *p-map*, subject to the following three axioms:

(R1) We have $\mathrm{ad}_{x^{[p]}} = (\mathrm{ad}_x)^p$ for all vectors $x \in \mathfrak{g}$.

(R2) Moreover $(\lambda \cdot x)^{[p]} = \lambda^p \cdot x^{[p]}$ for all vectors $x \in \mathfrak{g}$ and scalars $\lambda \in k$.

(R3) The formula $(x + y)^{[p]} = x^{[p]} + y^{[p]} + \sum_{r=1}^{p-1} s_r(x, y)$ holds for all $x, y \in \mathfrak{g}$.

Here, the summands $s_r(x, y)$ are universal expressions defined by

$$s_r(t_0, t_1) = -\frac{1}{r} \sum_u \big(\mathrm{ad}_{t_{u(1)}} \circ \mathrm{ad}_{t_{u(2)}} \circ \ldots \circ \mathrm{ad}_{t_{u(p-1)}}\big)(t_1),$$

where $\mathrm{ad}_a(x) = [a, x]$ denotes the *adjoint representation* and the index runs over all maps

$$u : \{1, \ldots, p-1\} \to \{0, 1\}$$

taking the value zero exactly r times. For $p = 2$, the expression simplifies to $s_1 = [t_0, t_1]$, whereas $p = 3$ gives $s_1 = [t_1, [t_0, t_1]]$ and $s_2 = [t_0, [t_0, t_1]]$. Restricted Lie algebras were introduced and studied by Jacobson [1937], and also go under the name *p-Lie algebras*. We refer to the monographs of Demazure and Gabriel [1970], in particular, Chapter II, §7, or Strade and Farnsteiner [1988] for more details.

Throughout the paper, terms like homomorphisms, subalgebras, ideals, extensions etc. are understood in the *restricted sense*, if not said otherwise. For example, an *ideal* $\mathfrak{a} \subset \mathfrak{g}$ is a vector subspace such that $[x, y], x^{[p]} \in \mathfrak{a}$ whenever $x \in \mathfrak{a}$ and $y \in \mathfrak{g}$. Note that this holds for the *center*

$$\mathfrak{C}(\mathfrak{g}) = \{a \in \mathfrak{g} \mid [a, x] = 0 \text{ for all } x \in \mathfrak{g}\},$$

because $[a^{[p]}, x] = (\mathrm{ad}_a)^p(x) = (\mathrm{ad}_a)^{p-1}([a, x]) = 0$.

For abelian $\mathfrak{g}$, the p-map becomes *semilinear*, which means that it corresponds to a linear map $\mathfrak{g} \to \mathfrak{g}$ when the scalar multiplication in the range is redefined via Frobenius. In turn, those $\mathfrak{g}$ correspond to modules over the associative polynomial ring $k[F]$, in which the relation $F\lambda = \lambda^p F$ holds. Every right ideal is principal; this also holds for left ideals, provided that k is perfect, and then the structure theory developed by Jacobson [1943, Chapter 3] applies.

In contrast, for nonabelian $\mathfrak{g}$, the p-map *fails to be additive*, and it is challenging to understand its structure. However, by (R1) it is determined by the bracket up to central elements, because $[a^{[p]}, x] = (\mathrm{ad}_a)^p(x)$. In particular, if the center is trivial, the p-map is unique, once it exists. This also explains the terminology *restricted*.

Recall that for each group scheme G, the *Lie algebra* $\mathfrak{g} = \mathrm{Lie}(G)$ is defined by the short exact sequence

$$0 \to \mathrm{Lie}(G) \to G(k[\epsilon]) \to G(k) \to 0,$$

where $k[\epsilon]$ is the ring of dual numbers, and the map is the restriction with respect to the inclusion $k \subset k[\epsilon]$. As explained in [Demazure and Gabriel 1970, Chapter II, §7], it carries the structure of a restricted Lie algebra, in a functorial way. Also recall that the relative Frobenius morphism $F : G \to G^{(p)}$ is a homomorphism. The resulting *Frobenius kernel* $G[F]$ is a group scheme whose underlying topological space is a singleton.

Let us call G *of height one* if it is of finite type and annihilated by the relative Frobenius map. We then also say that G is a *height-one group scheme*. According to [Demazure and Gabriel 1970, Chapter II, §7, Theorem 3.5], the canonical map

$$\mathrm{Hom}(G, H) \to \mathrm{Hom}(\mathrm{Lie}(G), \mathrm{Lie}(H))$$

is bijective whenever G has height one. In particular, the functor $G \mapsto \mathrm{Lie}(G)$ is an equivalence between the category of height-one group schemes and the category of finite-dimensional restricted Lie algebras. We call this the *Demazure–Gabriel correspondence*. The inverse functor sends $\mathfrak{g}$ to the spectrum of the dual for the Hopf algebra $U^{[p]}(\mathfrak{g})$, which is the universal enveloping algebra $U(\mathfrak{g})$ modulo the ideal generated by the elements $x^p - x^{[p]}$, for $x \in \mathfrak{g}$. From this, one deduces

$$|G| = h^0(\mathscr{O}_G) = p^{\dim(\mathfrak{g})} \quad \text{and} \quad \mathrm{edim}(\mathscr{O}_{G,e}) = \dim(\mathfrak{g}).$$

As customary, we write $\mathfrak{gl}_n(k)$ for the restricted Lie algebra of $n \times n$-matrices, where bracket and p-map are given by commutators and p-powers, and $\mathfrak{sl}_n(k)$ for the ideal of trace zero matrices. Furthermore, k^n denotes the standard vector space, endowed with trivial bracket and p-map.

Let $\mathfrak{a} \subset \mathfrak{g}$ be an ideal, and consider the vector space $\mathrm{Der}_k(\mathfrak{a})$ of all k-linear derivations. Then $\mathrm{Der}_k(\mathfrak{a}) \subset \mathfrak{gl}(\mathfrak{a})$ is a subalgebra. Derivations $D : \mathfrak{g} \to \mathfrak{g}$ satisfying the additional condition $D(a^{[p]}) = (\mathrm{ad}_a)^{p-1}(D(a))$ for all $a \in \mathfrak{a}$ are called *restricted derivations*. Write $\mathrm{Der}'_k(\mathfrak{a})$ for the vector space of all restricted k-derivations. According to [Jacobson 1941, Theorem 4], the inclusion $\mathrm{Der}'_k(\mathfrak{a}) \subset \mathrm{Der}_k(\mathfrak{a})$ is a subalgebra. By the Jacobi identity and (R1), the adjoint map defines a homomorphism

$$\mathfrak{g} \to \mathrm{Der}'_k(\mathfrak{a}), \quad x \mapsto (a \mapsto [x, a]). \tag{1}$$

Given restricted Lie algebras $\mathfrak{h}$ and $\mathfrak{a}$, we are now interested in *extensions*

$$0 \to \mathfrak{a} \to \mathfrak{g} \to \mathfrak{h} \to 0,$$

such that $\mathfrak{a} \subset \mathfrak{g}$ becomes an ideal with quotient $\mathfrak{g}/\mathfrak{a} = \mathfrak{h}$. The extension *splits* if the ideal $\mathfrak{a} \subset \mathfrak{g}$ admits a complementary subalgebra $\mathfrak{h}' \subset \mathfrak{g}$. Composing the inverse for the projection $\mathfrak{h}' \to \mathfrak{h}$ with (1), we obtain a homomorphism $\varphi : \mathfrak{h} \to \mathrm{Der}'_k(\mathfrak{a})$. Conversely, suppose we have such a homomorphism, written as $h \longmapsto (a \mapsto \varphi_h(a))$. On the vector space sum $\mathfrak{a} \oplus \mathfrak{h}$, we now define bracket and p-map by

$$\begin{aligned} [a + h, a' + h'] &= [a, a'] + [h, h'] + \varphi_h(a') - \varphi_{h'}(a), \\ (a + h)^{[p]} &= a^{[p]} + h^{[p]} + \sum_{r=1}^{p-1} s_r(a, h). \end{aligned} \tag{2}$$

Lemma 1.1. *The above endows the vector space $\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{h}$ with the structure of a restricted Lie algebra, such that $\mathfrak{a}$ and $\mathfrak{h}$ is an ideal and subalgebra, respectively.*

Proof. As explained in [Bourbaki 1989, Chapter I, §1.8], the bracket turns $\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{h}$ into a Lie algebra, having $\mathfrak{a}$ as an ideal and $\mathfrak{h}$ as a subalgebra. Now choose bases $a_i \in \mathfrak{a}$ and $h_j \in \mathfrak{h}$, such that a_i, h_j form a basis for $\mathfrak{g}$. We claim that

$$(\mathrm{ad}_{a_i})^p = \mathrm{ad}_{(a_i)^{[p]}} \quad \text{and} \quad (\mathrm{ad}_{h_j})^p = \mathrm{ad}_{(h_j)^{[p]}} \tag{3}$$

as k-linear endomorphisms of $\mathfrak{g}$. Indeed, since $\mathfrak{a}$ and $\mathfrak{h}$ are restricted, and by the definition of the bracket in $\mathfrak{g}$, it is enough to verify that $(\mathrm{ad}_{a_i})^p(h) = -\varphi_h((a_i)^{[p]})$ for every vector $h \in \mathfrak{h}$ and $(\mathrm{ad}_{h_j})^p(a) = \varphi_{(h_j)^{[p]}}(a)$ for every $a \in \mathfrak{a}$. Since the derivations φ_h are restricted, we have

$$-\varphi_h((a_i)^{[p]}) = -\,\mathrm{ad}_{a_i}^{p-1}(\varphi_h(a_i)) = -\,\mathrm{ad}_{a_i}^{p-1}([h, a_i]) = (\mathrm{ad}_{a_i})^p(h).$$

The argument for $(\mathrm{ad}_{h_j})^p(a)$ is similar. Thus, (3) holds. According to [Strade and Farnsteiner 1988, Theorem 2.3], there is a unique p-map satisfying (3) and the (R1)–(R3). By construction, this p-map on $\mathfrak{g}$ coincides with the given p-map on $\mathfrak{a}$ and $\mathfrak{h}$. It thus coincides with (2), in light of (R3). □

In the above situation, the restricted Lie algebras $\mathfrak{g} = \mathfrak{a} \rtimes_\varphi \mathfrak{h}$ are called *semidirect products*. Obviously, every split extension of $\mathfrak{h}$ by $\mathfrak{a}$ is of this form. Of particular importance for us is the case $\mathfrak{a} = k^n$ and $\mathfrak{b} = \mathfrak{gl}_1(k)$, where the homomorphism $\varphi : \mathfrak{gl}_1(k) \to \mathfrak{gl}(k^n) = \mathrm{Der}_k(k^n)$ sends scalars to scalar matrices.

The resulting restricted Lie algebra is written as $k^n \rtimes \mathfrak{gl}_1(k)$. Here, bracket and p-map are given by the formulas

$$[v+\lambda e, v'+\lambda' e] = \lambda v' - \lambda' v \quad \text{and} \quad (v+\lambda e)^{[p]} = \lambda^{p-1}(v+\lambda e), \tag{4}$$

where $e \in \mathfrak{gl}_1(k)$ is the unit element, $v, v' \in k^n$ are vectors and $\lambda, \lambda' \in k$ are scalars.

2. Toral rank and p-closed vectors

Let $\mathfrak{g}$ be a finite-dimensional restricted Lie algebra over a ground field k of characteristic $p > 0$ and G be the corresponding height-one group scheme such that $\mathrm{Lie}(G) = \mathfrak{g}$. Recall that $x \in \mathfrak{g}$ is called *p-closed* if $x^{[p]} \in kx$. Such vectors are called *multiplicative* if $x^{[p]} \neq 0$, and *additive* if $x^{[p]} = 0$. If the vector is nonzero, $\mathfrak{h} = kx$ is a one-dimensional subalgebra, hence corresponds to a subgroup scheme $H \subset G$ of order p. For multiplicative vectors, this is a twisted form of the diagonalizable group scheme $\mu_p = \mathbb{G}_m[F]$. In the additive case, it is isomorphic to the unipotent group scheme $\alpha_p = \mathbb{G}_a[F]$. This basic fact has many geometric applications: For results concerning K3 surfaces, Enriques surfaces and Kummer surfaces, see [Schröer 2007; 2021; Kondō and Schröer 2021].

Proposition 2.1. *Every vector in $\mathfrak{g} = k^n \rtimes \mathfrak{gl}_1(k)$ is p-closed. The same holds for $\mathfrak{g} = \mathfrak{sl}_2(k)$ in characteristic $p \geq 3$.*

Proof. The first assertion immediately follows from (4). Recall that $\mathfrak{sl}_2(k)$ is the restricted Lie algebra comprising the traceless matrices $A = \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right) \in \mathrm{Mat}_2(k)$. The characteristic polynomial $\chi_A(T) = T^2 + d$ depends only on the determinant $d = -a^2 - bc$, so the possible Jordan normal forms over k^{alg} are

$$\begin{pmatrix} \sqrt{d} & 0 \\ 0 & -\sqrt{d} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Computing p-powers via the above normal forms, we see that $A^{[p]} = d^{(p-1)/2} A$. □

The traceless matrices $h = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $x = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ form a basis of $\mathfrak{sl}_2(k)$, and the structural constants are given by

$$[h, x] = 2x, \quad [h, y] = 2y, \quad [x, y] = h^{[p]} = h, \quad x^{[p]} = y^{[p]} = 0.$$

One also says that (h, x, y) is an *$\mathfrak{sl}_2(k)$-triple*. For $p \geq 3$, it follows that for each nonzero $a \in \mathfrak{sl}_2(k)$, the adjoint map ad_a is bijective, hence $\mathfrak{sl}_2(k)$ is simple. In contrast, for $p = 2$ we have a central extension $0 \to \mathfrak{gl}_1(k) \to \mathfrak{sl}_2(k) \to k^2 \to 0$, where the kernel corresponds to scalar matrices. The extension does not split, because $A^{[2]} \neq 0$ for all matrices not contained in the kernel.

If k is algebraically closed, the *toral rank* for a restricted Lie algebra $\mathfrak{g}$ is the maximal integer $r \geq 0$ for which there is an embedding $\mathfrak{gl}_1(k)^{\oplus r} \subset \mathfrak{g}$. In terms of vectors, the condition means that there are linearly independent $x_1, \ldots, x_r \in \mathfrak{g}$, with $[x_i, x_j] = 0$ and $x_i^{[p]} = x_i$. For general fields k, we define the toral rank as the toral rank of the base-change $\mathfrak{g} \otimes_k k^{\mathrm{alg}}$. Following the notation in [Demazure and Grothendieck 1970, Exposé XII, Section 2], we denote this integer by $\rho_t(\mathfrak{g}) \geq 0$. By Hilbert's Nullstellensatz, the toral rank

does not change under field extensions. According to [Block and Wilson 1988, Lemma 1.7.2], it satisfies $\rho_t(\mathfrak{g}) = \rho_t(\mathfrak{n}) + \rho_t(\mathfrak{g}/\mathfrak{n})$ for each ideal $\mathfrak{a} \subset \mathfrak{g}$. In other words, it is additive in extensions. Obviously, $0 \leq \rho_t(\mathfrak{g}) \leq \dim(\mathfrak{g})$.

Proposition 2.2. *The following are equivalent*:

(i) *The restricted Lie algebra* $\mathfrak{g}$ *has maximal toral rank* $\rho_t(\mathfrak{g}) = \dim(\mathfrak{g})$.

(ii) *The group scheme* G *is a twisted form of some* $\mu_p^{\oplus r}$.

(iii) *The group scheme* G *is multiplicative.*

Proof. It suffices to treat the case that k is algebraically closed. The implications (i) $\iff$ (ii) $\implies$ (iii) are obvious. Now suppose that (iii) holds. Since $k = k^{\mathrm{alg}}$, the group scheme G is diagonalizable, whence is the spectrum of the Hopf algebra $k[\Lambda]$ for some finitely generated abelian group Λ. We have $p\Lambda = 0$, because G has height one. Choosing an $\mathbb{F}_p$-basis for Λ gives $G = \mu_p^{\oplus r}$, thus (ii) holds. □

The other extreme is somewhat more involved:

Proposition 2.3. *The following are equivalent*:

(i) *The restricted Lie algebra* $\mathfrak{g}$ *has minimal toral rank* $\rho_t(\mathfrak{g}) = 0$.

(ii) *There is some exponent* $v \geq 0$ *with* $x^{[p^v]} = 0$ *for all vectors* $x \in \mathfrak{g}$.

(iii) *There are ideals* $0 = \mathfrak{a}_0 \subset \cdots \subset \mathfrak{a}_r = \mathfrak{g}$ *inside* $\mathfrak{g}$ *with quotients* $\mathfrak{a}_i/\mathfrak{a}_{i-1} \simeq k$.

(iv) *There are normal subgroup schemes* $0 = N_0 \subset \cdots \subset N_r = G$ *inside* G *with quotients* $N_i/N_{i-1} \simeq \alpha_p$.

(v) *The group scheme* G *is unipotent.*

Proof. The implications (iv) $\implies$ (v) and (iii) $\implies$ (ii) and (ii) $\implies$ (i) are trivial, whereas (iv) $\iff$ (iii) follows from the Demazure–Gabriel correspondence.

We next verify (v) $\implies$ (i). Without loss of generality, we may assume that k is algebraically closed. Then there is a composition series G_j inside G such that G_j/G_{j-1} is isomorphic to a subgroup scheme of the additive group $\mathbb{G}_a$. This already lies in $\alpha_p = \mathbb{G}_a[F]$, because G has height one. For the corresponding subalgebras $\mathfrak{b}_j$ inside $\mathfrak{g}$, this means $\mathfrak{b}_j/\mathfrak{b}_{j-1} \subset k$. The additivity of toral rank implies $\rho_t(\mathfrak{g}) = 0$.

To see (i) $\implies$ (ii), we may assume that k is algebraically closed, and then the implication follows from [Premet 1989, Corollary 2]. For (ii) $\implies$ (iii), we use $(\mathrm{ad}_a)^{p^v} = \mathrm{ad}_{a^{[p^v]}} = 0$, and conclude with Engel's theorem [Bourbaki 1989, Chapter I, §4.2], that the underlying Lie algebra $\mathfrak{g}$ is nilpotent. Now, recall that the center $\mathfrak{C}(\mathfrak{g})$ is invariant under the p-map. In turn, the upper central series, which is recursively defined by $\mathfrak{g}_{i+1}/\mathfrak{g}_i = \mathfrak{C}(\mathfrak{g}/\mathfrak{g}_i)$, yields a sequence of ideals $0 = \mathfrak{g}_0 \subset \cdots \subset \mathfrak{g}_s = \mathfrak{g}$ having abelian quotients. This reduces our problem to the case that $\mathfrak{g}$ itself is abelian. We proceed by induction on $n = \dim(\mathfrak{g})$. The case $n = 0$ is trivial. Suppose now that $n > 0$ and that (iii) holds for $n - 1$. Fix some $x \neq 0$, and consider the largest exponent $d \geq 1$ such that $x^{[p^d]} \neq 0$. Replacing x with $x^{[p^d]}$, we may assume that $x^{[p]} = 0$. Then $\mathfrak{a}_1 = kx$ is a one-dimensional ideal. The quotient $\mathfrak{g}' = \mathfrak{g}/\mathfrak{a}$ has dimension $n' = n - 1$, and furthermore $\rho_t(\mathfrak{g}') = 0$ by additivity of toral rank. Applying the induction hypothesis to $\mathfrak{g}' = \mathfrak{g}/\mathfrak{a}$ and using the isomorphism theorem gives the desired ideals in $\mathfrak{g}$. □

3. Automorphism group schemes

Let k be a ground field. Write (Aff/k) for the category of affine k-schemes, which we usually write as $T = \mathrm{Spec}(R)$. Recall that an *algebraic space* is a contravariant functor $X : (\mathrm{Aff}/k) \to (\mathrm{Set})$ satisfying the sheaf axiom with respect to the étale topology, such that the diagonal $X \to X \times X$ is relatively representable by schemes, and that there is an étale surjection $U \to X$ from some scheme U. According to [Stacks 2005–, Lemma 076M], the sheaf axiom already holds with respect to the fppf topology. Throughout, we use the fppf topology if not stated otherwise. Algebraic spaces are important generalizations of schemes, because modifications, quotients, families, or moduli spaces of schemes are frequently algebraic spaces rather than schemes. We refer to the monographs of Olsson [2016], Laumon and Moret-Bailly [2000], Artin [1971], Knutson [1971], and to the stacks project [Stacks 2005–, Part 4].

Let X be a scheme, or more generally an algebraic space, that is separated and of finite type. Recall that the R-valued points of the Hilbert functor $\mathrm{Hilb}_{X/k}$ are the closed subschemes $Z \subset X \otimes R$ such that the projection $Z \to \mathrm{Spec}(R)$ is proper and flat. Regarding automorphisms $f : X \otimes R \to X \otimes R$ as graphs, we see that $\mathrm{Aut}_{X/k}$ is an open subfunctor. According to [Artin 1969, Theorem 6.1], the Hilbert functor is representable by an algebraic space that is separated and locally of finite type. In turn, the same holds for $\mathrm{Aut}_{X/k}$, which additionally carries a group structure. Using descent and translations, one sees that it must be schematic. The Lie algebra for the automorphism group scheme is given by

$$\mathrm{Lie}(\mathrm{Aut}_{X/k}) = H^0(X, \Theta_{X/k}),$$

where $\Theta_{X/k} = \underline{\mathrm{Hom}}(\Omega^1_{X/k}, \mathscr{O}_X)$ is the coherent sheaf dual to the sheaf of Kähler differentials.

We now assume that X is proper, and that the ground field has characteristic $p > 0$. Then $\mathfrak{g} = H^0(X, \Theta_X)$ is a restricted Lie algebra of finite dimension, which corresponds to the Frobenius kernel $G[F]$ for the automorphism group scheme $G = \mathrm{Aut}_{X/k}$. Note that $G[F]$ is a height-one group scheme, of order p^n, where $n = h^0(\Theta_{X/k})$.

Let H be a group scheme that is separated and locally of finite type, $f : H \to G$ be a homomorphism and P be a H-torsor. The latter is an algebraic space, endowed with a free and transitive H-action. The set of isomorphism classes comprise the nonabelian cohomology $H^1(k, H)$, formed with respect to the fppf topology. On the product $P \times X$, we get a diagonal action. This action is free, because it is free on the first factor. It follows that the quotient ${}^PX = H\backslash(P \times X)$ exists as an algebraic space (see, for example, [Laurent and Schröer 2021, Lemma 1.1]). We have ${}^PX \simeq X$ provided that P is trivial, that is, contains a rational point. In any case, there is an étale surjection $U \to P$ from some scheme U. According to Hilbert's Nullstellensatz, every closed point $a \in U$ defines a finite field extension $k' = \kappa(a)$, and we see that ${}^PX \otimes k' \simeq X \otimes k'$. We, therefore, say that ${}^PX$ is a *twisted form* of X. Indeed, every algebraic space Y that becomes isomorphic to X after some field extension is of this form, with $H = \mathrm{Aut}_{X/k}$.

Our $f : H \to G = \mathrm{Aut}_{X/k}$ induces a homomorphism $c : H \to \mathrm{Aut}_{G/k}$, which sends $h \in H(R)$ to the inner automorphism $g \mapsto f(h)gf(h)^{-1}$. This gives a twisted form ${}^PG$ of G, and its Lie algebra ${}^P\mathfrak{g}$ is a twisted form of $\mathfrak{g}$. In fact, one may view $\mathfrak{g}$ as a vector scheme as in Section 7, regard bracket and p-map

as morphisms of schemes and obtain ${}^P\mathfrak{g}$ by taking the rational points on the twisted form of the vector scheme, formed via the derivative $c' : H \to \mathrm{Aut}_{\mathfrak{g}/k}$.

Lemma 3.1. *There is a canonical identification* ${}^P\mathrm{Aut}_{X/k} = \mathrm{Aut}_{{}^PX/k}$, *where on the left we take the twist with respect to* $c : H \to \mathrm{Aut}_{G/k}$. *The restricted Lie algebra for this group scheme is* ${}^P\mathfrak{g}$, *where we twist with respect to* $c' : H \to \mathrm{Aut}_{\mathfrak{g}/k}$.

Proof. This follows from very general considerations in [Giraud 1971, Chapter III], which can be made explicit as follows: Consider the canonical morphism

$$P \times \mathrm{Aut}_{X/k} \longrightarrow \mathrm{Aut}_{{}^PX}, \quad (p, \psi) \longmapsto \big(H \cdot (p, x) \mapsto H \cdot (p, \psi(x))\big),$$

where the description on the right is viewed as a natural transformation for R-valued points. This is well-defined, because in the presence of $p \in P(R)$ the projection $\{p\} \times X(R) \to ({}^PX)(R)$ is bijective. For each $h \in H(R)$, the element $(hp, h\psi h^{-1})$ sends the orbit $H \cdot (p, x) = H \cdot (hp, hx)$ to the orbit $H \cdot (hp, h\psi(x)) = H \cdot (p, \psi(x))$. Thus, the above transformation descends to a morphism ${}^P\mathrm{Aut}_{X/k} \to \mathrm{Aut}_{{}^PX}$, where H acts via conjugacy on $\mathrm{Aut}_{X/k}$. The same argument applies for the Frobenius kernel, and equivalently to the restricted Lie algebra. □

We now change notation. Suppose that $G = X$ is a height-one group scheme, and write $\mathfrak{g} = \mathrm{Lie}(G)$. One easily checks that $\mathrm{Aut}_{G/k}$ is a closed subgroup scheme of the general linear group $\mathrm{GL}_{V/k}$, where $V = H^0(G, \mathscr{O}_G)$. By the Demazure–Gabriel correspondence, used in the relative form, we get an identification $\mathrm{Aut}_{G/k} = \mathrm{Aut}_{\mathfrak{g}/k}$. The latter can be constructed directly: Choose a basis $e_1, \ldots, e_n \in \mathfrak{g}$. Then $\mathrm{Aut}_{\mathfrak{g}/k}$ is the closed subgroup scheme inside $\mathrm{GL}_{k,n}$ respecting the structural equations

$$[e_r, e_s] = \sum \lambda_{r,s,i} e_i \quad \text{and} \quad e_r^{[p]} = \sum \mu_{r,j} e_j.$$

For later use, we compute some automorphism group schemes $\mathrm{Aut}_{\mathfrak{g}/k}$:

Proposition 3.2. *The following table lists the automorphism group schemes and the resulting cohomology groups or sets for the restricted Lie algebras* k, $\mathfrak{gl}_1(k)$, $k \rtimes \mathfrak{gl}_1(k)$ *and* $\mathfrak{sl}_2(k)$, *where the last column is only valid for* $p \geq 3$:

$\mathfrak{g}$	k	$\mathfrak{gl}_1(k)$	$k \rtimes \mathfrak{gl}_1(k)$	$\mathfrak{sl}_2(k)$
$\mathrm{Aut}_{\mathfrak{g}/k}$	$\mathbb{G}_m$	μ_{p-1}	$\mathbb{G}_a \rtimes \mathbb{G}_m$	PGL_2
$H^1(k, \mathrm{Aut}_{\mathfrak{g}/k})$	$\{1\}$	$k^\times / k^{\times(p-1)}$	*singleton*	*subset of* $\mathrm{Br}(k)[2]$

Here, $\mathrm{Br}(k)[2]$ *is the kernel of multiplication by two on the Brauer group.*

Proof. For the first case $\mathfrak{g} = k$, we immediately get $\mathrm{Aut}_{\mathfrak{g}/k} = \mathrm{GL}_1 = \mathbb{G}_m$, and Hilbert 90 gives $H^1(k, \mathbb{G}_m) = \{1\}$, at least for the étale topology. See the discussion at the beginning of Section 7 for the fppf topology.

In the second case, the restricted Lie algebra $\mathfrak{g} = \mathfrak{gl}_1(k)$ is generated by one element A_1, which gives an embedding $\mathrm{Aut}_{\mathfrak{g}/k} \subset \mathbb{G}_m$. The structure for $\mathfrak{g}$ is given by $A_1^{[p]} = A_1$. For each k-algebra R and each invertible scalar $\lambda \in R^\times$, we have $\lambda^p A_1^{[p]} = \lambda A_1$, and thus $\lambda^{p-1} = 1$. Conversely, each such λ gives an automorphism, hence $\mathrm{Aut}_{\mathfrak{g}/k} = \mu_{p-1}$. The Kummer sequence yields $H^1(k, \mathrm{Aut}_{\mathfrak{g}/k}) = k^\times / k^{\times(p-1)}$.

The restricted Lie algebra $\mathfrak{g} = k \rtimes \mathfrak{gl}_1(k)$ is generated inside $\mathfrak{gl}_2(k)$ by the matrices $A_1 = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ and $A_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, which gives an embedding $\mathrm{Aut}_{\mathfrak{g}/k} \subset \mathrm{GL}_2$. For each R-valued point $\varphi = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ from the automorphism group scheme, the condition $[\varphi(A_1), \varphi(A_2)] = \varphi(A_1)$ implies $c = 0$ and $a = ad$. It follows that $a \in R^\times$ and $d = 1$, and we obtain $\mathrm{Aut}_{\mathfrak{g}/k} \subset \mathbb{G}_a \rtimes \mathbb{G}_m$. Conversely, one easily sees that each matrix with $c = 0$ and $d = 1$ yields an automorphism of the restricted Lie algebra. Now, let T be a torsor over k with respect to $\mathbb{G}_a \rtimes \mathbb{G}_m$. The induced $\mathbb{G}_m$-torsor has a rational point, by Hilbert 90. Its preimage $T' \subset T$ is a torsor for $\mathbb{G}_a$. Over any affine scheme, the higher cohomology of $\mathbb{G}_a$ vanishes, so T' also contains a rational point, and the torsor T is trivial.

We come to the last case $\mathfrak{g} = \mathfrak{sl}_2(k)$, which is freely generated by the matrices $A_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $A_2 = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ and $A_3 = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$. This gives an inclusion $\mathrm{Aut}_{\mathfrak{g}/k} \subset \mathrm{GL}_3$. Conjugacy, $A \mapsto SAS^{-1}$, yields $\mathrm{PGL}_2 \subset \mathrm{Aut}_{\mathfrak{g}/k}$. We already saw in the proof for Proposition 2.1 that $A^{[p]} = \det(A)^{(p-1)/2} A$ for all $A = \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$. Moreover, $\det(A) = -a^2 - bc$ defines, up to sign, the standard smooth quadratic form on $\mathfrak{sl}_2(k)$ viewed as the affine space $\mathbb{A}^3$, which gives $\mathrm{Aut}_{\mathfrak{g}/k} \subset O(3)$. We have $\mathrm{PGL}_2 \subset \mathrm{SO}(3)$, because the former is connected, and this inclusion is an equality because both are smooth and three-dimensional. This shows $\mathrm{SO}(3) \subset \mathrm{Aut}_{\mathfrak{g}/k} \subset O(3)$. From $[-A_2, -A_3] = [A_2, A_3] = A_1 \neq -A_1$, we conclude that $A \mapsto -A$ is not an automorphism of $\mathfrak{g}$, so $\mathrm{PGL}_2 = \mathrm{SO}(3) \subset \mathrm{Aut}_{\mathfrak{g}/k}$ must be an equality.

Finally, we have a central extension $0 \to \mathbb{G}_m \to \mathrm{GL}_2 \to \mathrm{PGL}_2 \to 1$, and get maps in nonabelian cohomology

$$H^1(k, \mathrm{GL}_2) \to H^1(k, \mathrm{PGL}_2) \to H^2(k, \mathbb{G}_m).$$

The term on the left is a singleton, by Hilbert 90, whereas the term on the right equals the Brauer group $\mathrm{Br}(k)$. It follows that the coboundary map is injective [Giraud 1971, Chapter IV, Proposition 4.2.8], and its image is contained in the 2-torsion part of the Brauer group [Grothendieck 1968a, Proposition 1.4]. Thus, $H^1(k, \mathrm{Aut}_{\mathfrak{g}/k})$ is a certain subset inside the group $\mathrm{Br}(k)[2]$. □

Note that according to the theorem of Merkurjev [1981], the group $\mathrm{Br}(k)[2]$ is generated by classes from $H^1(k, \mathrm{PGL}_2)$. This set of generators, however, is not a subgroup in general (see [Gille and Szamuely 2006, Example 1.5.7]).

4. Quotients by height-one group schemes

Let k be a ground field of characteristic $p > 0$, and G a height-one group scheme, with restricted Lie algebra $\mathfrak{g}$. Suppose X is a scheme endowed with a G-action. Taking derivatives, we obtain a homomorphism $\mathfrak{g} \to H^0(X, \Theta_{X/k})$ of restricted Lie algebras. According to [Demazure and Gabriel 1970, Chapter II, §7, Proposition 3.10], any such homomorphism comes from a unique G-action. Note that this does not require any finiteness assumption for the scheme X.

We now show that such actions admit a *categorical quotient* in the category (Sch/k) [Mumford et al. 1994, Definition 0.5]. To this end we temporarily change notation and write the schemes in question as pairs, comprising a topological space and a structure sheaf. Our task is to construct the categorical quotient $(Y, \mathscr{O}_Y)$ for the action on $(X, \mathscr{O}_X)$. First, recall that the image $\mathscr{O}_X^p$ of the homomorphism $\mathscr{O}_X \to \mathscr{O}_X$,

where $f \mapsto f^p$, is a quasicoherent $\mathscr{O}_X$-algebra, with algebra structure $f \cdot g^p = (fg)^p$. In turn, the ringed space $(X, \mathscr{O}_X^p)$ is a $\mathbb{F}_p$-scheme. Choose a vector space basis $D_1, \ldots, D_n \in \mathfrak{g}$. The canonical inclusion $\mathscr{O}_X^p \subset \mathscr{O}_X$ turns $\mathscr{O}_X$ into a quasicoherent $\mathscr{O}_X^p$-algebra, and yields the absolute Frobenius morphism $(X, \mathscr{O}_X) \to (X, \mathscr{O}_X^p)$. The derivations $D_i : \mathscr{O}_X \to \mathscr{O}_X$ are $\mathscr{O}_X^p$-linear, and we write $\mathscr{O}_X^{\mathfrak{g}} = \bigcap_{i=1}^n \operatorname{Ker}(D_i)$ for the intersection of kernels. This is another quasicoherent $\mathscr{O}_X^p$-algebra. Setting $Y = X$ and $\mathscr{O}_Y = \mathscr{O}_X^{\mathfrak{g}}$, we obtain a scheme $(Y, \mathscr{O}_Y)$ that is affine over $(X, \mathscr{O}_X^p)$. The identity $\mathrm{id} : X \to Y$ and the canonical inclusion $\iota : \mathscr{O}_Y \subset \mathscr{O}_X$ define a morphism of $\mathbb{F}_p$-schemes

$$(\mathrm{id}, \iota) : (X, \mathscr{O}_X) \to (Y, \mathscr{O}_Y).$$

The following should be well known:

Lemma 4.1. *The above morphism of schemes is a categorical quotient in* (Sch/k). *Moreover, the formation of the quotient is compatible with flat base-change in the scheme* $(Y, \mathscr{O}_Y)$.

Proof. First, note that the inclusion $\mathscr{O}_Y \subset \mathscr{O}_X$ is invariant with respect to multiplication of scalars $\lambda \in k$, so the morphism belongs to the category (Sch/k). Furthermore, the formation of kernels and finite intersections for maps between quasicoherent sheaves on schemes is compatible with flat base-change, and, in particular, the formation of $(Y, \mathscr{O}_Y)$ is compatible with flat base-change.

We now verify the universal property. Let $(T, \mathscr{O}_T)$ be scheme endowed with the trivial G-action, and $(f, \varphi) : (X, \mathscr{O}_X) \to (T, \mathscr{O}_T)$ be an equivariant morphism. Obviously, there is a unique continuous map $g : Y \to T$ with $f = g \circ \mathrm{id}$. The trivial G-action on $(T, \mathscr{O}_T)$ corresponds to the zero map $\mathfrak{g} \to H^0(T, \mathscr{O}_T)$, and equivariance ensures that $f^{-1}(\mathscr{O}_T) \to \mathscr{O}_X$ factors over the injection $\mathscr{O}_Y \subset \mathscr{O}_X$. This gives a unique morphism $(g, \psi) : (Y, \mathscr{O}_Y) \to (T, \mathscr{O}_T)$ of ringed spaces that factors (f, φ). For each point $a \in X$, the local map $\mathscr{O}_{T, f(a)} \to \mathscr{O}_{X,a}$ factors over $\mathscr{O}_{Y,a}$, and it follows that $\psi : \mathscr{O}_{T,g(a)} \to \mathscr{O}_{Y,a}$ is local. Thus, (g, ψ) is a morphism in the category (Sch/k), which shows the universal property. □

We now revert back to the usual notation, and write $Y = X/G$ for the quotient of the action $\mu : G \times X \to X$, with quotient map $q : X \to Y$. Clearly, this map is surjective, Y carries the quotient topology, and the set-theoretical image of $\mu \times \mathrm{pr}_2 : G \times X \to X \times X$ equals the fiber product $X \times_Y X$. By construction, for each open set $U \subset Y$ and each local section $f \in \Gamma(U, q_*(\mathscr{O}_X))$, we have $f \in \Gamma(U, \mathscr{O}_Y)$ if and only if $f \circ \mu = f \circ \mathrm{pr}_2$ as morphisms $G \times q^{-1}(U) \to \mathbb{A}^1$. Summing up, our categorical quotient is also a *uniform geometric quotient*, in the sense of [Mumford et al. 1994, Definition 0.7]. The following observation will be useful:

Proposition 4.2. *Suppose that* X *is integral, with function field* $F = \mathscr{O}_{X,\eta}$. *Then* $\mathscr{O}_{Y,a} = \mathscr{O}_{X,a} \cap (F^{\mathfrak{g}})$ *for each point* $a \in X$. *Moreover, the scheme* Y *is normal provided this holds for* X.

Proof. Set $R = \mathscr{O}_{X,a}$, such that $R^{\mathfrak{g}} = \mathscr{O}_{Y,a}$. Choose a basis $D_1, \dots, D_n \in \mathfrak{g}$, and consider the resulting commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & R^{\mathfrak{g}} & \longrightarrow & R & \longrightarrow & R^{\oplus n} \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & F^{\mathfrak{g}} & \longrightarrow & F & \longrightarrow & F^{\oplus n} \end{array}$$

where the horizontal maps on the right are given by $s \mapsto (D_1(s), \dots, D_n(s))$. The commutativity of the left square gives $R^{\mathfrak{g}} \subset R \cap F^{\mathfrak{g}}$, and the injectivity of the vertical map on the right ensures the reverse inclusion, by a diagram chase. Now suppose that R is normal and $f \in F^{\mathfrak{g}}$ satisfies an integral equation over the subring $R^{\mathfrak{g}}$. This is also an integral equation over R, hence $f \in R \cap F^{\mathfrak{g}} = R^{\mathfrak{g}}$. □

5. Inertia and Jacobson correspondence

The goal of this section is provide a new, more geometric interpretation of the *Jacobson correspondence* [1937; 1944]. We start by recalling this correspondence, which relates certain subfields and restricted Lie algebras, in Bourbaki's formulation [Bourbaki 1990, Chapter V, §13, No. 3, Theorem 3]:

Let F be a field of characteristic $p > 0$. It comes with a subfield F^p and a restricted Lie algebra $\mathfrak{g} = \mathrm{Der}(F)$ over F^p that is also endowed with the structure of an F-vector space. Note that the bracket is F^p-linear, but, in general, not F-bilinear. Rather, we have the formula

$$[\lambda D, \lambda' D'] = \lambda\lambda' \cdot [D, D'] + \lambda D(\lambda') \cdot D' - \lambda' D'(\lambda) \cdot D. \tag{5}$$

Throughout, a subgroup $\mathfrak{h} \subset \mathfrak{g}$ is called an *F^p-subalgebra with F-multiplication* if it is stable under bracket, p-map, and multiplication by scalars $\lambda \in F$. It is thus a restricted Lie algebra over F^p, endowed with the F-multiplication as an *additional structure*. Consider the ordered sets

$$\Phi = \{E \mid F^p \subset E \subset F \text{ is an intermediate field}\},$$
$$\Psi = \{\mathfrak{h} \mid \mathfrak{h} \subset \mathfrak{g} \text{ is an } F^p\text{-subalgebra with } F\text{-multiplication}\}.$$

Similar to classical Galois theory for separable algebraic extensions, one has inclusion-reversing maps $\Phi \to \Psi$ and $\Psi \to \Phi$ given by

$$E \mapsto \mathrm{Der}_E(F) \quad \text{and} \quad \mathfrak{h} \mapsto F^{\mathfrak{h}},$$

respectively. Here, $F^{\mathfrak{h}}$ denotes the intersection of the kernels for $D : F \to F$, where $D \in \mathfrak{h}$ runs over all elements. Then the Jacobson correspondence asserts that the above maps induce a bijection between the intermediate fields $F^p \subset E \subset F$ having $[F : E] < \infty$ and the F^p-subalgebras with F-multiplication $\mathfrak{h} \subset \mathfrak{g}$ having $\dim_F(\mathfrak{h}) < \infty$. Moreover, under this bijection $[F : E] = p^{\dim_F(\mathfrak{h})}$ holds.

In particular, if F has *finite p-degree*, which means that $F^p \subset F$ is finite, we get an unconditional identification

$$\{\text{intermediate fields } E\} = \{F^p\text{-subalgebras } \mathfrak{h} \text{ with } F\text{-multiplication}\}.$$

Forgetting the F-multiplication, the restricted Lie algebra $\mathfrak{h} = \mathrm{Der}_E(F)$ corresponds to a height-one group scheme H, with $\mathfrak{h} = \mathrm{Lie}(H)$. By construction, this coincides with the Frobenius kernel of the affine group scheme $\mathrm{Aut}_{F/E}$.

We now consider the following set-up geared towards geometric applications: Let k be a ground field of characteristic $p > 0$ and F be some extension field; one should think of the function field of some proper integral scheme. Let H be a height-one group scheme over k, with corresponding restricted Lie algebra $\mathfrak{h} = \mathrm{Lie}(H)$. Suppose we have a faithful action of the group scheme H on the scheme $\mathrm{Spec}(F)$, in other words, a homomorphism $\mathfrak{h} \to \mathrm{Der}_k(F)$ that is k-linear and injective. Throughout, we regard this homomorphisms also as an inclusion.

Let $E = F^{\mathfrak{h}}$, such that $\mathfrak{h} \subset \mathrm{Der}_E(F)$. Then the field E contains the composite $k \cdot F^p$, and its spectrum is the categorical quotient $\mathrm{Spec}(F)/H$, according to Lemma 4.1. Moreover, we obtain the subspace $\mathfrak{h} \subset \mathfrak{h} \cdot E \subset \mathfrak{h} \cdot F$ inside $\mathrm{Der}_E(F)$. These are subvector spaces over k and E and F, respectively. Obviously,

$$\dim_F(\mathfrak{h} \cdot F) \leq \dim_E(\mathfrak{h} \cdot E) \leq \dim_k(\mathfrak{h}).$$

Let us unravel how these various fields and vector spaces are related:

Proposition 5.1. *In the above situation, the following holds*:

(i) *The subspace* $\mathfrak{h} \subset \mathrm{Der}_E(F)$ *contains an* F*-basis, such that* $\mathfrak{h} \cdot F = \mathrm{Der}_E(F)$.

(ii) *The canonical inclusions* $E = F^{\mathfrak{h}} \subset F^{\mathfrak{h} \cdot E} \subset F^{\mathfrak{h} \cdot F}$ *are equalities.*

(iii) *The subspace* $\mathfrak{h} \cdot E \subset \mathrm{Der}_E(F)$ *is stable with respect to bracket and* p*-map.*

(iv) *The extension* $E \subset F$ *is finite, of degree* $[F : E] = p^{\dim_F(\mathfrak{h} \cdot F)}$.

Proof. To see (ii), choose a k-generating set $D_1, \ldots, D_n \in \mathfrak{h}$. Clearly, $F^{\mathfrak{h}}$ coincides with the intersection of the $\mathrm{Ker}(D_i : F \to F)$. Since $D_1, \ldots, D_n \in \mathfrak{h} \cdot F$ is an F-generating set as well, this intersection coincides with $F^{\mathfrak{h} \cdot F}$, and the equalities $F^{\mathfrak{h}} = F^{\mathfrak{h} \cdot E} = F^{\mathfrak{h} \cdot F}$ follow.

We next verify that the F-vector subspace $\mathfrak{h} \cdot F \subset \mathrm{Der}_E(F)$ is stable under bracket and p-map. The former follows from (5). The latter is then a consequence of the Hochschild formula [1955, Lemma 1]

$$(vu)^p = v^p u^p + \mathrm{ad}_{vu}^{p-1}(v)u,$$

which holds for any u from an associative $\mathbb{F}_p$-algebra U and v from an ad_u-stable commutative subalgebra V. In turn, $\mathfrak{h} \cdot F \subset \mathrm{Der}_E(F)$ is an F^p-subalgebra with F-multiplication, obviously of finite F-dimension. Now the Jacobson correspondence applied to $E = F^{\mathfrak{h} \cdot F}$ shows (iv). Applying the correspondence once more reveals $\mathfrak{h} \cdot F = \mathrm{Der}_E(F)$, and (i) follows. The above reasoning likewise shows that the E-vector subspace $\mathfrak{h} \cdot E \subset \mathrm{Der}_E(F)$ is stable under bracket and p-map, which reveals (iii). □

We now seek a more geometric understanding of the above facts. Set $\mathfrak{h}_E = \mathfrak{h} \otimes_k E$, and consider the E-linearization $\mathfrak{h}_E \to \mathrm{Der}_E(F)$ of our inclusion $\mathfrak{h} \subset \mathrm{Der}_E(F)$. Write $\mathfrak{h}_E^{\mathrm{triv}} \subset \mathfrak{h}_E$ for the kernel. This is an ideal, giving an inclusion $\mathfrak{h}_E/\mathfrak{h}_E^{\mathrm{triv}} \subset \mathrm{Der}_E(F)$. Now recall that H denotes the height-one group scheme

with $\mathrm{Lie}(H) = \mathfrak{h}$. Write $H_E = H \otimes_k E$ for its base-change, and $H_E^{\mathrm{triv}} \subset H_E$ for the normal subgroup scheme corresponding to $\mathfrak{h}_E^{\mathrm{triv}}$. This acts trivially on $\mathrm{Spec}(F)$, whereas the quotient H_E/H_E^{triv} acts faithfully.

Proposition 5.2. *The action of the group scheme H_E on* $\mathrm{Spec}(F)$ *is transitive.*

Proof. Recall that for any site $\mathcal{C}$, the action of a group-valued sheaf G on a sheaf Z is called *transitive* if the morphism $\mu \times \mathrm{pr}_2 : G \times Z \to Z \times Z$ is an epimorphism, where $\mu : G \times Z \to Z$ denotes the action.

In our situation the site is (Aff/E), endowed with the fppf topology. Set $G = H_E/H_E^{\mathrm{triv}}$ and $Z = \mathrm{Spec}(F)$. We have to check that for any R-valued points $a, b \in Z(R)$, there is an fppf extension $R \subset R'$ and some $\sigma \in G(R')$ that sends the base-change $a \otimes R'$ to $b \otimes R'$. Replacing R by $R \otimes_E F$, we may assume that R is an F-algebra. Choose a p-basis for the extension $E \subset F$, such that

$$F = E[T_1, \ldots, T_r]/(T_1^p - \mu_1, \ldots, T_r^p - \mu_r)$$

for some scalars $\mu_i \in E$. Then

$$F \otimes_E R = R[s_1, \ldots, s_r]/(s_1^p, \ldots, s_r^p)$$

for the elements $s_i = T_i \otimes 1 - 1 \otimes T_i$. The R-valued points of Z thus correspond to $s_i \mapsto \lambda_i$, where $\lambda_i \in R$ satisfy $\lambda_i^p = 0$. It suffices to treat the case that $a, b \in Z(R)$ is given by $s_i \mapsto 0$ and $s_i \mapsto \lambda_i$, respectively.

The differentials $dT_i \in \Omega^1_{F/E}$ form an F-basis. The dual basis inside $\mathrm{Der}_E(F) = \mathrm{Hom}(\Omega^1_{F/E}, F)$ are the partial derivatives $\partial/\partial T_i$. Clearly, we have

$$\left[\frac{\partial}{\partial T_i}, \frac{\partial}{\partial T_j}\right] = \left(\frac{\partial}{\partial T_i}\right)^{[p]} = 0.$$

Consequently, the linear combination $D = \sum \lambda_i \partial/\partial T_i$ satisfies $D^{[p]} = 0$, thus D is an *additive* element inside $\mathrm{Der}_R(F \otimes_E R)$. Note that this would fail with coefficients from $F \otimes_E R$ rather than R. By the Demazure–Gabriel correspondence, it yields a homomorphism of group schemes $\alpha_{p,R} \to \mathrm{Aut}_{F/E} \otimes_E R$.

According to Proposition 5.1 we have $\mathrm{Der}_E(F) = \mathfrak{h} \cdot F$, so there are elements $D_1, \ldots, D_r \in \mathfrak{h} \cdot E = \mathfrak{h}_E/\mathfrak{h}_E^{\mathrm{triv}}$ that form an F-basis of $\mathrm{Der}_E(F)$. In particular, we may write $\sum \lambda_i \partial/\partial T_i = \sum \alpha_i D_i$ for some $\alpha_i \in R$. In turn, we get an additive element $D \in (\mathfrak{h}_E/\mathfrak{h}_E^{\mathrm{triv}}) \otimes_E R$, so our homomorphism of group schemes has a factorization $\alpha_{p,R} \to G_R$. For $R' = R[\sigma]/(\sigma^p)$, we get a canonical element $\sigma \in \alpha_{p,R'}$, whose image is likewise denoted by $\sigma \in G(R')$. By construction, we have

$$\sigma^*(s_j) = D(s_j) = \sum_i \lambda_i \frac{\partial T_j}{\partial T_i} = \lambda_j,$$

for all $1 \leq j \leq n$, and the desired property $\sigma \cdot a = b$ follows. □

Note that the E-scheme $Z = \mathrm{Spec}(F)$ does not contain a rational point, except for $\mathfrak{h} = 0$. The existence of such a point would allow us to form the inertia subgroup scheme and view Z as a *homogeneous space*. However, we can achieve this after further base-change:

Regard $A = F \otimes_E F$ as an F-algebra via $\lambda \mapsto 1 \otimes \lambda$. Then the multiplication map $\lambda \otimes \mu \mapsto \lambda\mu$ yields a canonical retraction. Indeed, A is a local Artin ring with residue field $A/\mathfrak{m}_A = F$. In turn, $Z_F = Z \otimes F$

has a unique rational point $z_0 \in Z_F$. Write $H_F^{\mathrm{inert}} = I(z_0)$ for the resulting *inertia subgroup scheme* inside $H_F = H \otimes_k F$. By the Demazure–Gabriel correspondence, it is given by a Lie subalgebra $\mathfrak{h}_F^{\mathrm{inert}}$ inside $\mathfrak{h}_F = \mathfrak{h} \otimes_k F$, which we call the *inertia Lie algebra*. We now interpret the base change Z_F as a homogeneous space:

Proposition 5.3. *The orbit morphism $H_F \cdot \{z_0\} \to Z_F$ induces an identification $H_F/H_F^{\mathrm{inert}} = \mathrm{Spec}(F \otimes_E F)$. Moreover, the inertia Lie algebra $\mathfrak{h}_F^{\mathrm{inert}}$ is the kernel for the canonical surjection*

$$\mathfrak{h} \otimes_k F \to \mathfrak{h} \cdot F = \mathrm{Der}_E(F).$$

Finally, the degree of the field extension $E \subset F$ can be expressed as $[F : E] = p^c$, where $c \geq 0$ is the codimension of the inertia Lie algebra $\mathfrak{h}_F^{\mathrm{inert}} \subset \mathfrak{h}_F$.

Proof. According to Proposition 5.2, the H_F-action on Z_F is transitive, and it follows that the orbit $H_F \cdot \{z_0\} \to Z_F$ is an epimorphism. By definition of the inertia subgroup scheme, the induced $H_F/H_F^{\mathrm{inert}} \to Z_F$ is a monomorphism. Hence, the latter is an isomorphism. This is a finite scheme, and the F-dimension for the ring of global sections for the homogeneous space is given by p^c. It follows that $[F : E] = p^c$.

It remains to see that the inertia Lie algebra $\mathfrak{h}_F^{\mathrm{inert}}$ coincides with the kernel K of the canonical surjection $\mathfrak{h}_F \to \mathfrak{h} \cdot F$. We saw in Proposition 5.1 and the preceding paragraph that

$$p^{\dim_F(\mathfrak{h} \cdot F)} = [F : E] = h^0(\mathscr{O}_Z \otimes_E F) = p^{\dim(\mathfrak{h}_F/\mathfrak{h}_F^{\mathrm{inert}})}.$$

It thus suffices to verify that the canonical map $\mathfrak{h}_F^{\mathrm{inert}} \to \mathrm{Der}_E(F)$ is zero. Suppose this is not the case, and fix some nonzero $D \in \mathfrak{h}_F^{\mathrm{inert}}$ with nonzero image. Choose a p-basis for $E \subset F$ and write

$$F = E[T_1, \ldots, T_r]/(T_1^p - \mu_1, \ldots, T_r^p - \mu_r)$$

for some scalars $\mu_i \in E^\times$. The partial derivatives $\partial/\partial T_i \in \mathrm{Der}_E(F)$ form another F-basis, and $D = \sum \lambda_i \partial/\partial T_i$. Without restriction, we may assume $\lambda_1 \neq 0$. Now make a base-change to $R = F$, such that

$$A = F \otimes_E F = R[s_1, \ldots, s_r]/(s_1^p, \ldots, s_r^p)$$

as in the proof for Proposition 5.2. Then $D(s_1) = \lambda_1 \otimes 1 \notin \mathfrak{m}_A$. But this implies that H_F^{inert} does not fix the closed point $z_0 \in Z_F = \mathrm{Spec}(A)$, a contradiction. □

6. Foliation rank

Throughout this section, k is a ground field of characteristic $p > 0$ and X is a proper scheme. Note that everything carries over verbatim to proper algebraic spaces. Let $H = \mathrm{Aut}_{X/k}[F]$ be the resulting height-one group scheme, whose restricted Lie algebra is $\mathfrak{h} = H^0(X, \Theta_{X/k})$. To simplify exposition, we also assume that X is integral. Let $\eta \in X$ be the generic point and $F = k(X)$ be the function field. The quotient $Y = X/H$ is integral as well, and we denote its function field by $E = k(Y)$. This field extension $E \subset F$ is finite and purely inseparable. This yields a numerical invariant:

Definition 6.1. The *foliation rank* of the proper integral scheme X is the integer $r \geq 0$ defined by the formula $\deg(X/Y) = p^r$.

In other words, we have $[F : E] = p^r$. Since the field extension $E \subset F$ has height one, the foliation rank $r \geq 0$ is also given by $r = \dim_F(\Omega^1_{F/E})$, which can also be seen as the rank of the coherent sheaf $\Omega^1_{X/Y}$. Dualizing the surjection $\Omega^1_{X/k} \to \Omega^1_{X/Y}$ gives an inclusion $\mathscr{F} = \Theta_{X/Y} \subset \Theta_{X/k}$. The subsheaf $\mathscr{F}$ is closed under Lie brackets and p-maps, hence constitutes a *foliation*, where the integer $\operatorname{rank}(\mathscr{F}) = \operatorname{rank}(\Omega^1_{X/Y})$ coincides with our foliation rank $r \geq 0$.

To obtain an interpretation of the foliation rank in terms of group schemes, consider the restricted Lie algebras

$$\mathfrak{h} = \operatorname{Lie}(H) = H^0(X, \Theta_{X/k}) \quad \text{and} \quad \mathfrak{g} = \operatorname{Der}_E(F) = \Theta_{X/Y,\eta}.$$

The former is finite-dimensional over the ground field k. The latter is finite-dimensional over the function field E, and can be seen as the Lie algebra for the automorphism group scheme for $\operatorname{Spec}(F)$ viewed as a finite E-scheme. The localization map $\mathfrak{h} = H^0(X, \Theta_{X/k}) \to \Theta_{X/k,\eta}$ respects brackets and p-powers, and factors over the subalgebra $\mathfrak{g} = \Theta_{X/Y,\eta}$. This gives a k-linear map $\mathfrak{h} \to \mathfrak{g}$, together with its E-linearization

$$\mathfrak{h} \otimes_k E \longrightarrow \mathfrak{g}, \quad \delta \otimes \lambda \longmapsto \big(f \mapsto \lambda \delta_\eta(f)\big).$$

The latter is a homomorphism of restricted Lie algebras over E. The map $\mathfrak{h} \to \mathfrak{g}$ is injective, because the coherent sheaf $\Theta_{X/k}$ is torsion free, and we often view it as an inclusion $\mathfrak{h} \subset \mathfrak{g}$. Note, however, that its E-linearization in general is *neither injective nor surjective*. This is perhaps the main difference to the classical situation of group actions rather than group scheme actions.

We are now in the situation studied in Section 5. Let $\mathfrak{h}^{\text{inert}}_F$ be the inertia Lie algebra inside the base-change $\mathfrak{h}_F = \mathfrak{h} \otimes_k F$, corresponding to the inertia group scheme with respect to the F-rational point in $\operatorname{Spec}(F \otimes_E F)$. From Proposition 5.3, we obtain:

Proposition 6.2. *The foliation rank $r \geq 0$ of the scheme X coincides with the codimension of $\mathfrak{h}^{\text{inert}}_F \subset \mathfrak{h}_F$.*

In some sense, this measures how free the Frobenius kernel of the automorphism group scheme acts generically.

Proposition 6.3. *The foliation rank of the scheme X satisfies $0 \leq r \leq h^0(\Theta_{X/k})$. We have $r = 0$ if and only if the Frobenius kernel $H = \operatorname{Aut}_{X/k}[F]$ vanishes. The condition $r = h^0(\Theta_{X/k})$ holds if and only if H acts freely on some dense open set $U \subset X$.*

Proof. The inequality $r \leq h^0(\Theta_{X/k})$ follows from Proposition 6.2. If the group scheme H is trivial we have $h^0(\Theta_{X/k}) = 0$, and hence $r = 0$. Conversely, if H is nontrivial there is a nonzero derivation $D : \mathscr{O}_X \to \mathscr{O}_X$. Since the structure sheaf is torsion-free, the derivation remains nonzero at the generic point, which implies that $E = F^{\mathfrak{h}}$ does not coincide with F, and thus $r > 0$.

If H acts freely on some dense open set, the projection $\epsilon : X \to Y$ to the quotient $Y = X/H$ is a principal homogeneous H-space over the dense open set $V \subset Y$ corresponding to U. In turn $[F : E] = h^0(\mathscr{O}_H)$, and thus $r = \dim(\mathfrak{h}) = h^0(\Theta_{X/k})$.

Finally, suppose the foliation rank takes the maximal possible value $r = h^0(\Theta_{X/k})$. Then the inertia Lie algebra $\mathfrak{h}_F^{\mathrm{inert}} \subset \mathfrak{h}_F$ has codimension $r = \dim(\mathfrak{h}_F)$, thus is trivial. It follows that the group scheme H_E acts freely on $\mathrm{Spec}(F)$ viewed as an E-scheme. Thus, there is an open dense set $V \subset Y$ over which the projection $\epsilon : X \to Y$ becomes a principal homogeneous H-space, and the H-action on $U = \epsilon^{-1}(V)$ is free. □

We next describe how the foliation rank behaves under birational maps.

Proposition 6.4. *Let $f : X \to X'$ be a birational morphism to another proper integral scheme X', with the property $\mathscr{O}_{X'} = f_*(\mathscr{O}_X)$. Then the respective foliation ranks satisfy $r \leq r'$.*

Proof. According to Blanchard's lemma, there is a unique homomorphism

$$f_* : \mathrm{Aut}^0_{X/k} \to \mathrm{Aut}^0_{X'/k}$$

of group schemes making the morphism $f : X \to X'$ equivariant. Indeed, the original form of the lemma for complex-analytic spaces [Blanchard 1956, Proposition I.1] was extended to schemes by Brion, Samuel and Uma [Brion et al. 2013, Proposition 4.2.1].

The homomorphism of group schemes is a monomorphism, because f is birational, and the schemes in question are integral. In particular, the induced homomorphism on Frobenius kernel gives a closed embedding $H \subset H'$, and an injection $\mathfrak{h} \subset \mathfrak{h}'$ of restricted Lie algebras. For the common function field $F = k(X) = k(X')$, we get $F^{\mathfrak{h}} \supset F^{\mathfrak{h}'}$, and $r \leq r'$ follows. □

The following gives an upper bound on the foliation rank:

Proposition 6.5. *Let $i \geq 0$ be some integer, and suppose that the coherent sheaf $\mathscr{F} = \underline{\mathrm{Hom}}(\Omega^i_{X/k}, \mathscr{O}_X)$ satisfies $h^0(\mathscr{F}) = 0$. Then X has foliation rank $r < i$.*

Proof. We have to show that the vector space $\mathfrak{h} \cdot F = \mathrm{Der}_E(F)$ has dimension at most $i - 1$. Seeking a contradiction, we suppose that there are k-derivations $D_1, \ldots, D_i : \mathscr{O}_X \to \mathscr{O}_X$ that are F-linearly independent. Then the same holds for the corresponding $\mathscr{O}_X$-linear maps $s_1, \ldots, s_i : \mathscr{O}_X \to \Theta_{X/k}$. Consequently, their wedge product $s_1 \wedge \cdots \wedge s_i : \mathscr{O}_X \to \Lambda^i(\Theta_{X/k})$ is generically nonzero. The universal property of exterior powers gives a canonical map $\Lambda^i(\Theta_{X/k}) \to \underline{\mathrm{Hom}}(\Omega^i_{X/k}, \mathscr{O}_X) = \mathscr{F}$, which is generically bijective. Thus $s_1 \wedge \cdots \wedge s_i$ yield a nonzero global section of $\mathscr{F}$, a contradiction. □

Recall that our proper integral X comes with a *dualizing sheaf* ω_X and a *trace map* $H^n(X, \omega_X) \to k$, such that the ensuing pairing $\mathrm{Hom}(\mathscr{F}, \omega_X) \times H^n(X, \mathscr{F}) \to k$ is nondegenerate. Here, $n = \dim(X)$ and $\mathscr{F}$ is coherent.

Corollary 6.6. *Let X be a geometrically normal surface with $h^0(\omega_X^\vee) = 0$. Then the foliation rank is $r \leq 1$.*

Proof. Replacing the ground field k by the field $H^0(X, \mathscr{O}_X)$, it suffices to treat the case $h^0(\mathscr{O}_X) = 1$. By Serre's criterion, the scheme X is regular in codimension one, so the locus of nonsmoothness $\mathrm{Sing}(X/k)$

is finite. Let $f : S \to X$ be a resolution of singularities. Suppose for the moment that the regular surface S is smooth. Then $\omega_S = \Omega^2_{S/k}$. Consider the chain of canonical maps

$$\Omega^2_{X/k} \to f_* f^*(\Omega^2_{X/k}) \to f_*(\Omega^2_{S/k}) \to f_*(\omega_S) \to \omega_X,$$

where to the right is the trace map. All these maps are bijective on the complement $U = X \smallsetminus \mathrm{Sing}(X/k)$, so the same holds for the dual map

$$\varphi : \omega_X^\vee \to \underline{\mathrm{Hom}}\big(\Omega^2_{X/k}, \mathscr{O}_X\big) = \mathscr{F}.$$

According to [Hartshorne 1994, Corollary 1.8 and Theorem 1.9], these rank-one sheaves are reflexive and satisfy the Serre condition (S_2). Since $\varphi|U$ is bijective, already φ is bijective, by loc. cit. Theorem 1.12. The assertion thus follows from the theorem.

It remains to treat the case that the ground field k is imperfect. Choose a perfect closure k'. The base-change $X' = X \otimes_k k'$ is normal, and the above reasoning applies to any resolution of singularities $S' \to X'$. It follows that $\omega_X^\vee$ and $\mathscr{F}$ become isomorphic after base-changing to k'. If follows that $\mathrm{Hom}(\omega_X, \mathscr{F})$ is one-dimensional. Choose a nonzero element $\varphi : \omega_X \to \mathscr{F}$. Then $\varphi \otimes k'$ must be bijective, and by descent the same holds for φ. □

This applies in particular to smooth surfaces S of Kodaira dimension $\mathrm{kod}(S) \geq 1$, which comprise surfaces of general type, and the properly elliptic surfaces, including those with quasielliptic fibration. It also applies to surfaces S with Kodaira dimension zero, provided that the dualizing sheaf of the minimal model X is nontrivial.

Let S be a smooth surface of general type, and X be its canonical model. This is the homogeneous spectrum $P(S, \omega_S)$ of the graded ring $R(S, \omega_S) = \oplus H^0(S, \omega_S^{\otimes t})$. Then X is normal, the singularities are at most rational double points and the dualizing sheaf ω_X is ample. We also say that X is a *canonically polarized surfaces*. Obviously $h^0(\omega_X^{\otimes -1}) = 0$, and X has foliation rank $r \leq 1$. According to Proposition 6.4, the same holds for S.

Proposition 6.7. *Suppose that X has foliation rank $r = 1$, and let $D \in H^0(X, \Theta_{X/k})$ be any nonzero global section. Then for each point $x \in X$, the local ring $\mathscr{O}_{Y,\epsilon(x)}$ is the kernel for the additive map $D : \mathscr{O}_{X,x} \to \mathscr{O}_{X,x}$.*

Proof. Set $y = \epsilon(x)$. The local ring is given by $\mathscr{O}_{Y,y} = \mathscr{O}_{X,x}^{\mathfrak{h}}$, which is contained in the kernel $\mathscr{O}_{X,x}^D$ of the derivation D. Let $f \in \mathscr{O}_{X,x}^D$, and $D' \in \mathfrak{h}$ be another derivation. Then $D' = \lambda D$ for some element λ from the function field $F = \mathrm{Frac}(\mathscr{O}_{X,x})$, and thus $D'(f) = \lambda D(f) = 0$ inside F. Since the localization map $\mathscr{O}_{X,x} \to F$ is injective, we already have $D'(f) = 0$ inside $\mathscr{O}_{X,x}$. This shows $f \in \mathscr{O}_{Y,y}$. In turn, the inclusion $\mathscr{O}_{Y,y} \subset \mathscr{O}_{X,x}^D$ is an equality. □

We will later see that for $r = 1$, each vector in $\mathfrak{g}$ is p-closed. Thus the nonzero elements $D \in \mathfrak{h}$ indeed yield height-one group schemes $N \subset H$ of order $|N| = p$, such that $Y = X/N$.

7. Invariant subspaces

Let k be a ground field of characteristic $p \geq 0$ and V be a finite-dimensional vector space of dimension $n \geq 0$. Let us write $\mathrm{GL}_{V/k}$ for the group-valued functor on the category (Aff/k) of affine k-schemes $T = \mathrm{Spec}(R)$ defined by

$$\mathrm{GL}_{V/k}(R) = \mathrm{Aut}_R(V \otimes_k R).$$

This satisfies the sheaf axiom with respect to the fppf topology. In fact, it is representable by an affine group scheme, and the choice of a basis $e_1, \ldots, e_n \in V$ yields $\mathrm{GL}_{V/k} \simeq \mathrm{GL}_{n,k}$.

Let us write $\underline{V}$ for the abelian functor whose group of R-valued points is $\underline{V}(R) = V \otimes_k R$. As explained in [Grothendieck 1960, Chapter I, Section 9.6], this is represented by an affine scheme, namely the spectrum of the symmetric algebra on the dual vector space V^*. Moreover, the structure morphism $\underline{V} \to \mathrm{Spec}(k)$ carries the structure of a *vector bundle* of rank n with $\underline{V}(k) = V$, and the canonical homomorphism $\mathrm{GL}_{V/k} \to \mathrm{Aut}_{\underline{V}/k}$ of group schemes is bijective. Combining [Grothendieck 1968b, Theorem 11.7] with [Artin et al. 1972, Exposé VIII, Corollary 2.3], and [Bourbaki 1990, Chapter V, §10, No. 5, Proposition 9], one sees that each $\mathrm{GL}_{V/k}$-torsor is trivial, that is, the nonabelian cohomology set $H^1(k, \mathrm{GL}_{V/k})$ with respect to the fppf topology is a singleton. In other words, all vector bundles $E \to \mathrm{Spec}(k)$ of rank n are isomorphic to $\underline{V}$.

Now, let $H \subset \mathrm{GL}_{V/k}$ be a subgroup scheme and $T \to \mathrm{Spec}(k)$ be a H-torsor. Then the quotient

$$^T\underline{V} = H\backslash(T \times \underline{V}) = T \wedge^H \underline{V}$$

with respect to the diagonal action $\sigma \cdot (t, v) = (\sigma t, \sigma v)$ is another vector bundle called the *T-twist*. Note that under the identification of left and right action, the above action can also be viewed as $\sigma \cdot (t, v) = (t\sigma^{-1}, \sigma v)$, which explains the notation $T \wedge^H \underline{V}$. *We now consider the following general problem*: *What subbundles exist in the T-twist whose pull-back to T are contained in the pullback of a fixed subbundle $\underline{V}' \subset \underline{V}$?* By fppf descent, these pullbacks correspond to subbundles inside the induced bundle $\underline{V} \times T \to T$ whose total space is invariant with respect to the diagonal H-action.

The n-dimensional vector space $^TV = (^T\underline{V})(k)$ of k-rational points is likewise called the *T-twist* of V. If H is finite and $T = \mathrm{Spec}(L)$ is the spectrum of a field, we are thus looking for k-vector subspaces $U \subset {}^TV$ such that $U \otimes_k L$ is contained in the base-change $V' \otimes_k L$, or equivalently to L-vector subspaces in $V' \otimes_k L$ that are invariant for the diagonal H-action.

Suppose that $p > 0$, and that $H = \alpha_p$ is the *infinitesimal group scheme* defined by $H(R) = \{\alpha \in R \mid \alpha^p = 0\}$, where the group law is given by addition. Recall that the Lie algebra of $\mathrm{GL}_{V/k}$ is the vector space $\mathfrak{gl}(V) = \mathrm{End}_k(V)$, where the Lie bracket is given by commutators $[f, g] = fg - gf$ and the p-map $f^{[p]} = f^p$ is the p-fold composition. The inclusion homomorphism $H \to \mathrm{GL}_{V/k}$ corresponds to a vector $f \in \mathfrak{gl}(V)$ that is nilpotent, with all Jordan blocks of size $\leq p$. On R-valued points, the map becomes

$$H(R) \to \mathrm{GL}_{V/k}(R), \quad \alpha \mapsto \sum_{i=0}^{p-1} \frac{(\alpha f)^i}{i!}.$$

Set $e^{\alpha f} = \sum_{i=0}^{p-1} (\alpha f)^i / i!$ to simplify notation. By naturality, the above maps are determined by the single matrix e^{tf} with entries in the truncated polynomial ring $R = k[t]/(t^p)$. The following is well known:

Lemma 7.1. *Each torsor T for the infinitesimal group scheme $H = \alpha_p$ is isomorphic to the spectrum of $L = k[s]/(s^p - \omega)$ for some $\omega \in k$, where the group elements $\alpha \in H(R)$ act via $s \mapsto s + \alpha$. The torsor T is nontrivial if and only if L is a field. Moreover, for each purely inseparable field extension $k \subset L$ of degree p, the spectrum* Spec(L) *admits the structure of a H-torsor.*

Proof. Consider the relative Frobenius map $F : \mathbb{G}_a \to \mathbb{G}_a$ on the additive group, which comes from the k-linear map $k[t] \to k[t]$ given by $t \mapsto t^p$. Then $H = \alpha_p$ is the kernel. The short exact sequence $0 \to H \to \mathbb{G}_a \xrightarrow{F} \mathbb{G}_a \to 0$ yields a long exact sequence

$$k \to k \to H^1(k, H) \to H^1(k, \mathbb{G}_a) \to H^1(k, \mathbb{G}_a).$$

The terms on the right vanish. It follows that each H-torsor T arises as the fiber for $F : \mathbb{G}_a \to \mathbb{G}_a$ over some rational point $\omega \in \mathbb{G}_a(k)$. Thus T is equivariantly isomorphic to the spectrum of $k[s]/(s^p - \omega)$, where the group elements $\alpha \in H(R)$ act via $s \mapsto s + \alpha$. If T is nontrivial, the polynomial $s^p - \omega \in k[s]$ has no root in k. We infer that it is irreducible, because the algebra $L = k[s]/(s^p - \omega)$ has prime degree p. Thus L is a field, which is purely inseparable over k. Conversely, if L is a field, then T has no rational point, and the torsor is nontrivial.

Finally, let $k \subset L$ be a purely inseparable extension of degree p. For each element in L not contained in k, we get an identification $L = k[s]/(s^p - \omega)$. Thus, Spec(L) arises as fiber of the relative Frobenius map, and hence admits the structure of a H-torsor. □

For the applications we have in mind, we now consider the particular situation that $V = k[t]/(t^p)$ is the underlying vector space of dimension $n = p$ coming from the truncated polynomial ring, and $V' = tk[t]/(t^p)$ is given by the maximal ideal. Each vector can be uniquely written as a polynomial $f(t) = \sum_{i=0}^{p-1} \lambda_i t^i$, with coefficients $\lambda_i \in k$. This vector space comes with a canonical action of the additive group $\mathbb{G}_a$, where the elements $\alpha \in \mathbb{G}_a(R) = R$ act via $f(t) \mapsto f(t + \alpha)$. With respect to the canonical basis $t^0, \ldots, t^{p-1} \in V \otimes_k R$, this automorphism is given by $\alpha \mapsto (\alpha_{ij})$, where the matrix entries are $\alpha_{ij} = \binom{j}{j-i} \alpha^{j-i}$. In turn, we get an induced action of the Frobenius kernel $H = \alpha_p$. Note that $V' \subset V$ is not H-invariant, because some $\alpha_{0j} = \alpha^j$ are nonzero for $\alpha \neq 0$.

Now, let $T = \text{Spec}(L)$ be a H-torsor. The resulting twist ${}^T V$ is another vector space of dimension $n = p$. Note that both V and ${}^T V$ are isomorphic to $k^{\oplus p}$, but there is no canonical isomorphism. The following observation will be crucial for later applications:

Proposition 7.2. *In the above situation, there is no vector $x \neq 0$ inside the twist ${}^T V$ such that the induced element $x \otimes 1$ inside ${}^T V \otimes_k L = V \otimes_k L$ is contained in the base change $V' \otimes_k L$.*

Proof. Seeking a contradiction, we assume that such an element exists. Its image $x \otimes 1$ inside ${}^T V \otimes_k L = V \otimes_k L$ takes the form $f(t) = \sum_{i=1}^{p-1} \lambda_i t^i$, with coefficients $\lambda_i \in L$. According to Lemma 7.1, we have $L = k[s]/(s^p - \omega)$ for some $\omega \in k$, and the group elements $\alpha \in H(R)$ act via $s \mapsto s + \alpha$.

Write $\lambda_i = \sum_{j=0}^{p-1} \lambda_{ij} s^j$, with coefficients $\lambda_{ij} \in k$. The H-invariance of the vector $f(t) \in V \otimes_k L$ with respect to the diagonal H-action means

$$\sum_{i=1}^{p-1} \sum_{j=0}^{p-1} \lambda_{ij} (s+\alpha)^j (t+\alpha)^i = \sum_{i=1}^{p-1} \sum_{j=0}^{p-1} \lambda_{ij} s^j t^i \tag{6}$$

for each $\alpha \in H(R)$. Our task is to infer $\lambda_{ij} = 0$. We now consider the universal situation, where α is the class of the indeterminate in the truncated polynomial ring $R = k[u]/(u^p)$. Then (6) becomes an equation in the residue class ring $k[t, s, u]/(t^p, s^p - \omega, u^p)$. Writing

$$(s+\alpha)^j (t+\alpha)^i = s^j t^i + \alpha(j s^{j-1} t^i + i s^j t^{i-1}) + \alpha^2(\cdots)$$

as a polynomial in α and comparing coefficients in (6) at the linear terms, we get

$$\sum_{i=1}^{p-1} \sum_{j=0}^{p-1} \lambda_{ij} (j s^{j-1} t^i + i s^j t^{i-1}) = 0. \tag{7}$$

The following argument, more elegant than our original reasoning, was indicated by the referee: To see that λ_{ij} vanishes, it suffices to check that the polynomial

$$F = \sum_{i=1}^{p-1} \sum_{j=0}^{p-1} \lambda_{ij} s^j t^i$$

is divisible by t^h for $1 \leq h \leq p$ inside the factorial ring $k[s, t]$. This is obvious for $h = 1$. Suppose now that $2 \leq h \leq p$, and that $F = t^{h-1} G$ for some polynomial G. Then

$$\frac{\partial F}{\partial s} = t^{h-1} \frac{\partial G}{\partial s} \quad \text{and} \quad \frac{\partial F}{\partial t} = t^{h-1} \frac{\partial G}{\partial t} + (h-1) t^{h-2} G.$$

Equation (7) means that $\partial F/\partial s + \partial F/\partial t = 0$. Together with the above computation, this gives $t \mid G$, and hence $t^h \mid F$. □

8. Automorphisms for prime-degree radical extensions

Let k be a ground field of characteristic $p > 0$. For each scalar $\omega \in k$, write

$$L = L_\omega = k[t]/(t^p - \omega)$$

for the resulting finite algebra of rank p. Each element can be uniquely written as $\sum_{i=0}^{p-1} \lambda_i t^i$, and we call such expressions *truncated polynomials*. Write $\mathrm{Aut}_{L/k}$ for the group-valued functor on the category (Aff/k) whose R-valued points are the R-linear automorphisms of $L \otimes R$. This functor is representable by an affine group scheme. In this section, we make a detailed study of the opposite group scheme

$$G = G_\omega = \mathrm{Aut}_{\mathrm{Spec}(L_\omega)/k} = (\mathrm{Aut}_{L_\omega/k})^{\mathrm{op}},$$

which comprises the automorphisms of the affine scheme $\mathrm{Spec}(L)$. We shall see that G is nonsmooth, so understanding the scheme structure is of paramount importance. Note that the Lie algebras $\mathfrak{g} = \mathrm{Lie}(G)$

were discovered by Witt, compare the discussions in [Chang 1941, Introduction] and also [Zassenhaus 1939, footnote on p. 3]. These so-called *Witt algebras* will be studied in the next section.

Any automorphism $g : L \otimes_k R \to L \otimes_k R$ is determined by the image of the generator t, which is some truncated polynomial $\varphi_g(t) = \sum_{i=0}^{p-1} \alpha_i t^i$. The multiplication $gh \in G(R)$ of group elements corresponds to the substitution $\varphi_h(\varphi_g(t))$ of truncated polynomials.

The inverse group element g^{-1} defines another truncated polynomial $\varphi_{g^{-1}} = \sum_{i=0}^{p-1} \beta_i t^i$, such that $\sum \alpha_i \big(\sum \beta_j t^j\big)^i = t = \sum \beta_i \big(\sum \alpha_j t^j\big)^i$. Note, however, that the truncated polynomials attached to group elements are never units in the polynomial ring $R[t]$, unless $R = 0$. To avoid this ambiguity in notation we use the additional symbol $\varphi_g(t)$ to denote the image of the indeterminate under $g \in G(R)$.

The coefficients in the truncated polynomials $\varphi_g(t) = \sum_{i=0}^{p-1} \lambda_i t^i$ for the group elements $g \in G(R)$ define a monomorphism $G \to \mathbb{A}^p$.

Proposition 8.1. *The monomorphism $G \to \mathbb{A}^p$ is an embedding, and its image is the intersection of the closed set defined by the Fermat equation*

$$\lambda_0^p + (\lambda_1 - 1)^p \omega + \lambda_2^p \omega^2 + \ldots + \lambda_{p-1}^p \omega^{p-1} = 0, \tag{8}$$

with the open set given by $\det(\alpha_{ij}) \neq 0$. *Here the matrix entries come from the truncated polynomials* $\big(\sum \lambda_i t^i\big)^j = \sum \alpha_{ij} t^i$, *with* $0 \leq i, j \leq p-1$.

Proof. For each $g \in G(R)$, with truncated polynomial $\varphi_g(t) = \sum \lambda_i t^i$, the images $\big(\sum \lambda_i t^i\big)^j$ of the basis vectors t^j form a R-basis of $L \otimes R$, thus $G \to \mathbb{A}^p$ factors over the open set $U \subset \mathbb{A}^p$ given by $\det(\alpha_{ij}) \neq 0$. Since $t^p = \omega$, we also have $\big(\sum \lambda_i t^i\big)^p = \omega$, so the monomorphism also factors over the closed set $Z \subset \mathbb{A}^p$ defined by (8). Any tuple $(\lambda_0, \ldots, \lambda_{p-1}) \in \mathbb{A}^p(R)$ lying in $U \cap Z$ gives, via the truncated polynomial $\sum \lambda_i t^i$, some group element $g \in G(R)$. It follows that the monomorphism $G \to \mathbb{A}^p$ is an embedding, with image $U \cap Z$. □

Note that throughout, we regard the coefficients λ_i either as scalars or as indeterminates, depending on the context. This abuse of notation simplifies exposition and should not cause confusion.

Proposition 8.2. *The neutral element $e \in G$ has coordinates* $(0, 1, 0, \ldots, 0)$ *with respect to the embedding $G \subset \mathbb{A}^p$. If the scalar $\omega \in k$ is not a p-power, then the group of rational points is $G(k) = \{e\}$.*

Proof. The truncated polynomial of the neutral element is $\varphi_e(t) = t$, which gives the coordinates of $e \in G$. Now suppose that $\omega \notin k^p$. By Proposition 8.1, it suffices to verify that the polynomial equation $\omega^0 T_0^p + \omega^1 T_1^p + \ldots + \omega^{p-1} T_{p-1}^p = 0$ has no nontrivial solution. The latter means that $1, \omega, \ldots, \omega^{p-1} \in k$ are linearly independent over k^p. This indeed holds, because $k^p \subset k$ is an extension of height ≤ 1, hence the minimal polynomial of any $\lambda \in k$ not contained in k^p is of the form $T^p - \lambda^p$. □

We now consider the Frobenius pullback $G^{(p)}$ and its reduced part $G^{(p)}_{\mathrm{red}} = (G^{(p)})_{\mathrm{red}}$. Note that over imperfect fields, reduced parts of group schemes may fail to be subgroup schemes, see [Fanelli and Schröer 2020, Proposition 1.6] for an example. The following shows that even if it is a subgroup scheme,

it might be nonnormal. Note that this phenomenon seems to be the crucial ingredient for the main results of this paper.

Proposition 8.3. *The reduced part $G^{(p)}_{\mathrm{red}} \subset G^{(p)}$ is a nonnormal subgroup scheme. Moreover, $G^{(p)}_{\mathrm{red}} \simeq U \rtimes \mathbb{G}_m$, where U has a composition series of length $p-2$ whose quotients are isomorphic to the additive group $\mathbb{G}_a$. In particular, G is affine, irreducible, and of dimension $p-1$.*

Proof. Recall that $G^{(p)}$ is defined as the base-change of G with respect to the absolute Frobenius map on $\mathrm{Spec}(k)$. Clearly, the Frobenius pullback of $L_\omega = k[t]/(t^p - \omega)$ is isomorphic to $L_0 = k[t]/(t^p)$, and for our automorphism group schemes this means $G^{(p)} \simeq G_0$. Thus, we may assume $\omega = 0$, and work with $G = G^{(p)}$.

The embedding $G \subset \mathbb{A}^p$ in Proposition 8.1 is now given by the conditions $\lambda_0^p = 0$ and $\det(\alpha_{ij}) \neq 0$. View the entries of the matrix (α_{ij}) as elements from the ring $A = k[\lambda_0, \ldots, \lambda_{p-1}]/(\lambda_0^p)$. Taken modulo the radical $\mathrm{Rad}(A) = (\lambda_0)$, the matrix takes lower triangular form, with diagonal entries $1, \lambda_1, \ldots, \lambda_1^{p-1}$. In turn, the embedding $G \subset \mathbb{A}^p$ is given by $\lambda_0^p = 0$ and $\lambda_1 \neq 0$. Consequently, the reduced part G_{red} is defined by $\lambda_0 = 0$ and $\lambda_1 \neq 0$, which is smooth. Moreover, we see that G is affine, irreducible and of dimension $p-1$.

Given two truncated polynomials $\varphi_g = \sum \alpha_i t^i$ and $\varphi_h = \sum \beta_i t^i$ with constant terms $\alpha_0 = \beta_0 = 0$, the substitution $\varphi_g(\varphi_h(t))$ also has constant term zero, so the subsets $G_{\mathrm{red}}(R) \subset G(R)$ are subgroups. Over $R = k[u, v, \epsilon]/(uv - 1, \epsilon^2)$, the truncated polynomials $\varphi_g = \epsilon + t$ and $\varphi_h = ut$ yield

$$\varphi_{g^{-1}}(t) = -\epsilon + t \quad \text{and} \quad \varphi_{g^{-1}}(\varphi_h(\varphi_g(t))) = \epsilon(u-1) + ut,$$

so the subgroup $G_{\mathrm{red}}(R) \subset G(R)$ fails to be normal.

Summing up, $G_{\mathrm{red}} \subset G$ is a smooth nonnormal subgroup scheme. The map $\sum_{i=1}^{p-1} \lambda_i t^i \mapsto \lambda_1$ defines a short exact sequence

$$0 \to U \to G_{\mathrm{red}} \to \mathbb{G}_m \to 0.$$

The inclusion $U \subset \mathbb{A}^p$ is given by $\lambda_0 = 0$ and $\lambda_1 = 1$, hence the underlying scheme of U is a copy of the affine space $\mathbb{A}^{p-2}$. By Lazard's theorem [Demazure and Gabriel 1970, Chapter IV, §4, 4.1], the group scheme U admits a composition series whose quotients are isomorphic to the additive group $\mathbb{G}_a$. Moreover, the projection $G_{\mathrm{red}} \to \mathbb{G}_m$ has a section via $\lambda_1 \mapsto \lambda_1 t$. This is a homomorphism, hence G_{red} is a semidirect product. □

Clearly, the group elements $g \in G(R)$ with linear truncated polynomial $\varphi_g = \lambda_0 + \lambda_1 t$ form a closed subgroup scheme $B \subset G$. It sits in a short exact sequence

$$0 \to \alpha_p \to B \to \mathbb{G}_m \to 0, \tag{9}$$

where the map on the left is given by $\lambda_0 \mapsto \lambda_0 + t$ and the map on the right comes from $\lambda_0 + \lambda_1 t \to \lambda_1$. In particular, B is a connected solvable group scheme. We see later that B is maximal with respect to this property, so one may regard it as a Borel group. However, we want to stress that this lies in a nonsmooth group scheme, and B itself is nonreduced. We, therefore, call $B \subset G$ a *nonreduced Borel group*.

An element $\lambda_1 \in \mathbb{G}_m(R)$ lies in the image if and only if $\lambda_0 = (1-\lambda_1)\omega^{1/p}$ exists in R. It follows that the extension (9) splits if and only if $\omega \in k$ is a p-power. Moreover, we see that the canonical map $\mathbb{G}_m \to \mathrm{Aut}_{\alpha_p/k} = \mathbb{G}_m$ is the identity. Note that the group of all such extension of $\mathbb{G}_m$ by α_p, with nontrivial $\mathbb{G}_m$-action, is identified with k/k^p, according to [Demazure and Gabriel 1970, Chapter III, §6, Corollary 6.4]. Note that for $p = 2$, the inclusion $B \subset G$ is an equality. In any case, the pullback of the extension (9) along the inclusion $\mu_p \subset \mathbb{G}_m$ admits a splitting given by $\lambda_1 \mapsto \lambda_1 t$, and one sees that $B \times_{\mathbb{G}_m} \mu_p = \alpha_p \rtimes \mu_p$.

Write $G[F]$ for the kernel of the relative Frobenius map $G \to G^{(p)}$, which is a normal subgroup scheme of height one. We now consider the resulting $G/G[F] \subset G^{(p)}$.

Proposition 8.4. *The group scheme $G/G[F]$ is smooth and coincides with the reduced part $G^{(p)}_{\mathrm{red}}$ inside the Frobenius pullback $G^{(p)}$.*

Proof. We may assume that k is algebraically closed. We first verify that $G/G[F]$ is reduced. The short exact sequence (9) yields an inclusion $\alpha_p \subset G$. This is not normal, but contained in the Frobenius kernel $G[F]$. The resulting projection $G/\alpha_p \to G/G[F]$ is faithfully flat, and it suffices to check that the homogeneous space G/α_p is reduced. Since G acts transitively, it is enough to verify that the local ring at the image in G/α_p of the origin $e \in G$ is regular. According to [Schröer 2007, Proposition 2.2], it is enough to check that in the local ring $\mathcal{O}_{G,e}$, the ideal $\mathfrak{a}$ corresponding to the subgroup scheme $\alpha_p \subset G$ has finite projective dimension. But this is clear, because it is given by the complete intersection $\lambda_1 = \cdots = \lambda_{p-1} = 0$.

Thus $G/G[F]$ is reduced. The reduced closed subschemes $G/G[F]$ and $G^{(p)}_{\mathrm{red}}$ inside the Frobenius pullback have the same underlying set, whence $G/G[F] = G^{(p)}_{\mathrm{red}}$. The latter is smooth by Proposition 8.3, thus the same holds for the former. □

Now consider the conjugacy map $c : G \to \mathrm{Aut}_{G/k}$, sending $g \in G(R)$ to the automorphism $x \mapsto gxg^{-1}$. In terms of truncated polynomials, gxg^{-1} is given by the triple substitution $\varphi_{g^{-1}}(\varphi_x(\varphi_g(t)))$.

Proposition 8.5. *The conjugacy map $c : G \to \mathrm{Aut}_{G/k}$ is an isomorphism.*

Proof. For $\omega = 0$, this holds by [Sancho de Salas 2000, Theorem 4.13]. The general case follows by base-changing to k^{alg} and using descent. □

In other words, the center and the scheme of outer automorphisms are trivial. One also says the group scheme G is *complete*. Now recall that $G = G_\omega$ depends on a scalar $\omega \in k$.

Proposition 8.6. *For each pair of scalars $\omega, \omega' \in k^\times$, the following are equivalent*:

(i) *The k-algebras L_ω and $L_{\omega'}$ are isomorphic.*

(ii) *The group schemes G_ω and $G_{\omega'}$ are isomorphic.*

(iii) *We have $k^p(\omega) = k^p(\omega')$ as subfields inside k.*

Proof. According to [Giraud 1971, Chapter III, Corollary 2.5.2], the category of twisted forms for L_ω and the category of twisted forms of G_ω are both equivalent to the category of G_ω-torsors. This implies the equivalence of (i) and (ii).

It remains to check (i) $\iff$ (iii). Write $L_\omega = k[t]/(t^p - \omega)$ and $L_{\omega'} = k[t']/(t'^p - \omega')$. Suppose first that these algebras are isomorphic. Choose an isomorphism and regard it as an identification $L_\omega = L_{\omega'}$. Then $t' = \sum_{i=0}^{p-1} \lambda_i t^i$, and consequently $\omega' = \sum \lambda_i^p \omega^i$. Hence, $k^p(\omega') \subset k^p(\omega)$. By symmetry, the reverse implication holds as well.

Conversely, suppose that $k^p(\omega) = k^p(\omega')$. If this subfield coincides with k^p, then both $\omega, \omega' \in k$ are p-powers, hence both algebras $L_\omega, L_{\omega'}$ are isomorphic to $k[t]/(t^p)$. Suppose now that the subfield is different from k^p. Taking p-th roots we get $k(\omega^{1/p}) = k(\omega'^{1/p})$ inside some perfect closure k^{perf}. These fields are isomorphic to L_ω and $L_{\omega'}$, because both scalars $\omega, \omega' \in k$ are not p-powers. □

In particular, each $L = L_\omega$ is a twisted form of L_0, and each $G = G_\omega$ is a twisted form of G_0. Up to isomorphism, these twisted forms correspond to classes in nonabelian cohomology set $H^1(k, G_0)$. We will use this throughout to gain insight into G, by using facts on G_0. For example, from Proposition 8.1, we see that the *locus of nonsmoothness* $\mathrm{Sing}(G_0/k)$, defined as in [Fanelli and Schröer 2020, Section 2], equals the whole scheme G_0. Hence the same holds for G, because it is a twisted form of G_0.

We now write $\mathrm{Sing}(G)$ for the *singular locus* of G, which comprise all points $a \in G$ where the local ring $\mathscr{O}_{G,a}$ is singular. Note that the formation of such loci commutes with base-changes along separable extension, but usually not with inseparable extensions.

Proposition 8.7. *The local ring at the origin is singular, with embedding dimension* $\mathrm{edim}(\mathscr{O}_{G,e}) = p$. *Moreover, the inclusion* $\mathrm{Sing}(G) \subset G$ *is not an equality if and only if* $\omega \in k$ *is not a* p*-power. In this case, the singular locus has codimension one in* G.

Proof. Since $e \in G$ is a rational point, the embedding dimension of $\mathscr{O}_{G,a}$ does not change under ground field extensions. If $\omega \in k^p$, we have $G \simeq G_0$, and thus for every point $a \in G$ the local ring $\mathscr{O}_{G,a}$ is singular. Now suppose that ω is not a p-power, and consider the p-Fermat hypersurface $X \subset \mathbb{P}^{p-1}$ defined by the homogeneous polynomial $\lambda_0 T_0^p + \cdots + \lambda_{p-1} T_{p-1}^p$, with coefficient $\lambda_i = \omega^i$. The field extension $k^p \subset E$ generated by $\lambda_i/\lambda_0 = \omega^i$ is nothing but $k^p(\omega)$. It has degree $[E : k] = p$, hence its p-degree is $d = 1$. According to [Schröer 2010, Theorem 3.3], the singular locus $\mathrm{Sing}(X) \subset X$ has codimension $d = 1$. It follows that $\mathrm{Sing}(G) \subset G$ is not an equality.

Seeking a contradiction, we now assume that $Z = \mathrm{Sing}(G)$ has codimension ≥ 2. Then the scheme G is normal, by Serre's criterion. Choose a normal compactification $Y = \overline{G}$. The canonical map $k \to H^0(Y, \mathscr{O}_Y)$ is bijective, because we have the rational point $e \in G$. According to [Schröer 2010, Lemma 1.3], the base-change $Y \otimes_k k(\omega^{1/p})$ remains integral. On the other hand, we just saw that $G \otimes k(\omega^{1/p})$ is nonreduced, a contradiction. □

9. Witt algebras

We keep the notation from the previous section. Our goal now is to understand the restricted Lie algebra $\mathfrak{g} = \mathfrak{g}_\omega$, or equivalently, the Frobenius kernel, attached to the automorphism group scheme $G = G_\omega$ of the spectrum of the ring $L = L_\omega = k[t]/(t^p - \omega)$.

From $G = \mathrm{Aut}_{\mathrm{Spec}(L)/k}$, we get an identification $\mathfrak{g} = \mathrm{Der}_k(L)$. Any k-derivation $\delta : L \to L$ can be seen as an L-linear map $\Omega^1_{L/k} \to L_\omega$. The module of Kähler differentials is a free L-module of rank one, generated by dt. Let $\partial \in \mathfrak{g}$ be the dual basis vector. In turn, we get the canonical k-basis $t^i\partial$, with $0 \le i \le p-1$, and the Lie bracket is given by

$$[t^i\partial, t^j\partial] = (j-i)t^{i+j-1}\partial.$$

Using this relation with $i = 0$, and also with $j = 0$, together with $[t^{p-1}\partial, t\partial] = (2-p)t^{p-1}$, one easily sees that $\mathfrak{g}$ is simple, provided $p \neq 2$.

The p-map $(f\partial)^{[p]} = (f\partial)^p$ is the p-fold composition in $\mathrm{End}_k(L)$. It can be made explicit as follows: For each truncated polynomial $f = \sum_{i=0}^{p-1} \lambda_i t^i$, we write $f^{p-1} = \sum_{i=0}^{p-1} C_i t^i$, where the $C_i \in k$ are certain polynomial expressions in the coefficients $\lambda_0, \ldots, \lambda_{p-1}$ and ω, which also depend on the prime $p > 0$. Set $C = C_{p-1}$. For example, with $p = 5$, the polynomial C becomes

$$(\lambda_0^3\lambda_4 + 2\lambda_0^2\lambda_1\lambda_3 + \lambda_0^2\lambda_2^2 + 2\lambda_0\lambda_1^2\lambda_2 + \lambda_1^4) + \omega(2\lambda_0\lambda_1\lambda_4^2 + 4\lambda_0\lambda_2\lambda_3\lambda_4 + 4\lambda_0\lambda_3^3 + 2\lambda_1^2\lambda_3\lambda_4 + 2\lambda_1\lambda_2^2\lambda_4 + 2\lambda_1\lambda_2\lambda_3^2 + 4\lambda_2^3\lambda_3) + \omega^2(4\lambda_2\lambda_4^3 + \lambda_3^2\lambda_4^2).$$

Proposition 9.1. *We have $(f\partial)^{[p]} = C \cdot f\partial$ for every element $f\partial \in \mathfrak{g}$. Moreover, the factor C is homogeneous of degree $p-1$ in the coefficients of $f = \sum \lambda_i t^i$.*

Proof. Clearly, we have $\partial^p = 0$. According to Hochschild's formula [1955, Lemma 1], the p-fold composition of $f\partial$ is given by

$$(f\partial)^p = f^p\partial^p + g\partial = g\partial,$$

where $g = (f\partial)^{p-1}(f)$. Consider the differential operator $D = \partial f\partial \cdots f\partial$, where the number of ∂-factors is $p-1$, such that $g = fD(f)$. According to [Evans and Fuchs 2002, Theorem 2], we have $D(f) = -\partial^{p-1}(f^{p-1})$. Note that this result is purely formal and holds in any $\mathbb{F}_p$-algebra with a chosen element f and some derivation ∂. Clearly, $\partial^{p-1}(t^i) = 0$ for $0 \le i \le p-2$, whereas $\partial^{p-1}(t^{p-1}) = (p-1)! = -1$. Summing up, we have $D(f) = C$, and hence $g = fC = Cf$. Then the statement on the p-map follows. From $\left(\sum \lambda_i t^i\right)^{p-1} = \sum C_i t^i$ one immediately sees that each $C_i = C_i(\lambda_0, \ldots, \lambda_{p-1})$ is homogeneous of degree $p-1$. □

This has a remarkable consequence:

Corollary 9.2. *Every vector in the restricted Lie algebra $\mathfrak{g}$ is p-closed.*

So each nonzero vector $f\partial \in \mathfrak{g}$ defines a subgroup scheme $H \subset G$ of order p. Note that the additive vectors might be viewed as rational points on the hypersurface of degree $p-1$ defined by the

homogeneous equation $C(\lambda_0, \dots, \lambda_{p-1}) = 0$. For the primes $p = 2$ and $p = 3$, we get $C(\lambda_0 + \lambda_1) = \lambda_1$ and $C(\lambda_0, \lambda_1, \lambda_2) = \lambda_1^2 - \lambda_0\lambda_2$, respectively, which then reveals the structure of $\mathfrak{g}$.

Corollary 9.3. *For $p = 2$, we have $\mathfrak{g} \simeq k \rtimes \mathfrak{gl}_1(k)$. For $p = 3$, we have $\mathfrak{g} \simeq \mathfrak{sl}_2(k)$.*

Proof. In the first case, one easily checks that the linear bijection $\mathfrak{g} \to k \rtimes \mathfrak{gl}_1(k)$ given by $(a+bt)\partial \mapsto (a, b)$ respects bracket and p-map. In the second case, the linear bijection

$$\mathfrak{g} \to \mathfrak{sl}_2(k), \quad (a + bt + ct^2)\partial \mapsto \begin{pmatrix} b & a \\ -c & -b \end{pmatrix}$$

likewise respects bracket and p-map. □

Consider the *adjoint representation* $\mathrm{Ad} : G \to \mathrm{Aut}_{\mathfrak{g}/k}$, which sends each $g \in G(R)$ to the derivative of the conjugacy map c_g given by $x \mapsto gxg^{-1}$. From [Waterhouse 1971, Theorem in Section 5.2], we get:

Proposition 9.4. *For $p \geq 5$ the adjoint representation $\mathrm{Ad} : G \to \mathrm{Aut}_{\mathfrak{g}/k}$ is an isomorphism of group schemes.*

So for $p \geq 5$ our G can be seen as the automorphism group scheme for the ring L, the group scheme G and the restricted Lie algebra $\mathfrak{g}$. Consequently, the three conditions in Proposition 8.6 are also equivalent to $\mathfrak{g}_\omega \simeq \mathfrak{g}_{\omega'}$. For $p = 2, 3$, the adjoint representation $G \to \mathrm{Aut}_{\mathfrak{g}/k}$ is not bijective, according to Proposition 3.2.

We now come to the crucial result of this paper.

Theorem 9.5. *Suppose that the scalar $\omega \in k$ is not a p-power, that $k^\times = k^{\times(p-1)}$ and that the Brauer group $\mathrm{Br}(k)$ contains no element of order two. Then each subalgebra $\mathfrak{g}' \subset \mathfrak{g}$ of dimension $1 \leq n \leq p-1$ is isomorphic to either k or $\mathfrak{gl}_1(k)$ or $k \rtimes \mathfrak{gl}_1(k)$ or $\mathfrak{sl}_2(k)$.*

Proof. In the special case $p = 2$, the dimension of $\mathfrak{g}'$ must be $n = 1$, and it follows that $\mathfrak{g}'$ is a twisted form of k or $\mathfrak{gl}_1(k)$. According to Proposition 3.2, all such twisted forms are trivial, so our assertion indeed holds.

From now on, we assume $p \geq 3$. Recall that $\mathfrak{g} = \mathrm{Lie}(G)$ is a twisted form of $\mathfrak{g}_0 = \mathrm{Lie}(G_0)$, where G_0 is the automorphism group scheme for the spectrum of $L_0 = k[t]/(t^p)$. Let $\mathfrak{g}_{0,\mathrm{red}}$ be the subalgebra corresponding to the reduced part $G_{0,\mathrm{red}}$. According to Proposition 10.3 below, there is no vector $x \neq 0$ in $\mathfrak{g}$ such that $x \otimes 1 \in \mathfrak{g} \otimes k(\omega^{1/p})$ is contained in $\mathfrak{g}_{0,\mathrm{red}} \otimes k(\omega^{1/p})$. In particular, the latter does not contain the base-change $\mathfrak{g}' \otimes k(\omega^{1/p})$.

It follows that the further base-change $\mathfrak{g}' \otimes k^{\mathrm{alg}}$ is not contained in $\mathfrak{g}_{0,\mathrm{red}} \otimes k^{\mathrm{alg}}$. Such subalgebras were studied by Premet and Stewart [2019, Section 2.2]. They remark on page 971 that a subalgebra in $\mathfrak{g}_0 \otimes k^{\mathrm{alg}}$ is not contained in $\mathfrak{g}_{0,\mathrm{red}} \otimes k^{\mathrm{alg}}$ if and only if it does not preserve any proper nonzero ideal, and they call such subalgebras *transitive*. We, thus, may apply loc. cit. Lemma 2.2 and infer that $\mathfrak{g}'$ is a twisted form of k or $\mathfrak{gl}_1(k)$ or $k \rtimes \mathfrak{gl}_1(k)$ or $\mathfrak{sl}_2(k)$. By assumption, the groups $k^\times / k^{\times(p-1)}$ and $\mathrm{Br}(k)[2]$ vanish. According to Proposition 3.2, the four restricted Lie algebras in question have no twisted forms over our field k, thus $\mathfrak{g}'$ is isomorphic to one of them. □

Consequently, for every $\mathfrak{g}' \subset \mathfrak{g}$ as above over any ground field k, one finds a finite separable extension, so that the base-change of $\mathfrak{g}'$ belongs to the given list.

10. Twisting adjoint representations

We keep the assumption of the preceding section and establish the crucial ingredients for the proof of Theorem 9.5. Recall that we are in characteristic $p > 0$ and that $G = G_\omega$ is the automorphism group scheme of the spectrum of $L = L_\omega = k[t]/(t^p - \omega)$, for some scalar $\omega \in k$. The resulting restricted Lie algebra $\mathfrak{g} = \mathrm{Lie}(G)$ is the p-dimensional vector space $\mathrm{Der}_k(L)$, which comprises the derivations $f(t)\partial$, where $f = \sum_{i=0}^{p-1} \mu_i t^i$ is a truncated polynomial. Moreover, the group elements $g \in G(R)$ act from the left on the spectrum of $L \otimes_k R$, and from the right on the coordinate ring $L \otimes_k R$ via the substitution $t \mapsto \varphi_g(t)$, for the corresponding truncated polynomial $\varphi_g(t) = \sum_{i=0}^{p-1} \lambda_i t^i$. The coefficients define an embedding $G \subset \mathbb{A}^p$ of the underlying scheme. For each $g \in G(R)$, write c_g for the induced inner automorphism $x \mapsto gxg^{-1}$. The resulting conjugacy map $c : G \to \mathrm{Aut}_{G/k}$ is given in terms of truncated polynomials by the formula

$$\varphi_{gxg^{-1}}(t) = \varphi_{g^{-1}}\big(\varphi_x(\varphi_g(t))\big).$$

By functoriality, the elements $c_g \in \mathrm{Aut}_{G/k}(R)$ induce an automorphism $\mathrm{Ad}_g = \mathrm{Lie}(c_g)$ of $\mathfrak{g} \otimes_k R$, which defines the adjoint representation $\mathrm{Ad} : G \to \mathrm{Aut}_{\mathfrak{g}/k}$.

Proposition 10.1. *Let $g \in G(R)$, and write $\varphi(t) = \varphi_{g^{-1}}(t)$ for the truncated polynomial of the inverse g^{-1}. Then the formal derivative $\varphi'(t)$ is a unit in the ring $L \otimes_k R$, and for each $f(t)\partial \in \mathfrak{g} \otimes_k R$, we have*

$$\mathrm{Ad}_g(f(t)\partial) = \frac{f(\varphi(t))}{\varphi'(t)}\partial.$$

Proof. By definition, the element $f(t)\partial \in \mathfrak{g} \otimes_k R \subset G(R[\epsilon])$ acts on the algebra $L \otimes R[\epsilon]$ via

$$h(t) \mapsto h(t) + \epsilon f(t)\partial(h) = h(t) + \epsilon f(t)h'(t).$$

Thus, the adjoint $\mathrm{Ad}_g(f(t)\partial) = g^{-1} \circ f(t)\partial \circ g$ is given by the following composition:

$$t \mapsto \varphi_g(t) \mapsto \varphi_g(t) + \epsilon f(t)\varphi_g'(t) \mapsto \varphi_g(\varphi_{g^{-1}}(t)) + \epsilon f(\varphi_{g^{-1}}(t))\varphi_g'(\varphi_{g^{-1}}(t)). \tag{10}$$

For a moment, let us regard the truncated polynomials $\varphi_g(t)$ and $\varphi_{g^{-1}}(t)$ as elements in the polynomial ring $R[t]$. Then $t = \varphi_g(\varphi_{g^{-1}}(t)) + (t^p - \omega)h(t)$ for some polynomial $h(t)$. Taking formal derivatives and applying the chain rule, we obtain

$$1 = \varphi_g'(\varphi_{g^{-1}}(t)) \cdot \varphi_{g^{-1}}'(t) + (t^p - \omega)h'(t).$$

This gives $1 = \varphi_g'(\varphi_{g^{-1}}(t)) \cdot \varphi_{g^{-1}}'(t)$ in the truncated polynomial ring $L \otimes_k R = R[t]/(t^p)$. It follows that $\varphi(t) = \varphi_{g^{-1}}'(t)$ is a unit, with inverse $\varphi_g'(\varphi_{g^{-1}}(t))$. Substituting for the term on the right in (10) gives the desired formula for $\mathrm{Ad}_g(f(t)\partial)$. □

Now consider the additive vector $\partial \in \mathfrak{g}$, which corresponds to an inclusion of the infinitesimal group scheme $H = \alpha_p$ into the group scheme G. The R-valued points $h \in H(R) = \{\lambda \in R \mid \lambda^p = 0\}$ correspond to truncated polynomials $\varphi_h(t) = t + \lambda$. The inverse R-valued point has $\varphi_{h^{-1}} = t - \lambda$, with formal derivative $\varphi_{h^{-1}}'(t) = 1$. This immediately gives:

Corollary 10.2. *With the above notation, we have* $\mathrm{Ad}_h(f(t)\partial) = f(t-\lambda)\partial$ *for every element* $f(t)\partial \in \mathfrak{g} \otimes_k R$.

Recall that $G = G_\omega$ depends on some scalar $\omega \in k$, and is a twisted form of G_0. The latter coincides with its own Frobenius pullback. By Proposition 8.3, the reduced part $G_{0,\mathrm{red}}$ is a nonnormal subgroup scheme. Recall that the embedding $G_0 \subset \mathbb{A}^p$ is given by $\lambda_0^p = 0$ and $\lambda_1 \neq 0$, such that $G_{0,\mathrm{red}}$ is defined by $\lambda_0 = 0$ and $\lambda_1 \neq 0$. Write $\mathfrak{g}_{0,\mathrm{red}} \subset \mathfrak{g}_0$ for the resulting subalgebra, which comprises the derivations $f\partial$, where the truncated polynomial $f = \sum_{i=0}^{p-1} \lambda_i t^i$ has $\lambda_0 = 0$. Write $H_0 \subset G_0$ for the copy of α_p given by the additive vector $\partial \in \mathfrak{g}_0$.

Now suppose that our ground field k is imperfect, that our scalar $\omega \in k$ is not a p-power and consider the resulting field extension $k(\omega^{1/p})$. In light of Lemma 7.1, we may endow its spectrum T with the structure of an H_0-torsor. Lemma 3.1 gives an identification ${}^T\mathfrak{g}_0 = \mathfrak{g}_\omega$, and thus an identification $\mathfrak{g}_0 \otimes_k k(\omega^{1/p}) = \mathfrak{g}_\omega \otimes_k k(\omega^{1/p})$. The following fact was a crucial ingredient for the proof of Theorem 9.5:

Proposition 10.3. *The twisted form* $\mathfrak{g}_\omega$ *contains no vector* $x \neq 0$ *such that the induced vector* $x \otimes 1$ *inside* $\mathfrak{g}_0 \otimes_k k(\omega^{1/p}) = \mathfrak{g}_\omega \otimes_k k(\omega^{1/p})$ *is contained in the base-change* $\mathfrak{g}_{0,\mathrm{red}} \otimes_k k(\omega^{1/p})$.

Proof. Setting $V = \mathfrak{g}_0$ and $V' = \mathfrak{g}_{0,\mathrm{red}}$, we see that action of $H_0 = \alpha_p$ via the adjoint representation $G_0 \to \mathrm{Aut}_{\mathfrak{g}_0/k}$ is exactly as described in Proposition 7.2, and the assertion follows. □

11. Subalgebras

Throughout this section, k is a field of characteristic $p > 0$ and $k \subset E$ is a field extension. Suppose we have a group scheme H of finite type over k, a group scheme G of finite type over E and a homomorphism $f : H \otimes_k E \to G$. We shall see that in certain circumstances, important structural properties of the Frobenius kernel $G[F]$ are inherited to $H[F]$.

Consider the finite-dimensional restricted Lie algebra $\mathfrak{h} = \mathrm{Lie}(H)$ over k and $\mathfrak{g} = \mathrm{Lie}(G)$ over E. Our homomorphism of group schemes induces an E-linear homomorphism

$$\mathrm{Lie}(f) : \mathfrak{h} \otimes_k E \to \mathfrak{g}, \quad x \otimes \alpha \mapsto \alpha x,$$

of restricted Lie algebras which corresponds to a k-linear homomorphism $\mathfrak{h} \to \mathfrak{g}$ of restricted Lie algebras. We are mainly interested in the case that E is the function field of an integral k-scheme X of finite type, such that $\mathfrak{g}$ is an infinite-dimensional k-vector space. Set $N = \mathrm{Ker}(f)$, with Lie algebra $\mathfrak{n} = \mathrm{Ker}(\mathrm{Lie}(f))$.

Proposition 11.1. *The following are equivalent*:

(i) *The* k*-linear homomorphism* $\mathfrak{h} \to \mathfrak{g}$ *is injective.*

(ii) *For every nontrivial subgroup scheme* $H' \subset H$ *that is minimal with respect to inclusion, the base-change* $H' \otimes_k E$ *is not contained in the kernel* $N \subset H \otimes_k E$.

Proof. We prove the contrapositive: Suppose $\mathfrak{h} \to \mathfrak{g}$ is not injective. Inside the kernel, choose a subalgebra $\mathfrak{h}' \neq 0$ that is minimal with respect to inclusion. Then the induced E-linear map $\mathfrak{h}' \otimes_k E \to \mathfrak{g}$ is zero. By the Demazure–Gabriel correspondence, the corresponding subgroup scheme $H' \subset H$ of height one is minimal with respect to inclusion, and $H' \otimes_k E \subset N$. Conversely, suppose $H' \otimes_k E \subset N$ for some H'

as in (ii). Choose some nonzero vector x from $\mathfrak{h}' = \mathrm{Lie}(H')$. By construction, it lies in the kernel for $\mathfrak{h} \to \mathfrak{g}$. □

We now suppose that the above equivalent conditions hold, and regard the injective map as an inclusion $\mathfrak{h} \subset \mathfrak{g}$. To simplify exposition, we also assume that k is algebraically closed and that $\mathfrak{h}$ contains an E-basis for $\mathfrak{g}$. In other words, the induced linear map $\mathfrak{h} \otimes_k E \to \mathfrak{g}$ is surjective. Note that this E-linear map is usually *not injective*. However, we shall see that important structural properties of $\mathfrak{g}$ transfer to $\mathfrak{h}$. We start with a series of three elementary but useful observations.

Lemma 11.2. *If every vector in* $\mathfrak{g}$ *is* p*-closed, the same holds for every vector in* $\mathfrak{h}$.

Proof. Fix some nonzero $x \in \mathfrak{h}$. By assumption, we have $x^{[p]} = \alpha x$ for some $\alpha \in E$, and our task is to verify that this scalar already lies in k. Since the latter is algebraically closed, it is enough to verify that α is algebraic over k. By induction on $i \geq 0$, we get $x^{[p^i]} = \alpha^{n_i} x$ for some strictly increasing sequence $0 = n_0 < n_1 < \cdots$ of integers. Since $\dim_k(\mathfrak{h}) < \infty$, there is a nontrivial relation $\sum_{i=0}^{r} \lambda_i x^{[p^i]}$ for some $r \geq 0$ and some coefficients $\lambda_i \in k$. This gives $\sum \lambda_i \alpha^{n_i} x = 0$. Since $x \neq 0$, we must have $\sum \lambda_i \alpha^{n_i} = 0$, hence $\alpha \in E$ is algebraic over k. □

Lemma 11.3. *The restricted Lie algebras* $\mathfrak{g}$ *and* $\mathfrak{h}$ *have the same toral rank, and the kernel* $\mathfrak{n}$ *for* $\mathfrak{h} \otimes_k E \to \mathfrak{g}$ *has toral rank* $\rho_t(\mathfrak{n}) = 0$.

Proof. It follows from [Block and Wilson 1988, Lemma 1.7.2] that $\rho_t(\mathfrak{h}) = \rho_t(\mathfrak{g}) + \rho_t(\mathfrak{n})$, and in particular $\rho_t(\mathfrak{g}) \leq \rho_t(\mathfrak{h})$. For the reverse inequality, suppose there are k-linearly independent vectors $x_1, \ldots, x_r \in \mathfrak{h}$ with $[x_i, x_j] = 0$ and $x_i^{[p]} = x_i$. We have to check that the vectors are E-linearly independent. Suppose there is a nontrivial relation. Without loss of generality, we may assume that $x_1, \ldots, x_{r-1}$ are E-linearly independent and that $x_r = \sum_{i=1}^{r-1} \lambda_i x_i$ for some coefficients $\lambda_i \in E$. From the axioms of the p-map, we get

$$\sum \lambda_i x_i = x_r = x_r^{[p]} = \Big(\sum \lambda_i x_i\Big)^{[p]} = \sum \lambda_i^p x_i^{[p]} = \sum \lambda_i^p x_i.$$

Comparing coefficients gives $\lambda_i^p = \lambda_i$. Thus, λ_i lie in the prime field, in particular in k. In turn, the vectors are k-linearly dependent, contradiction. □

Let us call the restricted Lie algebra $\mathfrak{h}$ *simple* if it is nonzero and contains no ideal besides $\mathfrak{a} = 0$ and $\mathfrak{a} = \mathfrak{h}$.

Lemma 11.4. *Suppose there is a restricted Lie algebra* $\mathfrak{h}'$ *over* k *such that* $\mathfrak{g}$ *is a twisted form of the base-change* $\mathfrak{h}' \otimes_k E$. *If* $\mathfrak{h}'$ *is simple of dimension* $n' \geq 2$, *we must have* $\mathfrak{h} \simeq \mathfrak{h}'$ *and* $\mathfrak{g} \simeq \mathfrak{h}' \otimes_k E$.

Proof. Let H and H' be the finite group schemes of height one corresponding to the restricted Lie algebras $\mathfrak{h}$ and $\mathfrak{h}'$, respectively. Consider the Hom scheme $X \subset \mathrm{Hilb}_{H \times H'}$ of surjective homomorphisms $H \to H'$. By assumption, this scheme contains a point with values in the algebraic closure E^{alg}. By Hilbert's Nullstellensatz, there must be a point with values in k, hence there is a surjective homomorphism $H \to H'$. It corresponds to a short exact sequence of restricted Lie algebras

$$0 \to \mathfrak{a} \to \mathfrak{h} \to \mathfrak{h}' \to 0.$$

We claim that the ideal $\mathfrak{a}$ vanishes. Suppose this is not the case. Clearly, $\mathfrak{h}'$ and $\mathfrak{g}$ have the same toral rank. By Lemma 11.3, $\mathfrak{g}$ and $\mathfrak{h}$ also have the same toral rank. According to [Block and Wilson 1988, Lemma 1.7.2], we have $\rho_t(\mathfrak{a}) = 0$, so the p-map on $\mathfrak{a}$ is nilpotent. On the other hand, the p-map on $\mathfrak{h}'$ is not nilpotent, because the Lie algebra is simple of dimension $\dim(\mathfrak{h}') \geq 2$. The same holds for $\mathfrak{g}$, and we infer that the induced map $\mathfrak{a} \otimes_k E \to \mathfrak{g}$ is not surjective. Its image $\mathfrak{b} \subsetneq \mathfrak{g}$ is nonzero, because $\mathfrak{h} \subset \mathfrak{g}$. Since $\mathfrak{g}$ is simple, there are elements $x \in \mathfrak{b}$ and $y \in \mathfrak{g}$ with $[x, y] \notin \mathfrak{b}$. Such vectors may be chosen with $x \in \mathfrak{a}$ and $y \in \mathfrak{h}$, because $\mathfrak{a} \subset \mathfrak{b}$ and $\mathfrak{h} \subset \mathfrak{g}$ contain E-bases. Consequently, $\mathfrak{a} \subset \mathfrak{h}$ is not an ideal, contradiction.

This shows that $\mathfrak{h} = \mathfrak{h}'$. In particular, $\mathfrak{h}$ and $\mathfrak{g}$ have the same dimension as vector spaces, so our surjection $\mathfrak{h} \otimes_k E \to \mathfrak{g}$ must be bijective. Our assertions follow. □

For each $a \in \mathfrak{h}$, the Lie bracket $\mathrm{ad}_a(x) = [a, x]$ defines a k-linear endomorphism of $\mathfrak{h}$, but also an E-linear endomorphism of $\mathfrak{g}$. Write $\mathrm{ad}_{\mathfrak{h},a}$ and $\mathrm{ad}_{\mathfrak{g},a}$ for the respective maps, and $\mu_{\mathfrak{h},a}(t) \in k[t]$ and $\mu_{\mathfrak{g},a}(t) \in E[t]$ for the resulting minimal polynomials.

Lemma 11.5. *We have $\mu_{\mathfrak{h},a}(t) = \mu_{\mathfrak{g},a}(t)$. In particular, the endomorphism $\mathrm{ad}_{\mathfrak{g},a}$ is trigonalizable, and its eigenvalues coincide with those of $\mathrm{ad}_{\mathfrak{h},a}$. Moreover, the former is diagonalizable if and only if this holds for the latter.*

Proof. The surjection $\mathfrak{h} \otimes_k E \to \mathfrak{g}$ already reveals that $\mu_{\mathfrak{g},a}(t)$ divides $\mu_{\mathfrak{h},a}(t)$. The latter decomposes into linear factors over k, because this field is algebraically closed. We conclude that $\mu_{\mathfrak{g},a}(t) = \sum \lambda_i t^i$ actually lies in $k[t]$, and decomposes into linear factors over k. Moreover, for each vector x from $\mathfrak{h} \subset \mathfrak{g}$, we have $\sum \lambda_i \, \mathrm{ad}^i_{\mathfrak{h},a}(x) = 0$, hence $\mu_{\mathfrak{h},a}(t)$ divides $\mu_{\mathfrak{g},a}(t)$. In turn, the two minimal polynomials coincide. The remaining assertions follow immediately. □

We now consider some special cases for $\mathfrak{g}$, and deduce structure results for $\mathfrak{h}$. Recall that k^n denotes the n-dimensional restricted Lie algebra over k with trivial bracket and p-map. The following fact is obvious:

Proposition 11.6. *If $\mathfrak{g}$ is isomorphic to E^m, then the restricted Lie algebra $\mathfrak{h}$ is isomorphic to k^n for some integer $n \geq m$.*

Recall that $k^n \rtimes_\varphi \mathfrak{gl}_1(k)$ denotes the semidirect product formed with respect to the homomorphism $\varphi : \mathfrak{gl}_1(k) \to \mathfrak{gl}(k^n) = \mathrm{Der}'_k(k^n)$ that sends scalars to scalar matrices.

Proposition 11.7. *If $\mathfrak{g}$ is isomorphic to $E^m \rtimes \mathfrak{gl}_1(E)$, then the restricted Lie algebra $\mathfrak{h}$ is isomorphic to $k^n \rtimes \mathfrak{gl}_1(k)$ for some $n \geq m$.*

Proof. Without loss of generality, we may assume $\mathfrak{g} = E^m \rtimes \mathfrak{gl}_1(E)$. First, recall that bracket and p-map are given by the formulas

$$[v + \lambda e, v' + \lambda' e] = \lambda v' - \lambda' v \quad \text{and} \quad (v + \lambda e)^{[p]} = \lambda^{p-1}(v + \lambda e), \tag{11}$$

where $v \in E^n$, and $e \in \mathfrak{gl}_1(E)$ denotes the unit. In particular, each vector is p-closed. Moreover, $a = v + \lambda e$ is multiplicative if and only if $\lambda \neq 0$, and $a^{[p]} = a$ if and only if $\lambda \in \mu_{p-1}(E)$. For any such vector, we see that the endomorphism $\mathrm{ad}_a(x) = [a, x]$ is diagonalizable, and $E^n \subset \mathfrak{g}$ is the eigenspace with respect to the eigenvalue $\alpha = \lambda$, whereas the line $Ea \subset \mathfrak{g}$ is the eigenspace for $\alpha = 0$.

From the extension $0 \to E^m \to \mathfrak{g} \to \mathfrak{gl}_1(E) \to 0$, one sees that $\mathfrak{g}$ has toral rank one. According to Lemma 11.3, the same holds for $\mathfrak{h}$. Choose some nonzero vector $a \in \mathfrak{h}$ with $a^{[p]} = a$. Then $a = v + \lambda e$ for some $\lambda \in \mu_{p-1}(E) \subset k^\times$. Replacing a by $\lambda^{-1}a$, we may assume $\lambda = 1$. By Lemma 11.5, the adjoint representation $\mathrm{ad}_{\mathfrak{h},a}$ is diagonalizable, with eigenvalues $\alpha = 0$ and $\alpha = 1$. Let $\mathfrak{h} = U_0 \oplus U_1$ be the corresponding eigenspace decomposition. Then U_0 lies in the corresponding eigenspace for $\mathrm{ad}_{\mathfrak{g},a}$, which is $E^n \subset \mathfrak{g}$. It follows that U_0 has trivial Lie bracket and p-map. The choice of a k-basis gives $U_0 = k^n$ for some $n \geq 0$. Likewise, U_1 is contained in Ea. Thus the bracket vanishes on U_1, and the p-map is injective. Using Lemma 11.3, we infer that $U_1 = ka$. The vector space decomposition $\mathfrak{h} = U_0 \oplus U_1$ thus becomes a semidirect product $\mathfrak{h} = k^n \rtimes \mathfrak{gl}_1(k)$. We must have $m \geq n$, because the map $\mathfrak{h} \otimes_k E \to \mathfrak{g}$ is surjective. □

Recall that $\mathfrak{sl}_2(E)$ is simple for $p \geq 3$. Using Lemma 11.4, we immediately obtain:

Proposition 11.8. *Suppose $p \geq 3$. If $\mathfrak{g}$ is isomorphic to a twisted form of $\mathfrak{sl}_2(E)$, then the restricted Lie algebra $\mathfrak{h}$ is isomorphic to $\mathfrak{sl}_2(k)$.*

12. Structure results for Frobenius kernels

We now come to our main result. Let k be an algebraically closed field of characteristic $p > 0$, and let X be a proper integral scheme or more generally a proper integral algebraic space, $H = \mathrm{Aut}_{X/k}[F]$ be the Frobenius kernel for the automorphism group scheme and $\mathfrak{h} = H^0(X, \Theta_{X/k})$ the corresponding restricted Lie algebra over k. Let $H_F = H \otimes_k F$ be the base-change to the function field $F = k(X)$, and $H_F^{\mathrm{inert}} \subset H_F$ the inertia subgroup scheme for the rational point in the spectrum of $F \otimes_E F$, with corresponding restricted Lie algebra $\mathfrak{h}_F^{\mathrm{inert}} \subset \mathfrak{h}_F$. Recall that the foliation rank $r \geq 0$ is given by

$$r = \dim\bigl(\mathfrak{h}_F/\mathfrak{h}_F^{\mathrm{inert}}\bigr) = \dim\bigl(\Omega^1_{F/E}\bigr) \quad \text{and} \quad \bigl[H_F : H_F^{\mathrm{inert}}\bigr] = [F : E] = p^r,$$

where $E = F^{\mathfrak{h}}$ is the kernel for all derivations $D : F \to F$ from the Lie algebra $\mathfrak{h}$. This is nothing but the function field $E = k(Y)$ of the quotient $Y = X/H$.

Theorem 12.1. *Suppose that the proper integral scheme X has foliation rank $r \leq 1$. Then the Frobenius kernel $H = \mathrm{Aut}_{X/k}[F]$ is isomorphic to the Frobenius kernel of one of the following three basic types of group schemes*:

$$\mathrm{SL}_2 \quad \textit{and} \quad \mathbb{G}_a^{\oplus n} \quad \textit{and} \quad \mathbb{G}_a^{\oplus n} \rtimes \mathbb{G}_m,$$

for some integer $n \geq 0$.

Proof. The case $r = 0$ is trivial, so we assume $r = 1$ such that $\mathfrak{h} \neq 0$. By assumption the subfield $E = F^{\mathfrak{h}}$ has $[F : E] = p$, and we thus have $F = E[T]/(T^p - \omega)$ for some $\omega \in E$. Thus, the restricted Lie algebra $\mathfrak{g} = \mathrm{Der}_E(F)$ is a twisted form of the Witt algebra $\mathfrak{g}_0$ over E. By construction, we have an inclusion $\mathfrak{h} \subset \mathfrak{g}$.

Suppose first that the induced homomorphism $\mathfrak{h} \otimes E \to \mathfrak{g}$ is surjective, such that the results of Section 11 apply. Suppose first $p \leq 3$. Then $\mathfrak{g}$ is isomorphic to either $E \rtimes \mathfrak{gl}_1(E)$ or $\mathfrak{sl}_2(E)$, by Corollary 9.3, and our assertion follows from Propositions 11.7 and 11.8. The case $p \geq 5$ actually does not occur: Then the Witt

algebra $\mathfrak{h}' = \mathrm{Der}_k(k[t]/(t^p))$ is simple, as remarked at the beginning of Section 9, and $\mathfrak{g}$ is a twisted form of $\mathfrak{h}' \otimes_k E$. It follows from Lemma 11.4 that $\mathfrak{g} \simeq \mathfrak{h}' \otimes_k E$. Combining Propositions 9.4 and 8.6, we get

$$E[T]/(T^p - \omega) \simeq E[T]/(T^p),$$

a contradiction.

It remains to treat the case that $\mathfrak{h} \otimes E \to \mathfrak{g}$ is not surjective. Then $\mathfrak{g}' = \mathfrak{h} \cdot E$ is a restricted subalgebra of dimension $1 \leq n \leq p-1$. We now replace the field E by some separable closure E^{sep}, and likewise F by $F \otimes_E E^{\mathrm{sep}}$. According to Theorem 9.5, the restricted Lie algebra $\mathfrak{g}'$ is isomorphic to either $\mathfrak{sl}_2(E)$ or E or $\mathfrak{gl}_1(E)$ or $E \rtimes \mathfrak{gl}_1(E)$. By the results in Section 11, this ensures that $\mathfrak{h}$ is isomorphic to $\mathfrak{sl}_2(k)$ or k^n or $k^n \rtimes \mathfrak{gl}_1(k)$ for some $n \geq 0$. These are the Frobenius kernels for the group schemes in question, and our assertion follows. □

In the former case, the Frobenius kernel is $\mathfrak{sl}_2(k)$. This indeed occurs for $X = \mathbb{P}^1$. In the latter two cases, the respective Frobenius kernels are $\alpha_p^{\oplus n}$ and $\alpha_p^{\oplus n} \rtimes \mu_p$. With Corollary 6.6, we immediately get the following consequence:

Corollary 12.2. *Suppose that X is a proper normal surface with $h^0(\omega_X^\vee) = 0$. Then $H = \mathrm{Aut}_{X/k}[F]$ is isomorphic to the Frobenius kernel of one of the three basic types of group schemes in Theorem 12.1.*

This applies, in particular, to smooth surfaces S of Kodaira dimension $\mathrm{kod}(S) \geq 1$, to surfaces of general type and their minimal models or normal surfaces X with $c_1 = 0$ and $\omega_X \neq \mathscr{O}_X$ having at most rational double points.

13. Canonically polarized surfaces

Let k be a ground field of characteristic $p > 0$ and X be a proper normal surface with $h^0(\mathscr{O}_X) = 1$ whose complete local rings $\mathscr{O}_{X,a}^\wedge$ are complete intersections. Then the cotangent complex $L_{X/k}^\bullet$ is perfect, and we obtain two *Chern numbers*

$$c_1^2 = c_1^2(L_{X/k}^\bullet) \quad \text{and} \quad c_2 = c_2(L_{X/k}^\bullet),$$

as explained by Ekedahl, Hyland and Shepherd–Barron [Ekedahl et al. 2012, Section 3]. In some sense, these integers are the most fundamental numerical invariants of the surface X. Note that c_1^2 is nothing but the self-intersection number $K_X^2 = (\omega_X \cdot \omega_X)$ of the dualizing sheaf. If the singularities are also rational, hence rational double points, the Chern numbers of X coincide with the Chern numbers of the minimal resolution of singularities S, according to loc. cit. Proposition 3.12 and Corollary 3.13. For more details on rational double points, we refer to [Lipman 1969; Artin 1977].

Recall that a *canonically polarized surface* is the canonical model X of a smooth surface S of general type. Then ω_X is ample, all local rings $\mathscr{O}_{X,a}$ are either regular or rational double points, and the above applies. Let us record the following facts:

Lemma 13.1. *Suppose that X is canonically polarized. Then*

$$\chi(\mathscr{O}_X) = \tfrac{1}{12}(c_1^2 + c_2) \quad \textit{and} \quad h^0(\omega_X) \leq \tfrac{1}{2}(c_1^2 + 4) \quad \textit{and} \quad c_2 \leq 5c_1^2 + 36.$$

Proof. Let $f : S \to X$ be the minimal resolution of singularities. Then S is a smooth minimal surface of general type, and the first formula holds for S instead of X by Hirzebruch–Riemann–Roch. We already observed that the surfaces X and S have the same Chern numbers, and the structure sheaves have the same cohomology. Thus the formula also holds for X. In particular, we have

$$h^0(\omega_X) = h^2(\mathscr{O}_X) = h^2(\mathscr{O}_S) = h^0(\omega_S),$$

and Noether's inequality (for example, [Liedtke 2013a, Section 8.3]) for the minimal surface of general type S gives the second formula. This ensures

$$\chi(\mathscr{O}_X) = 1 - h^1(\omega_X) + h^0(\omega_X) \leq 1 + h^0(\omega_X) = 1 + h^0(\omega_S) \leq \frac{c_1^2 + 6}{2}.$$

Combining with $\chi(\mathscr{O}_X) = (c_1^2 + c_2)/12$ we get the third inequality. □

Theorem 13.2. *Let X be canonically polarized surface, with Chern numbers c_1^2, c_2. Then the Lie algebra $\mathfrak{h} = H^0(X, \Theta_{X/k})$ for the Frobenius kernel $H = \mathrm{Aut}_{X/k}[F]$ has the property $\dim(\mathfrak{h}) \leq \Phi(c_1^2, c_2)$ for the polynomial*

$$\Phi(x, y) = \begin{cases} \frac{1}{144}(73x + y)^2 - 1, & \text{if } c_1^2 \geq 2, \\ \frac{1}{144}(121x + y)^2 - 1, & \text{if } c_1^2 = 1. \end{cases}$$

Moreover, we also have the weaker bound $\dim(\mathfrak{h}) \leq \Psi(c_1^2)$ with the polynomial

$$\Psi(x) = \begin{cases} \frac{169}{4}x^2 + 39x + 8, & \text{if } c_1^2 \geq 2, \\ \frac{441}{4}x^2 + 63x + 8, & \text{if } c_1^2 = 1. \end{cases}$$

Proof. Fix some $m \geq 3$. Serre Duality gives $h^i(\omega_X^{\otimes m}) = h^{2-i}(\omega_X^{\otimes 1-m})$. This vanishes for $i = 2$, because ω_X is ample, and also for $i = 1$ by [Ekedahl 1988, Chapter II, Theorem 1.7]. Thus, we have $h^0(\omega_X^{\otimes m}) = \chi(\omega_X^{\otimes m})$, and Riemann–Roch gives

$$h^0(\omega_X^{\otimes m}) = \chi(\mathscr{O}_X) + \tfrac{1}{2}(m^2 - m)c_1^2. \tag{12}$$

According to [Ekedahl 1988, Chapter III, Theorem 1.20], the invertible sheaf $\omega_X^{\otimes m}$ is very ample for $c_1^2 \geq 2$ and $m = 4$, or $c_1^2 = 1$ and $m = 5$. It then defines a closed embedding $X \subset \mathbb{P}^n$ with $\omega_X = \mathscr{O}_X(1)$ and $n + 1 = h^0(\omega_X^{\otimes m})$.

The following argument, which gives a better estimate than our original reasoning, was kindly communicated by the referee: The canonical linearization of ω_X and its power $\omega_X^{\otimes m}$ yields a homomorphism $\mathrm{Aut}_{X/k} \to \mathrm{Aut}_{\mathbb{P}^n/k} = \mathrm{PGL}_{n+1,k}$ such that the inclusion $X \subset \mathbb{P}^n$ is equivariant with respect to the action of $G = \mathrm{Aut}_{X/k}$. In particular, the homomorphism of group schemes is a closed embedding, and the resulting inclusion of tangent spaces $H^0(X, \Theta_{X/k}) \subset H^0(\mathbb{P}^n, \Theta_{\mathbb{P}^n/k})$ gives the estimate $h^0(\Theta_{X/k}) \leq h^0(\omega_X^{\otimes m})^2 - 1$. Substituting (12) and using $\chi(\mathscr{O}_X) = (c_1^2 + c_2)/12$, we get

$$h^0(\Theta_X) \leq \left(\frac{c_1^2 + c_2}{12} + \frac{(m^2 - m)}{2}c_1^2\right)^2 - 1 = \frac{1}{144}\big((6m^2 - 6m + 1)c_1^2 + c_2\big)^2 - 1.$$

By setting $m = 4$ and $m = 5$, we get the desired bound $\dim(\mathfrak{h}) \leq \Phi(c_1^2, c_2)$. Finally, the inequality $c_2 \leq 5c_1^2 + 36$ from Lemma 13.1 yields the weaker bound $\dim(\mathfrak{h}) \leq \Psi(c_1^2)$. □

14. Examples

Let k be a ground field of characteristic $p > 0$. In this section, we give examples of canonically polarized surfaces X where the Frobenius kernel of the automorphism group scheme is isomorphic to $\alpha_p^{\oplus n} \rtimes \mu_p$ and $\alpha_p^{\oplus m}$. Note that we do not have examples where $\mathrm{SL}_2[F]$ occurs.

To start with, view $\mathbb{P}^2$ as the homogeneous spectrum of $k[T_0, T_1, T_2]$. Fix some $d \geq 1$, set $\mathscr{L} = \mathscr{O}_{\mathbb{P}^2}(d)$ and consider the section

$$s = T_0T_1T_2^{pd-2} + T_1T_2T_0^{pd-2} + T_2T_0T_1^{pd-2} \in \Gamma(\mathbb{P}^2, \mathscr{L}^{\otimes p}). \tag{13}$$

Regarded as $\mathscr{L}^{\otimes -p} \to \mathscr{O}_{\mathbb{P}^2}$, this endows the coherent sheaf $\mathscr{A} = \bigoplus_{i=0}^{p-1} \mathscr{L}^{\otimes -i}$ with the structure of a $\mathbb{Z}/p\mathbb{Z}$-graded $\mathscr{O}_{\mathbb{P}^2}$-algebra, and we define $X = \mathrm{Spec}(\mathscr{A})$ as the relative spectrum.

Proposition 14.1. *In the above setting, suppose $p \neq 3$ and $d \geq 4$. Then*

$$\mathfrak{h} = k^n \rtimes \mathfrak{gl}_1(k) \quad \text{and} \quad \mathrm{Aut}_{X/k}[F] = \alpha_p^{\oplus n} \rtimes \mu_p,$$

where $n = (d+1)(d+2)/2$. Moreover, X is a canonically polarized surface with Chern invariants $c_1^2 = p(pd-d-3)^2$ and $c_2 = 3p + dp(p-1)(pd-3)$.

Proof. Being locally a hypersurface in affine three-space, the scheme X is Gorenstein. According to [Ekedahl 1988, Chapter I, Proposition 1.7], the dualizing sheaf is given by $\omega_X = \pi^*(\omega_{\mathbb{P}^2} \otimes \mathscr{L}^{p-1})$, which equals the pullback of $\mathscr{O}_{\mathbb{P}^2}(pd-d-3)$. The statement on c_1^2 follows. Using $d(p-1) - 3 \geq d - 3 \geq 1$, we see that ω_X is ample. Since $\pi : X \to \mathbb{P}^2$ is finite, the Euler characteristic $\chi(\mathscr{O}_X)$ equals

$$\sum_{i=0}^{p-1} \chi(\mathscr{O}_{\mathbb{P}^2}(-id)) = \sum_{i=0}^{p-1} \binom{2-id}{2} = \frac{12p - 9d(p-1)p + d^2(p-1)p(2p-1)}{12}.$$

Now suppose for the moment that we already know that X is geometrically normal, with only rational double points. Then X is a canonically polarized surface, and Lemma 13.1 yields the statement on c_2.

We proceed by computing $\mathfrak{h} = H^0(X, \Theta_{X/k})$ as a vector space. The grading of the structure sheaf $\mathscr{A} = \bigoplus_{i=0}^{p-1} \mathscr{L}^{\otimes -i}$ corresponds to an action of $G = \mu_p$ on the scheme X, with quotient $\mathbb{P}^2$. Let $D : \mathscr{O}_X \to \Theta_{X/k}$ be the corresponding multiplicative vector field, and $\mathscr{O}_X(\Delta) \subset \Theta_{X/k}$ the saturation of the image, for some effective Weil divisor $\Delta \subset X$. Lemma 14.5 below gives an exact sequence

$$0 \to \mathscr{O}_X(\Delta) \xrightarrow{D} \Theta_{X/k} \to \omega_X^{\otimes -1}(-\Delta).$$

The term on the right has no nonzero global sections, because ω_X is ample, and consequently, we get $H^0(X, \mathscr{O}_X(\Delta)) = H^0(X, \Theta_{X/k})$. We have $\omega_X = \pi^*(\omega_{\mathbb{P}^2}) \otimes \mathscr{O}_X((p-1)\Delta)$ by [Rudakov and Shafarevich 1976, Proposition 2 combined with Proposition 3], which gives $\mathscr{O}_X(\Delta) = \pi^*(\mathscr{L})$. Consequently,

$$H^0(X, \mathscr{O}_X(\Delta)) = H^0(\mathbb{P}^2, \mathscr{A} \otimes \mathscr{L}) = H^0(\mathbb{P}^2, \mathscr{L}) \oplus H^0(\mathbb{P}^2, \mathscr{O}_{\mathbb{P}^2}) = k^n \times k,$$

with the integer $n = (d+1)(d+2)/2$, as desired.

It is not difficult to compute bracket and p-map for $\mathfrak{h} = H^0(X, \Theta_{X/k})$. The coordinate rings for the affine open sets $U_i = D_+(T_i)$ of $\mathbb{P}^2$ are the homogeneous localizations $R_i = k[T_0, T_1, T_2]_{(T_i)}$, and the preimages $\pi^{-1}(U_i)$ are the spectra of $A_i = R_i[t_i]/(t_i^p - s_i)$. Here, s_i denotes the dehomogenization of (13) with respect to T_i. We have $\Theta_{A_i/R_i} = A_i\partial/\partial t_i$, and our multiplicative vector field restricts becomes $D = t_i\partial/\partial t_i$. For any $b_i, b_i' \in R_i$, one immediately calculates

$$\left[b_i\frac{\partial}{\partial t_i}, t_i\frac{\partial}{\partial t_i}\right] = b_i\frac{\partial}{\partial t_i}, \quad \left[b_i\frac{\partial}{\partial t_i}, b_i'\frac{\partial}{\partial t_i}\right] = 0 \quad \text{and} \quad \left(b_i\frac{\partial}{\partial t_i}\right)^{[p]} = 0.$$

Choosing a basis for $H^0(\mathbb{P}^2, \mathscr{L})$, we infer that the vector space decomposition $\mathfrak{h} = H^0(\mathbb{P}^2, \mathscr{L}) \oplus H^0(\mathbb{P}^2, \mathscr{O}_{\mathbb{P}^2})$ becomes a semidirect product structure $\mathfrak{h} = k^n \rtimes \mathfrak{gl}_1(k)$ for the restricted Lie algebra.

It remains to check that $\mathrm{Sing}(X/k)$ is finite, and that all singularities are rational double points. For this, we may assume that k is algebraically closed. In light of the symmetry in (13), it suffices to verify this on the preimage $V = \pi^{-1}(U)$ of the open set $U = D_+(T_0)$. Setting $x = T_1/T_0$ and $y = T_2/T_0$, we see that V has coordinate ring $A = k[x, y, t]/(f)$ with

$$f = t^p - xy - x^{pd-2}y - xy^{pd-2}.$$

The singular locus comprises the common zeros of f and the partial derivatives

$$\frac{\partial f}{\partial x} = -y + 2x^{pd-3}y - y^{pd-2} = 0,$$
$$\frac{\partial f}{\partial y} = -x - x^{pd-2} + 2xy^{pd-3} = 0.$$

Clearly there are only finitely many singularities with $x = 0$ or $y = 0$. For the remaining part of $\mathrm{Sing}(X)$, it suffices to examine the system of polynomial equations

$$-1 + 2x^{pd-3} - y^{pd-3} = 0 \quad \text{and} \quad -1 - x^{pd-3} + 2y^{pd-3} = 0. \tag{14}$$

This is a system of linear equations in the powers x^{pd-3} and y^{pd-3}, and one solution is $x^{pd-3} = y^{pd-3} = 1$. Using $p \neq 3$ we see that there are no other solutions.

It remains to verify that all singularities are rational double points. It would be tedious and cumbersome to do this explicitly. We resort to a trick of independent interest, where we actually show that there are only rational double points of A-type: By Lemma 14.3 and Proposition 14.4, it suffices to verify that no singular point is a zero for the polynomial

$$\left(\frac{\partial^2 f}{\partial x\,\partial y}\right)^2 - \frac{\partial^2 f}{\partial x^2}\cdot\frac{\partial^2 f}{\partial y^2},$$

which gives the additional equation

$$1 + 4x^{2pd-6} + 4y^{2pd-6} - 4x^{pd-3} - 4y^{pd-3} - 28(xy)^{pd-3} = 0. \tag{15}$$

Substituting $x^{pd-3} = y^{pd-3} = 1$, the left side becomes $1 + 4 + 4 - 4 - 4 - 28 = -27$, which is indeed nonzero because $p \neq 3$. □

Note that $\pi : X \to \mathbb{P}^2$ is a universal homeomorphism, so the geometric fundamental group of X is trivial, and $b_1 = 0$ and $b_2 = 1$. Let $x_1, \ldots, x_r$ be the geometric singularities on X. We saw above that they are rational double points of certain A_{n_i}. One referee pointed out that they all have $n_i = p - 1$, which can be seen by considering the action of the Frobenius on the local class group, which is multiplication by p on a cyclic of order $n_i + 1$. Since the Frobenius factors over the projective plane, one infers that $n_i + 1 \mid p$, hence $n_i + 1 = p$. As discussed in Section 13, the Chern number c_2 is the alternating sum of the Betti numbers on the minimal resolution of X, which yields the formula $c_2 - 3 = r(p-1)$.

One referee also pointed out that the arguments in the proof for Proposition 14.1 hold true for *general* polynomials $s \in \Gamma(\mathbb{P}^2, \mathscr{L}^{\otimes p})$ of degree pd, provided that $pd - d - 2 > 0$ and $d \geq 2$, by using the result of Liedtke [Liedtke 2013b, Theorem 3.4], which ensures that all occurring singularities must be rational double points of type A_{p-1}.

Let us remark that the surface $X \subset \mathbb{P}^3$ defined by the homogeneous polynomial

$$s = T_0 T_1 T_2^{2p-1} - T_0 T_1 T_3^{2p-1} + T_0^{2p} T_2 + T_1^{2p} T_3 + T_2^{2p+1} + T_3^{2p+1}$$

is a canonically polarized surface with

$$c_1^2 = (2p-3)^2(2p+1) \quad \text{and} \quad c_2 = 8p^3 - 4p^2 + 2p + 3,$$

such that $\mathfrak{h} = H^0(X, \Theta_{X/k})$ is isomorphic to $\mathfrak{sl}_1(k)$. We leave the details to the reader.

Next, we construct examples of smooth surfaces of general type X where the restricted Lie algebra $\mathfrak{h} = H^0(X, \Theta_{X/k})$ is isomorphic to k^m. The possibility of the following construction was suggested by one of the referees: Let C be a smooth curve with $h^0(\mathscr{O}_C) = 1$, together with an isomorphism $\varphi : \mathscr{L}^{\otimes pl} \to \Omega^1_{C/k}$ that is locally exact, for some invertible sheaf $\mathscr{L}$ of degree $d \geq 1$, and some integer $l \geq 1$ prime to the characteristic $p > 0$. This datum is called a *generalized Tango curve* of index l.

We are mainly interested in the case $l \equiv -1$ modulo p, and then write $l = pn - 1$. Lang [1983] used this situation to construct smooth surfaces X endowed with a fibration $f : X \to C$ with $\mathscr{O}_C = f_*(\mathscr{O}_X)$, where all geometric fibers are singular rational curves with a unique cuspidal singularity. One also says that $(C, \mathscr{L}, \varphi)$ is a *generalized Tango curve* of type (p, n, d), and X is the resulting *generalized Raynaud surface* of type (p, n, d).

Proposition 14.2. *In the above setting, suppose that $p \geq 3$ and $n \geq 2$. Then X is a minimal surface of general type with*

$$\mathfrak{h} = k^m \quad \textit{and} \quad \operatorname{Aut}_{X/k}[F] = \alpha_p^{\oplus m},$$

with $m = h^0(\mathscr{L})$. Further, the Chern invariants are given by $c_1^2 = d(p^4n^2 + 4p + 2np - n^2p^2 - 4np^2 - 2np^3)$ and $c_2 = 2pd(1 - np)$.

Proof. We may assume that k is algebraically closed. Since we assume that our Tango curve has index $l \equiv -1$ modulo p, and the characteristic is $p \geq 3$, we have $m = h^0(\mathscr{L})$, according to [Takeda 1992, Theorem 2.1]. Lang computed the Chern invariants, and observed that X is minimal and of general type [Lang 1983, Theorem 2 and beginning of Section 2].

Both restricted Lie algebras $k^m \rtimes \mathfrak{gl}_1(k)$ and $\mathfrak{sl}_2(k)$ contain nonzero multiplicative elements. In light of Theorem 12.1, our task is to verify that nonzero multiplicative vector fields do not exist on X. Seeking a contradiction, we suppose that $\delta \in H^0(X, \Theta_{X/k})$ is such a vector field. The saturation $\mathscr{O}_Y(\Delta)$ for the injection $\delta : \mathscr{O}_Y \to \Theta_{Y/k}$ defines an effective Cartier divisor $\Delta \subset X$. It follows from [Rudakov and Shafarevich 1976, Theorem 2], that every connected component is smooth. Hence, the irreducible components are pairwise disjoint, and horizontal for the fibration $f : X \to C$, because all closed fibers are singular.

To reach a contradiction we examine various curves on X and their intersection numbers. Write $F \subset X$ for a closed fiber, $D \subset X$ for reduced support of $\Omega^1_{X/C}$, and $S \subset X$ for the canonical section constructed in [Lang 1983, Section 2]. Note that D is also called the curve of cusps. According to loc. cit., one has

$$S^2 = d, \quad F^2 = 0, \quad (F \cdot S) = 1 \quad \text{and} \quad D = -pdF + pS.$$

Consequently $D^2 = -p^2 d$. For the curve $G = dF + nD$, we get $G^2 = dnp(2 - np) < 0$. According to loc. cit., Theorem 1, there is an exact sequence

$$0 \to \mathscr{O}_X(G) \to \Theta_{X/k} \to \omega_X^{\otimes -1}(-G) \to 0,$$

giving an identification $H^0(X, \mathscr{O}_X(G)) = H^0(X, \Theta_{X/k})$. Our global vector field δ factors over the inclusion $\mathscr{O}_X(G)$, which gives an equality $\mathscr{O}_X(\Delta) = \mathscr{O}_X(G)$ as subsheaves of $\Theta_{X/k}$. In particular, the curves Δ and G are linearly equivalent. Decompose the smooth curve $\Delta = \Delta_1 + \cdots + \Delta_r$ into irreducible components. We already observed that each Δ_i is horizontal. From $\Delta \cdot (dF + nD) = G^2 < 0$, we infer that $D \subset \Delta$. Now consider $\Delta' = \Delta - D$, which contains neither D nor F, and is linearly equivalent to $G' = dF + (n-1)D$. Then

$$pd(n-1)(2 - (n-1)p) = (G')^2 = (dF + (n-1)D) \cdot \Delta' \geq 0.$$

By our assumptions, we have $p \geq 3$ and $n \geq 2$, hence the left side is strictly negative, a contradiction. □

There are indeed generalized Tango curves C of type (p, n, d) with nonzero $m = h^0(\mathscr{L})$, for instance the curve C with affine equation $y^{lp} - y = x^{lp-1}$, where we set $l = pn - 1$, according to [Takeda 1992, Example 1.2].

It remains to verify some technical results used throughout this section. The following results are well known over the field of complex numbers (compare, for example, [Kollár and Mori 1998, Section 4.2] and [Arnold et al. 1985, Part II]). The arguments apparently work in all characteristics except $p = 2$. For the convenience of the reader, we give self-contained and characteristic-free proofs.

Let A be a complete local k-algebra that is regular of dimension three, with maximal ideal $\mathfrak{m}_A$ and residue field $k = A/\mathfrak{m}_A$. Note that for each choice of regular system of parameters $x, y, z \in A$, one obtains an identification $A = k[[x, y, z]]$.

Lemma 14.3. *Let $f \in A$ be an irreducible element such that $f \equiv x_0 y_0 + \lambda z_0^2$ modulo $\mathfrak{m}_A^3$ for some regular system of parameters x_0, y_0, z_0 and some $\lambda \in k$. Then there exists another regular system of parameters x, y, z such that $(f) = (xy + z^n)$, for some $n \geq 2$. Hence, $B = A/(f)$ is a rational double point of type A_{n-1}.*

Proof. We construct, by induction on $n \geq 0$, certain regular system of parameters $x_n, y_n, z_n \in A$ such that $x_n \equiv x_{n-1}$ and $y_n \equiv y_{n-1}$ modulo $\mathfrak{m}_A^n$, $z_n = z_0$ and

$$f = x_n y_n + x_n \phi_n + y_n \psi_n + h_n \tag{16}$$

for some $\phi_n, \psi_n \in \mathfrak{m}_A^{n+2}$ and $h_n \in z_n^2 k[[z_n]]$. For $n = 0$, we take x_0, y_0, z_0 as in our assumptions. If we already have defined $x_n, y_n, z_n \in A$, we set

$$x_{n+1} = x_n + \psi_n, \quad y_{n+1} = y_n + \phi_n \quad \text{and} \quad z_{n+1} = z_n. \tag{17}$$

Clearly $x_{n+1} \equiv x_n$ and $y_{n+1} \equiv y_n$ modulo $\mathfrak{m}_A^{n+1}$, and $z_{n+1} = z_0$. In particular the above is a regular system of parameters. Since $\phi_n \psi_n \in \mathfrak{m}_A^{2n+4}$, we may write

$$-\phi_n \psi_n = x_{n+1}\phi_{n+1} + y_{n+1}\psi_{n+1} + \sigma_n,$$

with $\phi_{n+1}, \psi_{n+1} \in \mathfrak{m}_A^{2n+3}$ and $\sigma_n \in z_{n+1}^{2n+4} k[[z_{n+1}]]$. Combining (16) and (17), we get

$$f = x_{n+1} y_{n+1} + x_{n+1}\phi_{n+1} + y_{n+1}\psi_{n+1} + h_{n+1},$$

where $h_{n+1} = h_n + \sigma_n$ belongs to $z_{n+1}^2 k[[z_{n+1}]]$. This completes our inductive definition. Note that $h_{n+1} \equiv h_n$ modulo $\mathfrak{m}_A^{2n+4}$.

By construction, the x_n, y_n, z_n are convergent sequences in A with respect to the $\mathfrak{m}_A$-adic topology. The limits $x, y, z \in A$ give the desired regular system of parameters: Since the ϕ_n, ψ_n converge to zero, we have $f = xy + h(z)$, where h is the limit of the $h_n \in k[[z]]$. We must have $h \neq 0$, because f is irreducible. Hence, $h = uz^n$ with $u \in k[[z]]^\times$ and $n \geq 2$. Replacing x by $u^{-1}x$, we finally get $(f) = (xy - z^n)$. Summing up, $B = A/(f)$ is a rational double point of type A_{n-1}. □

The condition in the proposition can be checked with partial derivatives, at least if k is algebraically closed. This makes the criterion applicable for computations:

Proposition 14.4. *Let $f \in \mathfrak{m}_A^2$. Suppose that k is algebraically closed and that*

$$\left(\frac{\partial^2 f}{\partial u_1 \partial u_2}\right)^2 - \left(\frac{\partial^2 f}{\partial u_1^2}\right) \cdot \left(\frac{\partial^2 f}{\partial u_2^2}\right) \notin \mathfrak{m}_A \tag{18}$$

for some system of parameters $u_1, u_2, u_3 \in A$. Then there exists another system of parameters x, y, z such that $f \equiv xy + \lambda z^2$ modulo $\mathfrak{m}_A^3$, for some $\lambda \in k$.

Proof. Write $f = q + g$, where $q = q(u_1, u_2, u_3)$ is a homogeneous polynomial of degree two and $g \in \mathfrak{m}_A^3$. Write $q = q_1 + u_3 l$, where $l = l(u_1, u_2, u_3)$ is homogeneous of degree one and $q_1 = q_1(u_1, u_2)$. If q_1 is a square, a straightforward computation with partial derivatives produces a contradiction to (18). Since k is algebraically closed, we have a factorization $q_1 = L_1 \cdot L_2$ where $L_1 = L_1(u_1, u_2)$ and $L_2 = L_2(u_1, u_2)$ are independent homogeneous polynomials of degree one. Then $w_1 = L_1$, $w_2 = L_2$ and w_3 form another regular system of parameters of A, and we have

$$q = w_1 w_2 + w_3 l = w_1 w_2 + a w_3 w_1 + b w_3 w_2 + c w_3^2,$$

with $a, b, c \in k$. We finally set $x = w_1 + b w_3$, $y = w_2 + a w_3$ and $z = w_3$. This is a further regular system of parameters, with $q = xy + \lambda z^2$, where $\lambda = c - ab$. Therefore, $f \equiv xy + \lambda z^2$ modulo $\mathfrak{m}_A^3$, as claimed. □

We also used a general fact on coherent sheaves: Let X be a noetherian scheme that is integral and normal, $\mathscr{E}$ be a coherent sheaf of rank two, $s : \mathscr{O}_X \to \mathscr{E}^\vee$ is a nonzero global section. The double dual $\mathscr{O}_X(-\Delta)$ for the image of the dual map $s^\vee : \mathscr{E}^{\vee\vee} \to \mathscr{O}_X$ defines an effective Weil divisor $\Delta \subset X$. By [Hartshorne 1994, Corollary 1.8], the duals of coherent sheaves on X are reflexive. Dualizing $\mathscr{E}^{\vee\vee} \to \mathscr{O}_X(-\Delta) \subset \mathscr{O}_X$, we see that the homomorphism s factors over an inclusion $\mathscr{O}_X(\Delta) \subset \mathscr{E}^\vee$. The latter is called the *saturation* of the section $s \in \Gamma(X, \mathscr{E}^\vee)$.

Lemma 14.5. *In the above setting there is a four-term exact sequence*

$$0 \to \mathscr{O}_X(\Delta) \to \mathscr{E}^\vee \to \mathscr{L}(-\Delta) \to \mathscr{N} \to 0,$$

where $\mathscr{L} = \underline{\mathrm{Hom}}(\Lambda^2(\mathscr{E}), \mathscr{O}_X)$ *and* $\mathscr{N}$ *is a coherent sheaf whose support has codimension at least two.*

Proof. According to [Hartshorne 1994, Theorem 1.12], it suffices to construct a short exact sequence $0 \to \mathscr{O}_X(\Delta) \to \mathscr{E}^\vee \to \mathscr{L}(-\Delta) \to 0$ on the complement of some closed set $Z \subset X$ of codimension at least two. Let $\mathscr{E}_0$ be the quotient of $\mathscr{E}$ by its torsion subsheaf. The surjection $\mathscr{E} \to \mathscr{E}_0$ induces an equality $\mathscr{E}_0^\vee = \mathscr{E}^\vee$, so we may assume that $\mathscr{E}$ is torsion free. It is then locally free in codimension one, so it suffices to treat the case that $\mathscr{E}$ is locally free. By construction, the cokernel $\mathscr{F}$ for $\mathscr{O}_X(\Delta) \subset \mathscr{E}^\vee$ is torsion-free of rank one, so we may assume that it is invertible. Taking determinants shows $\mathscr{F} \simeq \mathscr{L}(-\Delta)$. □

Acknowledgements

This research started during a visit of Schröer to the University of Cyprus, and he would like to thank the Department of Mathematics and Statistics for its hospitality. The research was also conducted in the framework of the research training group *GRK* 2240: *Algebro-Geometric Methods in Algebra, Arithmetic and Topology*. We would like to thank Yuya Matsumoto and Michel Brion for valuable comments. We also thank the referees for many helpful remarks and, in particular, for the suggestion to use Tango curves in Section 14.

References

[Arnold et al. 1985] V. I. Arnold, S. M. Guseĭn-Zade, and A. N. Varchenko, *Singularities of differentiable maps, I: The classification of critical points, caustics and wave fronts*, Monogr. Math. **82**, Birkhäuser, Boston, 1985. MR Zbl

[Artin 1969] M. Artin, "Algebraization of formal moduli, I", pp. 21–71 in *Global analysis*, edited by D. C. Spencer and S. Iyanaga, Univ. Tokyo Press, 1969. MR Zbl

[Artin 1971] M. Artin, *Algebraic spaces*, Yale Math. Monogr. **3**, Yale Univ. Press, 1971. MR Zbl

[Artin 1977] M. Artin, "Coverings of the rational double points in characteristic p", pp. 11–22 in *Complex analysis and algebraic geometry*, edited by W. L. Baily, Jr. and T. Shioda, Iwanami Shoten, Tokyo, 1977. MR Zbl

[Artin et al. 1972] M. Artin, A. Grothendieck, and J. L. Verdier, *Théorie des topos et cohomologie étale des schémas, Tome 2: Exposés V–VIII* (Séminaire de Géométrie Algébrique du Bois Marie 1963–1964), Lecture Notes in Math. **270**, Springer, 1972. MR Zbl

[Blanchard 1956] A. Blanchard, "Sur les variétés analytiques complexes", *Ann. Sci. École Norm. Sup.* (3) **73** (1956), 157–202. MR Zbl

[Block and Wilson 1988] R. E. Block and R. L. Wilson, "Classification of the restricted simple Lie algebras", *J. Algebra* **114**:1 (1988), 115–259. MR Zbl

[Bourbaki 1989] N. Bourbaki, *Lie groups and Lie algebras*, *Chapters* 1–3, Springer, 1989. MR Zbl

[Bourbaki 1990] N. Bourbaki, *Algebra, II: Chapters 4–7*, Springer, 1990. MR Zbl

[Brion et al. 2013] M. Brion, P. Samuel, and V. Uma, *Lectures on the structure of algebraic groups and geometric applications*, CMI Lect. Ser. Math. **1**, Hindustan, New Delhi, 2013. MR Zbl

[Chang 1941] H.-J. Chang, "Über Wittsche Lie–Ringe", *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 151–184. MR Zbl

[Demazure and Gabriel 1970] M. Demazure and P. Gabriel, *Groupes algébriques*, *I*: *Géométrie algébrique*, *généralités*, *groupes commutatifs*, Masson, Paris, 1970. MR Zbl

[Demazure and Grothendieck 1970] M. Demazure and A. Grothendieck, *Schémas en groupes, Tome II: Groupes de type multiplicatif, et structure des schémas en groupes généraux, Exposés VIII–XVIII* (Séminaire de Géométrie Algébrique du Bois Marie 1962–1964), Lecture Notes in Math. **152**, Springer, 1970. MR Zbl

[Ekedahl 1987] T. Ekedahl, "Foliations and inseparable morphisms", pp. 139–149 in *Algebraic geometry*, *II* (Brunswick, ME, 1985), edited by S. J. Bloch, Proc. Sympos. Pure Math. **46**, Amer. Math. Soc., Providence, RI, 1987. MR Zbl

[Ekedahl 1988] T. Ekedahl, "Canonical models of surfaces of general type in positive characteristic", *Inst. Hautes Études Sci. Publ. Math.* **67** (1988), 97–144. MR Zbl

[Ekedahl et al. 2012] T. Ekedahl, J. M. E. Hyland, and N. I. Shepherd-Barron, "Moduli and periods of simply connected Enriques surfaces", preprint, 2012. arXiv 1210.0342

[Evans and Fuchs 2002] T. J. Evans and D. B. Fuchs, "On the structure of the restricted Lie algebra for the Witt algebra in a finite characteristic", *Funktsional. Anal. i Prilozhen.* **36**:2 (2002), 69–74. In Russian; translated in *Funct. Anal. Appl.* **36**:2 (2002), 140–144. MR Zbl

[Fanelli and Schröer 2020] A. Fanelli and S. Schröer, "Del Pezzo surfaces and Mori fiber spaces in positive characteristic", *Trans. Amer. Math. Soc.* **373**:3 (2020), 1775–1843. MR Zbl

[Gille and Szamuely 2006] P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Stud. Adv. Math. **101**, Cambridge Univ. Press, 2006. MR Zbl

[Giraud 1971] J. Giraud, *Cohomologie non abélienne*, Grundlehren der Math. Wissenschaften **179**, Springer, 1971. MR Zbl

[Grothendieck 1960] A. Grothendieck, "Éléments de géométrie algébrique, I: Le langage des schémas", *Inst. Hautes Études Sci. Publ. Math.* **4** (1960), 5–228. MR Zbl

[Grothendieck 1968a] A. Grothendieck, "Le groupe de Brauer, I: Algèbres d'Azumaya et interprétations diverses", pp. 46–66 in *Dix exposés sur la cohomologie des schémas*, edited by A. Grothendieck and N. H. Kuiper, Adv. Stud. Pure Math. **3**, North-Holland, Amsterdam, 1968. MR Zbl

[Grothendieck 1968b] A. Grothendieck, "Le groupe de Brauer, III: Exemples et compléments", pp. 88–188 in *Dix exposés sur la cohomologie des schémas*, edited by A. Grothendieck and N. H. Kuiper, Adv. Stud. Pure Math. **3**, North-Holland, Amsterdam, 1968. MR Zbl

[Hartshorne 1994] R. Hartshorne, "Generalized divisors on Gorenstein schemes", *K-Theory* **8**:3 (1994), 287–339. MR Zbl

[Hochschild 1955] G. Hochschild, "Simple algebras with purely inseparable splitting fields of exponent 1", *Trans. Amer. Math. Soc.* **79** (1955), 477–489. MR Zbl

[Jacobson 1937] N. Jacobson, "Abstract derivation and Lie algebras", *Trans. Amer. Math. Soc.* **42**:2 (1937), 206–224. MR Zbl

[Jacobson 1941] N. Jacobson, "Restricted Lie algebras of characteristic p", *Trans. Amer. Math. Soc.* **50** (1941), 15–25. MR Zbl

[Jacobson 1943] N. Jacobson, *The theory of rings*, Amer. Math. Soc. Math. Surv. **2**, Amer. Math. Soc., New York, 1943. MR Zbl

[Jacobson 1944] N. Jacobson, "Galois theory of purely inseparable fields of exponent one", *Amer. J. Math.* **66** (1944), 645–648. MR Zbl

[Knutson 1971] D. Knutson, *Algebraic spaces*, Lecture Notes in Math. **203**, Springer, 1971. MR Zbl

[Kollár and Mori 1998] J. Kollár and S. Mori, *Birational geometry of algebraic varieties*, Cambridge Tracts in Math. **134**, Cambridge Univ. Press, 1998. MR Zbl

[Kondō and Schröer 2021] S. Kondō and S. Schröer, "Kummer surfaces associated with group schemes", *Manuscripta Math.* **166**:3-4 (2021), 323–342. MR Zbl

[Lang 1983] W. E. Lang, "Examples of surfaces of general type with vector fields", pp. 167–173 in *Arithmetic and geometry*, *II*, edited by M. Artin and J. Tate, Progr. Math. **36**, Birkhäuser, Boston, 1983. MR Zbl

[Laumon and Moret-Bailly 2000] G. Laumon and L. Moret-Bailly, *Champs algébriques*, Ergebnisse der Math. (3) **39**, Springer, 2000. MR Zbl

[Laurent and Schröer 2021] B. Laurent and S. Schröer, "Para-abelian varieties and Albanese maps", preprint, 2021. arXiv 2101.10829

[Liedtke 2013a] C. Liedtke, "Algebraic surfaces in positive characteristic", pp. 229–292 in *Birational geometry*, *rational curves*, *and arithmetic*, edited by F. Bogomolov et al., Springer, 2013. MR Zbl

[Liedtke 2013b] C. Liedtke, "The canonical map and Horikawa surfaces in positive characteristic", *Int. Math. Res. Not.* **2013**:2 (2013), 422–462. MR Zbl

[Lipman 1969] J. Lipman, "Rational singularities, with applications to algebraic surfaces and unique factorization", *Inst. Hautes Études Sci. Publ. Math.* **36** (1969), 195–279. MR Zbl

[Martin 2022a] G. Martin, "Automorphism group schemes of bielliptic and quasi-bielliptic surfaces", *Épijournal Géom. Algébrique* **6** (2022), art. id. 9. MR Zbl

[Martin 2022b] G. Martin, "Infinitesimal automorphisms of algebraic varieties and vector fields on elliptic surfaces", *Algebra Number Theory* **16**:7 (2022), 1655–1704. MR Zbl

[Martin-Deschamps and Lewin-Ménégaux 1978] M. Martin-Deschamps and R. Lewin-Ménégaux, "Applications rationnelles séparables dominantes sur une variété de type général", *Bull. Soc. Math. France* **106**:3 (1978), 279–287. MR Zbl

[Merkurjev 1981] A. S. Merkurjev, "On the norm residue symbol of degree 2", *Dokl. Akad. Nauk SSSR* **261**:3 (1981), 542–547. In Russian; translated in *Soviet Math. Dokl.* **24**:3 (1982), 546–551. MR Zbl

[Mumford et al. 1994] D. Mumford, J. Fogarty, and F. Kirwan, *Geometric invariant theory*, 3rd ed., Ergebnisse der Math. (2) **34**, Springer, 1994. MR Zbl

[Olsson 2016] M. Olsson, *Algebraic spaces and stacks*, Amer. Math. Soc. Colloq. Publ. **62**, Amer. Math. Soc., Providence, RI, 2016. MR Zbl

[Premet 1989] A. A. Premet, "Regular Cartan subalgebras and nilpotent elements in restricted Lie algebras", *Mat. Sb.* **180**:4 (1989), 542–557. In Russian; translated in *Math. USSR-Sb.* **66**:2 (1990), 555–570. MR Zbl

[Premet and Stewart 2019] A. Premet and D. I. Stewart, "Classification of the maximal subalgebras of exceptional Lie algebras over fields of good characteristic", *J. Amer. Math. Soc.* **32**:4 (2019), 965–1008. MR Zbl

[Rudakov and Shafarevich 1976] A. N. Rudakov and I. R. Shafarevich, "Inseparable morphisms of algebraic surfaces", *Izv. Akad. Nauk SSSR Ser. Mat.* **40**:6 (1976), 1269–1307. In Russian; translated in *Math. USSR-Izv.* **40**:6 (1976), 1205–1237. MR Zbl

[Russell 1984] P. Russell, "Factoring the Frobenius morphism of an algebraic surface", pp. 366–380 in *Algebraic geometry* (Bucharest, 1982), edited by L. Bădescu and D. Popescu, Lecture Notes in Math. **1056**, Springer, 1984. MR Zbl

[Sancho de Salas 2000] P. J. Sancho de Salas, "Automorphism scheme of a finite field extension", *Trans. Amer. Math. Soc.* **352**:2 (2000), 595–608. MR Zbl

[Schröer 2007] S. Schröer, "Kummer surfaces for the self-product of the cuspidal rational curve", *J. Algebraic Geom.* **16**:2 (2007), 305–346. MR Zbl

[Schröer 2010] S. Schröer, "On fibrations whose geometric fibers are nonreduced", *Nagoya Math. J.* **200** (2010), 35–57. MR Zbl

[Schröer 2021] S. Schröer, "Enriques surfaces with normal K3-like coverings", *J. Math. Soc. Japan* **73**:2 (2021), 433–496. MR Zbl

[Shepherd-Barron 1996] N. I. Shepherd-Barron, "Some foliations on surfaces in characteristic 2", *J. Algebraic Geom.* **5**:3 (1996), 521–535. MR Zbl

[Stacks 2005–] "The Stacks project", electronic reference, 2005–, http://stacks.math.columbia.edu.

[Strade 1993] H. Strade, "Die Klassifikation der einfachen Lie–Algebren über Körpern mit positiver Charakteristik: Methoden und Resultate", *Jahresber. Deutsch. Math.-Verein.* **95**:1 (1993), 28–46. MR Zbl

[Strade and Farnsteiner 1988] H. Strade and R. Farnsteiner, *Modular Lie algebras and their representations*, Monogr. Textb. Pure Appl. Math. **116**, Dekker, New York, 1988. MR Zbl

[Takeda 1992] Y. Takeda, "Vector fields and differential forms on generalized Raynaud surfaces", *Tohoku Math. J.* (2) **44**:3 (1992), 359–364. MR Zbl

[Tango 1972] H. Tango, "On the behavior of extensions of vector bundles under the Frobenius map", *Nagoya Math. J.* **48** (1972), 73–89. MR Zbl

[Waterhouse 1971] W. C. Waterhouse, "Automorphism schemes and forms of Witt Lie algebras", *J. Algebra* **17** (1971), 34–40. MR Zbl

[Xiao 1995] G. Xiao, "Bound of automorphisms of surfaces of general type, II", *J. Algebraic Geom.* **4**:4 (1995), 701–793. MR Zbl

[Zassenhaus 1939] H. Zassenhaus, "Über Lie'sche Ringe mit Primzahlcharakteristik", *Abh. Math. Sem. Univ. Hamburg* **13**:1 (1939), 1–100. MR Zbl

Communicated by Christopher Hacon
Received 2022-03-17 Revised 2022-06-15 Accepted 2022-08-18

schroeer@math.uni-duesseldorf.de *Mathematisches Institut, Heinrich-Heine-Universität, Düsseldorf, Germany*

tziolas@ucy.ac.cy *Department of Mathematics and Statistics, University of Cyprus, Nicosia, Cyprus*

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 17 No. 9 2023