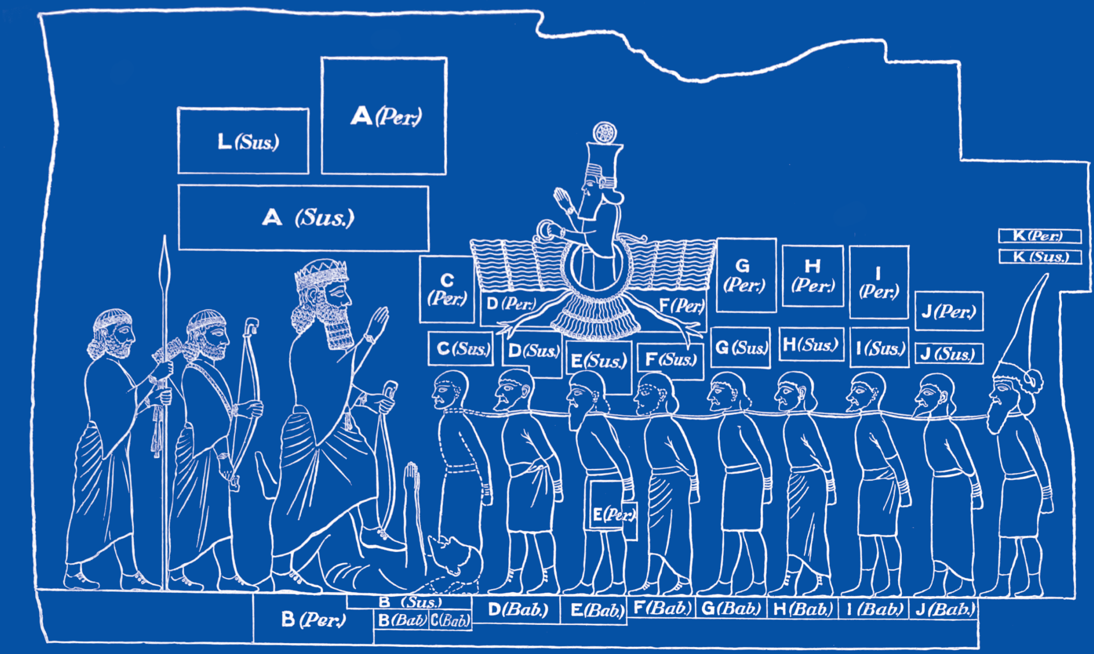
Moduli of abelian varieties via linear algebraic groups



Milan Lopuhaä-Zwakenberg

Moduli of abelian varieties via linear algebraic groups

Proefschrift
ter verkrijging van de graad van doctor
aan de Radboud Universiteit Nijmegen
op gezag van de rector magnificus prof. dr. J.H.J.M. van Krieken,
volgens besluit van het college van decanen
in het openbaar te verdedigen op dinsdag 25 september 2018
om 14:30 uur precies

door
Milan Abel Lopuhaä
geboren op 25 april 1990
te Amsterdam

Promotor: Prof.dr. B.J.J. Moonen

Manuscriptcommissie: Prof.dr. G.J. Heckman
Prof.dr. S.J. Edixhoven (Universiteit Leiden)
Dr. A.L. Kret (Universiteit van Amsterdam)
Prof.dr. L.D.J. Taelman (Universiteit van Amsterdam)
Prof.dr. T. Wedhorn (Technische Universität Darmstadt, Duitsland)

𐏐𐎠𐎭𐎶𐏐𐎭𐎠𐎼𐎹𐎺𐎢𐏁𐏐𐎧𐏁𐎠𐎹𐎰𐎡𐎹𐏐𐎺𐏀𐎼𐎣𐏐𐎧𐏁𐎠𐎹𐎰𐎡𐎹𐏐𐎧𐏁𐎠𐎹𐎰𐎡𐎹
𐎠𐎴𐎠𐎶𐏐𐎧𐏁𐎠𐎹𐎰𐎡𐎹𐏐𐎱𐎠𐎼𐎿𐎡𐎹𐏐𐎧𐏁𐎠𐎹𐎰𐎡𐎹𐏐𐎭𐏃𐎹𐎢𐎴𐎠𐎶𐏐𐎻𐏁𐎫
𐎠𐎿𐎱𐏃𐎹𐎠𐏐𐎱𐎢𐏂𐏐𐎠𐎼𐏁𐎠𐎶𐏃𐎹𐎠𐏐𐎴𐎱𐎠𐏐𐏃𐎧𐎠𐎶𐎴𐎡𐏁𐎡𐎹

Bīsotūn (Old Persian text) i 1-3, [28].

Contents

Chapter 0

General introduction

This dissertation focuses on two unrelated questions about group-theoretical invariants associated to abelian varieties: one concerning complex abelian varieties, and one concerning abelian varieties over finite fields. It turns out that both questions are best framed in the context of moduli spaces and stacks associated to abelian varieties. We can then answer these questions by studying these moduli spaces and stacks in the language of linear algebraic groups. For expository convenience, we discuss the two parts of this thesis in opposite order.

II: Integral Mumford–Tate groups of complex abelian varieties

Let A be a principally polarised complex abelian variety of dimension g. Let Λ be the integral Betti homology group $\mathrm{H}^1(A^{\mathrm{an}}, \mathbb{Z})$; this is a free abelian group of rank $2g$, and the polarisation induces a perfect pairing ψ on Λ. From Hodge theory, we know that Λ naturally is a polarised integral Hodge structure, i.e. there is a natural group homomorphism $h\colon \mathbb{C}^\times \to \mathrm{GSp}(\Lambda_\mathbb{R}, \psi_\mathbb{R})$. The Zariski closure $\mathtt{MT}(A)$ of $\mathrm{im}(h)$ in the integral group scheme $\mathtt{GSp}(\Lambda, \psi)$ is called the (integral) *Mumford–Tate group* of A; it is a flat group scheme over $\mathbb{Z}$. Its generic fibre $\mathtt{MT}(A)_\mathbb{Q}$ is a connected reductive algebraic group over $\mathbb{Q}$, and it is known to contain important information about A; for example, $\mathtt{MT}(A)_\mathbb{Q}$ is a torus if and only if A is a CM abelian variety. An advantage of looking at the generic fibre is that we have a well-developed theory of reductive algebraic groups and their representations, which makes it easier to study A via $\mathtt{MT}(A)_\mathbb{Q}$. A disadvantage of looking at only this generic fibre, however, is that it is invariant under isogenies; as such we can only obtain information about the isogeny class of A. In part II, we study how much 'extra' information we can obtain by taking additional integral information into account:

Question. *Let A be a complex abelian variety. To what extent does the integral group scheme* $\mathtt{MT}(A)$ *uniquely determine A?*

In general, the group scheme $\mathtt{MT}(A)$ does not determine A uniquely. We can see this by looking at a *moduli space* of g-dimensional abelian varieties: this is the complex scheme $\mathcal{A}_g$ such that for every complex scheme S, there is a natural bijection

$$\mathrm{Hom}(S, \mathcal{A}_g) \cong \Big\{g\text{-dim. princ. pol. abelian schemes } X/S + \text{extra data}\Big\}/\cong;$$

The extra data is needed to ensure that $\mathcal{A}_g$ exists as a quasiprojective complex variety. We can deform the abelian variety A by conjugating the Hodge structure morphism h with an element $x \in \mathrm{GSp}(\Lambda_{\mathbb{R}}, \psi_{\mathbb{R}})$. Let $\mathscr{G} = \mathtt{MT}(A)$; then the abelian varieties obtained by conjugating h by elements of $\mathscr{G}(\mathbb{R})$ define a complex subvariety of $\mathcal{A}_g$. The irreducible components of the subvarieties obtained in this way are called *special subvarieties*. they often admit a moduli interpretation; for instance, the subvariety of $\mathcal{A}_g$ parametrising abelian varieties with an action of a given ring R is a special subvariety. If $Y \subset \mathcal{A}_g$ is a special subvariety obtained from A as above, then a sufficiently generic point $y' \in Y(\mathbb{C})$ corresponds to a complex abelian variety A' satisfying $\mathtt{MT}(A') \cong \mathscr{G}$; as such we call $\mathscr{G}$ the *generic Mumford–Tate group of Y*, denoted $\mathtt{GMT}(Y)$. The question then becomes to what extent $\mathscr{G}$ uniquely determines Y. We answer this question in chapter 8:

Answer. (Theorem 8.1) *Let $\mathscr{G}$ be a group scheme over $\mathbb{Z}$. Then there are at most finitely many special subvarieties Y of $\mathcal{A}_g$ such that* $\mathtt{GMT}(Y) \cong \mathscr{G}$.

In general, this is the best we can hope for, since in general a class group-like obstruction will prevent $\mathscr{G}$ from corresponding to a single special subvariety. As might be expected from this short discussion, the main ingredient in the proof of theorem 8.1 is the theory of linear algebraic groups and their representations. In chapter 7, we prove a theorem (7.1) concerning the integral group schemes that appear in the context of representations of linear algebraic groups. In chapter 8 we use this result to prove theorem 8.1. We also study the consequences of this theorem in the context of the Mumford–Tate conjecture, a well-known conjecture concerning the compatibility between the singular and étale cohomology of an abelian variety.

I: Torsion subgroups of abelian varieties over finite fields

Let p be a prime number, let n be a positive integer, and let A be an abelian variety over a field k. Let $A[p^n]$ be the p^n-torsion subgroup of A, considered as a commutative group scheme over k. If $\mathrm{char}(k) \neq p$, then after replacing k by its algebraic closure we find $A[p^n] \cong (\mathbb{Z}/p^n\mathbb{Z})_k^{2\cdot\dim(A)}$. If $\mathrm{char}(k) = p$, we find a different behaviour: the group scheme $A[p^n]$ will no longer be smooth, and even over algebraically closed fields there are multiple nonisomorphic possibilities for how the infinitesimal structure manifests. For elliptic curves and $n = 1$, this gives us the distinction between supersingular and ordinary elliptic curves. If k is a finite field, then there are only finitely many options for $A[p^n]$, provided we fix $\dim(A)$. This leads to the following question:

Question. *Let k be a finite field of characteristic p, and let g and n be positive integers. How many options are there for the k-group scheme $A[p^n]$, where A ranges over the abelian varieties over k of dimension g?*

Such a group $A[p^n]$ is called a *truncated Barsotti–Tate group of level n*, or BT_n for short; for a given $\mathbb{F}_p$-scheme S, the BT_n over S with some given numerical invariants (such as its order $2g$) form a category $\mathsf{BT}_n(S)$. One way to answer the question above is to look at *moduli stacks* of BT_n. The theory of algebraic stacks is quite involved, but naïvely one should think of a moduli stack BT_n as a categorical construction such that for every $\mathbb{F}_p$-scheme S, we get a 'natural' geometrical structure on the category $\mathsf{BT}_n(S)$ (as opposed to a moduli space, where we get a geometrical structure on the *set* of isomorphism classes $[\mathsf{BT}_n(S)]$). Moduli stacks often appear in cases where moduli spaces fail to exist. For a given finite field k, we define the *point count of* BT_n *over* k to be

$$\#\mathsf{BT}_n(k) := \sum_{x \in [\mathsf{BT}_1(k)]} \frac{1}{\#\mathrm{Aut}(x)},$$

where $[\mathsf{BT}_n(k)]$ is the set of isomorphism classes in the category $\mathsf{BT}_n(k)$; in other words, we count the isomorphism classes of BT_n, but we count an object x with weight $(\#\mathrm{Aut}(x))^{-1}$. This choice is motivated by the fact that this definition of point counts has the same relation to the cohomology of the stack BT_n as what we would expect from the cohomology of schemes (see theorem 2.2). Because of this, we want to answer the question above by calculating $\#\mathsf{BT}_n(k)$. In chapter 2, we study the point counts of stacks as well as their zeta functions, which are rational power series that contain information about all point counts over finite fields. We develop methods to calculate the point counts and zeta functions of *quotient stacks*, which are stacks $[G\backslash X]$ that are algebro-geometric avatars of the quotient of a variety X by the action of a linear algebraic group G. In chapter 3, we apply these methods to stacks of the form BT_n, by studying how BT_n over finite fields can be described via linear algebraic groups, and how this relates the stack BT_n to quotient stacks. This allows us to answer the question above:

Answer. (Theorem 3.33) *Let BT_n be a moduli stack of BT_n. Then we can find direct formulas for the point counts and zeta functions of BT_n.*

We also apply these methods to two generalisations of the stack BT_1. In chapter 4 we consider flags of group schemes that can appear as flags in a BT_1. Although we cannot give a direct formula for the point counts and zeta functions of moduli stacks X of such flags, we will give an algorithm that finds a polynomial $R \in \mathbb{Z}[X, X^{-1}]$ such that $\#\mathsf{X}(\mathbb{F}_q) = R(q)$ for all powers q of p. In chapter 5 we consider stacks of BT_1 with some additional structure, such as a polarisation or a given endomorphism algebra; previous research ([55], [56]) has formalised these to so-called *G-zips*, which are objects in the theory of linear algebraic groups. Using the description of stacks of G-zips in [56], and our results on the point counts and zeta functions of quotient stacks, we are able to find a direct formula for both the point counts and the zeta functions of stacks of G-zips.

About the cover

The cover of this dissertation is adapted from plate XIII in [28]. It is a schematic depiction of the rock relief on Bīsotūn mountain (بیستون) in Iran. The relief depicts the Persian king Darius along with representatives of various conquered peoples. The relief is accompanied by a description of Darius' empire and his reign in the three languages Old Persian, Elamite, and Akkadian; the first lines of the Old Persian text form the motto of this dissertation. Transliterated and translated the text reads as follows:

Adam Dārayavauš, xšāyaθiya vazraka, xšāyaθiya xšāyaθiyā-
nām, xšāyaθiya Pārsaiy, xšāyathiya dahyūnām, Vištā-
spahyā puça, Aršāmahyā napā, Haxāmanišiya.

'I am Darius, the great king, king of kings, the king of Persia, the king of countries, the son of Hystaspes, the grandson of Arsames, the Achaemenid.'

I have chosen this cover for two reasons. The first reason concerns the title 'king of kings', i.e. *xšāyaθiya xšāyaθiyānām*. In the Achaemenid empire, and especially in the Median and Assyrian empires before that, this title was to be taken literally: a king was the ruler of a city or province, and the ruler of the entire empire had the same relation to these kings as a king had to its subjects.[1] In algebraic geometry, the position of king of kings is held by a (fine) moduli space, which can be considered a 'space of spaces': for example, an abelian variety can (somewhat naïvely) be considered as a set of points enriched with a geometric structure. In the same way a moduli space of abelian varieties enriches a set of abelian varieties with a geometric structure. As such the relation between a moduli space and abelian varieties is the same as the relation between an abelian variety and its points.

The second reason concerns the importance of this inscription for the decipherment of cuneiform. Cuneiform was used to write a wide variety of Near Eastern languages since 3100 BC. After it fell into disuse in the first century AD, the script remained undeciphered for a long time. The first cuneiform language to be deciphered was Old Persian in the 1830s, which could be deciphered due to the fact that it used an alphabetic system with only 50 signs, and because it was related to Modern Persian and Sanskrit, two languages already known to orientalists. Most cuneiform languages, however, used variants of the far more complicated Sumerian cuneiform, which had hundreds of signs. The key to deciphering this system was the inscription at Bīsotūn, which played the same role as the Rosetta stone did for the decipherment of Egyptian hieroglyphs: the fact that the Old Persian text could

[1] In the Achaemenid empire the satrapies were ruled by satraps (viceroys) rather than actual kings, and the king of kings was officially also king of each of the individual satrapies. Aside from terminological differences the same principle applied, however.

be read allowed for the decipherment of the Akkadian text, which was discovered to be a Semitic language. This provided a starting point for the translation of the vast amount of literature in Akkadian, and from there the decipherment of the other languages written in Sumerian cuneiform.

The theme of translation and decipherment plays a large role in this dissertation. In this analogy, the role of Akkadian is played by moduli spaces of abelian varieties, whose geometric structure we wish to understand. The role of Old Persian is played by linear algebraic groups: while to the layman these are as magical[2] as the moduli spaces themselves, algebraic geometers have extensively studied their structure and classification. By describing moduli spaces of abelian varieties in terms of linear algebraic groups we are given more tools to work with in order to understand these moduli spaces.

[2]The reader will be delighted to know that the English word *magic* is derived from the Old Persian word *maguš* 'Zoroastrian priest', which is attested in the Bīsotūn inscription.

Part I

Point counts and zeta functions

Chapter 1

Introduction

Throughout this part we fix a prime number p. Let k be a field of characteristic p. A *truncated Barsotti–Tate group of level* 1 (henceforth BT_1) of height h is a finite group scheme of order p^h over k of exponent p that can be realised as the p-torsion of a p-divisible group or Barsotti–Tate group (see definition 3.1). The motivating example for BT_1 comes from abelian varieties: if A is an abelian variety over k, then its p-torsion $A[p]$ is a BT_1 of height $2 \cdot \dim(A)$. The BT_1 over an algebraically closed field k were first classified in [32]. These results were used in [52] to obtain the so-called Ekedahl–Oort stratification on the moduli space of abelian varieties in characteristic p. We can describe this stratification in terms of algebraic stacks: BT_1 of a given height (plus some other numerical invariants) form an algebraic stack of finite type BT_1 over $\mathbb{F}_p$ (see [70]). If $\mathcal{A}_{g,N}$ is the moduli space of principally polarised abelian varieties of dimension g with full level N structure in characteristic p, then there exists a smooth, surjective morphism of $\mathbb{F}_p$-stacks $\mathcal{A}_{g,N} \to \mathsf{BT}_1$ (see [71]). The fibres of this morphism form the strata of the Ekedahl–Oort stratification.

The goal of this chapter is to study the stack BT_1 and several related stacks, via their *point counts* and their *zeta functions*. For a power q of p and an algebraic stack X over $\mathbb{F}_p$ one can define the point count of the category $\mathsf{X}(\mathbb{F}_q)$ (definition 2.1); by this we mean that we count the isomorphism classes in $\mathsf{X}(\mathbb{F}_q)$, where the class of an object x is given the weight $\frac{1}{\#\mathrm{Aut}(x)}$. As is the case for schemes this point count is in fact related to the ℓ-adic cohomology of X (theorem 2.2). The point counts $\#\mathsf{X}(\mathbb{F}_q)$ for varying q are organised in the *zeta function* $Z(\mathsf{X}, t) \in \mathbb{Q}[\![t]\!]$ (definition 2.22). The zeta function represents a meromorphic function that is defined on all of $\mathbb{C}$. Furthermore, if a stack is a Deligne–Mumford stack, then its zeta function is a rational function.

Via Dieudonné theory there is a one-to-one correspondence between BT_1 over a perfect field k of characteristic p and level 1 Dieudonné modules over k; these are k-vector spaces with some semilinear data (definition 3.4). In terms of algebraic stacks, we find a moduli stack D_1 of level 1 Dieudonné modules (with some numerical invariants), together with a morphism of stacks

$$\mathsf{BT}_1 \to \mathsf{D}_1$$

that is an equivalence of categories on perfect fields. As the zeta function of a stack only depends on its values on finite fields we find $Z(\mathsf{BT}_1, t) = Z(\mathsf{D}_1, t)$. The advantage of this approach is that we can describe the stack D_1 via quotient stacks $[G\backslash X]$, where G is an algebraic group over $\mathbb{F}_p$ acting on a variety X. In chapter 2 we develop methods to calculate the point counts and zeta functions of quotient stacks. We apply these methods to three generalisations of moduli stacks of BT_1:

1. Instead of looking at BT_1 we may look at BT_n for $n \geq 1$, i.e. truncated Barsotti–Tate groups of level $n \geq 1$. The main examples of these are p^n-torsion kernels $A[p^n]$ of abelian varieties A over a field k. Via Dieudonné theory these correspond to free modules over $\mathrm{W}_n(k)$, the n-th truncated Witt vector ring of k, along with some semi-linear data. Over an algebraically closed field the BT_{n+1} extending a given BT_n were classified via orbits under the action of an algebraic group on an affine space in [69] and [19]. By interpreting these results in a 'stacky' way we can use our results on zeta functions on quotient stacks to determine the zeta function of moduli stacks of BT_ns (see theorem 3.33).

2. Instead of looking at BT_1, we look at 'flags' of k-group schemes of the form $G_1 \subset G_2 \subset \cdots \subset G_r$, where G_r is a BT_1. On the level of abelian varieties this corresponds to the reduction of a moduli space with partial level n structure rather than full level n structure. If BTFlag is a moduli stack of such flags, then we provide an algorithm (4.24) to calculate a polynomial $R \in \mathbb{Z}[X, X^{-1}]$ such that $\#\mathsf{BTFlag}(\mathbb{F}_q) = R(q)$ for all powers q of p. This also gives us an expression for the zeta function $Z(\mathsf{BTFlag}, t)$.

3. We can generalise the concept of BT_1 to that of BT_1 with some additional structure, such as the action of a given ring of endomorphisms, or a polarisation. For instance, in the study of abelian varieties such objects arise if we replace $\mathcal{A}_g$ with the reduction of a Shimura variety of PEL type (see [70]). Over an algebraically closed field these were first classified in [43], in terms of the Weyl group of an associated reductive group G over $\mathbb{F}_p$. The underlying semilinear algebra objects were later generalised in [47] to so-called F-zips. The classification of F-zips, as well as the classification of F-zips with additional structure, could again be stated in terms of the Weyl group of a reductive group G. These F-zips were again generalised in [55] and [56] to so-called *G-zips*, where the reductive group G is the primordial object. In [56] moduli stacks of G-zips are realised as quotient stacks. We use this description, along with (a generalisation of) the description of the automorphism schemes of G-zips, to calculate the zeta functions of moduli stacks of G-zips (see theorem 5.25).

The structure of this part is as follows. In chapter 2 we define point counts and zeta functions, and we develop some methods to calculate them in the case of quotient stacks. In chapter 3 we discuss the relation between BT_n and Dieudonné modules, and we calculate the zeta function of moduli stacks of BT_n. In chapter 4 we find an algorithm to calculate the zeta function of moduli stacks of $\mathtt{BT}_1$-flags. In chapter 5 we introduce G-zips as defined in [56], and we calculate the zeta function of moduli stacks of G-zips.

Parts of this part of the dissertation, namely section 3.4 and chapter 5, are taken from [37], albeit slightly modified. Parts of section 2.1, in particular proposition 2.15 and the results leading up to it, are also present in this preprint.

As mentioned before we fix a prime number p. Furthermore, we will use the notation Hom, Aut, Stab, etc. for homomorphism sets (or abelian groups), automorphism groups, and stabiliser groups, while we will use $\mathtt{Hom}$, $\mathtt{Aut}$, $\mathtt{Stab}$, etc. for the underlying schemes, if these exist. For a power q of p we write Fr_q for the q-th power Frobenius map.

Chapter 2

Point counts and zeta functions of quotient stacks

In this chapter we develop some tools for determining the point counts and zeta functions of quotient stacks over finite fields. We will use these methods in the following chapters to calculate the zeta functions of moduli stacks related to truncated Barsotti–Tate groups. The main results of this chapter (propositions 2.15, 2.20, and 2.21, and theorem 2.27) are unfortunately quite technical in nature, but we need them in this form in order to apply them in the following chapters.

2.1 Point counts on torsion stacks

Throughout this section we let k be a finite field. In this section we study the point counts of categories, in particular those associated to quotient stacks. If C is an (essentially small) category, we write $[\mathsf{C}]$ for its set of isomorphism classes.

Definition 2.1. Let C be a category. Then C is *essentially finite* if it is equivalent to a category with finitely many objects and morphisms. If C is essentially finite, we define its *point count* to be

$$\#\mathsf{C} := \sum_{x \in [\mathsf{C}]} \frac{1}{\#\mathrm{Aut}(x)}.$$

If X is an algebraic stack of finite type over k, then for every finite extension k' of k the category $\mathsf{X}(k')$ is essentially finite. The following theorem relates the point count of an algebraic stack to its cohomology.

Theorem 2.2. (See [63, 1.1]) *Let* X *be an algebraic stack of finite type over* k*. Let* F *be the geometric Frobenius on* X*. Let* ℓ *be a prime number different from the characteristic of* k*, and let* $\iota\colon \bar{\mathbb{Q}}_\ell \xrightarrow{\sim} \mathbb{C}$ *be an isomorphism of fields. For an integer* n*, let* $\mathrm{H}^n_c(\mathsf{X}, \bar{\mathbb{Q}}_\ell)$ *be the cohomology with compact support of the constant sheaf* $\bar{\mathbb{Q}}_\ell$ *on* X *as in [35, 3.1]. Then the infinite sum*

$$\sum_{n\in\mathbb{Z}}(-1)^n \mathrm{Tr}(F, \mathrm{H}^n_c(\mathsf{X}_{\bar{k}}, \bar{\mathbb{Q}}_\ell))$$

converges to $\#\mathsf{X}(k)$ *when considered as a complex series via* ι*.* □

This theorem generalises the Lefschetz trace formula for separated schemes of finite type. As such, this theorem motivates our definition of point count. It also shows the relation between the point count of a stack and its geometry. In the rest of this section we develop methods to calculate the point counts of quotient stacks.

Let G be a smooth algebraic group over k. Let X be a *variety* over k, by which we mean in this thesis a reduced k-scheme of finite type. Suppose X has a left action of G. Recall that the *quotient stack* $[G\backslash X]$ is defined as follows: If S is a k-scheme, then the objects of the category $[G\backslash X](S)$ are pairs (T, f), where T is a left G-torsor over S in the étale topology, and $f\colon T \to X_S$ is a G_S-equivariant morphism of S-schemes. A morphism $(T, f) \to (T', f')$ in $[G\backslash X](S)$ is an isomorphism of G-torsors $\varphi\colon T \xrightarrow{\sim} T'$ such that $f = f'\varphi$. In order to calculate point counts we first need to set up a bit of notation.

Notation 2.3. Suppose G is a smooth algebraic group over k, and let z be a cocycle in $\mathrm{Z}^1(k, G)$. Recall that this means that z is a continuous map $z\colon \mathrm{Gal}(\bar{k}/k) \to G(\bar{k})$ (where the right hand side has the discrete topology) for which the following equation is satisfied for all $\pi, \pi' \in \mathrm{Gal}(\bar{k}/k)$:

$$z(\pi\pi') = z(\pi) \cdot {}^{\pi}z(\pi') \tag{2.4}$$

Let X be a k-variety with a left action of G, and let z be a cocycle in $\mathrm{Z}^1(k, G)$. We define the twisted scheme X_z as follows: Let $X_{z,\bar{k}}$ be isomorphic to $X_{\bar{k}}$ as $\bar{k}$-schemes with a $G_{\bar{k}}$-action via an isomorphism $\varphi_z\colon X_{z,\bar{k}} \xrightarrow{\sim} X_{\bar{k}}$. We define the Galois action on $X_{z,\bar{k}}$ by taking

$${}^{\pi}x := \varphi_z^{-1}(z(\pi) \cdot {}^{\pi}\varphi_z(x))$$

for all $x \in X_{z,\bar{k}}(\bar{k})$ and all $\pi \in \mathrm{Gal}(\bar{k}/k)$; this defines a variety X_z over k. Its isomorphism class only depends on the class of z in $\mathrm{H}^1(k, G)$. Two cases deserve special mention:

- We let G act on itself on the left by defining $g \cdot x := xg^{-1}$. Then G_z is a left G-torsor, and $\mathrm{H}^1(k, G)$ classifies the left G-torsors in this way.
- We let G act on itself on the left by inner automorphisms. The corresponding twisted group is denoted $G_{\mathrm{in}(z)}$. If X is a k-variety with a left G-action, then X_z naturally has a left $G_{\mathrm{in}(z)}$-action.

This terminology enables us to formulate the following proposition.

Proposition 2.5. *Let k' be a finite extension of k. Let G be a smooth algebraic group over k, and let X be a k-variety equipped with a left action of G. Then*

$$\#[G\backslash X](k') = \sum_{z \in \mathrm{H}^1(k',G)} \frac{\#X_z(k')}{\#G_{\mathrm{in}(z)}(k')}.$$

Proof. It suffices to show this for $k' = k$. Let T be a left G-torsor over k', and let $z \in \mathrm{Z}^1(k,G)$ be such that $T \cong G_z$. Then the automorphism group scheme of T as a left G-torsor is $G_{\mathrm{in}(z)}$, which acts by right multiplication on G_z. As such, we may consider T as a $(G, G_{\mathrm{in}(z)})$-bitorsor. If we look at the left G-action, we can define a variety T_z as in notation 2.3. This naturally has the structure of a $(G_{\mathrm{in}(z)}, G_{\mathrm{in}(z)})$-bitorsor; in fact, it is easily verified that it is a trivial bitorsor. If $f\colon T \to X_k$ is a (left) G-equivariant map, then the map $f_{\bar{k}}\colon T_{\bar{k}} \to X_{\bar{k}}$ is defined over k when considered as a map $T_{z,\bar{k}} \to X_{z,\bar{k}}$, and we denote the resulting map $T_z \to X_z$ by f_z; it is (left) $G_{\mathrm{in}(z)}$-equivariant. This gives a one-to-one correspondence between $\mathrm{Hom}_G(T,X)$ and $\mathrm{Hom}_{G_{\mathrm{in}(z)}}(T_z, X_z)$. Let t_0 be an element of $T_z(k)$, which exists since T_z is a trivial $G_{\mathrm{in}(z)}$-torsor. We may identify the sets $\mathrm{Hom}_{G_{\mathrm{in}(z)}}(T_z, X_z)$ and $X_z(k)$ by identifying a map with its image of t_0, and two maps $f_z, f'_z \in \mathrm{Hom}_{G_{\mathrm{in}(z)}}(T_z, X_z)$ correspond to isomorphic objects $(T,f), (T,f')$ in $[G\backslash X](k)$ if and only if $f_z(t_0)$ and $f'_z(t_0)$ are in the same $G_{\mathrm{in}(z)}(k)$-orbit in $X_z(k)$. On the other hand, the automorphism group of (T,f) is identified with $\mathrm{Stab}_{G_{\mathrm{in}(z)}(k)}(f_z(t_0))$. From the orbit-stabiliser formula we find

$$\sum_{\substack{(T',f') \in [[G\backslash X](k)],\\ T' \cong T}} \frac{1}{\#\mathrm{Aut}(T',f')} = \sum_{x \in G_{\mathrm{in}(z)}(k)\backslash X_z(k)} \frac{1}{\#\mathrm{Stab}_{G_{\mathrm{in}(z)}(k)}(x)} = \frac{\#X_z(k)}{\#G_{\mathrm{in}(z)}(k)}.$$

Summing over all cohomology classes in $\mathrm{H}^1(k,G)$ now proves the proposition. □

While proposition 2.5 gives a direct formula for the point count of a quotient stack over a given field extension k' of k, it is not as useful in a context where k' varies, as it is a priori unclear how $\mathrm{H}^1(k',G)$ varies with it. In propositions 2.15, 2.20 and 2.21 we give formulas for the point counts $[G\backslash X](k')$ that do not involve determining the cohomology set $\mathrm{H}^1(k',G)$, under some (quite technical) conditions on G and X. We first set up some notation.

Notation 2.6. As before let G be a smooth algebraic group over k, and let $\pi \in \mathrm{Gal}(\bar{k}/k)$ be the $\#k$-th power Frobenius. We let $G(\bar{k})$ act on itself on the left by defining

$$g \cdot x := gx({}^{\pi}g)^{-1}. \tag{2.7}$$

Its set of orbits is denoted $\mathrm{Conj}_k(G)$.

Lemma 2.8. *Let G be a smooth algebraic group over k. Let $\pi \in \mathrm{Gal}(\bar{k}/k)$ be the $\#k$-th power Frobenius. Then the map*

$$\begin{aligned} \mathrm{Z}^1(k,G) &\to G(\bar{k}) \\ z &\mapsto z(\pi) \end{aligned}$$

is a bijection, and it induces a bijection $\mathrm{H}^1(k,G) \xrightarrow{\sim} \mathrm{Conj}_k(G)$.

Proof. Let Π be the Galois group $\mathrm{Gal}(\bar{k}/k)$. Since $\langle\pi\rangle \subset \Pi$ is a dense subgroup, the map is certainly injective. To show that it is surjective, fix a $g \in G(\bar{k})$, and define a map $z\colon \langle\pi\rangle \to G(\bar{k})$ by

$$z(\pi^n) = \begin{cases} g \cdot ({}^{\pi}g) \cdots ({}^{\pi^{n-1}}g), & \text{if } n \geq 0; \\ ({}^{\pi^{-1}}g^{-1}) \cdots ({}^{\pi^{n}}g^{-1}) & \text{if } n < 0. \end{cases}$$

This satisfies the cocycle condition (2.4) on $\langle\pi\rangle$. Let e be the unit element of $G(\bar{k})$. To show that we can extend z continuously to Π, we claim that there is an integer n such that $z(\pi^N) = e$ for all $N \in n\mathbb{Z}$. To see this, let k' be a finite extension of k such that $g \in G(k')$. Then from the definition of the map z we see that z maps $\langle\pi\rangle$ to $G(k')$. The latter is a finite group, and hence there must be two nonnegative integers $m < m'$ such that $z(\pi^m) = z(\pi^{m'})$. Set $n = m' - m$. From the definition of z we see that

$$z(\pi^{m'}) = z(\pi^m) \cdot ({}^{\pi^m}g) \cdots ({}^{\pi^{m'-1}}g),$$

hence $({}^{\pi^m}g) \cdots ({}^{\pi^{m'-1}}g) = e$; but the left hand side of this is equal to ${}^{\pi^m}z(\pi^n)$, hence $z(\pi^n) = e$. The cocycle condition (2.4) now tells us that $z(\pi^N) = e$ for every multiple N of n; furthermore, we see that for general $f \in \mathbb{Z}$ the value $z(\pi^f)$ only depends on $\bar{f} \in \mathbb{Z}/n\mathbb{Z}$. Hence we can extend z to all of Π via the composite map

$$\Pi \twoheadrightarrow \Pi/n\Pi \xrightarrow{\sim} \langle\pi\rangle/\langle\pi^n\rangle \xrightarrow{z} G(\bar{k}),$$

and this is an element of $\mathrm{Z}^1(k,G)$ that sends π to g; hence the map in the lemma is surjective, as was to be shown. This map is also $G(\bar{k})$-equivariant with respect to the actions that give rise to the quotients $\mathrm{H}^1(k,G)$ and $\mathrm{Conj}_k(G)$, which proves the second statement of the lemma. □

Recall that the *classifying stack* of an algebraic group G is defined to be $\mathsf{B}(G) := [G\backslash *]$, where $* = \mathrm{Spec}(k)$ (with the trivial G-action).

Lemma 2.9. *Let G be a finite étale group scheme over k. Then for every finite extension k' of k we have $\#\mathsf{B}(G)(k') = 1$.*

Proof. It suffices to show this for $k = k'$. The category $\mathsf{B}(G)(k)$ is the category of G-torsors over k; its objects are classified by $\mathrm{H}^1(k,G)$. Let $\pi \in \mathrm{Gal}(\bar{k}/k)$ be the $\#k$-th power Frobenius, and let $z \in \mathrm{H}^1(k,G)$. Then the automorphism group (as an abstract group) of the torsor G_z is equal to $G_{\mathrm{in}(z)}(k)$, which equals

$$\begin{aligned} G_{\mathrm{in}(z)}(k) &\cong \left\{ g \in G(\bar{k}) : g = z(\pi) \cdot {}^{\pi}g \cdot z(\pi)^{-1} \right\} \\ &= \left\{ g \in G(\bar{k}) : z(\pi) = g \cdot z(\pi) \cdot ({}^{\pi}g)^{-1} \right\} \\ &= \mathrm{Stab}_{G(\bar{k})}(z(\pi)), \end{aligned}$$

where the action of $G(\bar{k})$ on itself in the last line is the one in (2.7). For every orbit $C \in \mathrm{Conj}_k(G)$ choose an element $x_C \in C$; then the orbit-stabiliser formula and lemma 2.8 yield

$$\begin{aligned}\sum_{z\in \mathrm{H}^1(k,G)} \frac{1}{\#\mathrm{Aut}(G_z)} &= \sum_{C\in \mathrm{Conj}_k(G)} \frac{1}{\#\mathrm{Stab}_{G(\bar{k})}(x_C)} \\ &= \sum_{C\in \mathrm{Conj}_k(G)} \frac{\#C}{\#G(\bar{k})} \\ &= 1.\end{aligned}$$

□

Lemma 2.10. *Let $1 \to A \to B \to C \to 1$ be a short exact sequence of smooth algebraic groups over k. Suppose that A is connected.*

1. *The natural map $\mathrm{H}^1(k, B) \to \mathrm{H}^1(k, C)$ is bijective.*
2. *For $z \in \mathrm{H}^1(k, B) = \mathrm{H}^1(k, C)$, let A_z be the twist of A induced by the image of z under the natural map $\mathrm{H}^1(k, B) \to \mathrm{H}^1(k, \mathrm{Aut}(A_{\bar{k}}))$. Then*

$$\#B_{\mathrm{in}(z)}(k) = \#A_z(k) \cdot \#C_{\mathrm{in}(z)}(k).$$

Proof. The short exact sequence of algebraic groups over k

$$1 \to A \to B \to C \to 1$$

induces an exact sequence of pointed cohomology sets

$$1 \to A(k) \to B(k) \to C(k) \to \mathrm{H}^1(k, A) \to \mathrm{H}^1(k, B) \to \mathrm{H}^1(k, C).$$

From Lang's theorem we know that $\mathrm{H}^1(k, A)$ is trivial. By [60, III.2.4.2] the last map is surjective, so by exactness it is bijective, which proves the first statement. Furthermore for a $z \in \mathrm{H}^1(k, B)$ the inclusion map $A_z(\bar{k}) \to B_{\mathrm{in}(z)}(\bar{k})$ is Galois-equivariant, and the quotient of $B_{\mathrm{in}(z)}(\bar{k})$ by the image of this map is isomorphic to $C_{\mathrm{in}(z)}(\bar{k})$. This shows that we get a twisted short exact sequence

$$1 \to A_z \to B_{\mathrm{in}(z)} \to C_{\mathrm{in}(z)} \to 1.$$

Since A_z is connected, we find $\mathrm{H}^1(k, A_z) = 1$, and then a long exact sequence analogous to the one above proves the second statement. □

Definition 2.11. Let X be an algebraic stack over a field k. Let $k' \subset k''$ be two field extensions of k, and let $X \in \mathsf{X}(k'')$. Then a *model of X over k'* is an object $Y \in \mathsf{X}(k')$ such that $Y_{k''} \cong X$.

Lemma 2.12. *Let G be a smooth algebraic group over k, and let X be a variety over k.*

1. *The isomorphism classes of $[G\backslash X](\bar{k})$ are classified by the quotient set $G(\bar{k})\backslash X(\bar{k})$.*
2. *Let k' be a finite extension of k, and let C be an element of $G(\bar{k})\backslash X(\bar{k})$, corresponding to a $(T, f) \in [G\backslash X](\bar{k})$. Then (T, f) has a model over k' if and only if C is fixed under the action of $\mathrm{Gal}(\bar{k}/k')$ on $G(\bar{k})\backslash X(\bar{k})$.*

Proof.

1. Over $\bar{k}$ every torsor is trivial, and a G-equivariant map $f\colon G_{\bar{k}} \to X_{\bar{k}}$ is determined by its image of the unit element $e \in G(\bar{k})$. Furthermore, two maps $f, f'\colon G_{\bar{k}} \to X_{\bar{k}}$ yield isomorphic elements $(G_{\bar{k}}, f), (G_{\bar{k}}, f')$ of $[G\backslash X](\bar{k})$ if and only if $f(e)$ and $f'(e)$ lie in the same $G(\bar{k})$-orbit. Since $f(G(\bar{k}))$ is a $G(\bar{k})$-orbit in $X(\bar{k})$, we get a bijection

$$\begin{aligned}[][G\backslash X](\bar{k})] &\to G(\bar{k})\backslash X(\bar{k}) \\ (G_{\bar{k}}, f) &\mapsto f(G(\bar{k})).\end{aligned}$$

2. Let (T, f) be an element of $[G\backslash X](k')$. Then $f\colon T(\bar{k}) \to X(\bar{k})$ is $\mathrm{Gal}(\bar{k}/k')$-equivariant. Hence $f(T(\bar{k}))$ is an element of $G(\bar{k})\backslash X(\bar{k})$ that is invariant under the action of $\mathrm{Gal}(\bar{k}/k')$; this proves one direction. For the other direction, let $\pi \in \mathrm{Gal}(\bar{k}/k')$ be the $\#k'$-th power Frobenius. Let $x \in C$; then there exists a $g \in G(\bar{k})$ such that $g \cdot \pi(x) = x$. Let $z \in \mathrm{Z}^1(k', G)$ be the unique cocycle such that $z(\pi) = g$ as in lemma 2.8. Then the G-equivariant map

$$\begin{aligned} G_{\bar{k}} &\to X_{\bar{k}} \\ g &\mapsto g \cdot x \end{aligned}$$

descends to a G-equivariant map of k'-varieties $G_z \to X_{k'}$ (where we identify $G_{z,\bar{k}}$ with $G_{\bar{k}}$ via φ_z as in notation 2.3). □

Remark 2.13. Let C be a $G(\bar{k})$-orbit in $X(\bar{k})$, and let x be an element of C. Then the automorphism group of the object of $[G\backslash X](\bar{k})$ corresponding to C by lemma 2.12 is isomorphic to $\mathtt{Stab}_{G_{\bar{k}}}(x)$. In particular its isomorphism class does not depend on the choice of x in C. We denote $\mathtt{A}(C)$ for the algebraic group $\mathtt{Stab}_{G_{\bar{k}}}(x)$ over $\bar{k}$.

The next theorem is a classical result:

Theorem 2.14. (See [58, Thm. 5]) *Let U be a connected unipotent group over k. Then U is isomorphic to $\mathbb{A}_k^{\dim(U)}$ as k-varieties.* □

What makes this theorem so useful for us is that it shows that the point count of a unipotent group remains the same under twisting. Under suitable conditions on X and G this allows us to simplify the expression in proposition 2.5.

Proposition 2.15. *Let G be an algebraic group over k. Let X be a k-variety with an action of G, such that for every $C \in G(\bar{k})\backslash X(\bar{k})$ the identity component of the algebraic group $\mathtt{A}(C)^{\mathrm{red}}$ is unipotent. Let k' be a finite field extension of k. Then*

$$\#[G\backslash X](k') = \sum_{C \in (G(\bar{k})\backslash X(\bar{k}))^{\mathrm{Gal}(\bar{k}/k')}} (\#k')^{-\dim(\mathtt{A}(C))}.$$

Proof. As before it suffices to show this for $k = k'$. For $C \in (G(\bar{k})\backslash X(\bar{k}))$, let $m(C)$ be the isomorphism class in $[G\backslash X](\bar{k})$ corresponding to C. We may then define the full subcategory $\mathsf{S}(C)$ of $[G\backslash X](k)$, the isomorphism classes of whose objects form the set

$$\left\{x \in [[G\backslash X](k)] : x_{\bar{k}} \in m(C)\right\}.$$

By lemma 2.12 this category is nonempty if and only if $C \in (G(\bar{k})\backslash X(\bar{k}))^{\mathrm{Gal}(\bar{k}/k)}$. Suppose this is true for C, and let x_0 be an object of $\mathsf{S}(C)$. Then the algebraic group $\mathtt{Aut}(x_0)$ is a k-form of $\mathtt{A}(C)$. By [20, Thm. III.2.5.1] $\mathsf{S}(C)$ is equivalent to the category $\mathsf{B}(\mathtt{Aut}(x_0))(k)$; its elements are classified by $\mathrm{H}^1(k, \mathtt{Aut}(x_0)) = \mathrm{H}^1(k, \mathtt{Aut}(x_0)^{\mathrm{red}})$. Write $L := \mathtt{Aut}(x_0)^{\mathrm{red}}$; we now find for the point count

$$\#\mathsf{S}(C) = \sum_{z \in \mathrm{H}^1(k,L)} \frac{1}{\#L_{\mathrm{in}(z)}(k)}. \tag{2.16}$$

Let L^0 be the identity component of L; this is a connected unipotent group of dimension $\dim(\mathtt{A}(C))$. Let $\pi_0(L)$ be the component group of L. By lemma 2.10, applied to the short exact sequence

$$1 \to L^0 \to L \to \pi_0(L) \to 1,$$

we see that the natural map $\mathrm{H}^1(k, L) \to \mathrm{H}^1(k, \pi_0(L))$ is a bijection. On the other hand, let $z \in \mathrm{H}^1(k, L)$; then the same lemma tells us that

$$\#L_{\mathrm{in}(z)}(k) = (\#L^0_{\mathrm{in}(z)}(k)) \cdot (\#\pi_0(L_{\mathrm{in}(z)})(k)). \tag{2.17}$$

By theorem 2.14 we get an equality

$$\#L^0_{\mathrm{in}(z)}(k) = (\#k)^{\dim(\mathtt{A}(C))} \tag{2.18}$$

and this does not depend on the choice of z. Furthermore, if we identify $\mathrm{H}^1(k, L)$ and $\mathrm{H}^1(k, \pi_0(L))$ as above, we find $\pi_0(L_{\mathrm{in}(z)}) \cong \pi_0(L)_{\mathrm{in}(z)}$. Applying lemma 2.9 to the finite étale group scheme $\pi_0(L)$ yields

$$\sum_{z \in \mathrm{H}^1(k,\pi_0(L))} \frac{1}{\#\pi_0(L)_{\mathrm{in}(z)}(k)} = \#\mathsf{B}(\pi_0(L)) = 1. \tag{2.19}$$

Combining (2.16), (2.17), (2.18), and (2.18) now gives us

$$\begin{aligned}\#\mathsf{S}(C) &= \sum_{z \in \mathrm{H}^1(k,L)} \frac{1}{\#L_{\mathrm{in}(z)}(k)} \\ &= \sum_{z \in \mathrm{H}^1(k,\pi_0(L))} \frac{1}{\#\pi_0(L)_{\mathrm{in}(z)}(k) \cdot (\#k)^{\dim(\mathtt{A}(C))}} \\ &= (\#k)^{-\dim(\mathtt{A}(C))}.\end{aligned}$$

Summing over all $C \in (G(\bar{k})\backslash X(\bar{k}))^{\mathrm{Gal}(\bar{k}/k)}$ now proves the proposition. □

Proposition 2.20. *Let G be a smooth algebraic group over k, and let X be a k-variety with a left action of G. Suppose $G \cong H \ltimes U$, where U is connected and unipotent. Let k' be a finite field extension of k. Then*

$$\#[G\backslash X](k') = \#[H\backslash X](k') \cdot (\#k')^{-\dim(U)}.$$

Proof. For a $z \in \mathrm{H}^1(k', G)$, let $U_{\mathrm{in}(z)}$ be the twist of U induced by the conjugation action of G on U. A straightforward computation using proposition 2.5, lemma 2.10, and theorem 2.14 shows

$$\begin{aligned}\#[G\backslash X](k') &= \sum_{z\in \mathrm{H}^1(k',G)} \frac{\#X_z(k')}{\#G_{\mathrm{in}(z)}(k')} \\ &= \sum_{z\in \mathrm{H}^1(k',H)} \frac{\#X_z(k')}{\#H_{\mathrm{in}(z)}(k')\cdot \#U_{\mathrm{in}(z)}(k')} \\ &= \#[H\backslash X](k')\cdot(\#k')^{-\dim(U)}.\end{aligned}$$

□

Proposition 2.21. *Let G be a smooth algebraic group over k of the form $G \cong (F\times H)\ltimes U$, where F has a unipotent identity component, H is connected, and U is connected and unipotent. Let X be a variety over k of the form $E\times V$, where E is finite and $V \cong \mathbb{A}^n_k$ for some nonnegative integer n. Suppose that G acts on X in such a way that there is an action of F on E and V such that the induced action of F on X is the product of these. Suppose furthermore that the action of F on V factors through the action of a connected algebraic group. Let k' be a finite field extension of k. Then*

$$\#[G\backslash X](k') = (F(\bar{k})\backslash E(\bar{k}))^{\mathrm{Gal}(\bar{k}/k')} \cdot \frac{(\#k')^{\dim(V)-\dim(U)-\dim(F)}}{\#H(k')}.$$

Proof. It suffices to prove this for $k'=k$. Since the map $\pi_0(F)\to\pi_0(G)$ is an isomorphism, by lemma 2.10 we find that the natural map $\mathrm{H}^1(k,\pi_0(F))\to \mathrm{H}^1(k,G)$ is an isomorphism as well. The same lemma also tells us that $\mathrm{H}^1(k,\pi_0(F)) = \mathrm{H}^1(k,F)$. By proposition 2.5 we get

$$[G\backslash X](k) = \sum_{z\in \mathrm{H}^1(k,F)} \frac{\#(E\times V)_z(k)}{\#G_{\mathrm{in}(z)}(k)}.$$

Let $z\in \mathrm{H}^1(k,F)$. Since $X\cong E\times V$ not just as k-varieties, but as k-varieties with an action of F, we find $(E\times V)_z \cong E_z\times V_z$. Furthermore, let $\tilde{F}$ be a connected algebraic group acting on V such that the action of F on V factors through $\tilde{F}$. Then the induced map $\mathrm{H}^1(k,F)\to \mathrm{H}^1(k,\mathrm{Aut}(V))$ factors through $\mathrm{H}^1(k,\tilde{F})$, which is trivial by Lang's theorem; hence we find $V_z\cong V$. Now consider $G_{\mathrm{in}(z)}$. Since $G\cong H\ltimes(F\ltimes U)$, we may write

$$G_{\mathrm{in}(z)} \cong H\ltimes (F_{\mathrm{in}(z)}\ltimes U_{\mathrm{in}(z)}).$$

Then $U_{\mathrm{in}(z)}$ is a connected unipotent group of dimension $\dim(U)$. Applying theorem 2.14, we get

$$\begin{aligned}
[G\backslash X](k) &= \sum_{z\in \mathrm{H}^1(k,F)} \frac{\#(E\times V)_z(k)}{\#G_{\mathrm{in}(z)}(k)} \\
&= \sum_{z\in \mathrm{H}^1(k,F)} \frac{\#(E_z)(k)\cdot \#(V_z)(k)}{\#H(k)\cdot \#F_{\mathrm{in}(z)}(k)\cdot \#U_{\mathrm{in}(z)}(k)} \\
&= \sum_{z\in \mathrm{H}^1(k,F)} \frac{\#(E_z)(k)}{\#F_{\mathrm{in}(z)}(k)}\cdot \frac{(\#k)^{\dim(V)-\dim(U)}}{\#H(k)} \\
&= \#[F\backslash E](k)\cdot \frac{(\#k)^{\dim(V)-\dim(U)}}{\#H(k)}. \\
&= (F(\bar{k})\backslash E(\bar{k}))^{\mathrm{Gal}(\bar{k}/k)}\cdot \frac{(\#k)^{\dim(V)-\dim(U)-\dim(F)}}{\#H(k)},
\end{aligned}$$

where the last equality follows from proposition 2.15. □

2.2 Zeta functions of algebraic stacks

In this section we define the zeta function of an algebraic stack over a finite field, and we discuss a few of its properties. The main result is theorem 2.27.

Definition 2.22. Let q be a power of p. Let X be an algebraic stack of finite type over $\mathbb{F}_q$. Then the *zeta function* of X is defined to be the element of $\mathbb{Q}[\![t]\!]$ given by

$$Z(\mathsf{X},t) := \exp\left(\sum_{v\geq 1} \frac{t^v}{v}\#\mathsf{X}(\mathbb{F}_{q^v})\right).$$

In the case that X is sufficiently nice the zeta function will satisfy some nice properties itself:

Theorem 2.23. (see [63, Thm 1.3]) *Let X be an algebraic stack of finite type over a finite field $\mathbb{F}_q$. Then $Z(\mathsf{X},t)$ defines a meromorphic function that is defined on all of $\mathbb{C}$. If X is a Deligne-Mumford stack, then $Z(\mathsf{X},t)$ is rational.* □

This theorem shows that there is some 'structure' in the point counts $\#\mathsf{X}(\mathbb{F}_{q^v})$ for varying v. Our main goal is to prove theorem 2.27, which contains two statements that will be important for us when calculating zeta functions of various moduli stacks. First, if $\#\mathsf{X}(\mathbb{F}_{q^v})$ is given by an integral polynomial in q^v, we have a direct expression for $Z(\mathsf{X},t)$. Second, if $\#\mathsf{X}(\mathbb{F}_{q^v})$ is given by a rational function R in q^v of a certain form, and the zeta function $Z(\mathsf{X},t)$ is rational, then R is actually an integral polynomial, and we may apply the first statement. This theorem rests on two lemmas, the proof of the first of which is a straightforward calculation and therefore omitted.

Lemma 2.24. *Let $R \in \mathbb{Z}[X, X^{-1}]$, and write $R = \sum_{n\in\mathbb{Z}} r_n X^n$. Let $q > 1$ be an integer. Then*

$$\exp\left(\sum_{v\geq 1} \frac{t^v}{v} R(q^v)\right) = \prod_{n\in\mathbb{Z}} (1 - q^n t)^{-r_n}$$

as rational power series in t. □

Lemma 2.25. *Let $q > 1$ be an integer. Let $\mathcal{R}$ be the subring of $\mathbb{Q}(X)$ given by*

$$\mathcal{R} = \mathbb{Z}\left[\{X, X^{-1}\} \cup \left\{\frac{1}{X^n - 1} : n \geq 1\right\}\right]. \tag{2.26}$$

Suppose $R \in \mathcal{R}$ is such that the rational power series

$$Z(t) := \exp\left(\sum_{v\geq 1} \frac{t^v}{v} R(q^v)\right)$$

defines a meromorphic function that is defined on all of $\mathbb{C}$, and suppose that this meromorphic function is rational. Then $R \in \mathbb{Z}[X, X^{-1}]$.

Proof. Using the identity $\frac{1}{X^n-1} = X^{-n} + X^{-2n} + X^{-3n} + \cdots$ in $\mathbb{Q}((X))$ we may regard R as an element of $\mathbb{Z}[X][\![X^{-1}]\!]$. Write $R = \sum_{n\in\mathbb{Z}} r_n X^n$, with all $r_n \in \mathbb{Z}$ and $r_n = 0$ for $n \gg 0$. First I claim that $r_n \leq O((-n)^k)$ for some $k \in \mathbb{Z}_{\geq 0}$ as $n \to -\infty$. To see this, note that it suffices to prove this claim for $R = \prod_{i=1}^m (X^{n_i} - 1)^{-1}$, where m and the n_i are positive integers. In this case,

$$r_n = \#\left\{(c_1, \ldots, c_m) \in \mathbb{Z}^m_{>0} : \sum_i c_i n_i = -n\right\},$$

and we see that $r_n \leq O((-n)^m)$ as $n \to -\infty$. It follows that for every $v \geq 1$ the sum $\sum_{n\in\mathbb{Z}} r_n q^{nv}$ converges absolutely and is equal to $R(q^v)$. For any integer m, define the following elements of $\mathbb{R}[\![t]\!]$ (these are actually elements of $\mathbb{Q}[\![t]\!]$, but we are taking infinite sums in $\mathbb{Q}$ using the Archimedean topology):

$$L_{\geq m}(t) = \sum_{v\geq 1}\left(\frac{\sum_{n\geq m} r_n q^{nv}}{v} t^v\right);$$

$$L_{<m}(t) = \sum_{v\geq 1}\left(\frac{\sum_{n<m} r_n q^{nv}}{v} t^v\right);$$

$$Z_{\geq m}(t) = \exp(L_{\geq m}(t));$$

$$Z_{<m}(t) = \exp(L_{<m}(t)).$$

Since $\sum_{n\in\mathbb{Z}} r_n q^{nv}$ converges absolutely to $R(q^v)$, we find the following equality in $\mathbb{R}[\![t]\!]$:

$$\sum_{v\geq 1} \frac{t^v}{v} R(q^v) = L_{\geq m}(t) + L_{<m}(t).$$

It follows that $Z(t) = Z_{\geq m}(t) \cdot Z_{<m}(t)$. Furthermore, $Z_{\geq m}(t) = \prod_{n \geq m}(1 - q^n t)^{-r_n}$. As such $Z_{\geq m}(t)$ and $Z_{<m}(t)$ are both rational functions. Now consider the value of Z at $t = t_0 := q^{-m}$ for some integer m. If $r_m < 0$, then t_0 is a root of $Z_{\geq m}$, while it is a pole of $Z_{\geq m}$ if $r_m > 0$. On the other hand, from the fact that r_n grows polynomially in $(-n)$ as $n \to -\infty$, we find that the infinite sum

$$L_{<m}(t_0) = \sum_{v \geq 1} \sum_{n<m} \frac{r_n (q^{n-m})^v}{v}$$

converges absolutely in $\mathbb{R}$ in the archimedean topology. We conclude that $Z_{<m}(t_0) = e^{L_{<m}(t_0)} \in \mathbb{R}_{>0}$. This shows that t_0 is neither a root nor a pole of $Z_{<m}$. We conclude that $t_0 = q^{-m}$ is a root or a pole of Z if and only if $r_m \neq 0$. Since Z is rational by assumption, this means that only finitely many r_m may be nonzero; hence R is an element of $\mathbb{Z}[X, X^{-1}]$. □

The following theorem is now a direct consequence of the previous two lemmas.

Theorem 2.27. *Let* X *be an algebraic stack of finite type over a finite field* $\mathbb{F}_q$*. Suppose there exists an* $R \in \mathbb{Q}(X)$ *such that for every* $v \in \mathbb{Z}_{\geq 1}$ *we have that* $R(q^v)$ *is defined and is equal to* $\#\mathsf{X}(\mathbb{F}_{q^v})$*.*

1. *Suppose* $R \in \mathbb{Z}[X, X^{-1}]$*, and write* $R = \sum_{n \in \mathbb{Z}} r_n X^n$*. Then*

$$Z(\mathsf{X}, t) = \prod_{n \in \mathbb{Z}} (1 - q^n t)^{-r_n}.$$

2. *Suppose* $Z(\mathsf{X}, t)$ *is a rational function and that* R *is an element of the ring* $\mathcal{R}$ *from (2.26). Then* $R \in \mathbb{Z}[X, X^{-1}]$*, and the previous point applies.* □

Chapter 3

Stacks of truncated Barsotti–Tate groups

The aim of this chapter is threefold. First we introduce truncated Barsotti–Tate groups, Dieudonné modules, and the relation between the two. The second goal is to state the classification of BT_1 over algebraically closed fields and to determine their automorphism schemes. We do this in two ways: we give the classification in terms of graph theory as developed in [32], and the classification in terms of the Weyl group of an algebraic group as developed in [43]. The second classification can be stated more succinctly, especially the description of the automorphism schemes, but the first classification has the advantage that it also gives us the classification of general p-groups over algebraically closed fields; we will need this in chapter 4. The third goal is to calculate the zeta function of moduli stacks of BT_n; the exact result is stated in theorem 3.33. The first two sections contain only 'classical' material, and only the sections from section 3.3 onwards contain new material.

3.1 Dieudonné modules

In this chapter we will define (truncated) Barsotti–Tate groups, and how they are classified by Dieudonné crystals. Although the general setting is quite involved, for our purposes we only need to describe this relation over finite fields. For the general setting the reader is referred to [2].

Definition 3.1. Let S be a scheme of characteristic p. A *Barsotti–Tate group of height h over S*, or a *p-divisible group over S*, is a sequence $(G_i)_{i\geq 1}$ of finite commutative group schemes of order p^{ih} over S, together with inclusions $\iota_i \colon G_i \hookrightarrow G_{i+1}$, such that the induced sequence

$$1 \to G_i \xrightarrow{\iota_i} G_{i+1} \xrightarrow{p^i} G_{i+1}$$

is exact. A *truncated Barsotti–Tate group of level n and height h over S*, or BT_n for short, is a commutative group scheme G over S such that there exists a Barsotti–Tate group $(G_i)_{i\geq 1}$ of height h over S such that $G \cong G_n$. As an abuse of notation we will sometimes refer to a Barsotti–Tate group as a truncated Barsotti–Tate group of level ∞.

Remark 3.2. There is also a direct definition of a truncated Barsotti–Tate group that depends on intrinsic properties of the group scheme G, rather than on the existence of a lift; see [23, Def. II.3.2].

Example 3.3. Let A be an abelian scheme over S. Then $A[p^n]$ is a commutative group scheme of order $p^{2n\cdot\dim(A)}$ over S. The sequence $(A[p^n])_{n\geq 1}$ is a Barsotti–Tate group of height $2\cdot\dim(A)$ over S.

Let S be a scheme of characteristic p, and let $n \in \mathbb{Z}_{\geq 1} \cup \{\infty\}$. Let $\mathsf{BT}_n^{h,d}(S)$ be the category of truncated Barsotti–Tate groups of level n, height h and dimension d (see [12, II.7 Def.]). Together with the obvious notion of pullback these form an algebraic stack $\mathsf{BT}_n^{h,d}$ over $\mathbb{F}_p$, which is of finite type if $n < \infty$ (see [70, Prop. 1.8]). Let $\mathsf{Crys}_n^{h,d}$ be the $\mathbb{F}_p$-stack of truncated Dieudonné crystals D of level n that are locally of rank h, for which the Frobenius map $F\colon D \to D^{(p)}$ has rank d locally (see [27, Rem. 2.4.10]; again we use the convention that truncated crystals of level ∞ are just untruncated crystals). Then covariant Dieudonné theory (see [56, §9.3] and [2, 3.3.6 & 3.3.10]) tells us that there is a morphism of stacks over $\mathbb{F}_p$

$$\mathbb{D}_n \colon \mathsf{BT}_n^{h,d} \to \mathsf{Crys}_n^{h,d}$$

that is an equivalence over perfect fields. This implies $\#\mathsf{BT}_n^{h,d}(\mathbb{F}_q) = \#\mathsf{Crys}_n^{h,d}(\mathbb{F}_q)$ for all powers q of p, and $Z(\mathsf{BT}_n^{h,d}, t) = Z(\mathsf{Crys}_n^{h,d}, t)$. Since point counts and zeta functions are our main objects of interest, we will study Barsotti–Tate groups mainly via their connection to Dieudonné crystals. In the case that we are working over finite fields we can describe categories of Dieudonné crystals more explicitely, but first we need some more notation.

Definition 3.4. Let k be a perfect field of characteristic p, and let $n \in \mathbb{Z}_{\geq 1} \cup \{\infty\}$. Denote by $\mathrm{W}_n(k)$ the ring of truncated Witt vectors of length n over k (truncated Witt vectors of length ∞ are just untruncated Witt vectors). Let $\sigma \in \mathrm{Aut}(\mathrm{W}_n(k))$ be the automorphism induced by the p-power Frobenius on k.

1. A *level n Dieudonné module over k of height h* is a triple (D, F, V), where D is a free $\mathrm{W}_n(k)$-module of rank h and $F\colon D \to D$ and $V\colon D \to D$ are σ- and σ^{-1}-semilinear maps, respectively, satisfying $FV = VF = p$. We will often omit F and V from the notation if there is no danger of confusion.

2. A level 1 Dieudonné module is called *exact* if $\ker(F) = \mathrm{im}(V)$ (or $\ker(V) = \mathrm{im}(F)$, which is equivalent).

3. The *dimension* of a Dieudonné module (D, F, V) is the k-dimension of the image of the induced map $F\colon D/pD \to D/pD$.

4. If $n > 1$, then category of level n Dieudonné modules over k of height h and dimension d is denoted $\mathsf{D}_n^{h,d}(k)$. The category of *exact* level 1 Dieudonné modules of height h and dimension d is denoted $\mathsf{D}_1^{h,d}(k)$; the category of level 1 Dieudonné modules over k of height h is denoted $\mathsf{D}_{1,\mathrm{nex}}^{h,d}(k)$ (here 'nex' stands for 'non-exact'). In both cases the morphisms are isomorphisms of Dieudonné modules (i.e. isomorphisms of $\mathrm{W}_n(k)$-modules that commute with F and V).

Remark 3.5. If $n > 1$ and (D, F, V) is a level n Dieudonné module, then the level 1 Dieudonné module $(D/pD, F, V)$ is always exact. This is why in definition 3.4.4 we take exact level 1 Dieudonné modules to be the 'correct' analogue of level n Dieudonné modules. However, we are also interested in non-exact level 1 Dieudonné modules, because of the role they will play in chapter 4.

Remark 3.6. Dieudonné modules and p-groups can also be defined over general schemes of characteristic p (see [27, Def. 2.3.4]). This gives rise to algebraic stacks $\mathsf{D}_n^{h,d}$ and $\mathsf{D}_{1,\mathrm{nex}}^{h,d}$ over $\mathbb{F}_p$. The latter is of finite type, and the first one is of finite type if $n < \infty$.

Definition 3.7. Let S be a scheme of characteristic p. A *p-group over S* is a finite commutative group scheme over S of exponent p. The category of p-groups over S of order p^h is denoted $p\text{-}\mathsf{Grp}^h(S)$.

The following facts show us that for the purposes of point counts and zeta functions we are only concerned with Dieudonné modules. For proofs the reader is referred to [12] and [3].

Fact 3.8. Let k be a perfect field of characteristic p. Let h and d be nonnegative integers, and let n be an element of $\mathbb{Z}_{\geq 1} \cup \{\infty\}$.

1. Let $n > 1$. There is a natural equivalence of categories

$$\Phi_n\colon \mathsf{Crys}_n^{h,d}(k) \xrightarrow{\sim} \mathsf{D}_n^{h,d}(k).$$

2. Let $p\text{-}\mathsf{Grp}^h(k)$ be the category of p-groups over k of order p^h. Then there are natural equivalences Φ_1, Ψ that fit into the following commutative diagram:

$$\begin{array}{ccccc}
\mathsf{BT}_1^{h,d}(k) & \xrightarrow[\sim]{\mathbb{D}_1(k)} & \mathsf{Crys}_1^{h,d}(k) & \xrightarrow[\sim]{\Phi_1} & \mathsf{D}_1^{h,d}(k) \\
\big\downarrow & & & & \big\downarrow \\
p\text{-}\mathsf{Grp}^h(k) & & \xrightarrow[\sim]{\Psi} & & \mathsf{D}_{1,\mathrm{nex}}^{h}(k)
\end{array}$$

3.2 Classification of p-groups

In this section we discuss the classification of p-groups (or, to be more precise, level 1 Dieudonné modules) over an algebraically closed field k of characteristic p. There are two approaches to this: The formulation of the first classification (proposition 3.26) is compact and can be generalised to Dieudonné modules with extra structure, but it only classifies exact level 1 Dieudonné modules. The second approach (theorem 3.23) is more involved and requires some combinatorial notation, but the advantage is that it also classifies the non-exact level 1 Dieudonné modules. We will only need the first classification to determine the zeta function of moduli stacks of the form $\mathsf{BT}_n^{h,d}$; the second classification is needed in chapter 4. We start by defining so-called Kraft types, which form the basis of the classification introduced in [32].

Notation 3.9. If X is a set, we denote by $\mathcal{W}(X)$ the set of (possibly infinitely long) words $W_1 W_2 W_3 \cdots$, where each W_i is an element of X.

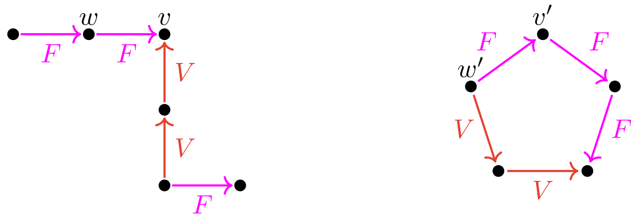
Definition 3.10. Let Δ be a finite directed graph, in which every edge is coloured with one of two colours F (fuchsia) or V (vermilion). We call Δ a *primitive Kraft graph* if it is of one of the following two types:

Type 'T' Let $W = W_1 \cdots W_k$ be a finite, possibly empty word in $\mathcal{W}(\{F, V^{-1}\})$. Then the associated primitive Kraft graph of type T has $\{v_0, v_1, \ldots, v_k\}$ as its set of vertices, and for every integer i an edge $v_{i-1} \xrightarrow{F} v_i$ if $W_i = F$, and an edge $v_{i-1} \xleftarrow{V} v_i$ if $W_i = V^{-1}$.

Type 'Z' Let $W = W_1 \cdots W_k$ be a finite nonempty word in $\mathcal{W}(\{F, V^{-1}\})$ that is *nonrepeating*, i.e. there is no word W' such that W is a concatenation of multiple copies of W'. Then the associated primitive Kraft graph of type Z has as its set of vertices $\{v_i : i \in \mathbb{Z}/k\mathbb{Z}\}$, and for every $i \in \mathbb{Z}/k\mathbb{Z}$ an edge $v_{i-1} \xrightarrow{F} v_i$ if $W_i = F$, and an edge $v_{i-1} \xleftarrow{V} v_i$ if $W_i = V^{-1}$.

Notation 3.11. The set of primitive Kraft graphs of type T is denoted $\mathcal{P}_{\mathrm{T}}$, the set of primitive Kraft graphs of type Z is denoted $\mathcal{P}_{\mathrm{Z}}$, and we define $\mathcal{P} := \mathcal{P}_{\mathrm{T}} \sqcup \mathcal{P}_{\mathrm{Z}}$. If Δ is a primitive Kraft graph, then we define the *length* of Δ, denoted $\ell(\Delta)$, to be the number of vertices of Δ. Furthermore, we let $\ell_F(\Delta)$ be the number of F-edges in Δ, and we let $\ell_V(\Delta)$ be the number of V-edges in Δ; note that $\ell(\Delta) \geq \ell_F(\Delta) + \ell_V(\Delta)$ for all Δ.

Example 3.12. Consider the word $W = F^2V^{-2}F := FFV^{-1}V^{-1}F$. Then the Kraft graphs of types T and Z corresponding to W, are depicted below. The figure should illustrate why the types are denoted T (ostensibly from German *Treppe* 'stairs') and Z (from German *Zyklus* 'cycle') (in this picture v, v', w and w' are marked because they will be mentioned in later examples).



Remark 3.13. We see that a primitive Kraft graph of type T uniquely determines its corresponding word. For a primitive Kraft graph of type Z this is true only up to cyclic permutation of the letters in the word.

Definition 3.14. A *Kraft type* is a formal sum $K = \sum_{\Delta\in\mathcal{P}} K(\Delta)\cdot\Delta$, where each $K(\Delta)$ is a nonnegative integer, only finitely many of which are allowed to be nonzero. For such a K we define its *set of vertices* $|K|$ to be $\bigsqcup_{\Delta:K(\Delta)>0}|\Delta|$, where $|\Delta|$ denotes the set of vertices in Δ. For a $v\in|K|$ we furthermore define $K(v) := K(\Delta)$, where Δ is the primitive Kraft graph containing v. The set of Kraft types is denoted $\mathcal{K}$.

Definition 3.15. Let $K = \sum_{\Delta\in\mathcal{P}} K(\Delta)\cdot\Delta$ be a Kraft type. We define:

- The *height* of K to be $\sum_{\Delta\in\mathcal{P}} K(\Delta)\cdot\ell(\Delta)$;
- The F*-height* of K to be $\sum_{\Delta\in\mathcal{P}} K(\Delta)\cdot\ell_F(\Delta)$;
- The V*-height* of K to be $\sum_{\Delta\in\mathcal{P}} K(\Delta)\cdot\ell_V(\Delta)$.

For a nonnegative integer h, we let $\mathcal{K}(h)$ denote the set of Kraft types of height h. If a and b are nonnegative integers satisfying $a\geq b$, then we denote by $\mathcal{K}(a,b)$ the set of Kraft types of height a, F-height b and V-height $a-b$. Note that this is only possible if all primitive Kraft graphs in such a Kraft type are of type Z.

We need a little more notation on Kraft types in order to describe their homomorphism and automorphism schemes in section 3.3. Let K be a Kraft type, and let $v\in|K|$ be a vertex. We now define two words associated with v: The F*-route of* v, denoted $R_F(v)$, which is a (possibly infinitely long) word in $\mathcal{W}(\{F,V^{-1}\})$, and the V*-route of* v, denoted $R_V(v)$, which is a (possibly infinitely long) word in $\mathcal{W}(\{V,F^{-1}\})$. They are defined as follows: suppose v lies on a primitive Kraft graph Δ of type T, and let $W = W_1\cdots W_k$ be the word corresponding to Δ. There is a unique integer $0\leq i$ such that v corresponds to the vertex v_i in Δ in the description of definition 3.10; then set

$$R_F(v) := W_{i+1}\cdots W_k,$$
$$R_V(v) := W_i^{-1}W_{i-1}^{-1}\cdots W_1^{-1},$$

with $(V^{-1})^{-1} := V$. Suppose v lies on a primive Kraft graph Δ of type Z. There is a unique word $W = W_1\cdots W_k$ such that Δ corresponds to the word W and v corresponds to the vertex v_0 in the description of definition 3.10; then set

$$R_F(v) := (W_1 \cdots W_k)^{\mathbb{N}},$$
$$R_V(v) := (W_k^{-1} W_{k-1}^{-1} \cdots W_1^{-1})^{\mathbb{N}},$$

where $W^{\mathbb{N}}$ stands for 'W repeated infinitely often'. We order the sets $\mathcal{W}(F, V^{-1})$ and $\mathcal{W}(V, F^{-1})$ lexicographically by taking $V^{-1} < \emptyset < F$ and $F^{-1} < \emptyset < V$.

Notation 3.16. If K and K' are Kraft types with vertices $v \in |K|$ and $v' \in |K'|$, then we write $v \succeq v'$ if $R_F(v) \geq R_F(v')$ and $R_V(v) \geq R_V(v')$. If $v \succeq v'$ and $v' \succeq v$, we write $v \approx v'$.

Example 3.17. Let v and v' be as in example 3.12. Then

$$R_F(v) = V^{-2}F, \qquad R_F(v') = (F^2V^{-2}F)^{\mathbb{N}},$$
$$R_V(v) = F^{-2}, \qquad R_V(v') = (F^{-1}V^2F^{-2})^{\mathbb{N}}.$$

As such we see $R_F(v') > R_F(v)$, $R_V(v') > R_V(v)$, hence $v' \succeq v$ but $v \not\succeq v'$.

Note that in notation 3.16 we have $v \approx v'$ precisely if there is an isomorphism between the primitive Kraft graphs containing v and v' that maps v to v'. Because of this we get the following result:

Lemma 3.18. *Let K be a Kraft type. Then $\succeq$ is a partial order on $|K|$.* □

Definition 3.19. Let K and K' be two Kraft types. For (v, v') and $(w, w') \in |K| \times |K'|$ we write $(v, v') \sim_F (w, w')$ if v and w lie on the same primitive Kraft graph Δ, v' and w' lie on the same primitive Kraft graph Δ', and either of the following sets of edges exist in Δ and Δ':

- $v \xrightarrow{F} w$ and $v' \xrightarrow{F} w'$;
- $v \xleftarrow{V} w$ and $v' \xleftarrow{V} w'$.

Similarly, we write $(v, v') \sim_V (w, w')$ if either of the following sets of edges exist in Δ and Δ':

- $v \xleftarrow{F} w$ and $v' \xleftarrow{F} w'$;
- $v \xrightarrow{V} w$ and $v' \xrightarrow{V} w'$.

We say that (v, v') and (w, w') are *equivalent* if they are equivalent under the minimal equivalence relation on $|K| \times |K'|$ containing $\sim_F$ (or, equivalently, $\sim_V$); this equivalence relation is denoted $\sim$.

Example 3.20. In example 3.12 we have $(v, v') \sim_V (w, w')$, and $(w, w') \sim_F (v, v')$.

Remark 3.21. Note that if $(v, v') \sim (w, w')$, then $v \succeq v'$ if and only if $w \succeq w'$.

Let K be a Kraft type, and let k be a perfect field of characteristic p. Then to K we can associate a level 1 Dieudonné module $\mathrm{St}_k(K)$, called its *standard Dieudonné module*, as follows: a k-basis of $\mathrm{St}_k(K)$ is given by the set

$$\Big\{e_{v,j} : v \in |K|, 1 \leq j \leq K(v)\Big\}, \tag{3.22}$$

where $K(v)$ is as in definition 3.14. Furthermore, we define $F\colon \mathrm{St}_k(K) \to \mathrm{St}_k(K)$ to be the Fr_p-semilinear map given as follows: for each vertex $v \in |K|$ on a primitive Kraft graph Δ, if there exists an edge $v \xrightarrow{F} v'$ in Δ, then v' is unique and $K(v) = K(v')$. If such an i' exists, we set $F(e_{v,j}) = e_{v',j}$ for all $j \leq K(v)$; otherwise, we set $F(e_{v,j}) = 0$. Similarly, $V\colon \mathrm{St}_k(\Delta) \to \mathrm{St}_k(\Delta)$ is the Fr_p^{-1}-semilinear map that for each vertex $v \in |K|$ on a primitive Kraft graph Δ satisfies $V(e_{v,j}) = e_{v',j}$ if there exists an edge $v \xrightarrow{V} v'$ in Δ (such a v' is then necessarily unique), and $V(e_{v,j}) = 0$ otherwise.

Theorem 3.23. (See [32, §5]) *Let k be an algebraically closed field of characteristic p.*

1. *St_k gives a bijection between the set of isomorphism classes of types, and the set of isomorphism classes of level 1 Dieudonné modules over k;*
2. *Dieudonné modules of height h correspond to Kraft types of height h;*
3. *Dieudonné modules of dimension d correspond to Kraft types of F-height d;*
4. *Indecomposable Dieudonné modules correspond to primitive Kraft graphs;*
5. *Exact Dieudonné modules correspond to Kraft types whose primitive Kraft graphs are all of type Z.* □

Notation 3.24. If D is a level 1 Dieudonné module over a field k of characteristic p, then we define the *type* of D to be the Kraft type K such that $\mathrm{St}_{\bar{k}}(K) \cong D_{\bar{k}}$.

The exact level 1 Dieudonné modules over an algebraically closed field k can also be classified more explicitely by means of abstract group theory (that in chapter 5 will turn out to be algebraic group theory).

Notation 3.25. Let n and d be nonnegative integers such that $d \leq n$. For an integer h, consider the Coxeter system (W, S), where $W = S_h$, and S is the set of generators $\{(1\ \ 2), \ldots, (h-1\ \ h)\}$. Let $d \leq h$, and let $I = S \setminus \{(d\ \ d+1)\}$. Let $W_I \subset W$ be the subgroup generated by I, and let ${}^IW$ be the subset of W of all elements w that are of minimal length $\ell(w)$ in their coset W_Iw (see subsection 5.1.1). For a $w \in {}^IW$, we can consider the Kraft type K_w, which is constructed as follows. Consider the directed graph Γ_w with $\{F, V\}$-coloured edges whose vertices are $v_1 \ldots, v_n$, and where we have an edge $v_i \xrightarrow{F} v_{w(i)}$ if $i \leq d$, and an edge $v_i \xleftarrow{V} v_{w(i)}$ if $i > d$. Then the undirected connected components of Γ_w are primitive Kraft graphs of type Z. For a primitive Kraft graph Δ, let $m(\Delta)$ be the number of copies of Δ in Γ_w; then we define K_w by taking $K_w(\Delta) = m(\Delta)$ for all $\Delta \in \mathcal{P}_Z$.

Proposition 3.26. *Let k be an algebraically closed field of characteristic p, and let h, d, and ${}^I W$ be as in notation 3.25. Then the map $w \mapsto \mathrm{St}_k(K_w)$ is a bijection between ${}^I W$ and the set of isomorphism classes of exact level 1 Dieudonné modules of height h and dimension d.*

Proof. This is proven in [43, Thm. 4.7]. Alternatively, this follows from applying proposition 5.13 to example 5.11. □

3.3 Morphism and automorphism schemes

Let K_1 and K_2 be two Kraft types, and let k be a perfect field of characteristic p. The aim of this section is to give explicit descriptions for the algebraic groups $\mathtt{Hom}(\mathrm{St}_k(K_1), \mathrm{St}_k(K_2))^{\mathrm{red}}$ and $\mathtt{Aut}(\mathrm{St}_k(K_1))^{\mathrm{red}}$. These results are stated in propositions 3.28 and 3.29. There is a more compact description of the automorphism group in the case that K_1 only has summands of type Z (i.e. $\mathrm{St}_k(K_1)$ is an exact Dieudonné module); this is given in proposition 3.32.

Notation 3.27. Let $\mathcal{K}$ and $\mathcal{P}_{\mathrm{T}}$ again denote the set of Kraft types and the set of primitive Kraft graphs of type T, respectively. Let $\mathcal{A}$ be the set

$$\mathcal{A} = \Big\{(v_1, v_2) \in |K_1| \times |K_2| : v_1 \succ v_2\Big\}/\sim .$$

We define two maps $d, e \colon \mathcal{K} \times \mathcal{K} \to \mathbb{Z}_{\geq 0}$ given by

$$d(K_1, K_2) := \sum_{(v_1,v_2)\in\mathcal{A}} K_1(v_1) \cdot K_2(v_2),$$
$$e(K_1, K_2) := \sum_{\Delta\in\mathcal{P}_{\mathrm{T}}} K_1(\Delta) \cdot K_2(\Delta).$$

Furthermore, we define $d(K) := d(K, K)$.

In the next two propositions, we consider $\mathrm{Mat}_{a\times b}(\mathbb{F}_{p^c})$ and $\mathrm{GL}_a(\mathbb{F}_{p^c})$ (for integers $a, b, c > 0$) as finite étale group schemes over $\mathbb{F}_p$ by having them be the abstract group of $\bar{\mathbb{F}}_p$-points of these group schemes, along with the action of $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$.

Proposition 3.28. *Let K_1 and K_2 be two Kraft types, and let k be a perfect field of characteristic p. Then as additive group schemes $\mathtt{Hom}(\mathrm{St}_k(K_1), \mathrm{St}_k(K_2))^{\mathrm{red}}$ is isomorphic to*

$$\left(\prod_{\Delta\in\mathcal{P}_{\mathrm{Z}}} \mathrm{Mat}_{K_2(\Delta)\times K_1(\Delta)}(\mathbb{F}_{p^{\ell(\Delta)}})\right) \times \mathbb{G}_{\mathrm{a},k}^{d(K_1,K_2)+e(K_1,K_2)}.$$

Proposition 3.29. *Let K be a Kraft diagram, and let k be perfect a field of characteristic p. Then $\mathtt{Aut}(K)^{\mathrm{red}} \cong (F \times H) \ltimes U$, where U is unipotent of dimension $d(K)$ and*

$$F \cong \prod_{\Delta\in\mathcal{P}_{\mathrm{Z}}} \mathrm{GL}_{K(\Delta)}(\mathbb{F}_{p^{\ell(\Delta)}}),$$
$$H \cong \prod_{\Delta\in\mathcal{P}_{\mathrm{T}}} \mathtt{GL}_{K(\Delta),k}.$$

We start by proving proposition 3.28. Choose bases $(e_{1,v,j})_{v,j}$ and $(e_{2,v,j})_{v,j}$ for $\mathrm{St}_k(K_1)$ and $\mathrm{St}_k(K_2)$ respectively, as in (3.22). From this basis we see that the scheme of linear maps between $\mathrm{St}_k(K_1)$ and $\mathrm{St}_k(K_2)$ can be given as a commutative group scheme as

$$\mathtt{Lin}_k(\mathrm{St}_k(K_1), \mathrm{St}_k(K_2)) = \bigoplus_{\substack{v\in|K_1|,\\ v'\in|K_2|}} \mathtt{Mat}_{K_2(v')\times K_1(v),k}.$$

Our goal is to determine its subgroup scheme of morphisms of Dieudonné modules. For an element $x \in \mathrm{Lin}_{\bar{k}}(\mathrm{St}_{\bar{k}}(K_1), \mathrm{St}_{\bar{k}}(K_2))$ we write $x = (x_{v,v'})_{v\in|K_1|,v'\in|K_2|}$ according to the decomposition above. For positive integers m, n and a matrix $g \in \mathrm{Mat}_{m\times n}(\bar{k})$ we write $g^{(p)}$ for the matrix where every entry is of the form $(g^{(p)})_{i,j} = (g_{i,j})^p$. The following two lemmas are straightforward consequences of the fact that morphisms of Dieudonné modules have to commute with F and V.

Lemma 3.30. *Let $x \in \mathrm{Hom}(\mathrm{St}_{\bar{k}}(K_1), \mathrm{St}_{\bar{k}}(K_2)) \subset \mathrm{Lin}_{\bar{k}}(\mathrm{St}_{\bar{k}}(K_1), \mathrm{St}_{\bar{k}}(K_2))$. Let v, w be two elements of $|K_1|$ and let v', w' be two elements of $|K_2|$. If $(v, v') \sim_F (w, w')$, then $x_{w,w'} = x^{(p)}_{v,v'}$.* □

Lemma 3.31. *Let $x \in \mathrm{Hom}(\mathrm{St}_{\bar{k}}(K_1), \mathrm{St}_{\bar{k}}(K_2)) \subset \mathrm{Lin}_{\bar{k}}(\mathrm{St}_{\bar{k}}(K_1), \mathrm{St}_{\bar{k}}(K_2))$. Then following two statements hold (also for $\xrightarrow{V}$ instead of $\xrightarrow{F}$):*

- *Let $v', w' \in |K_2|$ be on the same primitive Kraft graph such that there exists an edge $v' \xrightarrow{F} w'$ in the primitive Kraft graph containing them, and let $v \in |K_1|$ be such that that there is no $v \xrightarrow{F} w$ in the primitive Kraft graph containing v. Then $x_{v,v'} = 0$.*
- *Let $v, w \in |K_1|$ be on the same primitive Kraft graph such that there exists an edge $w \xrightarrow{F} v$ in the primitive Kraft graph containing them, and let $v' \in |K_2|$ be such that that there is no $w' \xrightarrow{F} v'$ in the primitive Kraft graph containing w. Then $x_{v,v'} = 0$.* □

Proof of proposition 3.28. Since we are only interested in the reduced scheme, it suffices to determine the subset

$$\mathtt{Hom}(\mathrm{St}_k(K_1), \mathrm{St}_k(K_2))(\bar{k}) = \mathrm{Hom}(\mathrm{St}_{\bar{k}}(K_1), \mathrm{St}_{\bar{k}}(K_2)) \subset \mathrm{Lin}_{\bar{k}}(\mathrm{St}_{\bar{k}}(K_1), \mathrm{St}_{\bar{k}}(K_2)).$$

Let $X \subset |K_1|\times|K_2|$ be a set of representatives for $\sim$. By lemma 3.30 we see that an element $g \in \mathrm{Hom}(\mathrm{St}_{\bar{k}}(K_1), \mathrm{St}_{\bar{k}}(K_2))$ is determined by $(g_{v,v'})_{(v,v')\in X}$. Now let $(v, v') \in X$ be such that $v \not\succeq v'$. Let Δ_1 and Δ_2 be the primitive Kraft graphs such that $v \in \Delta_1$, $v' \in \Delta_2$. Then there exists a pair $(w, w') \in |\Delta_1| \times |\Delta_2|$ equivalent to (v, v') that satisfies at least one of the following conditions:

- there exists a $w' \xrightarrow{F} u'$ in Δ_2 but no $w \xrightarrow{F} u$ in Δ_1;
- there exists a $w \xleftarrow{V} u$ in Δ_1 but no $w' \xleftarrow{V} u'$ in Δ_2;
- there exists a $w' \xrightarrow{V} u'$ in Δ_2 but no $w \xrightarrow{V} u$ in Δ_1;

- there exists a $w \overset{F}{\longleftarrow} u$ in Δ_1 but no $w' \overset{F}{\longleftarrow} u'$ in Δ_2.

By lemma 3.31 we see that this implies that $g_{w,w'} = 0$; by lemma 3.30 this means that $g_{v,v'} = 0$. Now let $(v, v') \in X$ be such that $v \succeq v'$, and suppose that either $v \succ v'$, or $v \approx v'$ and the primitive Kraft diagram on which v lies is of type T. In these cases, for every $(w, w') \in |K_1| \times |K_2|$ such that $(v, v') \sim (w, w')$, there is a unique $n = n(w, w')$ such that either n is nonnegative and there exist $(v, v') = (v_0, v_0'), (v_1, v_1'), \ldots, (v_n, v_n') = (w, w')$ such that $(v_i, v_i') \sim_F (v_{i+1}, v_{i+1}')$ for all i, or n is nonpositive and there exist

$$(v, v') = (v_0, v_0'), \;\; (v_{-1}, v_{-1}'), \;\; \ldots, \;\; (v_n, v_n') = (w, w')$$

such that $(v_i, v_i') \sim_V (v_{i-1}, v_{i-1}')$ for all i. If x is any element of $\mathrm{Mat}_{K_2(v'),K_1(v)}(\bar{k})$, then the element $g \in \mathrm{Lin}_{\bar{k}}(\mathrm{St}_{\bar{k}}(K_1), \mathrm{St}_{\bar{k}}(K_2))$ given by

$$g_{w,w'} = \begin{cases} x^{(p^{n(w,w')})} & \text{if } (w, w') \sim (v, v'); \\ 0 & \text{otherwise} \end{cases}$$

is a morphism of Dieudonné modules. In the case that $v \approx w$ and the primitive Kraft diagram Δ on which v lies is of type Z, then for $(w, w') \sim (v, v')$ the integer $n(w, w')$ is defined only up to a multiple of $l(\Delta)$. As such, the construction above is a well-defined morphism of Dieudonné modules if and only if $x \in \mathrm{Mat}_{K_2(v'),K_1(v)}(\mathbb{F}_{p^{l(\Delta)}})$. To conclude, we find that a morphism of Dieudonné modules g is determined by $(g_{v,v'})_{(v,v')\in X}$, and we may freely choose $g_{v,v'}$ from:

- $\{0\}$ if $v \not\succeq v'$;
- $\mathrm{Mat}_{K_2(v'),K_1(v)}(\bar{k})$ if $v \succ v'$, or $v \approx v'$ and the associated primitive Kraft diagram Δ is of type T;
- $\mathrm{Mat}_{K_2(v'),K_1(v)}(\mathbb{F}_{p^{\ell(\Delta)}})$ if $v \approx v'$ and the associated primitive Kraft diagram Δ is of type Z.

This proves the proposition. □

Proof of proposition 3.29. Let X be as in the proof of proposition 3.29 (for $K = K_1 = K_2$). Choose a linear order on $|K|$ that extends the partial order $\succeq$ on $|K|$, and consider elements of $\mathrm{Lin}_{\bar{k}}(\mathrm{St}_{\bar{k}}(K_1), \mathrm{St}_{\bar{k}}(K_2))$ as block matrices with respect to this linear order; then the proof of the previous proposition shows that the group G of Dieudonné morphisms is contained in the group of upper triangular matrices with respect to this block structure. The elements (v, v') of X such that $v \succ v'$ give the strictly upper triangular part of G, which is unipotent; by the proof of the previous proposition this has dimension $d(K)$. The diagonal blocks correspond to elements of X of the form (v, v), and these blocks have the form $\mathrm{GL}_{K(v)}(\mathbb{F}_{p^{l(\Delta)}})$ if v lies on a primitive Kraft diagram Δ of type Z, and the form $\mathrm{GL}_{K(v)}(\bar{k})$ if v lies on a primitive Kraft diagram of type T. □

In the case that the Kraft type K only contains primitive Kraft graphs of type Z, proposition 3.29 tells us that $\mathtt{Aut}(\mathrm{St}_k(K))^{\mathrm{red}}$ is a semidirect product of a finite group and a unipotent group. The alternative classification of exact level 1 Dieudonné modules from proposition 3.26 allows us to express its dimension more explicitely:

Proposition 3.32. *Let h, d, and ${}^I W$ be as in notation 3.25, and let ℓ be the length function as in subsection 5.1.1. Let $w \in {}^I W$; then $\mathtt{Aut}(\mathrm{St}_k(K_w))^{\mathrm{red}}$ is a semidirect product of a finite group and a unipotent group of dimension $d(h-d) - \ell(w)$.*

Proof. This is proven in [44, Thm. 2.1.2]. Alternatively, one can apply proposition 5.33.2 to example 5.11. ☐

3.4 Zeta functions of stacks of $\mathbf{BT}_n$

Let $n, h > 0$ and $0 \leq d \leq h$ be integers. The goal of this section is to determine the zeta function of the algebraic stack $\mathsf{BT}_n^{h,d}$ over $\mathbb{F}_p$. The result is as follows:

Theorem 3.33. *Let $h, n > 0$ and $0 \leq d \leq h$ be integers. Let ${}^I W$ be as in notation 3.25. Then for every power q of p one has*

$$\#\mathsf{BT}_n^{h,d}(\mathbb{F}_q) = \sum_{w \in {}^I W} q^{\ell(w) - d(h-d)},$$

and consequently

$$Z(\mathsf{BT}_n^{h,d}, t) = \prod_{w \in {}^I W} \frac{1}{1 - p^{\ell(w)-d(h-d)} t}.$$

In particular the point counts and the zeta function of the stack $\mathsf{BT}_n^{h,d}$ do not depend on n.

Our strategy will be to interpret the results of [69] and [19], which concerns the set of BT_{n+1} over $\bar{k}$ extending a given BT_n, in a 'stacky' sense over a finite k. This allows us to invoke the results of chapter 2.

Let q be a power of p. As discussed in fact 3.8 Dieudonné theory gives us an equivalence of categories $\mathsf{BT}_n^{h,d}(\mathbb{F}_q) \to \mathsf{D}_n^{h,d}(\mathbb{F}_q)$, so it suffices for our purposes to find the point count of the second category. Fix h and d, and choose a (non-truncated) Barsotti–Tate group $\mathcal{G}$ of height h and dimension d over $\mathbb{F}_p$. For $n \in \mathbb{Z}_{\geq 1} \cup \{\infty\}$, let (D_n, F_n, V_n) be the Dieudonné module of $\mathcal{G}[p^n]$, and choose a $\mathrm{W}_\infty(\mathbb{F}_q)$-basis for D_∞; this induces a $\mathrm{W}_n(\mathbb{F}_q)$-basis for every D_n. Then for every power q of p, every element in $\mathsf{D}_n^{h,d}(\mathbb{F}_q)$ is isomorphic to

$$D_{n,g} := (\mathrm{W}_n(\mathbb{F}_q) \otimes_{\mathbb{Z}/p^n\mathbb{Z}} D_n, gF_n, V_n g^{-1})$$

for some $g \in \mathrm{GL}_h(\mathrm{W}_n(\mathbb{F}_q))$ (See [69, 2.2.2]).

For a smooth affine group scheme $\mathscr{G}$ over $\mathrm{Spec}(\mathbb{Z}_p)$, let $\mathbb{W}_n(\mathscr{G})$ be the group scheme over $\mathrm{Spec}(\mathbb{F}_p)$ defined by $\mathbb{W}_n(\mathscr{G})(R) = G(\mathrm{W}_n(R))$ (see [69, 2.1.4]); it is again smooth and affine. For every n there is a natural reduction morphism $\mathbb{W}_{n+1}(\mathscr{G}) \to \mathbb{W}_n(\mathscr{G})$.

Proposition 3.34. *Let $\mathcal{D}_n := \mathbb{W}_n(\mathtt{GL}_h)$. Then there exists a smooth affine group scheme $\mathcal{H}$ over $\mathbb{Z}_p$ and for every n an action of $\mathcal{H}_n := \mathbb{W}_n(\mathcal{H})$ on $\mathcal{D}_n$, compatible with the reduction maps $\mathcal{H}_{n+1} \to \mathcal{H}_n$ and $\mathcal{D}_{n+1} \to \mathcal{D}_n$, such that for every power q of p, there exists for every $g, g' \in \mathcal{D}_n(\mathbb{F}_q)$ an isomorphism of $\mathbb{F}_q$-varieties*

$$\varphi_{g,g'} \colon \mathtt{Transp}_{\mathcal{H}_{n,\mathbb{F}_q}}(g, g')^{\mathrm{red}} \xrightarrow{\sim} \mathtt{Isom}(D_{n,g}, D_{n,g'})^{\mathrm{red}}$$

that is compatible with compositions in the sense that for every $g, g', g'' \in \mathcal{D}_n(\mathbb{F}_q)$ the following diagram commutes, where the horizontal maps are the natural composition morphisms:

$$\begin{array}{ccc} \mathtt{Transp}_{\mathcal{H}_{n,\mathbb{F}_q}}(g, g')^{\mathrm{red}} \times \mathtt{Transp}_{\mathcal{H}_{n,\mathbb{F}_q}}(g', g'')^{\mathrm{red}} & \longrightarrow & \mathtt{Transp}_{\mathcal{H}_{n,\mathbb{F}_q}}(g, g'')^{\mathrm{red}} \\ \Big\downarrow{\scriptstyle \varphi_{g,g'} \times \varphi_{g',g''}} & & \Big\downarrow{\scriptstyle \varphi_{g,g''}} \\ \mathtt{Isom}(D_{n,g}, D_{n,g'})^{\mathrm{red}} \times \mathtt{Isom}(D_{n,g'}, D_{n,g''})^{\mathrm{red}} & \longrightarrow & \mathtt{Isom}(D_{n,g}, D_{n,g''})^{\mathrm{red}} \end{array}$$

Proof. The group $\mathcal{H}$ and the action $\mathcal{H}_n \times \mathcal{D}_n \to \mathcal{D}_n$ are defined in [69, 2.1.1 & 2.2] over an algebraically closed field k of characteristic p, but the definition still makes sense over $\mathbb{F}_p$. The isomorphism of groups $\varphi_{g,g}$ is given on k-points in [69, 2.4(b)]. The definition of the map there shows that it is algebraic and defined over $\mathbb{F}_p$. Since it is an isomorphism on $\bar{\mathbb{F}}_p$-points, it is an isomorphism of reduced group schemes over $\mathbb{F}_p$. Furthermore, a morphism $\mathtt{Transp}_{\mathcal{H}_{n,\mathbb{F}_q}}(g, g') \to \mathtt{Isom}(D_{n,g}, D_{n,g'})$ is given in the proof of [69, 2.2.1]. It is easily seen that this map is compatible with compositions in the sense of the diagram above, and that it is equivariant under the action of $\mathtt{Stab}_{\mathcal{H}_n}(g)(\bar{\mathbb{F}}_p) \cong \mathtt{Isom}(D_{n,g})(\bar{\mathbb{F}}_p)$. Since both varieties are torsors under this action, this must be an isomorphism as well. □

Corollary 3.35. *For every power q of p the categories $\mathsf{D}_n^{h,d}(\mathbb{F}_q)$ and $[\mathcal{H}_n \backslash \mathcal{D}_n](\mathbb{F}_q)$ are equivalent.*

Proof. For every object $D \in \mathsf{D}_n^{h,d}(\mathbb{F}_q)$ choose a $g_D \in \mathcal{D}_n(\mathbb{F}_q)$ such that $D \cong D_{n,g_D}$. Define a functor

$$E \colon \mathsf{D}_n^{h,d}(\mathbb{F}_q) \to [\mathcal{H}_n \backslash \mathcal{D}_n](\mathbb{F}_q)$$

that sends a D to the pair $(\mathcal{H}_n, f_D)$, where $f_D \colon \mathcal{H}_n \to \mathcal{D}_n$ is given by $f_D(h) = h \cdot g_D$. We send an isomorphism from D to D' to the corresponding element of

$$\mathrm{Isom}((\mathcal{H}_n, f_D), (\mathcal{H}_n, f_{D'})) = \mathrm{Transp}_{\mathcal{H}_n(\mathbb{F}_q)}(g_D, g_{D'}).$$

This functor is fully faithful and essentially surjective, hence an equivalence of categories. □

By proposition 3.26 the isomorphism classes in $\mathsf{D}_n^{h,d}(k)$ for an algebraically closed field k are classified by ${}^I W$. For each $w \in {}^I W$, let $\mathsf{D}_n^{h,d,w}$ be the substack of $\mathsf{D}_n^{h,d}$ consisting of truncated Barsotti–Tate groups of level n, rank h, and with F of rank d, whose associated BT_1 are of type K_w at all geometric points. Then over fields k of characteristic p one has $\mathsf{D}_n^{h,d}(k) = \coprod_{w \in {}^I W} \mathsf{D}_n^{h,d,w}(k)$ as categories, hence (for all powers q of p)

$$\#\mathsf{D}_n^{h,d}(\mathbb{F}_q) = \sum_{w \in {}^I W} \mathsf{D}_n^{h,d,w}(\mathbb{F}_q).$$

For every $w \in {}^I W$, let $g_{1,w} \in \mathcal{D}_1(\mathbb{F}_p)$ be such that $D_{1,g_{1,w}} \cong \mathrm{St}_{\mathbb{F}_p}(K_w)$. For every n, let $\mathcal{D}_{n,w}$ be the preimage of $g_{1,w}$ under the reduction map $\mathcal{D}_n \to \mathcal{D}_1$. Let $\mathcal{H}_{n,w}$ be the preimage of $\mathtt{Stab}_{\mathcal{H}_1}(g_{1,w})$ in $\mathcal{H}_n$; then analogous to corollary 3.35 for every power q of p we get an equivalence of categories (see [19, 3.2.3 Lem. 2(b)])

$$\mathsf{D}_n^{h,d,w}(\mathbb{F}_q) \cong [\mathcal{H}_{n,w} \backslash \mathcal{D}_{n,w}](\mathbb{F}_q).$$

Proof of Theorem 3.33. Let q be a power of p. By the discussion above we see that

$$\#\mathsf{BT}_n^{h,d}(\mathbb{F}_q) = \sum_{w \in {}^I W} \#[\mathcal{H}_{n,w} \backslash \mathcal{D}_{n,w}](\mathbb{F}_q).$$

By proposition 3.32 the group scheme $\mathtt{Stab}_{\mathcal{H}_1}(g_w)^{\mathrm{red}} \cong \mathtt{Aut}(D_{1,g_1})^{\mathrm{red}}$ has an identity component that is unipotent of dimension $d(h-d) - \ell(w)$. The reduction morphism $\mathcal{H}_n \to \mathcal{H}_1$ is surjective and its kernel is unipotent of dimension $h^2(n-1)$, see [19, 3.1.1 & 3.1.3]. This implies that $\mathcal{H}_{n,w}$ has a unipotent identity component of dimension $h^2(n-1) + d(h-d) - \ell(w)$. Now fix a $g_{n,w} \in \mathcal{D}_{n,w}(\mathbb{F}_p)$; then we can identify $\mathcal{D}_{n,w}$ with the affine group $X = \mathbb{W}_{n-1}(\mathtt{Mat}_{h\times h})$, by sending an $x \in X$ to $g_{n,w} + ps(x)$, where $s\colon \mathbb{W}_{n-1}(\mathtt{Mat}_{h\times h}) \xrightarrow{\sim} p\mathbb{W}_n(\mathtt{Mat}_{h\times h}) \subset \mathbb{W}_n(\mathtt{Mat}_{h\times h})$ is the canonical identification. Furthermore, the action of an element $z \in \mathcal{H}_{n,w}$ on some $y = (g_{n,w} + ps(x)) \in \mathcal{D}_{n,w}$ is given by $z \cdot y = f(z)(g_{n,w} + ps(x))f'(z)$ for some algebraic maps $f, f'\colon \mathcal{H}_{n,w} \to \mathbb{W}_n(\mathtt{GL}_h)$ (see [69, 2.2.1a]). From this we see that the induced action of an element $z \in \mathcal{H}_{n,w}$ on the variety X is given by

$$z \cdot x = f(z)xf'(z) + \frac{1}{p}(f(z)g_{n,w}f'(z) - g_{n,w}), \tag{3.36}$$

which makes sense because $f(z)g_{n,w}f'(z)$ is equal to $g_{n,w}$ modulo p. If we regard X as $\mathbb{W}_{n-1}(\mathbb{G}_a^{h^2})$ via its canonical coordinates, (3.36) shows us that the action of $\mathcal{H}_{n,w}$ factors through the action of $\mathbb{W}_{n-1}(\mathtt{Aff}_{h^2})$, which is a connected algebraic group over $\mathbb{F}_p$; here $\mathtt{Aff}_{h^2}$ is the $\mathbb{Z}_p$-group scheme of affine transformations of h^2-dimensional affine space. Applying proposition 2.21 with $F = \mathcal{H}_{n,w}$, $H = U = E = 1$, $V = \mathcal{D}_{n,w}$ now yields $\#\mathsf{D}_n^{h,d,w}(\mathbb{F}_q) = q^{\ell(w)-d(h-d)}$. The formula for the zeta function is provided by theorem 2.27. □

Remark 3.37. Since the zeta function $Z(\mathsf{BT}_n^{h,d}, t)$ does not depend on n, one might be tempted to think that the stack $\mathsf{BT}_\infty^{h,d}$ of non-truncated Barsotti–Tate groups of height h and dimension d has the same zeta function. However, this stack is not of finite type. For instance, every Barsotti–Tate group $\mathcal{G}$ over $\mathbb{F}_q$ has a natural injection $\mathbb{Z}_p^\times \hookrightarrow \mathrm{Aut}(\mathcal{G})$, which shows us that the zeta function of $\mathsf{BT}_\infty^{h,d}$ is not well-defined.

Chapter 4

Stacks of BT_1-flags

In this chapter we define so-called *BT_1-flags*: these are inclusion chains

$$G_1 \subset G_2 \subset \cdots \subset G_r$$

of p-groups over a scheme S, such that G_r is a BT_1. Under some numerical constraints these BT_1-flags form an algebraic stack of finite type over $\mathbb{F}_p$; this chapter is dedicated to calculating the point counts and zeta functions of these stacks. Although we cannot find a direct formula as in theorem 3.33, we provide an algorithm (4.24) that calculates the point count over $\mathbb{F}_q$ of such a stack as an integral polynomial in q and q^{-1}. Furthermore, in section 4.3 we provide some shortcuts for calculating the point count manually. Finally, we give an example of such a manual calculation in section 4.4.

Before diving straight into the formal approach, it is helpful to sketch an informal example. Suppose we want to determine the point counts of the stack of chains of p-groups

$$G_1 \subset G_2 \subset G_3$$

where G_1 is of height $h_1 := 2$, G_2 is of height $h_2 := 3$, and G_3 is of height $h_3 := 6$. Furthermore, we demand that G_3 is a BT_1 of dimension 2. Since we are working over finite fields, we might as well consider the stack of quintuples $(D_1, D_2, D_3, f_1, f_2)$, where

- Each D_i is a level 1 Dieudonné module of height h_i;
- D_3 is exact of dimension 2;
- Each f_i is an injective morphism of Dieudonné modules $f_i\colon D_i \hookrightarrow D_{i+1}$.

Schematically, we may denote the numerical data by the 'word' $2 \hookrightarrow 3 \hookrightarrow (6, 2)$, and the category of these quintuples over $\mathbb{F}_q$ by $\mathsf{C}(2 \hookrightarrow 3 \hookrightarrow (6, 2), \mathbb{F}_q)$ (in this category, morphisms are isomorphisms of the D_i that are compatible with the f_i). To determine the point count of this category, we would like to know the structure of the scheme of injective morphisms $\mathtt{Inj}(D, D')$ for two Dieudonné modules D and D'. Unfortunately, we only have a description of the full scheme of morphisms $\mathtt{Hom}(D, D')$ from proposition 3.28. Therefore it is initially easier to look at a bigger category $\mathsf{C}(2 \to 3 \to (6,2), \mathbb{F}_q)$, which has the same definition as $\mathsf{C}(2 \hookrightarrow 3 \hookrightarrow (6,2), \mathbb{F}_q)$, except that we do not require f_1 and f_2 to be injective. We can calculate the point count of this bigger category as follows: recall that the set of Kraft types is denoted $\mathcal{K}$. For a triple $(K_1, K_2, K_3) \in \mathcal{K}^3$ with appropriate numerical invariants (see definition 4.7), let $\mathsf{C}(K_1 \to K_2 \to K_3, \mathbb{F}_q)$ be the full subcategory of $\mathsf{C}(2 \to 3 \to (6,2), \mathbb{F}_q)$ such that each D_i is of type K_i. Then there is a finite subset $X \subset \mathcal{K}^3$ such that

$$\mathsf{C}(2 \to 3 \to (6,2), \mathbb{F}_q) = \bigsqcup_{(K_1,K_2,K_3)\in X} \mathsf{C}(K_1 \to K_2 \to K_3, \mathbb{F}_q).$$

We can relate such a category $\mathsf{C}(K_1 \to K_2 \to K_3, \mathbb{F}_q)$ to a quotient stack, and then use the results of chapter 2 to calculate its point count (see theorem 4.20). By summing over X we find an expression for $\#\mathsf{C}(2 \to 3 \to (6,2), \mathbb{F}_q)$.

Let us return to the difference between the point counts $\#\mathsf{C}(2 \to 3 \to (6,2), \mathbb{F}_q)$ and $\#\mathsf{C}(2 \hookrightarrow 3 \hookrightarrow (6,2), \mathbb{F}_q)$. If f_1 is not injective, we get a chain

$$D_1 \twoheadrightarrow \mathrm{im}(f_1) \hookrightarrow D_2 \to D_3,$$

where $\mathrm{im}(f_1)$ has height either 1 or 0. From this we get an equivalence of categories

$$\begin{aligned}\mathsf{C}(2 \to 3 \to (6,2), \mathbb{F}_q) \quad &\cong \quad \mathsf{C}(2 \hookrightarrow 3 \to (6,2), \mathbb{F}_q) \\ &\quad\sqcup \mathsf{C}(2 \twoheadrightarrow 1 \hookrightarrow 3 \to (6,2), \mathbb{F}_q) \\ &\quad\sqcup \mathsf{C}(2 \twoheadrightarrow 0 \hookrightarrow 3 \to (6,2), \mathbb{F}_q),\end{aligned}$$

where the categories are defined as one would expect (see definition 4.7 for more details). As such we find

$$\begin{aligned}\#\mathsf{C}(2 \hookrightarrow 3 \to (6,2), \mathbb{F}_q) \quad &= \quad \#\mathsf{C}(2 \to 3 \to (6,2), \mathbb{F}_q) \\ &\quad -\#\mathsf{C}(2 \twoheadrightarrow 1 \hookrightarrow 3 \to (6,2), \mathbb{F}_q) \\ &\quad -\#\mathsf{C}(2 \twoheadrightarrow 0 \hookrightarrow 3 \to (6,2), \mathbb{F}_q).\end{aligned} \tag{4.1}$$

Applying similar reasoning to the second $\hookrightarrow$ yields a decomposition

$$\begin{aligned}\#\mathsf{C}(2 \hookrightarrow 3 \hookrightarrow (6,2), \mathbb{F}_q) \quad &= \quad \#\mathsf{C}(2 \hookrightarrow 3 \to (6,2), \mathbb{F}_q) \\ &\quad -\#\mathsf{C}(2 \hookrightarrow 3 \twoheadrightarrow 2 \hookrightarrow (6,2), \mathbb{F}_q) \\ &\quad -\#\mathsf{C}(2 \hookrightarrow 3 \twoheadrightarrow 1 \hookrightarrow (6,2), \mathbb{F}_q) \\ &\quad -\#\mathsf{C}(2 \hookrightarrow 3 \twoheadrightarrow 0 \hookrightarrow (6,2), \mathbb{F}_q).\end{aligned}$$

Together these two equations describe the difference between $\#\mathsf{C}(2 \to 3 \to (6,2), \mathbb{F}_q)$ and $\#\mathsf{C}(2 \hookrightarrow 3 \hookrightarrow (6,2), \mathbb{F}_q)$ in terms of the point counts of other categories. Unfortunately, we do not have a direct formula for these point counts. However, we can get an expression for such a point count (e.g. #$\mathsf{C}(2 \hookrightarrow 3 \twoheadrightarrow 1 \hookrightarrow (6,2), \mathbb{F}_q)$) by first calculating the point count of a similar category of chains where we allow more morphisms within a chain (e.g. #$\mathsf{C}(2 \to 3 \to 1 \to (6,2), \mathbb{F}_q)$), and then expressing the difference in terms of point counts of other categories. We then continue this process with our newly-found set of point counts. This process eventually terminates (see lemma 4.11), and this gives us a recursive method to determine the point count #$\mathsf{C}(2 \hookrightarrow 3 \hookrightarrow (6,2), \mathbb{F}_q)$. In the rest of this chapter, we formalise this approach into algorithm 4.24, which allows us to calculate the point counts of chains of arbitrary length and numerical invariants.

4.1 Chain words and categories

In this section we formally define BT_1-flags; these arise as invariants of points on moduli spaces of abelian varieties with non-full level structure. We also introduce their moduli stacks, whose point counts and zeta functions will be the subject of this chapter. To study these moduli stacks, we relate them to so-called *chain categories*, which are categories of Dieudonné theory objects related to BT_1-flags.

Definition 4.2. Let r be a positive integer. Let S be a scheme of characteristic p, and let $\underline{h} = (h_1, \cdots, h_r)$ be an increasing sequence of positive integers. Then a *BT_1-flag of height $\underline{h}$ over S* is an increasing sequence of p-groups $G_1 \subset \cdots \subset G_r$ over S, such that each G_i is of height h_i, and such that G_r is a BT_1. The *dimension* of the sequence is the dimension of G_r (see [12, II.7 Def.]).

Analogously to [70, Prop. 1.8] and fact 3.8 one can prove the following.

Fact 4.3. Let r be a positive integer. Let $\underline{h} = (h_1, \cdots, h_r)$ be an increasing sequence of positive integers, and let $d \leq h_r$ be a nonnegative integer.

1. The BT_1-flags of height $\underline{h}$ and dimension d form an algebraic stack $\mathsf{BTFlag}^{\underline{h},d}$ of finite type over $\mathbb{F}_p$.
2. Let k be a perfect field, and let $\mathsf{DFlag}^{\underline{h},d}(k)$ be the category of flags of level 1 Dieudonné modules $D_1 \subset \cdots \subset D_r$, such that each D_i is of height h_i, and D_r is exact of dimension d (we take the morphisms of this categories to be isomorphisms of Dieudonné modules $D_r \xrightarrow{\sim} D_r'$ that preserve the flags). Then there is an equivalence of categories
$$\mathsf{BTFlag}^{\underline{h},d}(k) \xrightarrow{\sim} \mathsf{DFlag}^{\underline{h},d}(k)$$
coming from the natural equivalences in fact 3.8.2. □

Example 4.4. Let $\underline{h} = (h_1, \cdots, h_r)$ be an increasing sequence of integers, with h_r even. In characteristic p, let S be the moduli stack of pairs $(X, H_1, \cdots, H_{r-1})$, where X is a principally polarised abelian variety of dimension $\frac{h_r}{2}$, and $H_1 \subset \cdots \subset H_{r-1} \subset X[p]$ is a flag of subgroup schemes where each H_i has order p^{h_i}. Then we get a natural morphism of $\mathbb{F}_p$-stacks

$$\mathsf{S} \to \mathsf{BTFlag}^{\underline{h}, \frac{h_r}{2}}$$
$$(X, H_1, \cdots, H_r) \mapsto H_1 \subset \cdots \subset H_r \subset X[p].$$

BT_1-flags of this type occur in the study of polarised abelian varieties with a $\Gamma_0(p)$-structure (see for example [26]).

Remark 4.5. There are two reasons why we demand G_r to be a BT_1 in definition 4.2. First, example 4.4 shows that this is what we find in the study of moduli of abelian varieties. Second, this extra assumption ensures that the stack $\mathsf{BTFlag}^{\underline{h},d}$ has a rational zeta function, which we will be able to determine explicitely.

As before it suffices for our purposes to consider the point counts of categories of the form $\mathsf{DFlag}^{\underline{h},d}(\mathbb{F}_q)$. If we replace the inclusions in the definition of $\mathsf{DFlag}^{\underline{h},d}$ by injective morphisms, we see that it consists of tuples $\underline{D} = ((D_i)_{i\leq r}, (f_i)_{i<r})$, where each D_i is a Dieudonné module (subject to some numerical conditions), and each map $f_i\colon D_i \hookrightarrow D_{i+1}$ is an injective morphism of Dieudonné modules. To determine the point count of this category, it will prove useful to extend or restrict the category by playing around with the restrictions on the D_i and the f_i: for example, we might want to restrict a D_i to a certain Kraft type, or we might drop the condition that an f_i is injective. A convenient way to denote what restriction we place on a category of chains of Dieudonné modules is given in the definition below.

Definition 4.6. Let $r \geq 1$ be an integer. Let $\mathcal{K}$ denote the set of Kraft types. A *chain word of length r* is a word (see 3.9)

$$L = A_1B_1A_2B_2\cdots A_{r-1}B_{r-1}A_r \in \mathcal{W}\Big(\mathcal{K} \sqcup \mathbb{Z}_{\geq 0} \sqcup \mathbb{Z}^2_{\geq 0} \sqcup \{\to, \hookrightarrow, \twoheadrightarrow\}\Big)$$

of one of the following types such that:

- Each A_i is either a Kraft type, a nonnegative integer, or a pair of nonnegative integers (a, b) satisfying $a \geq b$;
- Each B_i is an element of the set $\{\to, \hookrightarrow, \twoheadrightarrow\}$.

A chain word is called *regular* if each B_i equals $\to$, *injective* if each B_i equals $\hookrightarrow$, and *surjective* if each B_i equals $\twoheadrightarrow$. Furthermore a chain word is called *of numeric type* if each A_i is either an integer or a pair of integers, and *of Kraft type* if each A_i is a Kraft type.

Definition 4.7. Let $L = A_1B_1\cdots A_n$ be a chain word of length r, and let k be a perfect field field of characteristic p. Then the *chain category of L over k*, denoted $\mathsf{C}(L, k)$, is defined as follows. Its objects are collections $\underline{D} = ((D_i)_{i\leq r}, (f_i)_{i<r})$, where each D_i is a level 1 Dieudonné module over k whose type

- is an element of $\mathcal{K}(A_i)$ if A_i is either an integer, or a pair of integers (a, b) with $a \geq b$ (see definition 3.15);

- is equal to A_i if A_i is a Kraft type.

Furthermore, each f_i is a morphism of Dieudonné modules $f_i\colon D_i \to D_{i+1}$ that is injective if $B_i = \hookrightarrow$, and surjective if $B_i = \twoheadrightarrow$. A morphism $\varphi\colon \underline{D} \to \underline{D}'$ in $\mathsf{C}(L,k)$ is a collection of isomorphisms $\varphi_i\colon D_i \xrightarrow{\sim} D_i'$ of Dieudonné modules, satisfying $\varphi_{i+1}f_i = f_i'\varphi_i$ for all $i < n$.

Example 4.8.

1. Consider the chain word of numeric type $2 \hookrightarrow 3 \hookrightarrow (6,2)$, and let k be a perfect field of characteristic p. Then the category $\mathsf{C}(2 \hookrightarrow 3 \hookrightarrow (6,2), k)$ consists of sequences

$$D_1 \overset{f_1}{\hookrightarrow} D_2 \overset{f_2}{\hookrightarrow} D_3$$

Where D_1 is a Dieudonné module of height 2, D_2 is a Dieudonné module of height 3, and D_3 is a Dieudonné module of height 6 and dimension 2; furthermore, both f_1 and f_2 have to be injective. A morphism φ between two such sequences $\underline{D}$ and $\underline{D}'$ is a commutative diagram as below.

$$\begin{array}{ccccc} D_1 & \overset{f_1}{\hookrightarrow} & D_2 & \overset{f_2}{\hookrightarrow} & D_3 \\ \wr\downarrow \varphi_1 & & \wr\downarrow \varphi_2 & & \wr\downarrow \varphi_3 \\ D_1' & \overset{f_1'}{\hookrightarrow} & D_2' & \overset{f_2'}{\hookrightarrow} & D_3' \end{array}$$

2. Let Δ_6 and Δ_8 be the elements of $\mathcal{K}$ as defined in section 4.4. Consider the chain word of Kraft type $\Delta_6 \hookrightarrow \Delta_8 \twoheadrightarrow 5$. Then $\mathsf{C}(\Delta_6 \hookrightarrow \Delta_8 \twoheadrightarrow 5, k)$ consists out of sequences

$$D_1 \overset{f_1}{\hookrightarrow} D_2 \overset{f_2}{\twoheadrightarrow} D_3$$

where D_1 is of type Δ_6, D_2 is of type Δ_8, D_3 is of height 5, f_1 is injective and f_2 is surjective. In particular $D_{1,\bar{k}}$ is isomorphic to $\mathrm{St}_{\bar{k}}(\Delta_6)$ and $D_{2,\bar{k}}$ is isomorphic to $\mathrm{St}_{\bar{k}}(\Delta_8)$. However, as we will see in section 4.4, there do not exist any injective homomorphisms $\mathrm{St}_{\bar{k}}(\Delta_6) \hookrightarrow \mathrm{St}_{\bar{k}}(\Delta_8)$; hence $\mathsf{C}(\Delta_6 \hookrightarrow \Delta_8 \twoheadrightarrow 5, k)$ is the empty category.

3. Let $\underline{h} = (h_1, \ldots, h_r)$ be a sequence of increasing positive integers, and let $d \leq h_r$ be a nonnegative integer. Let k be a perfect field of characteristic p. Then we get an equivalence of categories

$$\mathsf{BTFlag}^{\underline{h},d}(k) \xrightarrow{\sim} \mathsf{DFlag}^{\underline{h},d}(k) \xrightarrow{\sim} \mathsf{C}(L^{\underline{h},d}, k)$$

with $L^{\underline{h},d} := h_1 \hookrightarrow \ldots \hookrightarrow h_{r-1} \hookrightarrow (h_r, d)$.

Remark 4.9. Similar to remark 3.6 we can extend the definition of $\mathsf{C}(L,k)$ from perfect fields k to general schemes of characteristic p, and this gives us an algebraic stack $\mathsf{C}(L)$ of finite type over $\mathbb{F}_p$. As usual, however, we are only concerned with its points over finite fields.

Remark 4.10. Let $L = A_1 B_1 \cdots A_r$ be a chain word of numeric type, and let k be a perfect field of characteristic p. Let $\underline{D} = ((D_i)_i, (f_i)_i)$ be an object of $\mathsf{C}(L, k)$, and for every i, let K_i be the type of D_i; this is an element of $\mathcal{K}(A_i)$. Let L' be the chain word of Kraft type $L' = K_1 B_1 \cdots K_n$; then we can consider $\underline{D}$ as an element of $\mathsf{C}(L', k)$. This gives a decomposition

$$\mathsf{C}(L, k) \cong \bigsqcup_{(K_i)_i \in \prod_i \mathcal{K}(A_i)} \mathsf{C}(K_1 B_1 \cdots K_r, k).$$

Although our definition allows for a wide variety of chain words, we are mainly interested in chain words of two types:

1. injective chain words of numeric type, because their chain categories correspond to categories of BT_1-flags by example 4.8.3;
2. regular chain words of Kraft type, because we will be able to explicitely calculate the point counts of their chain categories (see theorem 4.20).

As such, the goal for the remainder of this section is to find a way to express the point count of a chain category of a (not necessarily regular) chain word of numeric type in terms of the point counts of chain categories of regular chain words of Kraft type:

Proposition 4.11. *Let L be a chain word of numeric type. There exists a finite set of regular chain words of Kraft type $\mathcal{L}'$ and integers $c_{L'}$ such that*

$$\#\mathsf{C}(L, k) = \sum_{L' \in \mathcal{L}'} c_{L'} \#\mathsf{C}(L', k) \tag{4.12}$$

for every finite field k of characteristic p.

To prove this proposition we first need an auxiliary lemma. It is in the proof of this lemma, and in the proof of proposition 4.11, that we need chain words of greater generality than the two types discussed above. The philosophy of the lemma is that if in a chain word we replace a letter $\hookrightarrow$ or $\twoheadrightarrow$ by $\to$, we will allow more objects in corresponding chain categories, so this will increase their point counts. However, it turns out that we can express this increase in terms of point counts of other chain categories. We have seen an illustration of this phenomenon in (4.1).

Lemma 4.13. *Let k be a finite field of characteristic p. Consider two chain words of numeric type $L = A_1 B_1 \cdots A_r$ and $L' = A'_1 B'_1 \cdots A'_{r'}$.*

1. *Consider the chain word of numeric type $L \hookrightarrow L'$. Let a be such that A_r is either an integer a, or a pair of integers (a, b). Then*

$$\#\mathsf{C}(L \hookrightarrow L', k) = \#\mathsf{C}(L \to L', k) - \sum_{x < a} \#\mathsf{C}(L \twoheadrightarrow x \hookrightarrow L', k). \tag{4.14}$$

2. *Consider the chain word of numeric type $L \twoheadrightarrow L'$. Let a' be such that A'_1 is either an integer a', or a pair of integers (a', b'). Then*

$$\#\mathsf{C}(L \twoheadrightarrow L', k) = \#\mathsf{C}(L \to L', k) - \sum_{x<a'} \#\mathsf{C}(L \twoheadrightarrow x \hookrightarrow L', k). \tag{4.15}$$

Proof. We only prove the first point, as the other point can be proven analogously. Consider the set $\mathbb{Z}$ as a category whose only morphisms are identities. Then we get a functor

$$\begin{aligned} \Phi\colon \mathsf{C}(L \to L', k) &\to \mathbb{Z} \\ \underline{D} = ((D_i)_i, (f_i)_i) &\mapsto \dim(\operatorname{im}(f_r)); \end{aligned}$$

note that the numbering is such that the map $f_r\colon D_r \to D_{r+1}$ is the morphism corresponding to the '$\to$' in $L \to L'$. The fibre over $a \in \mathbb{Z}$ consists of those $\underline{D}$ for which f_r is injective, hence it is naturally identified with $\mathsf{C}(L \hookrightarrow L', k)$. For $x < a$ we get a functor from $\Phi^{-1}(x)$ to $\mathsf{C}(L \twoheadrightarrow x \hookrightarrow L', k)$ by sending an object

$$D_1 \xrightarrow{f_2} D_2 \to \cdots \to D_r \xrightarrow{f_r} D_{r+1} \to \cdots \to D_{r+r'-1} \xrightarrow{f_{r+r'-1}} D_{r+r'}$$

to

$$D_1 \xrightarrow{f_2} D_2 \to \cdots \to D_r \xrightarrow{g} \operatorname{im}(f_r) \xrightarrow{h} D_{r+1} \to \cdots \to D_{r+r'-1} \xrightarrow{f_{r+r'-1}} D_{r+r'}$$

where g is the surjective map induced by f_r, and h is the inclusion. It is easily seen that this is an equivalence of categories, hence we get an equivalence of categories

$$\mathsf{C}(L \to L', k) \cong \mathsf{C}(L \hookrightarrow L', k) \sqcup \bigsqcup_{x<a} \mathsf{C}(L \twoheadrightarrow x \hookrightarrow L', k),$$

from which the first point follows. The second point is proven in an analogous way. □

Proof of proposition 4.11. First we claim that there is a set $\mathcal{L}''$ of chain regular chain words *of numeric type* and integers $c_{L''}$ such that

$$\#\mathsf{C}(L, k) = \sum_{L'' \in \mathcal{L}''} c_{L''} \#\mathsf{C}(L'', k)$$

for every k. If L is regular, then this statement is trivially true. If not, then at least one of its 'arrows' must be equal to either $\hookrightarrow$ or $\twoheadrightarrow$. If this is the case we can, using lemma 4.13, express $\#\mathsf{C}(L, k)$ as an integral combination of some other $\#\mathsf{C}(L'', k)$; the L'' involved do not depend on the choice of k. If some of these L'' again are not regular, we can use the same method to rewrite each of them as a sum of other $\#\mathsf{C}(L'', k)$. We want to show that this process eventually ends. For this, we wish to assign to every numeric chain word L a constant $J(L) \in \mathbb{Z}_{\geq 0}$ such that

- In (4.14) we have $J(L \hookrightarrow L') > J(L \to L')$ and $J(L \hookrightarrow L') > J(L \twoheadrightarrow x \hookrightarrow L)$ for all $x < a$;

- In (4.15) we have $J(L \twoheadrightarrow L') > J(L \to L')$ and $J(L \twoheadrightarrow L') > J(L \twoheadrightarrow x \hookrightarrow L')$ for all $x < a'$.

Together, these properties ensure that every time we invoke lemma 4.13 we replace the point count of a chain category by an integral combination of point counts of chain categories whose associated chain words have lower J-values. Since all $J(L)$ are nonnegative integers, this means that we will always arrive at a point where we cannot invoke lemma 4.13; this is only possible if we are at a point where we all chain words in our integral combination are regular. Hence, if we prove the existence of such a J, we have proven the claim. To define such a J, let $L = A_1B_1 \cdots A_r$ be a chain word of length r of numeric type. Let $\tilde{L} = \tilde{A}_1\tilde{B}_1 \cdots \tilde{A}_r$ be the same as L, except that we have replace a letter A_i by the integer $\tilde{A}_i := a$ if A_i is a pair (a, b). For $i < r$ we set

$$J_i(L) := \begin{cases} 3^{\tilde{A}_i + \tilde{A}_{i+1}}, & \text{if } B_i \neq \ \to; \\ 0, & \text{if } B_i = \ \to. \end{cases}$$

and we define $J(L) := \sum_{i<r} J_i(L)$. A straightforward check shows that this J satisfies the properties above, and this proves our claim.

To prove the proposition, it now suffices to show that for every regular chain word M of numeric type there is a finite set $\mathcal{M}'$ of regular chain words of Kraft type such that

$$\#\mathsf{C}(M, k) = \sum_{M' \in \mathcal{M}'} \#\mathsf{C}(M', k)$$

for all k. We can find such a set using remark 4.10: if $M = A_1 \to \cdots \to A_r$, then the set

$$\mathcal{M}' := \Big\{ K_1 \to \cdots \to K_r : K_i \in \mathcal{K}(A_i) \text{ for all } i \leq r \Big\}$$

satisfies this property. ☐

4.2 Point counts of chain stacks

In this section we give an algorithm (4.24) to calculate the point count $\#\mathsf{DFlag}^{\underline{h},d}(\mathbb{F}_q)$. The strategy is as follows: if L is a regular chain word of Kraft type, we define a variety X_L and an algebraic group G_L acting on X_L such that $\mathsf{C}(L, \mathbb{F}_q) \cong [G_L \backslash X_L](\mathbb{F}_q)$. Using methods of section 2.1 we can then calculate the point count of $\mathsf{C}(L, \mathbb{F}_q)$. Finally, we may express $\#\mathsf{BTFlag}^{\underline{h},d}(\mathbb{F}_q)$ in terms of such $\#\mathsf{C}(L, \mathbb{F}_q)$ via proposition 4.11.

Notation 4.16. Let L be a regular chain word of Kraft type of length r. We define a scheme X_L over $\mathbb{F}_p$, with an action of an algebraic group G_L as follows: For $i \leq r$, define $G_i := \mathtt{Aut}(\mathrm{St}_{\mathbb{F}_p}(L_i))^{\mathrm{red}}$, where where $\mathrm{St}_{\mathbb{F}_p}$ is as in section 3.2. Furthermore define $G_L := \prod_{i \leq r} G_i$, and for $i < r$, define

$$X_i = \mathtt{Hom}(\mathrm{St}_{\mathbb{F}_p}(L_i), \mathrm{St}_{\mathbb{F}_p}(L_{i+1}))^{\mathrm{red}}.$$

Since $G_i \times G_{i+1}$ acts on X_i on the left by $(g, g') \cdot x = gxg'^{-1}$, we get a left action of G_L on $X_L := \prod_{i<r} X_i$.

Lemma 4.17. *Let k be a perfect field of characteristic p, and let L be a chain word of Kraft type. Let X_L and G_L be as in notation 4.16. Then there is a contravariant equivalence of categories*

$$\mathsf{C}(L, k) \overset{\sim}{\longleftrightarrow} [G_L \backslash X_L](k).$$

Proof. Let $L = A_1 B_1 \cdots A_r$, and let $\underline{D} := ((D_i), (f_i)) \in \mathsf{C}(L, k)$. Then

$$T_{\underline{D}} := \prod_{i \le r} \mathtt{Isom}(D_i, \mathrm{St}_k(A_i))$$

is a left G_L-torsor over k. Furthermore we get a map

$$f_{\underline{D}} \colon T_{\underline{D}} \to \prod_{i<n} X_i$$
$$(\zeta_i)_{i \le r} \mapsto \zeta_{i+1} \circ f_i \circ \zeta_i^{-1}.$$

This map is G_L-equivariant, and as such $(T_{\underline{D}}, f_{\underline{D}}) \in [G_L \backslash X_L](k)$. If $\varphi \colon \underline{D} \to \underline{D}'$ is a morphism in $\mathsf{C}(L, k)$, then we get an induced isomorphism of G_i-torsors

$$\varphi_i^* \colon \mathtt{Isom}(D_i', \mathrm{St}_k(A_i)) \xrightarrow{\sim} \mathtt{Isom}(D_i, \mathrm{St}_k(A_i)).$$

Together these form a morphism $(T_{\underline{D}'}, f_{\underline{D}'}) \to (T_{\underline{D}}, f_{\underline{D}})$ in $[G_L \backslash X_L](k)$. One can check that this is fully faithful and essentially surjective, hence a contravariant equivalence of categories. □

As might be expected our next aim is to calculate point counts of categories of the form $[G_L \backslash X_L](\mathbb{F}_q)$. For this we need a little more notation.

Notation 4.18. Let r be a positive integer, and let $d_1, \ldots, d_r$ be nonnegative integers. We define $N(d_1, \ldots, d_r)$ to be the set of sequences of nonnegative integers $(a_{i,j})_{1 \le i \le j \le r}$ satisfying the following relations:

- $a_{i,j} \le a_{i+1,j}$ for all $1 \le i < j \le r$;
- $a_{j,j} = d_j$ for all $j \le r$;
- $a_{i,j} - a_{i-1,j} \ge a_{i,j+1} - a_{i-1,j+1}$ for all $1 < i \le j < r$;
- $a_{i,j} \ge a_{i,j+1}$ for all $1 \le i \le j < r$.

Lemma 4.19. *Let k be a field, and let $d_1, \ldots, d_r$ be nonnegative integers. For each $i < r$, let $\mathrm{GL}_{d_i}(k) \times \mathrm{GL}_{d_{i+1}}(k)$ act on the left on $\mathrm{Mat}_{d_{i+1} \times d_i}(k)$ in the natural way. Then there is a bijection*

$$\left(\prod_{j \le r} \mathrm{GL}_{d_j}(k) \right) \Big\backslash \left(\prod_{i<r} \mathrm{Mat}_{d_{i+1} \times d_i}(k) \right) \overset{\sim}{\longleftrightarrow} N(d_1, \ldots, d_r).$$

If k is Galois over a subfield $k' \subset k$, then this is an isomorphism of $\mathrm{Gal}(k/k')$-sets, where $\mathrm{Gal}(k/k')$ acts trivially on the right hand side.

Proof. For every $j \leq r$, let V_j be the vector space k^{d_j}. Let f_i be an element of $\mathrm{Mat}_{d_{i+1}\times d_i}(k)$ for each $i < r$, and consider each f_i as a map $V_i \to V_{i+1}$. For each $i \leq j$, set

$$V_{i,j} := (f_{j-1} \circ \cdots \circ f_i)(V_i) \subset V_j;$$

then the integers $a_{i,j} := \dim(V_{i,j})$ satisfy the inequalities of notation 4.18, and this gives us a map

$$\prod_{i<r} \mathrm{Mat}_{d_{i+1}\times d_i}(k) \to N(d_1, \ldots, d_r).$$

A straightforward verification shows that this map is invariant under the left actions of both $\prod_{j\leq r} \mathrm{GL}_{d_j}(k)$ and $\mathrm{Gal}(k/k')$, and that it is indeed a bijection. □

Theorem 4.20. *Let q be a power of p, and let $L = A_1 \to \cdots \to A_r$ be a regular chain word of Kraft type. Let $d, e \colon \mathcal{K} \times \mathcal{K} \to \mathbb{Z}$ and $d \colon \mathcal{K} \to \mathbb{Z}$ be as in notation 3.27, and define*

$$m(L) := \sum_{i<r} (d(A_i, A_{i+1}) + e(A_i, A_{i+1})) - \sum_{i\leq r} d(A_i).$$

Then

$$\#\mathsf{C}(L, \mathbb{F}_q) = \frac{\prod_{\Delta\in\mathcal{P}_{\mathrm{Z}}} \#N(A_1(\Delta), \cdots, A_r(\Delta))}{\prod_{i\leq r}\prod_{\Delta\in\mathcal{P}_{\mathrm{T}}} \#\mathrm{GL}_{A_i(\Delta)}(\mathbb{F}_q)} q^{m(L)}.$$

Proof. By lemma 4.17 we know that $\#\mathsf{C}(L, \mathbb{F}_q) = \#[G_L \backslash X_L](\mathbb{F}_q)$. From proposition 3.29 we get an isomorphism $G_L \cong (F \times H) \ltimes U$, where U is unipotent of dimension $\sum_{i\leq r} d(A_i)$ and

$$F \cong \prod_{i\leq r}\prod_{\Delta\in\mathcal{P}_{\mathrm{Z}}} \mathrm{GL}_{A_i(\Delta)}(\mathbb{F}_{p^{\ell(\Delta)}}),$$

$$H \cong \prod_{i\leq r}\prod_{\Delta\in\mathcal{P}_{\mathrm{T}}} \mathtt{GL}_{A_i(\Delta),\mathbb{F}_p}.$$

Furthermore, by proposition 3.28 we know that $X_L = E \times V$, where V is a vector space of dimension $\sum_{i<r} (d(A_i, A_{i+1}) + e(A_i, A_{i+1}))$, and

$$E \cong \prod_{i<r}\prod_{\Delta\in\mathcal{P}_{\mathrm{Z}}} \mathrm{Mat}_{A_{i+1}(\Delta)\times A_i(\Delta)}(\mathbb{F}_{p^{\ell(\Delta)}}).$$

Furthermore the decomposition $X_L = E \times V$ is a decomposition of varieties with an F-action, and the action of F on V is given by linear transformations. We may apply proposition 2.21 to find

$$\#[G_L \backslash X_L](\mathbb{F}_q) = (F(\bar{\mathbb{F}}_p)\backslash E(\bar{\mathbb{F}}_p))^{\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)} \cdot \frac{q^{m(L)}}{\prod_{i\leq r}\prod_{\Delta\in\mathcal{P}_{\mathrm{T}}} \#\mathrm{GL}_{A_i(\Delta)}(\mathbb{F}_q)}.$$

The action of F on E is the natural action as in lemma 4.19. Applying this lemma yields the required result. □

Corollary 4.21. *Let $\underline{h} = (h_1, \dots, h_r)$ be an increasing sequence of positive integers, and let $0 \leq d \leq h_r$. Then there exists a $R \in \mathbb{Q}(X)$ such that R is an element of the ring $\mathcal{R}$ in (2.26) and such that for every power q of p one has*

$$\#\mathsf{BTFlag}^{\underline{h},d}(\mathbb{F}_q) = R(q).$$

Proof. By example 4.8 and proposition 4.11 it suffices to prove this statement for regular chain words of Kraft type. The result now follows from theorem 4.20 and the formula

$$\#\mathrm{GL}_n(\mathbb{F}_q) = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}). \qquad \square$$

This corollary allows us to express the point count of a moduli stack of $\mathtt{BT}_1$-flags over $\mathbb{F}_q$ as a rational function in q. It turns out, however, that this rational function is actually an integral polynomial in q and q^{-1}. A key ingredient for this is the following lemma.

Lemma 4.22. *The zeta function of the $\mathbb{F}_p$-stack $\mathsf{BTFlag}^{\underline{h},d}$ is a rational function.*

Proof. Recall that $\#\mathsf{BTFlag}^{\underline{h},d}(k) = \#\mathsf{C}(L^{\underline{h},d}, k)$, where

$$L^{\underline{h},d} := h_1 \hookrightarrow \cdots \hookrightarrow h_{r-1} \hookrightarrow (h_r, d)$$

as in example 4.8. Let k be a finite field of characteristic p, and for every $K \in \mathcal{K}(h_r, d)$, define

$$L_K := h_1 \hookrightarrow \cdots \hookrightarrow h_{r-1} \hookrightarrow K;$$

Then

$$\#\mathsf{C}(L^{\underline{h},d}, k) = \sum_{K \in \mathcal{K}(h_r,d)} \#\mathsf{C}(L_K, k);$$

as such it suffices to show that for each $K \in \mathcal{K}(h_r, d)$ the 'zeta function'

$$Z_K(t) := \exp\left(\sum_{v \geq 1} \frac{t^v}{v} \#\mathsf{C}(L_K, \mathbb{F}_{p^v})\right)$$

is rational. Now fix a $K \in \mathcal{K}(h_r, d)$. For a vector space V and an integer n, let $\mathtt{Gr}(n, V)$ be the Grassmannian scheme of n-dimensional subspaces of V. Let X be the closed subscheme of the $\mathbb{F}_p$-scheme $\prod_{i \leq r} \mathtt{Gr}(h_i, \mathrm{St}_{\mathbb{F}_p}(K))$ consisting of elements $S = (S_i)_{i \leq r}$ satisfying:

- $S_i \subset S_{i+1}$ for all $i < r$;
- each S_i is mapped to itself under the semilinear maps F and V.

The group scheme $G := \mathtt{Aut}(\mathrm{St}_{\mathbb{F}_p}(K))^{\mathrm{red}}$ acts on X on the left. We get a contravariant functor

$$\Phi \colon \mathsf{C}(L_K, k) \to [G \backslash X](k)$$

as follows: let $\underline{D} \in \mathsf{C}(L_K, k)$. Since all the f_i are injective, we may regard each D_i as a Dieudonné submodule of D_r. As such, we may assign to $\underline{D}$ the G-torsor $\mathtt{Isom}(D_r, \mathrm{St}_k(K))$ over k, and the G-equivariant map $T \to X$ given by

$$\begin{array}{rcl} \mathtt{Isom}(D_r, \mathrm{St}_k(K)) & \to & X_k \\ \varphi & \mapsto & (\varphi(D_i))_{i \leq r}. \end{array}$$

Similar to lemma 4.17 we can prove that Φ is a contravariant equivalence of categories; hence $Z_K(t) = Z([G\backslash X], t)$. On the other hand, we know from proposition 3.29 that $G \cong \Gamma \ltimes U$, with Γ finite and U unipotent. From proposition 2.20 it now follows that $Z([G\backslash X], t) = Z([\Gamma\backslash X], p^{\text{-dim}(U)}t)$. Since $[\Gamma\backslash X]$ is a Deligne–Mumford stack, theorem 2.23 tells us that $Z([\Gamma\backslash X], t)$ is rational; hence $Z_K(t)$ is rational, as was to be shown. □

Corollary 4.23. *Let $\underline{h} = (h_1, \ldots, h_r)$ be an increasing sequence of positive integers, and let d be an integer such that $0 \leq d \leq h_r$. Then there exists a $R \in \mathbb{Z}[X, X^{-1}]$ such that for all powers q of p one has*

$$\#\mathsf{BTFlag}^{\underline{h},d}(\mathbb{F}_q) = R(q).$$

If $R = \sum_{n \in \mathbb{Z}} r_n X^n$, then $Z(\mathsf{BTFlag}^{\underline{h},d}, t) = \prod_n (1 - p^n t)^{-r_n}$.

Proof. By lemma 4.22 we may apply theorem 2.27 to corollary 4.21. □

As a result of this we can formulate the following algorithm to calculate $Z(\mathsf{BTFlag}^{\underline{h},d}, t)$:

Algorithm 4.24. Let $\underline{h} = (h_1, \ldots, h_r)$ be an increasing sequence of positive integers, and let $0 \leq d \leq h_r$. To calculate $Z(\mathsf{BTFlag}^{\underline{h},d}, t)$, perform the following steps:

1. Define the chain word $L^{\underline{h},d} = h_1 \hookrightarrow \cdots \hookrightarrow h_{r-1} \hookrightarrow (h_r, d)$.
2. Using proposition 4.11, find a finite set $\mathcal{L}'$ of regular chain words of Kraft type and an integer $c_{L'}$ for every $L' \in \mathcal{L}'$ such that
$$\#\mathsf{C}(L^{\underline{h},d}, k) = \sum_{L' \in \mathcal{L}'} c_{L'} \cdot \#\mathsf{C}(L', k).$$
3. Using theorem 4.20, determine for each $L' \in \mathcal{L}'$ the rational function $Q_{L'} \in \mathbb{Q}(X)$ such that $\#\mathsf{C}(L', \mathbb{F}_q) = Q_{L'}(q)$ for all powers q of p.
4. Then $R := \sum_{L' \in \mathcal{L}'} c_{L'} Q_{L'}$ is an element of $\mathbb{Z}[X, X^{-1}]$, see corollary 4.23. if $R = \sum_n r_n X^n$, then $Z(\mathsf{BTFlag}^{\underline{h},d}, t) = \prod_n (1 - p^n t)^{-r_n}$.

Remark 4.25. One can verify that the polynomial R in the algorithm above does not depend on the prime number p.

4.3 Shortcuts for manual calculation

Although in the previous section we have given algorithm 4.24 to calculate the zeta function of the $\mathbb{F}_p$-stack $\mathsf{BTFlag}^{\underline{h},d}$, this calculation can become quite cumbersome if performed manually, as the number of terms in the sum in proposition 4.11 grows quickly as either the length of the sequence $\underline{h}$ or its entries increase. In this section we discuss a few shortcuts that will make manual computation slightly easier. The overall strategy is as follows: in the proof of proposition 4.11, we express the point count of a chain category of a chain word of numeric type in terms of the point counts of chain categories corresponding to regular chain words of Kraft type. We did this in two steps:

1. We reduce to *regular* chain words of numeric type using lemma 4.13;
2. We reduce to regular chain words *of Kraft type* using remark 4.10.

We can also do this the other way around:

1. We reduce to chain words *of Kraft type* using lemma 4.34.1;
2. We reduce to *regular* chain words of Kraft type using lemma 4.34.2 & 4.34.3.

The advantage of the second approach is that the number of terms on the right hand side of (4.12) will be a lot less, making manual computation considerably easier. The downside is that it involves calculations that can be done by hand in small examples, but are not fully automatisable to my knowledge; this makes a general implementation more difficult (see remark 4.35).

Notation 4.26. Let Δ_0 be the primitive Kraft graph of type Z corresponding to the word F, and let Δ_1 be the primitive Kraft graph of type Z corresponding to the word V. For a Kraft type K we define its *étale part* to be $K^{\text{ét}} := K(\Delta_0)\cdot\Delta_0$, its *infinitesimal multiplicative part* to be $K^{\text{im}} := K(\Delta_1)\cdot\Delta_1$, and its *infinitesimal unipotent part* to be

$$K^{\text{iu}} := \sum_{\Delta\in\mathcal{P}\setminus\{\Delta_0,\Delta_1\}} K(\Delta)\cdot\Delta.$$

A Kraft type K is called *étale* (resp. *infinitesimal multiplicative*, *infinitesimal unipotent*) if K equals $K^{\text{ét}}$ (resp. K^{im}, K^{iu}). Note that $K = K^{\text{ét}} + K^{\text{im}} + K^{\text{iu}}$.

Remark 4.27. Let k be a perfect field of characteristic p. Then we get a natural decomposition

$$\mathrm{St}_k(K) = \mathrm{St}_k(K^{\text{ét}}) \oplus \mathrm{St}_k(K^{\text{im}}) \oplus \mathrm{St}_k(K^{\text{ét}}).$$

Via Dieudonné theory this corresponds to the decomposition of the corresponding p-group into its étale, infinitesimal unipotent, and infinitesimal multiplicative part as in [13, IV,§3, n°5].

Let K be a Kraft type. Let v_0 be the unique vertex of Δ_0, let v_1 be the unique vertex of Δ_1, and let v be any vertex of K^{iu}. Let R_F and R_V be as in section 3.2. Then $R_F(v_0) > R_F(v) > R_F(v_1)$ and $R_V(v_0) < R_V(v) < R_V(v_1)$; hence if $w, w' \in \{v_0, v, v_1\}$, then $w \succeq w'$ if and only if $w = w'$. If we apply this to propositions 3.28 and 3.29 we now find the following lemma:

Lemma 4.28. *Let K be a Kraft type, and let k be a perfect field of characteristic p.*

1. *Let w and w' be any of the designations* ét, im, iu, *such that $w \neq w'$. Then*

$$\mathrm{Hom}(\mathrm{St}_k(K^w), \mathrm{St}_k(K^{w'})) = 0.$$

2. *The inclusion map*

$$\mathrm{Aut}(\mathrm{St}_k(K^{\text{ét}})) \times \mathrm{Aut}(\mathrm{St}_k(K^{\mathrm{im}})) \times \mathrm{Aut}(\mathrm{St}_k(K^{\mathrm{iu}})) \hookrightarrow \mathrm{Aut}(\mathrm{St}_k(K))$$

is an isomorphism. □

For a Dieudonné module D over a perfect field k of characteristic p we now obtain a canonical decomposition $D = D^{\text{ét}} \oplus D^{\mathrm{im}} \oplus D^{\mathrm{iu}}$ as follows. Let K be the Kraft type of D and choose an isomorphism $\varphi\colon D_{\bar{k}} \xrightarrow{\sim} \mathrm{St}_{\bar{k}}(K)$. Then $\mathrm{St}_{\bar{k}}(K) = \mathrm{St}_{\bar{k}}(K^{\text{ét}}) \oplus \mathrm{St}_{\bar{k}}(K^{\mathrm{im}}) \oplus \mathrm{St}_{\bar{k}}(K^{\mathrm{iu}})$; set $D^{\text{ét}}_{\bar{k}} := \varphi^{-1}(\mathrm{St}_{\bar{k}}(K^{\text{ét}}))$. By lemma 4.28.2 this does not depend on the choice of φ; in particular, it is Galois-invariant, hence it descends to a canonically defined Dieudonné submodule $D^{\text{ét}} \subset D$. We can define D^{im} and D^{iu} analogously.

If $L = A_1 B_1 \cdots A_r$ is a chain word of Kraft type, we denote by $L^{\text{ét}}$ the chain word where every A_i is replaced by $A_i^{\text{ét}}$. Suppose k is a perfect field of characteristic p and $\underline{D} \in \mathsf{C}(L,k)$. Then $\underline{D}^{\text{ét}} := ((D_i^{\text{ét}})_{i \leq n}, (f_i|_{D_i^{\text{ét}}})_{i<n})$ is an element of $\mathsf{C}(L^{\text{ét}}, k)$. As such we get a functor $\Phi^{\text{ét}}\colon \mathsf{C}(L,k) \to \mathsf{C}(L^{\text{ét}}, k)$; we define words L^{im}, L^{iu} and functors Φ^{im}, Φ^{iu} analogously. The following proposition is now a straightforward corollary of lemma 4.28.

Lemma 4.29. *Let L be a chain word of Kraft type, and let k be a perfect field of characteristic p. Then the functor*

$$\Phi^{\text{ét}} \times \Phi^{\mathrm{im}} \times \Phi^{\mathrm{iu}}\colon \mathsf{C}(L,k) \to \mathsf{C}(L^{\text{ét}},k) \times \mathsf{C}(L^{\mathrm{im}},k) \times \mathsf{C}(L^{\mathrm{iu}},k)$$

is an equivalence of categories. □

Lemma 4.30. *Let L be an injective chain word of Kraft type of length r. Let k be a finite field of characteristic p. Let w be one of the designations* ét *or* im. *If K is a Kraft type, denote its height by $a(K)$. Then*

$$\#\mathsf{C}(L^w, k) = \begin{cases} 1, & \text{if } a(L_1^w) \leq a(L_2^w) \leq \cdots \leq a(L_r^w); \\ 0, & \text{otherwise}. \end{cases}$$

Proof. Define $a_i := a(L_i^w)$. By proposition 3.28 we have

$$\mathtt{Hom}(\mathrm{St}_k(L_i^w), \mathrm{St}_k(L_{i+1}^w)^{\mathrm{red}}) \cong \mathrm{Lin}(\mathbb{F}_p^{a_i}, \mathbb{F}_p^{a_{i+1}});$$

hence

$$\mathtt{Inj}(\mathrm{St}_k(L_i^w), \mathrm{St}_k(L_{i+1}^w)^{\mathrm{red}}) \cong \mathrm{Inj}(\mathbb{F}_p^{a_i}, \mathbb{F}_p^{a_{i+1}}).$$

Applying lemma 4.17 we find $\mathsf{C}(L^w, k) \cong [G \backslash X](k)$, where G and X are the finite étale $\mathbb{F}_p$-schemes whose $\bar{\mathbb{F}}_p$-points with Galois action are given by

$$\begin{aligned} G(\bar{\mathbb{F}}_p) &= \prod_{i \leq r} \mathrm{GL}_{a_i}(\mathbb{F}_p), \\ X(\bar{\mathbb{F}}_p) &= \prod_{i < r} \mathrm{Inj}(\mathbb{F}_p^{a_i}, \mathbb{F}_p^{a_{i+1}}), \end{aligned}$$

where G acts on X in the natural way. If there is an i such that $a_i > a_{i+1}$, then X is empty and $\#\mathsf{C}(L^w, k) = 0$. If no such i exists, then an object of X corresponds to a flag in $\mathbb{F}_p^{a_n}$ of dimensions $(a_1, \ldots, a_r)$. The group $\mathrm{GL}_{d_n}(\mathbb{F}_p)$ acts transitively on this set, so in particular G acts transitively on X. Since both G and X are finite, we may apply proposition 2.21 (with H, U, V trivial), and we find $\#\mathsf{C}(L^w, k) = 1$. □

Corollary 4.31. *Let L be an injective chain word of Kraft type. Let k be a finite field of characteristic p. Then $\#\mathsf{C}(L, k) = \#\mathsf{C}(L^{\mathrm{iu}}, k)$.*

Proof. By lemma 4.29 we find $\#\mathsf{C}(L, k) = \#\mathsf{C}(L^{\text{ét}}, k) \cdot \#\mathsf{C}(L^{\mathrm{im}}, k) \cdot \#\mathsf{C}(L^{\mathrm{iu}}, k)$, and by lemma 4.30 the first two factors are equal to 1. □

In the proof of proposition 4.11 we expressed $\#\mathsf{C}(L^{\underline{h},d}, \mathbb{F}_q)$ (see 4.8) in terms of the point counts of chain categories of straight chain words of Kraft type by first removing all letters of the form $\hookrightarrow$ and $\twoheadrightarrow$, and then replacing all integers and triples by Kraft types. Lemma 4.34 gives us a way to do this the other way around.

Notation 4.32. Let K_1 and K_2 be Kraft types, and let $\bar{k}$ be an algebraically closed field of characteristic p. We write $K_1 \lhd K_2$ (respectively $K_1 \rhd K_2$) if there exists an injective (resp. surjective) morphism of Dieudonné modules $\mathrm{St}_{\bar{k}}(K_1) \hookrightarrow \mathrm{St}_{\bar{k}}(K_2)$; this does not depend on the choice of $\bar{k}$. Let a be either a nonnegative integer or a pair of nonnegative integers (x, y) satisfying $x \geq y$. Then we denote:

$$S(K_1, K_2, a) = \left\{ K \in \mathcal{K} : K_1 \rhd K, K \lhd K_2, K \in \mathcal{K}(a) \right\} \setminus \{K_1, K_2\}.$$

In this notation, we may replace an argument by $\bullet$ to drop the restrictions imposed by that argument; for instance, $S(\bullet, K_2, \bullet)$ is the set of $K \in \mathcal{K}$ satisfying $K \lhd K_2$ that are not equal to K_2.

Lemma 4.33. *Let K_1 and K_2 be Kraft types. Then $K_1 \lhd K_2$ (respectively $K_1 \rhd K_2$) if and only if $K_1(\Delta_0) \leq K_2(\Delta_0)$, $K_1(\Delta_1) \leq K_2(\Delta_1)$, and $K_1^{\mathrm{iu}} \lhd K_2^{\mathrm{iu}}$ (respectively $K_1(\Delta_0) \geq K_2(\Delta_0)$, $K_1(\Delta_1) \geq K_2(\Delta_1)$, and $K_1^{\mathrm{iu}} \rhd K_2^{\mathrm{iu}}$).*

Proof. This is a straightforward consequence of lemma 4.29. □

Lemma 4.34. *Let k be a finite field of characteristic p.*

1. *Let $\underline{h} = (h_1, \ldots, h_r)$ be an increasing sequence of positive integers, and let $0 \leq d \leq h_r$. Let $L^{\underline{h},d}$ be as in example 4.8. Define the set*

$$\mathcal{X} = \left\{ (K_1, \cdots, K_r) \in \mathcal{K}^r : \begin{array}{l} K_r \in \mathcal{K}(h_r, d), \\ K_i \in S(\bullet, K_{i+1}, h_i) \ \forall i < r \end{array} \right\}.$$

   Then

$$\begin{aligned} \#\mathsf{C}(L^{\underline{h},d}, k) &= \sum_{(K_1, \cdots, K_r) \in \mathcal{X}} \#\mathsf{C}(K_1 \hookrightarrow \cdots \hookrightarrow K_r, k) \\ &= \sum_{(K_1, \cdots, K_r) \in \mathcal{X}} \#\mathsf{C}(K_1^{\mathrm{iu}} \hookrightarrow \cdots \hookrightarrow K_r^{\mathrm{iu}}, k). \end{aligned}$$

2. *Let* $L = A_1B_1\cdots A_n$ *and* $L' = A'_1B'_1\cdots A'_{n'}$ *be two chain words of Kraft type. Then* $\#\mathsf{C}(L \hookrightarrow L', k)$ *is equal to:*

   - 0, *if* $A_n \not\trianglelefteq A'_1$;
   - $\#\mathsf{C}(A_1B_1\cdots A_nB'_1A'_2B'_2\cdots A'_{n'}, k)$, *if* $A_n = A'_1$;
   - $\#\mathsf{C}(L \to L', k) - \sum_{K\in S(A_n,A'_1,\bullet)} \#\mathsf{C}(L \twoheadrightarrow K \hookrightarrow L', k)$, *if* $A'_1 \in S(\bullet, A_n, \bullet)$.

3. *Let* $L = A_1B_1\cdots A_n$ *and* $L' = A'_1B'_1\cdots A_{n'}$ *be two chain words of Kraft type. Then* $\#\mathsf{C}(L \twoheadrightarrow L', k)$ *is equal to:*

   - 0, *if* $A_n \not\trianglerighteq A'_1$;
   - $\#\mathsf{C}(A_1B_1\cdots A_nB'_1A'_2B'_2\cdots A'_{n'}, k)$, *if* $A_n = A'_1$;
   - $\#\mathsf{C}(L \to L', k) - \sum_{K\in S(A_n,A'_1,\bullet)} \#\mathsf{C}(L \twoheadrightarrow K \hookrightarrow L', k)$, *if* $A_n \in S(A'_1, \bullet, \bullet)$.

Proof. The first equality of the first point is straightforward, as $\mathcal{X}$ contains precisely those sequences $(K_1, \cdots, K_r) \in \mathcal{K}^r$ where each of the K_i has the right numerical invariants, and where each K_i is chosen such that it admits an injective morphism $\mathrm{St}_k(K_i) \hookrightarrow \mathrm{St}_k(K_{i+1})$; in other words, these are precisely the sequences for which the associated chain category $\mathsf{C}(K_1 \hookrightarrow \cdots \hookrightarrow K_r, k)$ is nonempty. The second equality follows from corollary 4.31. The second and third point are proven analogously, so we will only prove the second point. If $A_n \not\trianglelefteq A'_1$, then there exist no D_n of type A_n, D_{n+1} of type A'_1 such that there exists an injective morphism of Dieudonné modules $f_n\colon D_n \hookrightarrow D_{n+1}$. In particular the category $\#\mathsf{C}(L \hookrightarrow L', k)$ is empty. If $A_n = A'_1$, we get an equivalence of categories

$$\mathsf{C}(L \hookrightarrow, k) \cong \mathsf{C}(A_1B_1\cdots A_nB'_1A'_2B'_2\cdots A'_{n'}, k),$$

by sending an object

$$D_1 \to \cdots \to D_n \overset{f_n}{\to} D_{n+1} \overset{f_{n+1}}{\to} D_{n+2} \to \cdots \to D_{n+n'}$$

to

$$D_1 \to \cdots \to D_n \xrightarrow{f_{n+1}\circ f_n} D_{n+2} \to \cdots \to D_{n+n'}.$$

Its inverse is given by sending an object

$$D'_1 \to \cdots \to D'_n \overset{f'_n}{\to} D'_{n+1} \to \cdots \to D'_{n+n'-1}$$

to

$$D'_1 \to \cdots \to D'_n \overset{\mathrm{id}}{\to} D'_n \overset{f'_n}{\to} D'_{n+1} \to \cdots \to D'_{n+n'-1}.$$

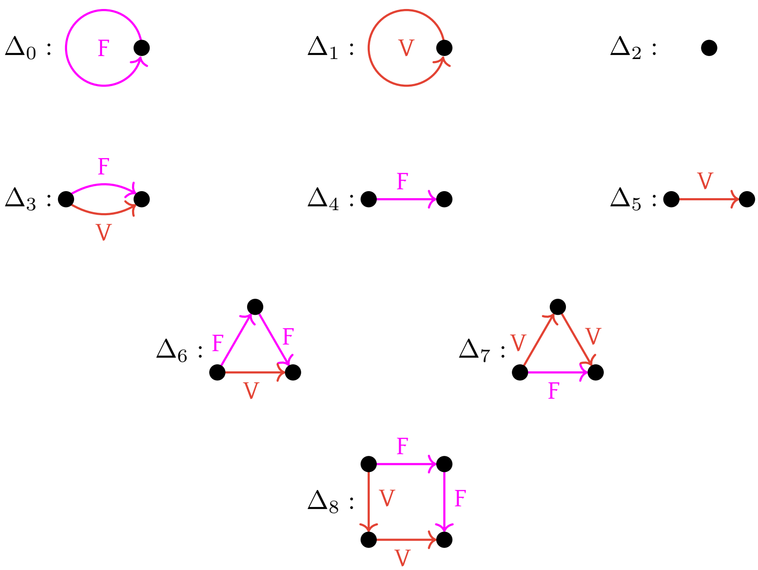
One can check that these two are indeed inverses (note that f_n has to be an isomorphism). The case that $A_n \in S(A'_1, \bullet, \bullet)$ is proven analogously to lemma 4.13. □

Alternate proof of proposition 4.11 for $L = L^{\underline{h},d}$. First, use lemma 4.34.1 to write $\#\mathsf{C}(L,k)$ as an integral combination $\sum_{L'' \in \mathcal{L}''} \#\mathsf{C}(L'',k)$, where each L'' is a chain word of Kraft type. Then use lemma 4.34.2 & 4.34.3 to replace any arrow $\hookrightarrow$ and $\twoheadrightarrow$ in L'' by $\rightarrow$, adding extra terms to our sum in the process. Analogously to the first proof of proposition 4.11, we may show that this process eventually terminates, leaving us with a set of regular chain words of Kraft type. □

Remark 4.35. Using the proof above rather than the first proof of proposition 4.11 when performing algorithm 4.24 has two advantages: First, we can use lemma 4.34.1 to work with Kraft types of lower height, which makes computations easier. Second, in this way, we disregard chain words whose associated chain categories are actually empty (e.g. example 4.8.2) at an early stage, which leads to fewer terms in the sum. This makes manual calculation less cumbersome. The disadvantage of this method is that we have no general method to compute the sets $S(K_1, K_2, a)$ beyond lemma 4.33. Because of this, this method is harder to automatise. In the next section, however, we will see that we can compute these sets in small examples.

4.4 An example

We finish this chapter with a somewhat lengthy example: we will calculate the zeta function of the $\mathbb{F}_p$-stack $\mathsf{BTFlag}^{(2,4),2}$. This will showcase the techniques developed in section 4.3 for calculating point counts and zeta functions manually. In order to do so in an efficient manner, we will need some additional notation. To start, all Kraft types involved in the calculation will be integral combinations of the following primitive Kraft graphs:



Since the involved Kraft types are small in height, we can explicitely work out the homomorphism sets to see whether there exist any injective homomorphisms. For example, if we label the vertices in Δ_6 and Δ_8 clockwise, starting at the bottom left in Δ_6 and at the top left in Δ_8, an actual computation of the group of homomorphisms as in the proof of proposition 3.28 show us that for any perfect field k of characteristic p we have

$$\mathrm{Hom}(\mathrm{St}_k(\Delta_6), \mathrm{St}_k(\Delta_8)) = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ a & 0 & 0 \\ b & a^p & 0 \\ 0 & 0 & 0 \end{pmatrix} : a, b \in k \right\}.$$

This does not contain any injective linear maps, hence $\Delta_6 \not\lhd \Delta_8$. This method allows us manually check the relations $\lhd$ and $\rhd$ for other Kraft types as well.

We have $\mathcal{K}(4,2) = \{2\Delta_0+2\Delta_1, \Delta_0+\Delta_1+\Delta_3, 2\Delta_3, \Delta_1+\Delta_6, \Delta_0+\Delta_7, \Delta_8\}$. Furthermore, by determining the relation $\lhd$ between elements of $\mathcal{K}(2)$ and elements of $\mathcal{K}(4,2)$ we find the following sets:

$$\begin{aligned} S(\bullet, 2\Delta_0 + 2\Delta_1, 2) &= \{2\Delta_0, 2\Delta_1, \Delta_0 + \Delta_1\} \\ S(\bullet, \Delta_0 + \Delta_1 + \Delta_3, 2) &= \{\Delta_0 + \Delta_1, \Delta_0 + \Delta_2, \Delta_1 + \Delta_2, \Delta_3\} \\ S(\bullet, 2\Delta_3, 2) &= \{2\Delta_2, \Delta_3\} \\ S(\bullet, 2\Delta_0 + 2\Delta_1, 2) &= \{\Delta_1 + \Delta_2, \Delta_4\} \\ S(\bullet, 2\Delta_0 + 2\Delta_1, 2) &= \{\Delta_0 + \Delta_2, \Delta_5\} \\ S(\bullet, 2\Delta_0 + 2\Delta_1, 2) &= \{\Delta_3, \Delta_4, \Delta_5\}. \end{aligned}$$

Hence we find, for any power q of p,

$$\begin{aligned} \#\mathsf{BTFlag}^{(2,4),2}(\mathbb{F}_q) &= \#\mathsf{C}(2 \hookrightarrow (4,2), \mathbb{F}_q) \\ &= \#\mathsf{C}(2\Delta_0 \hookrightarrow 2\Delta_0 + 2\Delta_1, \mathbb{F}_q) \\ &\quad +\#\mathsf{C}(2\Delta_1 \hookrightarrow 2\Delta_0 + 2\Delta_1, \mathbb{F}_q) \\ &\quad +\#\mathsf{C}(\Delta_0 + \Delta_1 \hookrightarrow 2\Delta_0 + 2\Delta_1, \mathbb{F}_q) \\ &\quad +\#\mathsf{C}(\Delta_0 + \Delta_1 \hookrightarrow \Delta_0 + \Delta_1 + \Delta_3, \mathbb{F}_q) \\ &\quad +\#\mathsf{C}(\Delta_0 + \Delta_2 \hookrightarrow \Delta_0 + \Delta_1 + \Delta_3, \mathbb{F}_q) \\ &\quad +\#\mathsf{C}(\Delta_1 + \Delta_2 \hookrightarrow \Delta_0 + \Delta_1 + \Delta_3, \mathbb{F}_q) \\ &\quad +\#\mathsf{C}(\Delta_3 \hookrightarrow \Delta_0 + \Delta_1 + \Delta_3, \mathbb{F}_q) \\ &\quad +\#\mathsf{C}(2\Delta_2 \hookrightarrow 2\Delta_3, \mathbb{F}_q) \\ &\quad +\#\mathsf{C}(\Delta_3 \hookrightarrow 2\Delta_3, \mathbb{F}_q) \\ &\quad +\#\mathsf{C}(\Delta_1 + \Delta_2 \hookrightarrow \Delta_1 + \Delta_6, \mathbb{F}_q) \\ &\quad +\#\mathsf{C}(\Delta_4 \hookrightarrow \Delta_1 + \Delta_6, \mathbb{F}_q) \\ &\quad +\#\mathsf{C}(\Delta_0 + \Delta_2 \hookrightarrow \Delta_0 + \Delta_7, \mathbb{F}_q) \end{aligned}$$

$$
\begin{aligned}
&+\#\mathsf{C}(\Delta_5 \hookrightarrow \Delta_0 + \Delta_7, \mathbb{F}_q)\\
&+\#\mathsf{C}(\Delta_3 \hookrightarrow \Delta_8, \mathbb{F}_q)\\
&+\#\mathsf{C}(\Delta_4 \hookrightarrow \Delta_8, \mathbb{F}_q)\\
&+\#\mathsf{C}(\Delta_5 \hookrightarrow \Delta_8, \mathbb{F}_q).
\end{aligned}
$$

We now calculate each of the summands individually using lemma 4.34 to reduce to straight chains, and theorem 4.20 to calculate the associated point count. From the definition of the functions $d, e\colon \mathcal{K} \times \mathcal{K} \to \mathbb{Z}$ in notation 3.27 we easily see that d and e are distributive functions on the semigroup $\mathcal{K}$. As such, to determine the function m from theorem 4.20 on all words involved in the calculation, it suffices to calculate d on all the Δ_i depicted above. The results are in the following table:

$d(\downarrow, \rightarrow)$	Δ_2	Δ_3	Δ_4	Δ_5	Δ_6	Δ_7	Δ_8
Δ_2	0	1	1	1	1	1	1
Δ_3	1	1	1	1	1	1	2
Δ_4	1	1	1	1	2	1	2
Δ_5	1	1	1	1	1	2	2
Δ_6	1	1	1	1	2	1	2
Δ_7	1	1	1	1	1	2	2
Δ_8	1	2	2	2	2	2	3

The last two ingredients we need for our calculation are the other relevant sets of the form $S(K_1, K_2, \bullet)$ for two Kraft types K_1 and K_2, and the integers $\#N(d_1, \cdots, d_n)$. The sets $S(K_1, K_2, \bullet)$ are readily determined analogously to the sets $S(\bullet, K, 2)$ above. Furthermore, the vast majority of the $\#N(d_1, \cdots, d_n)$ that appear in the calculation below have no two consecutive nonzero d_i; in this case we easily see from notation 4.18 that $\#N(d_1, \cdots, d_n) = 1$. The only exception is that we find one instance of $\#N(1, 2)$, which equals 2. Using this we can calculate all the $\#\mathsf{C}(K_1 \hookrightarrow K_2, \mathbb{F}_q)$ that appear in our calculation. The results are as follows:

$$
\begin{aligned}
\#\mathsf{C}(2\Delta_0 \hookrightarrow 2\Delta_0 + 2\Delta_1, \mathbb{F}_q) &= \#\mathsf{C}(0 \hookrightarrow 0, \mathbb{F}_q)\\
&= 1;\\
\#\mathsf{C}(2\Delta_1 \hookrightarrow 2\Delta_0 + 2\Delta_1, \mathbb{F}_q) &= \#\mathsf{C}(0 \hookrightarrow 0, \mathbb{F}_q)\\
&= 1;\\
\#\mathsf{C}(\Delta_0 + \Delta_1 \hookrightarrow 2\Delta_0 + 2\Delta_1, \mathbb{F}_q) &= \#\mathsf{C}(0 \hookrightarrow 0, \mathbb{F}_q)\\
&= 1;\\
\#\mathsf{C}(\Delta_0 + \Delta_1 \hookrightarrow \Delta_0 + \Delta_1 + \Delta_3, \mathbb{F}_q) &= \#\mathsf{C}(0 \hookrightarrow \Delta_3, \mathbb{F}_q)\\
&= \#\mathsf{C}(0 \rightarrow \Delta_3, \mathbb{F}_q)\\
&= q^{-1};\\
\#\mathsf{C}(\Delta_0 + \Delta_2 \hookrightarrow \Delta_0 + \Delta_1 + \Delta_3, \mathbb{F}_q) &= \#\mathsf{C}(\Delta_2 \hookrightarrow \Delta_3, \mathbb{F}_q)
\end{aligned}
$$

$$
\begin{aligned}
&= \#\mathsf{C}(\Delta_2 \to \Delta_3, \mathbb{F}_q) - \#\mathsf{C}(\Delta_2 \twoheadrightarrow 0 \hookrightarrow \Delta_3, \mathbb{F}_q) \\
&= \#\mathsf{C}(\Delta_2 \to \Delta_3, \mathbb{F}_q) - \#\mathsf{C}(\Delta_2 \to 0 \to \Delta_3, \mathbb{F}_q) \\
&= \frac{1}{\#(\mathbb{F}_q^\times)} - \frac{q^{-1}}{\#(\mathbb{F}_q^\times)} \\
&= \frac{1}{q-1} - \frac{q^{-1}}{q-1} \\
&= q^{-1};
\end{aligned}
$$

$$
\begin{aligned}
\#\mathsf{C}(\Delta_1 + \Delta_2 \hookrightarrow \Delta_0 + \Delta_1 + \Delta_3, \mathbb{F}_q) &= \#\mathsf{C}(\Delta_2 \hookrightarrow \Delta_3, \mathbb{F}_q) \\
&= q^{-1};
\end{aligned}
$$

$$
\begin{aligned}
\#\mathsf{C}(\Delta_3 \hookrightarrow \Delta_0 + \Delta_1 + \Delta_3, \mathbb{F}_q) &= \#\mathsf{C}(\Delta_3 \hookrightarrow \Delta_3, \mathbb{F}_q) \\
&= \#\mathsf{C}(\Delta_3, \mathbb{F}_q) \\
&= q^{-1};
\end{aligned}
$$

$$
\begin{aligned}
\#\mathsf{C}(2\Delta_2 \hookrightarrow 2\Delta_3, \mathbb{F}_q) &= \#\mathsf{C}(2\Delta_2 \to 2\Delta_3, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(2\Delta_2 \twoheadrightarrow \Delta_2 \hookrightarrow 2\Delta_3, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(2\Delta_2 \to 0 \to 2\Delta_3, \mathbb{F}_q) \\
&= \#\mathsf{C}(2\Delta_2 \to 2\Delta_3, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(2\Delta_2 \to \Delta_2 \hookrightarrow 2\Delta_3, \mathbb{F}_q) \\
&\quad +\#\mathsf{C}(2\Delta_2 \to 0 \to \Delta_2 \hookrightarrow 2\Delta_3, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(2\Delta_2 \to 0 \to 2\Delta_3, \mathbb{F}_q) \\
&= \#\mathsf{C}(2\Delta_2 \to 2\Delta_3, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(2\Delta_2 \to \Delta_2 \to 2\Delta_3, \mathbb{F}_q) \\
&\quad +\#\mathsf{C}(2\Delta_2 \to \Delta_2 \to 0 \to 2\Delta_3, \mathbb{F}_q) \\
&\quad +\#\mathsf{C}(2\Delta_2 \to 0 \to \Delta_2 \to 2\Delta_3, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(2\Delta_2 \to 0 \to \Delta_2 \to 0 \to 2\Delta_3, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(2\Delta_2 \to 0 \to 2\Delta_3, \mathbb{F}_q) \\
&= \frac{1}{\#\mathrm{GL}_2(\mathbb{F}_q)} \\
&\quad - \frac{1}{\#\mathrm{GL}_2(\mathbb{F}_q) \cdot (q-1)} \\
&\quad + \frac{q^{-2}}{\#\mathrm{GL}_2(\mathbb{F}_q) \cdot (q-1)} \\
&\quad + \frac{q^{-2}}{\#\mathrm{GL}_2(\mathbb{F}_q) \cdot (q-1)} \\
&\quad - \frac{q^{-4}}{\#\mathrm{GL}_2(\mathbb{F}_q) \cdot (q-1)}
\end{aligned}
$$

$$
\begin{aligned}
& -\frac{q^{-4}}{\#\mathrm{GL}_2(\mathbb{F}_q)} \\
&= \frac{q-2+2q^{-2}-q^{-3}}{(q^2-1)(q^2-q)(q-1)} \\
&= q^{-4}; \\
\#\mathsf{C}(\Delta_3 \hookrightarrow 2\Delta_3, \mathbb{F}_q) &= \#\mathsf{C}(\Delta_3 \to 2\Delta_3, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_3 \twoheadrightarrow \Delta_2 \hookrightarrow 2\Delta_3, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_3 \to 0 \to 2\Delta_3, \mathbb{F}_q) \\
&= \#\mathsf{C}(\Delta_3 \to 2\Delta_3, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_3 \to \Delta_2 \hookrightarrow 2\Delta_3, \mathbb{F}_q) \\
&\quad +\#\mathsf{C}(\Delta_3 \to 0 \to \Delta_2 \hookrightarrow 2\Delta_3, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_3 \to 0 \to 2\Delta_3, \mathbb{F}_q) \\
&= \#\mathsf{C}(\Delta_3 \to 2\Delta_3, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_3 \to \Delta_2 \to 2\Delta_3, \mathbb{F}_q) \\
&\quad +\#\mathsf{C}(\Delta_3 \to \Delta_2 \to 0 \to 2\Delta_3, \mathbb{F}_q) \\
&\quad +\#\mathsf{C}(\Delta_3 \to 0 \to \Delta_2 \to 2\Delta_3, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_3 \to 0 \to \Delta_2 \to 0 \to 2\Delta_3, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_3 \to 0 \to 2\Delta_3, \mathbb{F}_q) \\
&= 2q^{-3} - \frac{q^{-2}}{q-1} + \frac{q^{-4}}{q-1} + \frac{q^{-3}}{q-1} - \frac{q^{-5}}{q-1} - q^{-5} \\
&= q^{-3}; \\
\#\mathsf{C}(\Delta_1 + \Delta_2 \hookrightarrow \Delta_1 + \Delta_6, \mathbb{F}_q) &= \#\mathsf{C}(\Delta_2 \hookrightarrow \Delta_6, \mathbb{F}_q) \\
&= \#\mathsf{C}(\Delta_2 \to \Delta_6, \mathbb{F}_q) - \#\mathsf{C}(\Delta_2 \to 0 \to \Delta_6, \mathbb{F}_q) \\
&= \frac{q^{-1}}{q-1} - \frac{q^{-2}}{q-1} \\
&= q^{-2}; \\
\#\mathsf{C}(\Delta_4 \hookrightarrow \Delta_1 + \Delta_6, \mathbb{F}_q) &= \#\mathsf{C}(\Delta_4 \hookrightarrow \Delta_6, \mathbb{F}_q) \\
&= \#\mathsf{C}(\Delta_4 \to \Delta_6, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_4 \twoheadrightarrow \Delta_2 \hookrightarrow \Delta_6, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_4 \to 0 \to \Delta_6, \mathbb{F}_q) \\
&= \#\mathsf{C}(\Delta_4 \to \Delta_6, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_4 \to \Delta_2 \hookrightarrow \Delta_6, \mathbb{F}_q) \\
&\quad +\#\mathsf{C}(\Delta_4 \to 0 \to \Delta_2 \hookrightarrow \Delta_6, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_4 \to 0 \to \Delta_6, \mathbb{F}_q) \\
&= \#\mathsf{C}(\Delta_4 \to \Delta_6, \mathbb{F}_q)
\end{aligned}
$$

$$
\begin{aligned}
& -\#\mathsf{C}(\Delta_4 \to \Delta_2 \to \Delta_6, \mathbb{F}_q) \\
& +\#\mathsf{C}(\Delta_4 \to \Delta_2 \to 0 \to \Delta_6, \mathbb{F}_q) \\
& +\#\mathsf{C}(\Delta_4 \to 0 \to \Delta_2 \to \Delta_6, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_4 \to 0 \to \Delta_2 \to 0 \to \Delta_6, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_4 \to 0 \to \Delta_6, \mathbb{F}_q) \\
= \; & \frac{q^{-1}}{q-1} - \frac{q^{-1}}{(q-1)^2} + \frac{q^{-2}}{(q-1)^2} \\
& + \frac{q^{-2}}{(q-1)^2} - \frac{q^{-3}}{(q-1)^2} - \frac{q^{-3}}{q-1} \\
= \; & q^{-2};
\end{aligned}
$$

$$
\begin{aligned}
\#\mathsf{C}(\Delta_0 + \Delta_2 \hookrightarrow \Delta_0 + \Delta_7, \mathbb{F}_q) &= \#\mathsf{C}(\Delta_2 \hookrightarrow \Delta_7, \mathbb{F}_q) \\
&= \#\mathsf{C}(\Delta_2 \to \Delta_7, \mathbb{F}_q) - \#\mathsf{C}(\Delta_2 \to 0 \to \Delta_7, \mathbb{F}_q) \\
&= \frac{q^{-1}}{q-1} - \frac{q^{-2}}{q-1} \\
&= q^{-2};
\end{aligned}
$$

$$
\begin{aligned}
\#\mathsf{C}(\Delta_5 \hookrightarrow \Delta_0 + \Delta_7, \mathbb{F}_q) &= \#\mathsf{C}(\Delta_5 \hookrightarrow \Delta_7, \mathbb{F}_q) \\
&= \#\mathsf{C}(\Delta_5 \to \Delta_7, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_5 \twoheadrightarrow \Delta_2 \hookrightarrow \Delta_7, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_5 \to 0 \to \Delta_7, \mathbb{F}_q) \\
&= \#\mathsf{C}(\Delta_5 \to \Delta_7, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_5 \to \Delta_2 \hookrightarrow \Delta_7, \mathbb{F}_q) \\
&\quad +\#\mathsf{C}(\Delta_5 \to 0 \to \Delta_2 \hookrightarrow \Delta_7, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_5 \to 0 \to \Delta_7, \mathbb{F}_q) \\
&= \#\mathsf{C}(\Delta_5 \to \Delta_7, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_5 \to \Delta_2 \to \Delta_7, \mathbb{F}_q) \\
&\quad +\#\mathsf{C}(\Delta_5 \to \Delta_2 \to 0 \to \Delta_7, \mathbb{F}_q) \\
&\quad +\#\mathsf{C}(\Delta_5 \to 0 \to \Delta_2 \to \Delta_7, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_5 \to 0 \to \Delta_2 \to 0 \to \Delta_7, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_5 \to 0 \to \Delta_7, \mathbb{F}_q) \\
&= \frac{q^{-1}}{q-1} - \frac{q^{-1}}{(q-1)^2} + \frac{q^{-2}}{(q-1)^2} \\
&\quad + \frac{q^{-2}}{(q-1)^2} - \frac{q^{-3}}{(q-1)^2} - \frac{q^{-3}}{q-1} \\
&= q^{-2};
\end{aligned}
$$

$$
\begin{aligned}
\#\mathsf{C}(\Delta_3 \hookrightarrow \Delta_8, \mathbb{F}_q) &= \#\mathsf{C}(\Delta_3 \to \Delta_8, \mathbb{F}_q) \\
&\quad -\#\mathsf{C}(\Delta_3 \twoheadrightarrow \Delta_2 \hookrightarrow \Delta_8, \mathbb{F}_q)
\end{aligned}
$$

$$
\begin{aligned}
& -\#\mathsf{C}(\Delta_3 \to 0 \to \Delta_8, \mathbb{F}_q) \\
= \ & \#\mathsf{C}(\Delta_3 \to \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_3 \to \Delta_2 \hookrightarrow \Delta_8, \mathbb{F}_q) \\
& +\#\mathsf{C}(\Delta_3 \to 0 \to \Delta_2 \hookrightarrow \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_3 \to 0 \to \Delta_8, \mathbb{F}_q) \\
= \ & \#\mathsf{C}(\Delta_3 \to \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_3 \to \Delta_2 \to \Delta_8, \mathbb{F}_q) \\
& +\#\mathsf{C}(\Delta_3 \to \Delta_2 \to 0 \to \Delta_8, \mathbb{F}_q) \\
& +\#\mathsf{C}(\Delta_3 \to 0 \to \Delta_2 \to \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_3 \to 0 \to \Delta_2 \to 0 \to \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_3 \to 0 \to \Delta_8, \mathbb{F}_q) \\
= \ & q^{-2} - \frac{q^{-2}}{q-1} + \frac{q^{-3}}{q-1} \\
& + \frac{q^{-3}}{q-1} - \frac{q^{-4}}{q-1} - q^{-4} \\
= \ & q^{-2} - q^{-3}; \\
\#\mathsf{C}(\Delta_4 \hookrightarrow \Delta_8, \mathbb{F}_q) = \ & \#\mathsf{C}(\Delta_4 \to \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_4 \twoheadrightarrow \Delta_2 \hookrightarrow \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_4 \to 0 \to \Delta_8, \mathbb{F}_q) \\
= \ & \#\mathsf{C}(\Delta_4 \to \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_4 \to \Delta_2 \hookrightarrow \Delta_8, \mathbb{F}_q) \\
& +\#\mathsf{C}(\Delta_4 \to 0 \to \Delta_2 \hookrightarrow \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_4 \to 0 \to \Delta_8, \mathbb{F}_q) \\
= \ & \#\mathsf{C}(\Delta_4 \to \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_4 \to \Delta_2 \to \Delta_8, \mathbb{F}_q) \\
& +\#\mathsf{C}(\Delta_4 \to \Delta_2 \to 0 \to \Delta_8, \mathbb{F}_q) \\
& +\#\mathsf{C}(\Delta_4 \to 0 \to \Delta_2 \to \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_4 \to 0 \to \Delta_2 \to 0 \to \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_4 \to 0 \to \Delta_8, \mathbb{F}_q) \\
= \ & \frac{q^{-2}}{q-1} - \frac{q^{-2}}{(q-1)^2} + \frac{q^{-3}}{(q-1)^2} \\
& + \frac{q^{-3}}{(q-1)^2} - \frac{q^{-4}}{(q-1)^2} - \frac{q^{-4}}{q-1} \\
= \ & q^{-3}; \\
\#\mathsf{C}(\Delta_5 \hookrightarrow \Delta_8, \mathbb{F}_q) = \ & \#\mathsf{C}(\Delta_5 \to \Delta_8, \mathbb{F}_q)
\end{aligned}
$$

$$
\begin{aligned}
& -\#\mathsf{C}(\Delta_5 \twoheadrightarrow \Delta_2 \hookrightarrow \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_5 \to 0 \to \Delta_8, \mathbb{F}_q) \\
= \quad & \#\mathsf{C}(\Delta_5 \to \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_5 \to \Delta_2 \hookrightarrow \Delta_8, \mathbb{F}_q) \\
& +\#\mathsf{C}(\Delta_5 \to 0 \to \Delta_2 \hookrightarrow \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_5 \to 0 \to \Delta_8, \mathbb{F}_q) \\
= \quad & \#\mathsf{C}(\Delta_5 \to \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_5 \to \Delta_2 \to \Delta_8, \mathbb{F}_q) \\
& +\#\mathsf{C}(\Delta_5 \to \Delta_2 \to 0 \to \Delta_8, \mathbb{F}_q) \\
& +\#\mathsf{C}(\Delta_5 \to 0 \to \Delta_2 \to \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_5 \to 0 \to \Delta_2 \to 0 \to \Delta_8, \mathbb{F}_q) \\
& -\#\mathsf{C}(\Delta_5 \to 0 \to \Delta_8, \mathbb{F}_q) \\
= \quad & \frac{q^{-2}}{q-1} - \frac{q^{-2}}{(q-1)^2} + \frac{q^{-3}}{(q-1)^2} \\
& + \frac{q^{-3}}{(q-1)^2} - \frac{q^{-4}}{(q-1)^2} - \frac{q^{-4}}{q-1} \\
= \quad & q^{-3.}
\end{aligned}
$$

Adding all these terms, we find

$$\#\mathsf{C}(2 \hookrightarrow (4,2), \mathbb{F}_q) = 3 + 4q^{-1} + 5q^{-2} + 2q^{-3} + q^{-4};$$

as predicted by corollary 4.23 this is indeed an integral combination of summands q^n. From this point count formula we deduce

$$Z(\mathsf{BTFlag}^{(2,4),2}, t) = (1-t)^{-3}(1-p^{-1}t)^{-4}(1-p^{-2}t)^{-5}(1-p^{-3}t)^{-2}(1-p^{-4}t)^{-1}.$$

While this computation is still quite cumbersome, we can see the strength of lemma 4.34 in action: if we would have used lemma 4.13 instead in algorithm 4.24, we would have needed to calculate $\#\mathsf{C}(L, \mathbb{F}_q)$ for 702 regular chain words of Kraft type, instead of the 49 we needed now.

Chapter 5

Stacks of G-zips

Following the classification of the BT_1 over algebraically closed fields in [32], and the application of this classification to obtain the Ekedahl–Oort stratification on moduli spaces of abelian varieties in [52], various efforts have been made to generalise these results to BT_1 with additional structure. In [43] the BT_1 with a given action of an endomorphism ring and/or a polarisation were classified over an algebraically closed field; this can be used to define an Ekedahl–Oort stratification on Shimura varieties of PEL type as in [70]. The dimensions of these strata were calculated in [44], and the key ingredient in this result is the description of the automorphism groups of the corresponding BT_1. Both the classification of BT_1 with extra structure, and their automorphisms groups, can be expressed in terms of the Weyl group of an associated reductive algebraic group over $\mathbb{F}_p$.

In [47] the Dieudonné modules associated to BT_1 were generalised to semilinear algebra objects called *F-zips*; these also appear in the de Rham cohomology of smooth proper schemes. The classification of F-zips, as well as the classification of F-zips with additional structure, could again be stated in terms of the Weyl group of a reductive group G. In [55] and [56] so-called *G-zips* were introduced, which are objects in algebraic group theory in which the reductive group G is the primordial object. For specific choices of G these generalise F-zips (and BT_1) with additional structure. Its relationship to Shimura varieties can be described as follows: Let S be a be a Shimura variety of Hodge type governed by an algebraic group G over $\mathbb{Q}$, and assume G is hyperspecial at p. Let $\mathscr{S}_0$ be the reduction of the canonical model of S at p (see [29]), and let $\mathscr{G}$ be a reductive model of G over $\mathbb{Z}_p$. Then by [71] there exists a smooth surjective morphism from $\mathscr{S}_0$ to a moduli stack of $\mathscr{G}_{\mathbb{F}_p}$-zips.

The goal of this chapter is to calculate the point counts and zeta functions of moduli stacks of G-zips; the main result is theorem 5.25. Because of the relation between G-zips on one hand and BT_1 and F-zips with additional structure on the other hand, this result can also be used to determine the point counts and zeta functions of moduli stacks of the latter; see [56,

§8 & §9] for more details on how to express stacks of F-zips in terms of G-zips. The main ingredients of this proof are the classification of G-zips over an algebraically closed field and the description of their automorphism groups from [56], and the methods for calculating point counts of quotient stacks developed in chapter 2. In [56] the automorphism groups are only described for connected G, so we need to generalise these results to the non-connected case.

5.1 Weyl groups and Levi decompositions

In this section we briefly review some relevant facts about Weyl groups and Levi decompositions, in particular those of nonconnected reductive groups.

5.1.1 The Weyl group of a connected reductive group

Let G be a connected reductive algebraic group over a field k. For any pair (T, B) of a Borel subgroup $B \subset G_{\bar{k}}$ and a maximal torus $T \subset B$, let $\Phi_{T,B}$ be the based root system of G with respect to (T, B), and let $W_{T,B}$ be the Weyl group of this based root system, i.e. the Coxeter group generated by the set $S_{T,B}$ of simple reflections. As an abstract group $W_{T,B}$ is isomorphic to $\mathrm{Norm}_{G(\bar{k})}(T(\bar{k}))/T(\bar{k})$. If (T', B') is another choice of a Borel subgroup and a maximal torus, then there exists a $g \in G(\bar{k})$ such that $(T', B') = (gTg^{-1}, gBg^{-1})$. Furthermore, such a g is unique up to right multiplication by $T(\bar{k})$, which gives us a unique isomorphism $\Phi_{T,B} \xrightarrow{\sim} \Phi_{T',B'}$. As such, we can simply talk about *the* based root system Φ of G, with corresponding Coxeter system (W, S). By these canonical identifications Φ, W and S come with an action of $\mathrm{Gal}(\bar{k}/k)$.

The set of parabolic subgroups of $G_{\bar{k}}$ containing B is classified by the power set of S, by associating to $I \subset S$ the parabolic subgroup $P = L \cdot B$, where L is the reductive group with maximal torus T whose root system is Φ_I, the root subsystem of Φ generated by the roots whose associated reflections lie in I. We call I the *type* of P. Let $U := \mathrm{R_u}P$ be the unipotent radical of P; then $P = L \ltimes U$ is the Levi decomposition of P with respect to T (see subsection 5.1.3). For every subset $I \subset S$, let W_I be the subgroup of W generated by I; it is the Weyl group of the root system Φ_I, with I as its set of simple reflections.

For $w \in W$, define the *length* $\ell(w)$ of w to be the minimal integer such that there exist $s_1, s_2, ..., s_{\ell(w)} \in S$ such that $w = s_1 s_2 \cdots s_{\ell(w)}$. Since $\mathrm{Gal}(\bar{k}/k)$ acts on W by permuting S, the length is Galois invariant. Let $I, J \subset S$; then every (left, double, right) coset $W_I w, W_I w W_J$ or $w W_J$ has a unique element of minimal length, and we denote the subsets of W of elements of minimal length in their (left, double, right) cosets by ${}^I W, {}^I W^J$, and W^J.

Proposition 5.1. (See [14, Prop. 4.18]) *Let $I, J \subset S$. Let $x \in {}^I W^J$, and set $I_x = J \cap x^{-1} I x \subset$*

W. Then for every $w \in W_I x W_J$ there exist unique $w_I \in W_I, w_J \in {}^{I_x}W_J$ such that $w = w_I x w_J$. Furthermore $\ell(w) = \ell(w_I) + \ell(x) + \ell(w_J)$. □

Lemma 5.2. (See [55, Prop. 2.8]) *Let $I, J \subset S$. Every element $w \in {}^I W$ can uniquely be written as $x w_J$ for some $x \in {}^I W^J$ and $w_J \in {}^{I_x}W_J$.* □

Lemma 5.3. (See [55, Lem. 2.13]) *Let $I, J \subset S$. Let $w \in {}^I W$ and write $w = x w_J$ with $x \in {}^I W^J, w_J \in W_J$. Then*

$$\ell(w) = \#\Big\{\alpha \in \Phi^+ \backslash \Phi_J : w\alpha \in \Phi^- \backslash \Phi_I\Big\}. \qquad \square$$

5.1.2 The Weyl group of a nonconnected reductive group

Now let us drop the assumption that our group is connected. Let $\hat{G}$ be a reductive algebraic group and write G for its connected component. Let B be a Borel subgroup of $G_{\bar{k}}$, and let T be a maximal torus of B. Define the following groups:

$$\begin{aligned} W &= \mathrm{Norm}_{G(\bar{k})}(T)/T(\bar{k}); \\ \hat{W} &= \mathrm{Norm}_{\hat{G}(\bar{k})}(T)/T(\bar{k}); \\ \Omega &= (\mathrm{Norm}_{\hat{G}(\bar{k})}(T) \cap \mathrm{Norm}_{\hat{G}(\bar{k})}(B))/T(\bar{k}). \end{aligned}$$

Lemma 5.4.

1. *One has $\hat{W} = W \rtimes \Omega$.*
2. *The composite map $\Omega \hookrightarrow G(\bar{k})/T(\bar{k}) \twoheadrightarrow \pi_0(G(\bar{k}))$ is an isomorphism of groups.*

Proof.

1. First note that W is a normal subgroup of $\hat{W}$, since it consists of the elements of $\hat{W}$ that have a representative in $G(\bar{k})$, and G is a normal subgroup of $\hat{G}$. Furthermore, $\hat{W}$ acts on the set X of Borel subgroups of $G_{\bar{k}}$ containing T. The stabiliser of B under this action is Ω, whereas W acts simply transitively on X; hence $\Omega \cap W = 1$ and $W\Omega = \hat{W}$, and together this proves $\hat{W} = W \rtimes \Omega$.

2. By the previous point, we see that

$$\Omega \cong \hat{W}/W \cong \mathrm{Norm}_{\hat{G}(\bar{k})}(T)/\mathrm{Norm}_{G(\bar{k})}(T),$$

so it is enough to show that every connected component of $\hat{G}(\bar{k})$ has an element that normalises T. Let $x \in \hat{G}(\bar{k})$; then xTx^{-1} is another maximal torus of $G_{\bar{k}}$, so there exists a $g \in G(\bar{k})$ such that $xTx^{-1} = gTg^{-1}$. From this we find that $T = (g^{-1}x)T(g^{-1}x)^{-1}$, and $g^{-1}x$ is in the same connected component as x. □

We call $\hat{W}$ the Weyl group of $\hat{G}$ with respect to (T, B). Again, choosing a different (T, B) leads to a canonical isomorphism, so we may as well talk about *the* Weyl group of $\hat{G}$. The two statements of lemma 5.4 are then to be understood as isomorphisms of groups with an action of $\mathrm{Gal}(\bar{k}/k)$. Note that we can regard W as the Weyl group of the connected reductive group G; as such we can apply the results of the previous subsection to it. Let $S \subset W$ be the generating set of simple reflections.

Now let us define an extension of the length function to a suitable subset of $\hat{W}$. First, let I and J be subsets of the set S of simple reflections in W, and consider the set ${}^I\hat{W} := {}^I W\Omega$. Define a subset ${}^I\hat{W}^J$ of ${}^I\hat{W}$ as follows: every element $w \in {}^I\hat{W}$ can uniquely be written as $w = w'\omega$, with $w' \in {}^I W$ and $\omega \in \Omega$. We rewrite this as $w = \omega w''$, with $w'' = \omega^{-1}w'\omega \in {}^{\omega^{-1}I\omega}W$; then per definition $w \in {}^I\hat{W}^J$ if and only if $w'' \in {}^{\omega^{-1}I\omega}W^J$. Note that ${}^I W^J$ is contained in ${}^I\hat{W}^J$.

Now let $w \in {}^I\hat{W}$; write $w = \omega w''$. Since w'' is an element of ${}^{\omega^{-1}I\omega}W$, we can uniquely write $w'' = yw_J$ by lemma 5.2, with $y \in {}^{\omega^{-1}I\omega}W^J$ and $w_J \in {}^{I_{\omega y}}W_J$. Then define the *extended length function* $\ell_{I,J} \colon {}^I\hat{W} \to \mathbb{Z}_{\geq 0}$ by

$$\ell_{I,J}(w) := \#\Big\{\alpha \in \Phi^+ \backslash \Phi_J : \omega y\alpha \in \Phi^- \backslash \Phi_I\Big\} + \ell(w_J). \tag{5.5}$$

Remark 5.6.

1. By proposition 5.1 and lemma 5.3 the map $\ell_{I,J} \colon {}^I\hat{W} \to \mathbb{Z}_{\geq 0}$ extends the length function $\ell \colon {}^I W \to \mathbb{Z}_{\geq 0}$.
2. Analogously to proposition 5.1 we see that every $w \in {}^I\hat{W}$ can be uniquely written as xw_J with $x \in {}^I\hat{W}^J$, $w_J \in {}^{I_x}W_J$, and $\ell_{I,J}(w) = \ell_{I,J}(x) + \ell(w_J)$.
3. A straightforward calculation shows that for $\pi \in \mathrm{Gal}(\bar{k}/k)$ we get $\ell_{{}^\pi I, {}^\pi J}({}^\pi w) = \ell_{I,J}(w)$. In particular, if I and J are fixed under the action of $\mathrm{Gal}(\bar{k}/k)$, the map $\ell_{I,J} \colon {}^I\hat{W} \to \mathbb{Z}_{\geq 0}$ is Galois-invariant.
4. In general $\ell_{I,J}$ depends on J. It also depends on I, in the sense that if $I, I' \subset S$, then $\ell_{I,J}(w)$ and $\ell_{I',J}(w)$ for $w \in {}^I\hat{W} \cap {}^{I'}\hat{W} = {}^{I \cap I'}\hat{W}$ need not coincide. As an example, consider over any field the group $G = \mathrm{SL}_2$. Let $\Omega = \langle\omega\rangle$ be cyclic of order 2, and let $\hat{G} = G \rtimes \Omega$ be the extension given by $\omega g \omega^{-1} = g^{\mathrm{T},-1}$. Then ω acts as -1 on the root system, and S has only one element. Then a straightforward calculation shows $\ell_{\varnothing,\varnothing}(\omega) = 1$, whereas $\ell_{\varnothing,S}(\omega) = \ell_{S,S}(\omega) = \ell_{S,\varnothing}(\omega) = 0$.

5.1.3 Levi decomposition of nonconnected groups

Let P be a connected smooth linear algebraic group over a field k. A *Levi subgroup* of P is the image of a section of the map $P \twoheadrightarrow P/\mathrm{R_u}P$, i.e. a subgroup $L \subset P$ such that $P = L \ltimes \mathrm{R_u}P$. In characteristic p, such a Levi subgroup need not always exist, nor need it be unique. However, if P is a parabolic subgroup of a connected reductive algebraic group, then for every maximal torus $T \subset P$ there exists a unique Levi subgroup of P containing T (see [15, Proposition 1.17]). The following proposition generalises this result to the non-connected case.

Proposition 5.7. *Let $\hat{G}$ be a reductive group over a field k, and let $\hat{P}$ be a subgroup of $\hat{G}$ whose identity component P is a parabolic subgroup of G. Let T be a maximal torus of P. Then there exists a unique Levi subgroup of $\hat{P}$ containing T, i.e. a subgroup $\hat{L} \subset \hat{P}$ such that $\hat{P} = \hat{L} \ltimes \mathrm{R_u} P$.*

Proof. Let L be the Levi subgroup of P containing T. Then any $\hat{L}$ satisfying the conditions of the proposition necessarily has L has its identity component, hence $\hat{L} \subset \mathtt{Norm}_{\hat{P}}(L)$. On the other hand we know that $\mathtt{Norm}_P(L) = L$, so the only possibility is $\hat{L} = \mathtt{Norm}_{\hat{P}}(L)$, and we have to check that $\pi_0(\mathtt{Norm}_{\hat{P}}(L)) = \pi_0(\hat{P})$, i.e. that every connected component in $\hat{P}_{\bar{k}}$ has an element normalising L. Let $x \in \hat{P}(\bar{k})$. Then xTx^{-1} is another maximal torus of $P_{\bar{k}}$, so there exists a $y \in P(\bar{k})$ such that $xTx^{-1} = yTy^{-1}$. Then $y^{-1}x$ is in the same connected component as x, and $(y^{-1}x)T(y^{-1}x)^{-1} = T$. Since L is the unique Levi subgroup of P containing T, and $(y^{-1}x)L(y^{-1}x)^{-1}$ is another Levi subgroup of P, we see that $y^{-1}x$ normalises L, which completes the proof. ☐

5.2 G-zips

In this section we give the definition of G-zips from [56] along with their classification and their connection to BT_1. We will need the discussion on Weyl groups from subsection 5.1.2. As before, we denote the component group of a nonconnected algebraic group A by $\pi_0(A)$.

Let q_0 be a power of p. Let $\hat{G}$ be a reductive group over $\mathbb{F}_{q_0}$, and write G for its identity component. Let q be a power of q_0, and let $\chi\colon \mathbb{G}_{\mathrm{m},\mathbb{F}_q} \to G_{\mathbb{F}_q}$ be a cocharacter of $G_{\mathbb{F}_q}$. Let $L = \mathtt{Cent}_{G_{\mathbb{F}_q}}(\chi)$, and let $U_+ \subset G_{\mathbb{F}_q}$ be the unipotent subgroup defined by the property that $\mathrm{Lie}(U_+) \subset \mathrm{Lie}(G_{\mathbb{F}_q})$ is the direct sum of the weight spaces of positive weight; define U_- similarly. Note that L is connected (see [15, Proposition 0.34]). This defines parabolic subgroups $P_\pm = L \ltimes U_\pm$ of $G_{\mathbb{F}_q}$. Now take an $\mathbb{F}_q$-subgroup scheme Θ of $\pi_0(\mathtt{Cent}_{\hat{G}_{\mathbb{F}_q}}(\chi))$, and let $\hat{L}$ be the inverse image of Θ under the canonical map $\mathtt{Cent}_{\hat{G}_{\mathbb{F}_q}}(\chi) \to \pi_0(\mathtt{Cent}_{\hat{G}_{\mathbb{F}_q}}(\chi))$; then $\hat{L}$ has L as its identity component and $\pi_0(\hat{L}) = \Theta$. We may regard Θ as a subgroup of $\pi_0(\hat{G})$ via the inclusion

$$\pi_0(\mathtt{Cent}_{\hat{G}_{\mathbb{F}_q}}(\chi)) = \mathtt{Cent}_{\hat{G}_{\mathbb{F}_q}}(\chi)/L \hookrightarrow \pi_0(\hat{G}_{\mathbb{F}_q}).$$

We may then define the algebraic subgroups $\hat{P}_\pm := \hat{L} \ltimes U_\pm$ of $\hat{G}_{\mathbb{F}_q}$, whose identity components $P_\pm$ are equal to $L \ltimes U_\pm$. Let $\pi \in \mathrm{Gal}(\bar{\mathbb{F}}_{q_0}/\mathbb{F}_{q_0})$ be the q_0-th power Frobenius. Then $\hat{G}$ and $\hat{G}_\pi$ are canonically isomorphic; as such we can regard $\hat{P}_{\pm,\pi}$, $\hat{L}_{\pm,\pi}$, etc. as subgroups of $\hat{G}$. They correspond to the parabolic and Levi subgroups associated to the cocharacter $\varphi \circ \chi$ of $\hat{G}_k$ and the subgroup $\varphi(\Theta)$ of $\pi_0(\hat{G})$, where $\varphi\colon \hat{G} \to \hat{G}$ is the relative q_0-th Frobenius isogeny.

Definition 5.8. Let A be an algebraic group over a field k, and let B be a subgroup of A. Let T be an A-torsor over some k-scheme S. A *B-subtorsor of T* is an S-subscheme Y of T, together with an action of B_S, such that Y is a B-torsor over S and such that the inclusion map $Y \hookrightarrow T$ is equivariant under the action of B_S.

Definition 5.9. Let S be a scheme over $\mathbb{F}_q$. A *$\hat{G}$-zip of type (χ, Θ) over S* is a tuple $\mathcal{Y} = (Y, Y_+, Y_-, \upsilon)$ consisting of:

- A right-$\hat{G}_{\mathbb{F}_q}$-torsor Y over S;
- A right-$\hat{P}_+$-subtorsor Y_+ of Y;
- A right-$\hat{P}_{-,\pi}$-subtorsor Y_- of Y;
- An isomorphism $\upsilon\colon Y_{+,\pi}/U_{+,\pi} \xrightarrow{\sim} Y_-/U_{-,\pi}$ of right-$\hat{L}_\pi$-torsors.

Together with the obvious notions of pullbacks and morphisms we get a fibred category $\hat{G}\text{-}\mathsf{Zip}^{\chi,\Theta}_{\mathbb{F}_q}$ over $\mathbb{F}_q$. If $\hat{G}$ is connected there is no choice for Θ, and we will omit it from the notation.

Proposition 5.10. (See [56, Prop. 3.2 & 3.11]) *The fibred category $\hat{G}\text{-}\mathsf{Zip}^{\chi,\Theta}_{\mathbb{F}_q}$ is a smooth algebraic stack of finite type over $\mathbb{F}_q$.* □

Example 5.11. Let $0 \leq d \leq h$ be integers, let k be a perfect field, and let $(D, F, V) \in \mathsf{D}_1^{h,d}(k)$. On D we have a descending filtration $D \supset \ker(F) \supset 0$ and an ascending filtration $0 \subset \ker(V) \subset D$. Furthermore, $\ker(F)$ has dimension $h - d$ and $\ker(V)$ has dimension d. Consider the algebraic group $G := \mathtt{GL}_h$ over $\mathbb{F}_{q_0} := \mathbb{F}_p$. and a cocharacter $\chi\colon \mathbb{G}_{\mathrm{m},\mathbb{F}_p} \to G$ that sends a $z \in \mathbb{G}_{\mathrm{m},\mathbb{F}_p}$ to the diagonal matrix

$$\operatorname{diag}(\underbrace{z, \ldots, z}_{d \text{ times}}, \underbrace{z^2, \ldots, z^2}_{h-d \text{ times}}).$$

Since G is connected we have $\hat{P}_\pm = P_\pm$, and since χ is defined over $\mathbb{F}_p$ we have $P_{-,\pi} = P_-$ and $U_{-,\pi} = U_-$. Consider the vector space $W = \mathbb{F}_p^h$ with the natural action of G, and let A and B be the cocharacter spaces in W on which $\chi(z)$ acts as z and z^2, respectively. Furthermore, define an ascending filtration $W_\bullet$ and a descending filtration $W^\bullet$ on W given by

$$\begin{aligned} W_0 &= 0, & W^0 &= W, \\ W_1 &= A, & W^1 &= B, \\ W_2 &= W, & W^2 &= 0. \end{aligned}$$

Then P_+ is the stabiliser of $W^\bullet$, and P_- is the stabiliser of the ascending filtration $W_\bullet$. Now define the following torsors:

- A right G-torsor $Y = \mathtt{Isom}(W_k, D)$ over k;
- A right P_+-subtorsor $Y_+ = \mathtt{Isom}(W_k^\bullet, D \supset \ker(F) \supset 0)$ of Y;

- A right P_--subtorsor $Y_- = \mathtt{Isom}(W_{\bullet,k}, 0 \subset \ker(V) \subset D)$ of Y.

Then $L \cong \mathtt{GL}(W^0/W^1) \times \mathtt{GL}(W^1) \cong \mathtt{GL}(W_1) \times \mathtt{GL}(W_2/W_1)$ via the identifications $W/A \cong B$ and $W/B \cong A$. As L-torsors we find:

$$Y_+/U_+ \cong \mathtt{Isom}(W_k^0/W_k^1, D/\ker(F)) \times \mathtt{Isom}(W_k^1, \ker(F)),$$
$$Y_-/U_- \cong \mathtt{Isom}(W_{1,k}, \ker(V)) \times \mathtt{Isom}(W_{2,k}/W_{1,k}, D/\ker(V)).$$

The k-vector space isomorphisms

$$V^{-1} \colon {}^{\pi}(D/\ker(F)) \xrightarrow{\sim} \ker(V)$$
$$F \colon {}^{\pi}(\ker(F)) \xrightarrow{\sim} D/\ker(V)$$

yield an isomorphism $\upsilon \colon Y_{+,\pi}/U_{+,\pi} \xrightarrow{\sim} Y_-/U_{-,\pi}$ of right-L_π-torsors. Then the quadruple (Y, Y_+, Y_-, υ) is a $\mathtt{GL}_h$-zip of type χ over k; since $G = \hat{G}$ there is no choice for Θ. This gives us a natural equivalence of categories (see [56, §8.1 & §9.3]):

$$\mathsf{D}_1^{h,d}(k) \xrightarrow{\sim} \mathtt{GL}_h\text{-}\mathsf{Zip}^{\chi}(k).$$

If we replace $\mathtt{GL}_h$ with a suitable reductive group G (e.g. $\mathrm{Res}_{\mathbb{F}_{p^2}/\mathbb{F}_p}\mathtt{GL}_{h/2}$) we get a natural equivalence between a category of G-zips, and a stack of exact level 1 Dieudonné modules with additional structure (e.g. with a given action of $\mathbb{F}_{p^2}$); see [56, §8] for several examples. As such the concept of G-zips generalises the concept of level 1 Dieudonné modules with additional structure. This construction extends to isomorphisms of $\mathbb{F}_p$-stacks (see remark 3.6), and it can be applied to stacks of F-zips as defined in [47].

Now let $q_0, q, \hat{G}, \chi, \Theta, \hat{L}, U_\pm$ and $\hat{P}_\pm$ be as above. As in subsection 5.1.2 let $\hat{W} = W \rtimes \Omega$ be the Weyl group of $\hat{G}$. Let $I \subset S$ be the type of P_+ and let J be the type of $P_{-,\pi}$. If $w_0 \in W$ is the unique longest word, then $J = \pi(w_0 I w_0^{-1}) = w_0 \pi(I) w_0^{-1}$. Let $w_1 \in {}^J W^{\pi(I)}$ be the element of minimal length in $W_J w_0 W_{\pi(I)}$, and let $w_2 = \pi^{-1}(w_1)$; then we may write this relation as $J = \pi(w_2 I w_2^{-1}) = w_1 \pi(I) w_1^{-1}$.

The group Θ can be considered as a subgroup of $\Omega \cong \pi_0(\hat{G})$. Let $\hat{\psi}$ be the automorphism of $\hat{W}$ given by $\hat{\psi} = \mathrm{inn}(w_1) \circ \pi = \pi \circ \mathrm{inn}(w_2)$, and let Θ act on $\hat{W}$ by

$$\theta \cdot w := \theta w \hat{\psi}(\theta)^{-1}.$$

Lemma 5.12. *The subset ${}^I\hat{W} \subset \hat{W}$ is invariant under the Θ-action.*

Proof. Since $\hat{L}$ normalises the parabolic subgroup P_+ of $G_{\mathbb{F}_q}$, the subset $I \subset S$ is stable under the action of Θ by conjugation; hence for each $\theta \in \Theta$ one has $\theta({}^I W)\theta^{-1} = {}^I W$, so

$$\theta({}^I\hat{W})\hat{\psi}(\theta)^{-1} = (\theta({}^I W)\theta^{-1}) \cdot (\theta\Omega\hat{\psi}(\theta)^{-1}) = {}^I W \Omega = {}^I \hat{W}. \qquad \square$$

Let us write $\Xi^{\chi,\Theta} := \Theta \backslash {}^I\hat{W}$.

Proposition 5.13. (See [56, Rem. 3.21]) *There is a natural bijection between the sets* $\Xi^{\chi,\Theta}$ *and* $[\hat{G}\text{-}\mathsf{Zip}^{\chi,\Theta}_{\mathbb{F}_q}(\bar{\mathbb{F}}_q)]$. □

This bijection can be described as follows. Choose a Borel subgroup B of $G_{\bar{\mathbb{F}}_q}$ contained in $P_{-,\pi}$, and let T be a maximal torus of B. Let $\gamma \in G(\bar{\mathbb{F}}_q)$ be such that $(\gamma B\gamma^{-1})_\pi = B$ and $(\gamma T\gamma^{-1})_\pi = T$. For every $w \in \hat{W} = \mathrm{Norm}_{\hat{G}(\bar{\mathbb{F}}_q)}(T)/T(\bar{\mathbb{F}}_q)$, choose a lift $\dot{w}$ to $\mathrm{Norm}_{\hat{G}(\bar{\mathbb{F}}_q)}(T)$, and set $g = \gamma\dot{w}_2$. Then $\xi \in \Xi^{\chi,\Theta}$ corresponds to the $\hat{G}$-zip $\mathcal{Y}_w = (\hat{G}, \hat{P}_+, g\dot{w}\hat{P}_{-,\pi}, g\dot{w}\cdot)$ for any representative $w \in {}^I\hat{W}$ of ξ; its isomorphism class does not depend on the choice of the representatives w and $\dot{w}$. Note that this description differs from the one given in [56, Remark 3.21], as that description seems to be wrong. Since there it is assumed that $B \subset P_{-,K}$ rather than that $B \subset P_{-,\pi,K}$, the choice of (B, T, g) presented there will not be a frame for the connected zip datum $(G_K, P_{+,K}, P_{-,\pi,K}, \varphi\colon L_K \to L_{\pi,K})$. Also, the choice for g given there needs to be modified to account for the fact that $P_{+,K}$ and $P_{-,\pi,K}$ might not have a common maximal torus.

The rest of this subsection is dedicated to the extended length functions $\ell_{I,J}$ defined in subsection 5.1.2. We need lemma 5.14 in order to show a result on the dimension of the automorphism group of a $\hat{G}$-zip that extends [56, Prop. 3.34(a)] to the nonconnected case (see proposition 5.33.2).

Lemma 5.14. *The length function* $\ell_{I,J}\colon {}^I\hat{W} \to \mathbb{Z}_{\geq 0}$ *is invariant under the semilinear conjugation action of* Θ.

Proof. Let $w \in {}^I\hat{W}$, let $\theta \in \Theta$, and let $\tilde{w} = \theta w\hat{\psi}(\theta)^{-1}$. Let $w = \omega y w_J$ be the decomposition as in subsection 5.1.2. A straightforward computation shows $\tilde{w} = \tilde{\omega}\tilde{w}'' = \tilde{\omega}\tilde{y}\tilde{w}_J$ with

$$\begin{aligned}
\tilde{\omega} &= \theta\omega\hat{\psi}(\theta)^{-1} \in \Omega;\\
\tilde{w}'' &= \hat{\psi}(\theta)w''\hat{\psi}(\theta)^{-1} \in {}^{\tilde{\omega}^{-1}I\tilde{\omega}}W;\\
\tilde{y} &= \hat{\psi}(\theta)y\hat{\psi}(\theta)^{-1} \in {}^{\tilde{\omega}^{-1}I\tilde{\omega}}W^J;\\
\tilde{w}_J &= \hat{\psi}(\theta)w_J\hat{\psi}(\theta)^{-1} \in {}^{I_{\tilde{\omega}\tilde{y}}}W_J,
\end{aligned}$$

since conjugation by $\hat{\psi}(\theta)$ fixes J. Furthermore, $\hat{\psi}(\Theta)$ fixes Φ_J (as a subset of Φ) and Θ fixes Φ_I, and Ω fixes Φ^+ and Φ^-, hence

$$\begin{aligned}
\ell_{I,J}(\tilde{w}) &= \#\Big\{\alpha \in \Phi^+\backslash\Phi_J : \tilde{\omega}\tilde{y}\alpha \in \Phi^-\backslash\Phi_I\Big\} + \ell(\tilde{w}_J)\\
&= \#\Big\{\alpha \in \Phi^+\backslash\Phi_J : \theta\omega y\hat{\psi}(\theta)^{-1}\alpha \in \Phi^-\backslash\Phi_I\Big\} + \ell(\tilde{w}_J)\\
&= \#\Big\{\alpha \in \Phi^+\backslash\Phi_J : \omega y\alpha \in \Phi^-\backslash\Phi_I\Big\} + \ell(w_J)\\
&= \ell_{I,J}(w).
\end{aligned}$$ □

Let $\Pi := \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. By remark 5.6.3 we know that the function $\ell_{I,J}$ is not only invariant under the action of Θ, but also under the action of Π. As such, we can also consider $\ell_{I,J}$ as a function $\Xi^{\chi,\Theta} \to \mathbb{Z}_{\geq 0}$ or as a function $\Gamma\backslash\Xi^{\chi,\Theta} \to \mathbb{Z}_{\geq 0}$.

Example 5.15. Let p be an odd prime, let V be the $\mathbb{F}_p$-vector space $\mathbb{F}_p^4$, and let ψ be the symmetric nondegenerate bilinear form on V given by the matrix

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Let $\hat{G}$ be the algebraic group $\mathtt{O}(V,\psi)$ over $\mathbb{F}_p$; it has two connected components. The Weyl group W of its identity component $G = \mathtt{SO}(V,\psi)$ is of the form $W \cong \{\pm 1\}^2$ (with trivial Galois action), and its root system is of the form $\Psi \cong \{r_1, r_2, -r_1, -r_2\}$, where the i-th factor of W acts on $\{r_i, -r_i\}$. The set of generators of W is $S = \{(-1,1),(1,-1)\}$. Furthermore, $\#\Omega = 2$, and the nontrivial element σ of Ω permutes the two factors of W (as well as e_1 and e_2); hence $\hat{W} \cong \{\pm 1\}^2 \rtimes S_2$.

Let $\chi\colon \mathbb{G}_\mathrm{m} \to G$ be the cocharacter that sends t to $\mathrm{diag}(t,t,t^{-1},t^{-1})$. Its associated Levi factor L is isomorphic to $\mathtt{GL}_2$; the isomorphism is given by the injection $\mathtt{GL}_2 \hookrightarrow \hat{G}$ that sends a $g \in \mathtt{GL}_2$ to $\mathrm{diag}(g, g^{-1,\mathrm{T}})$. The associated parabolic subgroup P_+ is the product of L with the subgroup $B \subset \hat{G}$ of upper triangular orthogonal matrices. The type of P_+ is a singleton subset of S; without loss of generality we may choose the isomorphism $W \cong \{\pm 1\}^2$ in such a way that P^+ has type $I = \{(-1,1)\}$. Recall that J denotes the type of the parabolic subgroup $P_{-,\pi}$ of G. Since W is abelian and has trivial Galois action, the formula $J = w_0\pi(I)w_0^{-1}$ shows us that $J = I$. Furthermore, since $\mathtt{Cent}_{\hat{G}}(\chi)$ is connected, the group Θ has to be trivial.

An element of $\hat{W}$ is of the form (a,b,c), with $a,b \in \{\pm 1\}$ and $c \in S_2 = \{1,\sigma\}$; then ${}^I\hat{W}$ is the subset of $\hat{W}$ consisting of elements for which $a = 1$. Also, note that $\Phi^+ \setminus \Phi_J = \{e_2\}$, $\Phi^- \setminus \Phi_I = \{-e_2\}$, so to calculate the length function $\ell_{I,J}$ as in (5.5) we only need to determine $\ell(w_J)$ and whether ωy sends e_2 to $-e_2$ or not. If we use the terminology ω, w'', y, w_J from subsection 5.1.2, we get the following results:

	w			
	$(1,1,1)$	$(1,-1,1)$	$(1,1,\sigma)$	$(1,-1,\sigma)$
ω	$(1,1,1)$	$(1,1,1)$	$(1,1,\sigma)$	$(1,1,\sigma)$
w''	$(1,-1,1)$	$(1,1,1)$	$(1,1,1)$	$(-1,1,1)$
y	$(1,1,1)$	$(1,-1,1)$	$(1,1,1)$	$(1,1,1)$
w_J	$(1,1,1)$	$(1,1,1)$	$(1,1,1)$	$(1,1,-1)$
$\omega y e_2 = -e_2$?	no	yes	no	no
$\ell(w_J)$	0	0	0	1
$\ell_{I,J}(\hat{w})$	0	1	0	1

5.3 Algebraic zip data

In this section we discuss algebraic zip data, which are needed to prove statements about the automorphism group of a $\hat{G}$-zip. This section copies a lot from sections 3–8 of [55], except that there the reductive group is assumed to be to be connected. A lot carries over essentially unchanged; in particular, if we cite a result from [55] without comment, we mean that the same proof holds for the nonconnected case. Throughout this section, we will be working over an algebraically closed field k of characteristic p, and for simplicity, we will identify algebraic groups with their set of k-points (which means that we take all groups to be reduced). Furthermore, if $\hat{A}$ is an algebraic group, then we denote its identity component by A. Finally for an algebraic group $\hat{G}$ we denote by $\mathrm{r}_{\hat{G}}$ the quotient map $\mathrm{r}_{\hat{G}}\colon \hat{G} \to \hat{G}/\mathrm{R}_\mathrm{u}G$, where $\mathrm{R}_\mathrm{u}G$ is the unipotent radical of G.

Definition 5.16. An *algebraic zip datum* over k is a quadruple $\hat{\mathcal{Z}} = (\hat{G}, \hat{P}, \hat{Q}, \varphi)$ consisting of:

- a reductive group $\hat{G}$ over k;
- two subgroups $\hat{P}, \hat{Q} \subset \hat{G}$ such that P and Q are parabolic subgroups of G;
- an isogeny $\varphi\colon \hat{P}/\mathrm{R}_\mathrm{u}P \to \hat{Q}/\mathrm{R}_\mathrm{u}Q$, i.e. a morphism of algebraic groups with finite kernel that is faithfully flat on identity components.

For an algebraic zip datum $\hat{\mathcal{Z}}$, we define its *zip group* $E_{\hat{\mathcal{Z}}}$ to be

$$E_{\hat{\mathcal{Z}}} = \Big\{(y, z) \in \hat{P} \times \hat{Q} : \varphi(\mathrm{r}_{\hat{P}}(y)) = \mathrm{r}_{\hat{Q}}(z)\Big\}.$$

It acts on $\hat{G}$ by $(y, z) \cdot g = ygz^{-1}$. Note that if $\hat{\mathcal{Z}}$ is an algebraic zip datum, then we have an associated *connected algebraic zip datum* $\mathcal{Z} := (G, P, Q, \varphi)$. Its associated zip group $E_{\mathcal{Z}}$ is the identity component of $E_{\hat{\mathcal{Z}}}$, and as such also acts on $\hat{G}$.

Definition 5.17. A *frame* of $\hat{\mathcal{Z}}$ is a tuple (B, T, g) consisting of a Borel subgroup B of G, a maximal torus T of B, and an element $g \in G$, such that

- $B \subset Q$;
- $gBg^{-1} \subset P$;
- $\varphi(\mathrm{r}_{\hat{P}}(gBg^{-1})) = \mathrm{r}_{\hat{Q}}(B)$;
- $\varphi(\mathrm{r}_{\hat{P}}(gTg^{-1})) = \mathrm{r}_{\hat{Q}}(T)$.

Proposition 5.18. (See [55, Prop. 3.7]) *For every algebraic zip datum $\hat{\mathcal{Z}} = (\hat{G}, \hat{P}, \hat{Q}, \varphi)$, every Borel subgroup B of G contained in Q and every maximal torus T of B there exists an element $g \in G$ such that (B, T, g) is a frame of $\mathcal{Z}$.* □

We now fix a frame (B, T, g) of $\hat{\mathcal{Z}}$. Let $\hat{P} = U \rtimes \hat{L}$ and $\hat{Q} = V \rtimes \hat{M}$ be the Levi decompositions of $\hat{P}$ and $\hat{Q}$ with respect to T; these exist by proposition 5.7. In this notation

$$E_{\hat{\mathcal{Z}}} = \Big\{(ul, v\varphi(l)) : u \in U, v \in V, l \in \hat{L}\Big\}. \tag{5.19}$$

Furthermore, let I be the type of the parabolic P, and let J be the type of the parabolic Q. Let $w \in {}^I\hat{W} \subset \mathrm{Norm}_{\hat{G}}(T)/T$, and choose a lift $\dot{w} \in \mathrm{Norm}_{\hat{G}}(T)$. If H is a subgroup of $(g\dot{w})^{-1}L(g\dot{w})$, we may compare it with its image under $\varphi \circ \mathrm{inn}(g\dot{w})$, viewed as subgroups of $\hat{G}$ via the chosen Levi splitting of $\hat{Q}$. The collection of all such H for which $H = \varphi \circ \mathrm{inn}(g\dot{w})(H)$ has a unique largest element, namely the subgroup generated by all such subgroups.

Definition 5.20. Let H_w be the unique largest subgroup of $(g\dot{w})^{-1} \cdot L \cdot (g\dot{w})$ that satisfies the relation $H_w = \varphi \circ \mathrm{inn}(g\dot{w})(H_w)$. Let $\varphi_{\dot{w}} \colon H_w \to H_w$ be the isogeny induced by $\varphi \circ \mathrm{inn}(g\dot{w})$, and let H_w act on itself by $h \cdot h' := hh'\varphi_{\dot{w}}(h)^{-1}$.

Since $\varphi \circ \mathrm{inn}(g\dot{w})(T) = T$, the group H_w does not depend on the choice of $\dot{w}$, even though $\varphi_{\dot{w}}$ does. One of the main results of this section is the following result about certain stabilisers.

Theorem 5.21. (See [55, Thm. 8.1]) *Let $w \in {}^I\hat{W}$ and $h \in H_w$. Then the stabiliser $\mathtt{Stab}_{E_{\mathcal{Z}}}(g\dot{w}h)$ is the semidirect product of a connected unipotent normal subgroup and the subgroup*

$$\left\{\Big(\mathrm{int}(g\dot{w})(h'), \varphi\Big(\mathrm{int}(g\dot{w})(h')\Big)\Big) : h' \in \mathtt{Stab}_{H_w}(h)\right\},$$

where the action of H_w on itself is given by semilinear conjugation as in definition 5.20. ☐

Definition 5.22. The algebraic zip datum $\hat{\mathcal{Z}}$ is called *orbitally finite* if for any $w \in {}^I\hat{W}$ the number of fixed points of the endomorphism $\varphi \circ \mathrm{inn}(g\dot{w})$ of H_w is finite; this does not depend on the choice of $\dot{w}$ (see [55, Prop. 7.1]).

We will see later (lemma 5.27) that $\hat{\mathcal{Z}}$ is orbitally finite in the case that is of main interest to us, i.e. when $\hat{\mathcal{Z}}$ comes from the $\hat{G}, \chi, \Theta$ defining a stack of $\hat{G}$-zips (see (5.26)).

Theorem 5.23. (See [55, Thm. 7.5c]) *Suppose $\hat{\mathcal{Z}}$ is orbitally finite. Then for any $w \in {}^I\hat{W}$ the orbit $E_{\mathcal{Z}} \cdot (g\dot{w})$ has dimension $\dim(P) + \ell_{I,J}(w)$.* ☐

Remark 5.24. Although the proofs of these two theorems carry over from the connected case without much difficulty, we feel compelled to make some comments about what exactly changes in the non-connected case, since the proofs of these theorems require most of the material of [55]. The key change is that in [55, Section 4] we allow x to be an element of ${}^I\hat{W}^J$, rather than just ${}^IW^J$; however, one can keep working with the connected algebraic zip datum $\mathcal{Z}$, and define from there a connected algebraic zip datum $\mathcal{Z}_{\dot{x}}$ as in [55, Constr. 4.3]. There, one needs the Levi decomposition for non-connected parabolic groups; but this is handled in our proposition 5.7. The use of non-connected groups does not give any problems in the proofs of most propositions and lemmas in [55, §4–8]. In [55, Prop. 4.8], the term $\ell(x)$ in the formula will now be replaced by $\ell_{I,J}(x)$. The only property of $\ell(x)$ that is used in the proof is that if $x \in {}^IW^J$, then $\ell(x) = \#\{\alpha \in \Phi^+\backslash\Phi_J : x\alpha \in \Phi^-\backslash\Phi_I\}$. In our case, we have $x \in {}^I\hat{W}^J$, and $\ell_{I,J}\colon {}^I\hat{W}^J \to \mathbb{Z}_{\geq 0}$ is the extension of $\ell\colon {}^IW^J \to \mathbb{Z}_{\geq 0}$ that gives the correct formula. Furthermore, in the proof of [55, Prop. 4.12] the assumption $x \in {}^IW^J$ is used, to conclude that $x\Phi_J^+ \subset \Phi^+$. However, the same is true for $x \in {}^I\hat{W}^J$: write $x = \omega x'$ with $\omega \in \Omega$ and $x' \in {}^{\omega^{-1}I\omega}W^J$; then $x'\Phi_J^+ \subset \Phi^+$, and $\omega\Phi^+ = \Phi^+$, since Ω acts on the based root system. Finally, the proofs of both [55, Thm. 7.5c] and [55, Thm. 8.1] rest on an induction argument, where the authors use that an element $w \in {}^IW$ can uniquely be written as $w = xw_J$, with $x \in {}^IW^J$, $w_J \in {}^{I_x}W_J$, and $\ell(w) = \ell(x)+\ell(w_J)$. The analogous statement that we need to use is that any $w \in {}^I\hat{W}$ can uniquely be written as $w = xw_J$, with $x \in {}^I\hat{W}^J$, $w_J \in {}^{I_x}W_J$, and $\ell_{I,J}(w) = \ell_{I,J}(x) + \ell(w_J)$, see remark 5.6.2. The proofs of the other lemmas, propositions and theorems work essentially unchanged.

5.4 Zeta functions of stacks of G-zips

We fix q_0, G, q, χ and Θ as in section 5.2. The aim of this section is to calculate the point counts and the zeta function of the stack $\hat{G}\text{-}\mathsf{Zip}_{\mathbb{F}_q}^{\chi,\Theta}$, as described in the following theorem.

Theorem 5.25. *Let q_0 be a power of p, and let $\hat{G}$ be a reductive group over $\mathbb{F}_{q_0}$. Let q be a power of q_0, let $\chi\colon \mathbb{G}_{\mathrm{m},\mathbb{F}_q} \to \hat{G}_{\mathbb{F}_q}$ be a cocharacter, and let Θ be a subgroup scheme of $\pi_0(\mathtt{Cent}_{\hat{G}_{\mathbb{F}_q}}(\chi))$. Let $\Xi^{\chi,\Theta}$ and Π be as in section 5.2 and $A, B\colon \Pi\backslash\Xi^{\chi,\Theta} \to \mathbb{Z}_{\geq 0}$ be as in notation 5.32. Then for every $v \geq 1$ one has*

$$\#\hat{G}\text{-}\mathsf{Zip}_{\mathbb{F}_q}^{\chi,\Theta}(\mathbb{F}_{q^v}) = \sum_{\substack{\xi\in\Xi^{\chi,\Theta}:\\ B(\xi)\mid v}} q^{-A(\xi)\cdot v}$$

and

$$Z(\hat{G}\text{-}\mathsf{Zip}_{\mathbb{F}_q}^{\chi,\Theta}, t) = \prod_{\bar{\xi}\in\Pi\backslash\Xi^{\chi,\Theta}} \frac{1}{1-(q^{-A(\bar{\xi})}t)^{B(\bar{\xi})}}.$$

The functions A and B depend on some finite combinatorial data, namely the Weil group $\hat{W}$ of $\hat{G}$, the action of $\hat{W}$ on the root system of G, and the action of $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_{q_0})$ on $\hat{W}$. For a given $\hat{G}$ these data, and the functions A and B, are readily calculated.

Before proving this theorem we first need to introduce some auxiliary results. Let φ be as in section 5.2. To the triple $(\hat{G}, \chi, \Theta)$ we can associate the algebraic zip datum

$$\hat{\mathcal{Z}} = (\hat{G}, \hat{P}_+, \hat{P}_{-,\pi}, \varphi|_{\hat{L}}). \tag{5.26}$$

As in section 5.3 the zip group $E_{\hat{\mathcal{Z}}}$ acts on $\hat{G}_{\mathbb{F}_q}$ by $(y_+, y_-)\cdot g' = y_+g'y_-^{-1}$.

Lemma 5.27. (See [56, Rem. 3.9]) *The algebraic zip data $\hat{\mathcal{Z}}$ is orbitally finite.*

Proof. Let $w \in {}^I\hat{W}$, and choose a lift $\dot{w}$ of w to $\mathrm{Norm}_{\hat{G}(\bar{\mathbb{F}}_p)}(T(\bar{\mathbb{F}}_p))$ (for some chosen frame (B,T,g) of $\hat{\mathcal{Z}}$). Then $\varphi_{\dot{w}} = \varphi \circ \mathrm{inn}(g\dot{w})$ is a π-semilinear automorphism of H_w, hence it defines a model $\tilde{H}_{\dot{w}}$ of H_w over $\mathbb{F}_{q_0}$. The fixed points of $\varphi_{\dot{w}}$ in H_w then correspond to $\tilde{H}_{\dot{w}}(\mathbb{F}_{q_0})$, which is a finite set; hence $\hat{\mathcal{Z}}$ is orbitally finite. □

Proposition 5.28. (See [56, Prop. 3.11]) *There is an isomorphism $\hat{G}\text{-Zip}_{\mathbb{F}_q}^{\chi,\Theta} \cong [E_{\hat{\mathcal{Z}}} \backslash \hat{G}_{\mathbb{F}_q}]$ of $\mathbb{F}_q$-stacks.* □

Lemma 5.29. *Let $B \subset P_{-,\pi}$ be a Borel subgroup defined over $\mathbb{F}_q$, and let $T \subset B$ be a maximal torus defined over $\mathbb{F}_q$. Then there exists an element $g \in G(\mathbb{F}_q)$ such that (B, T, g) is a frame of $\hat{\mathcal{Z}}$.*

Proof. Consider the algebraic subset

$$X = \Big\{ g \in G(\bar{\mathbb{F}}_q) : \varphi(gBg^{-1}) = B, \varphi(gTg^{-1}) = T \Big\}$$

of $G(\bar{\mathbb{F}}_q)$. Since $\mathtt{Norm}_G(B) \cap \mathtt{Norm}_G(T) = T$, we see that X forms a T-torsor over $\mathbb{F}_q$. By Lang's theorem such a torsor is trivial, hence X has a rational point. □

For the rest of this section we fix a frame (B, T, g) as in the previous lemma.

Lemma 5.30. *Choose, for every $w \in \hat{W} = \mathrm{Norm}_{\hat{G}(\bar{\mathbb{F}}_q)}(T(\bar{\mathbb{F}}_q))/T(\bar{\mathbb{F}}_q)$, a lift $\dot{w}$ of w to the group $\mathrm{Norm}_{\hat{G}(\bar{\mathbb{F}}_q)}(T(\bar{\mathbb{F}}_q))$. Then the map*

$$\begin{aligned} \Xi^{\chi,\Theta} &\to E_{\hat{\mathcal{Z}}}(\bar{\mathbb{F}}_q) \backslash \hat{G}(\bar{\mathbb{F}}_q) \\ \Theta \cdot w &\mapsto E_{\hat{\mathcal{Z}}}(\bar{\mathbb{F}}_q) \cdot g\dot{w} \end{aligned}$$

is well-defined, and it is an isomorphism of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$-sets that does not depend on the choices of w and $\dot{w}$.

Proof. In [55, Thm. 10.10] it is proven that this map is a well-defined bijection independent of the choices of w and $\dot{w}$. Furthermore, if τ is an element of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$, then the fact that T and g are defined over $\mathbb{F}_q$ implies that $\tau(\dot{w})$ is a lift of $\tau(w)$ to $\mathrm{Norm}_{\hat{G}}(T)$; this shows that the map is Galois-equivariant. □

Remark 5.31. The isomorphism above, together with the identification $[[E_{\hat{\mathcal{Z}}} \backslash \hat{G}_{\mathbb{F}_q}](\bar{\mathbb{F}}_q)] \cong E_{\hat{\mathcal{Z}}}(\bar{\mathbb{F}}_q) \backslash \hat{G}(\bar{\mathbb{F}}_q)$ from lemma 2.12.1, gives the natural bijection in proposition 5.13.

Notation 5.32. Let $\Pi = \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. We define functions $A, B \colon {}^I\hat{W} \to \mathbb{Z}_{\geq 0}$ on ${}^I\hat{W}$ as follows:

- $A(w) = \dim(G/P_+) - \ell_{I,J}(w)$;
- $B(w)$ is the cardinality of the Π-orbit of $\Theta \cdot w$ in $\Xi^{\chi,\Theta}$, i.e.

$$B(w) = \# \Big\{ \xi \in \Xi^{\chi,\Theta} : \xi \in \Pi \cdot (\Theta \cdot w) \Big\}.$$

The fact that $A(w)$ is nonnegative for every $w \in {}^I\hat{W}$ follows from proposition 5.33.2. The function B is clearly Θ-invariant, and A is Θ-invariant by lemma 5.14. As such these functions can also be regarded as functions $A, B \colon \Xi^{\chi,\Theta} \to \mathbb{Z}_{\geq 0}$, or alternatively as functions $A, B \colon \Pi \backslash \Xi^{\chi,\Theta} \to \mathbb{Z}_{\geq 0}$.

Proposition 5.33. *For $\xi \in \Xi^{\chi,\Theta}$, let $\mathcal{Y}_\xi$ be the $\hat{G}$-zip over $\bar{\mathbb{F}}_q$ corresponding to ξ.*

1. *The $\hat{G}$-zip $\mathcal{Y}_\xi$ has a model over $\mathbb{F}_{q^v}$ (see definition 2.11) if and only if v is divisible by $B(\xi)$.*
2. *One has $\dim(\mathtt{Aut}(\mathcal{Y}_\xi)) = A(\xi)$ and the identity component of the group scheme $\mathtt{Aut}(\mathcal{Y}_\xi)^{\mathrm{red}}$ is unipotent.*

Proof.

1. This follows directly from lemma 2.12.2.
2. Note that $\dim(E_{\hat{\mathcal{Z}}}) = \dim(G)$. Let $w \in {}^I\hat{W}$ be such that $\xi = \Theta \cdot w$. By remark 2.13, lemma 5.27 and theorem 5.23 we have

$$\begin{aligned}\dim(\mathtt{Aut}(\mathcal{Y}_\xi)) &= \dim(\mathtt{Stab}_{E_{\hat{\mathcal{Z}}}}(g\dot{w})) \\ &= \dim(E_{\hat{\mathcal{Z}}}) - \dim(E_{\hat{\mathcal{Z}}} \cdot g\dot{w}) \\ &= \dim(G) - \dim(E_{\hat{\mathcal{Z}}} \cdot g\dot{w}) \\ &= \dim(G) - \dim(P_+) - \ell_{I,J}(\xi) \\ &= A(\xi).\end{aligned}$$

Furthermore, by theorem 5.21 the identity component of $\mathtt{Aut}(\mathcal{Y}_\xi)^{\mathrm{red}}$ is unipotent. □

Remark 5.34. The formula $\dim(\mathtt{Aut}(\mathcal{Y}_\xi)) = \dim(G/P) - \ell_{I,J}(\xi)$ from proposition 5.33.2 apparently contradicts the proof of [56, Thm. 3.26]. There an extended length function $\ell \colon \hat{W} \to \mathbb{Z}_{\geq 0}$ is defined by $\ell(w\omega) = \ell(w)$ for $w \in W, \omega \in \Omega$. It is stated that the codimension of $E_{\hat{\mathcal{Z}}} \cdot (g\dot{w})$ in $\hat{G}$ is equal to $\dim(G/P_+) - \ell(w)$. In other words, if this were correct, $\dim(\mathtt{Aut}(\mathcal{Y}_\xi))$ would be equal to $\dim(G/P^+) - \ell(w)$ rather than $\dim(G/P^+) - \ell_{I,J}(w)$. However, the proof seems to be incorrect (and the theorem itself as well); the dimension formula should follow from [55, Thm. 5.11], but that result only holds for the connected case. In the nonconnected case one can construct a counterexample as follows. Let $\hat{G}$ be the example of remark 5.6.4 (over $\mathbb{F}_p$), and consider the cocharacter

$$\begin{aligned}\chi \colon \mathbb{G}_{\mathrm{m}} &\to G \\ x &\mapsto \left(\begin{smallmatrix} x & 0 \\ 0 & x^{-1} \end{smallmatrix}\right).\end{aligned}$$

Then L is the diagonal subgroup of G, P_+ the upper triangular matrices, and $P_- = P_{-,\pi}$ the lower triangular matrices, and we can take $g = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Employing the notation of (5.19), the stabiliser of $g\omega$ in $E_{\hat{\mathcal{Z}}}(\bar{\mathbb{F}}_q)$ is then equal to

$$\Big\{(lu_+, \varphi(l)u_-) \in E_{\hat{\mathcal{Z}}}(\bar{\mathbb{F}}_q) : lu_+ = g\omega\varphi(l)u_-\omega^{-1}g^{-1}\Big\}.$$

Conjugation by g and ω both exchange P_+ and P_-, so in the equation

$$lu_+ = g\omega\varphi(l)u_-\omega^{-1}g^{-1}$$

the left hand side is in P_+, while the right hand side is in P_-. This means that both sides have to be in L, hence $u_+ = u_- = 1$, and the equation simplifies to $l = -\varphi(l)$. This has only finitely many solutions, hence

$$\operatorname{codim}(E_{\mathcal{Z}} \cdot (g\dot{w})) = \dim(\mathtt{Stab}_{E_{\hat{\mathcal{Z}}}}(g\dot{w})) = 0 = \dim(G/P_+) - \ell_{I,J}(\omega)$$

while $\dim(G/P_+) - \ell(\omega) = 1$.

Remark 5.35. In general $\mathtt{Aut}(\mathcal{Y}_\xi)$ will not be reduced; see [44, Rem. 3.1.7] for the first found instance of this phenomenon, or [56, Rem. 3.35] for the general case.

Proof of theorem 5.25. With all the previous results all that is left is a straightforward calculation. As in proposition 5.33 let $\mathcal{Y}_\xi$ be the $\hat{G}$-zip over $\bar{\mathbb{F}}_q$ corresponding to ξ, for every $\xi \in \Xi^{\chi,\Theta}$. Furthermore, for an integer $v \geq 1$, we set $\Xi^{\chi,\Theta}(\mathbb{F}_{q^v}) := (\Xi^{\chi,\Theta})^{\operatorname{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_{q^v})}$ and $(E_{\hat{\mathcal{Z}}}\backslash\hat{G})(\mathbb{F}_{q^v}) := (E_{\hat{\mathcal{Z}}}(\bar{\mathbb{F}}_q)\backslash\hat{G}(\bar{\mathbb{F}}_q))^{\operatorname{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_{q^v})}$. We get for every $v \geq 1$:

$$\begin{aligned}
\#\hat{G}\text{-}\mathsf{Zip}^{\chi,\Theta}_{\mathbb{F}_q}(\mathbb{F}_{q^v}) &\overset{5.28}{=} \#[E_{\hat{\mathcal{Z}}}\backslash\hat{G}](\mathbb{F}_{q^v}) \\
&\overset{\substack{2.15,\\5.33.2}}{=} \sum_{C\in(E_{\hat{\mathcal{Z}}}\backslash\hat{G})(\mathbb{F}_{q^v})} q^{-\dim(\mathtt{A}(C))\cdot v} \\
&\overset{5.30}{=} \sum_{\xi\in\Xi^{\chi,\Theta}(\mathbb{F}_{q^v})} q^{-\dim(\mathtt{Aut}(\mathcal{Y}_\xi))\cdot v} \\
&\overset{5.33.2}{=} \sum_{\xi\in\Xi^{\chi,\Theta}(\mathbb{F}_{q^v})} q^{-A(\xi)\cdot v} \\
&\overset{5.33.1}{=} \sum_{\substack{\xi\in\Xi^{\chi,\Theta}:\\ B(\xi)|v}} q^{-A(\xi)\cdot v},
\end{aligned}$$

hence

$$\begin{aligned}
Z(\hat{G}\text{-}\mathsf{Zip}^{\chi,\Theta}_{\mathbb{F}_q}, t) &= \exp\left(\sum_{v\geq 1}\frac{t^v}{v}\sum_{\substack{\xi\in\Xi^{\chi,\Theta}:\\ B(\xi)|v}} q^{-A(\xi)\cdot v}\right) \\
&= \exp\left(\sum_{\xi\in\Xi^{\chi,\Theta}}\sum_{\substack{v\geq 1:\\ B(\xi)|v}} \frac{1}{v}(q^{-A(\xi)}t)^v\right) \\
&= \prod_{\xi\in\Xi^{\chi,\Theta}} \exp\left(\sum_{v'\geq 1}\frac{1}{B(\xi)v'}(q^{-A(\xi)}t)^{B(\xi)v'}\right) \\
&= \prod_{\xi\in\Xi^{\chi,\Theta}} (1-(q^{-A(\xi)}t)^{B(\xi)})^{-\frac{1}{B(\xi)}} \\
&= \prod_{\bar{\xi}\in\Pi\backslash\Xi^{\chi,\Theta}}\prod_{\xi\in\bar{\xi}}(1-(q^{-A(\xi)}t)^{B(\xi)})^{-\frac{1}{B(\xi)}}
\end{aligned}$$

$$\overset{5.32}{=} \prod_{\bar{\xi}\in\Pi\backslash\Xi^{\chi,\Theta}} (1-(q^{-A(\bar{\xi})}t)^{B(\bar{\xi})})^{-1}. \qquad \square$$

Example 5.36. Using the language of G-zips and theorem 5.25, we can give an alternative proof for theorem 3.33 for the case $n = 1$. Let G and χ be as in example 5.11. Since G is connected we get $\hat{W} = W$, $\Theta = 1$, and I and W are as in notation 3.25. Furthermore, G is split, so we get $\Pi\backslash\Xi^{\chi,\Theta} = \Xi^{\chi,\Theta} = {}^{I}W$ and $B(w) = 1$ for all $w \in {}^{I}W$. Since $\hat{W} = W$ we find that $A(w) = \dim(G/P^{+}) - \ell(w)$, and we readily calculate that $\dim(G) = h^2$, $\dim(P^{+}) = h^2 - hd + d^2$, hence $\dim(G/P^{+}) = d(h-d)$. Taking all of this together, we find that theorem 5.25 gives the same formula for $Z(\mathtt{GL}_h\text{-}\mathtt{Zip}^{\chi}_{\mathbb{F}_p}, t) = Z(\mathtt{BT}_1^{h,d}, t)$ as theorem 3.33.

Part II

Integral models of reductive groups

Chapter 6

Introduction

Let K be a number field or a p-adic field, and let R be its ring of integers. Let G be a connected reductive group over K. By a *model* $\mathscr{G}$ of G we mean a flat group scheme of finite type over R such that $\mathscr{G}_K \cong G$. An important way to construct models of G is the following. Let V be a finite dimensional K-vector space, and let $\varrho\colon G \hookrightarrow \mathtt{GL}(V)$ be an injective map of algebraic groups (again we use $\mathtt{GL}(V)$ for the algebraic group underlying the abstract group $\mathrm{GL}(V)$). We consider G as a subgroup of $\mathtt{GL}(V)$ via ϱ. Now let Λ be a lattice in V, i.e. a locally free R-submodule of V that generates V as a K-vector space. Then $\mathtt{GL}(\Lambda)$ is a group scheme over R whose generic fibre is canonically isomorphic to $\mathtt{GL}(V)$. Let $\mathtt{mod}_G(\Lambda)$ be the Zariski closure of G in $\mathtt{GL}(\Lambda)$; this is a model of G. In general, the group scheme $\mathtt{mod}_G(\Lambda)$ depends on the choice of Λ, and one can ask the following question:

Question. *Suppose that G, its representation V, and its model $\mathtt{mod}_G(\Lambda)$ are given. To what extent can we recover the lattice $\Lambda \subset V$?*

As a partial answer we can say that the group scheme $\mathtt{mod}_G(\Lambda)$ certainly does not determine Λ uniquely. Let $g \in \mathrm{GL}(V)$; then the automorphism $\mathrm{inn}(g)$ of $\mathtt{GL}(V)$ extends to an isomorphism $\mathtt{GL}(\Lambda) \xrightarrow{\sim} \mathtt{GL}(g\Lambda)$. As such, we obtain an isomorphism between the group schemes $\mathtt{mod}_G(\Lambda)$ and $\mathtt{mod}_{gGg^{-1}}(g\Lambda)$. This shows that the group scheme $\mathtt{mod}_G(\Lambda)$ only depends on the $N(K)$-orbit of Λ, where N is the scheme-theoretic normaliser of G in $\mathtt{GL}(V)$. The following theorem shows that the correspondence between models of G and $N(K)$-orbits of lattices is finite.

Theorem 7.1. *Let G be a connected reductive group over a number field or p-adic field K, and let V be a finite dimensional faithful representation of G. Let N be the scheme-theoretic normaliser of G in $\mathtt{GL}(V)$. Let $\mathscr{G}$ be a model of G. Then the lattices Λ in V such that $\mathtt{mod}_G(\Lambda) \cong \mathscr{G}$ are contained in at most finitely many $N(K)$-orbits.*

In general, a model of G will correspond to more than one $N(K)$-orbit of lattices, see examples 7.7 and 7.10.

A variant of theorem 7.1 can be applied in the context of Shimura varieties. Let g and $n > 2$ be positive integers, and let $\mathcal{A}_{g,n}$ be the moduli space of complex principally polarised abelian varieties of dimension g with a given level n structure. Let Y be a special subvariety of $\mathcal{A}_{g,n}$, and let G be the generic (rational) Mumford–Tate group of Y (with respect to the variation of rational Hodge structures coming from the homology of the universal abelian variety with $\mathbb{Q}$-coefficients). Then the inclusion $Y \hookrightarrow \mathcal{A}_{g,n}$ is induced by a morphism of Shimura data $\varrho\colon (G, X) \hookrightarrow (\mathtt{GSp}_{2g,\mathbb{Q}}, \mathscr{H}_g)$ that is injective on the level of algebraic groups. On the other hand the variation of rational Hodge structures on $\mathcal{A}_{g,n}$ comes from a variation of integral Hodge structures related to homology with $\mathbb{Z}$-coefficients. This integral variation of Hodge structures corresponds to a lattice Λ in the standard representation V of $\mathtt{GSp}_{2g,\mathbb{Q}}$. Let $\mathtt{GMT}(Y)$ be the generic integral Mumford-Tate group of Y with respect to this variation of integral Hodge structures; then $\mathtt{GMT}(Y)$ is isomorphic to $\mathtt{mod}_G(\Lambda)$ (where V is regarded as a faithful representation of G via ϱ). Replacing Y by a Hecke translate corresponds to replacing the inclusion $G \hookrightarrow \mathtt{GSp}_{2g,\mathbb{Q}}$ by a conjugate, or equivalently to choosing another lattice in V. By applying theorem 7.1 we are able to prove the following theorem.

Theorem 8.1. *Let g and n be positive integers with $n > 2$, and let $\mathscr{G}$ be a group scheme over $\mathbb{Z}$. Then there are only finitely many special subvarieties Y of $\mathcal{A}_{g,n}$ such that $\mathtt{GMT}(Y) \cong \mathscr{G}$.*

In other words, a special subvariety $Y \subset \mathcal{A}_{g,n}$ is determined, up to some finite ambiguity, by its generic integral Mumford–Tate group. We can also apply this result to the *Mumford–Tate conjecture*: Let A be an abelian variety over a number field $K \subset \mathbb{C}$, and denote for every prime number ℓ the ℓ-adic Galois monodromy group of A by $\mathtt{G}_\ell(A)$ (see definition 8.20 for details); this is a flat group scheme of finite type over $\mathbb{Z}_\ell$ whose generic fibre is a reductive algebraic group over $\mathbb{Q}_\ell$. Furthermore, let $\mathtt{MT}(A)$ denote the Mumford–Tate group of A; this is a flat group scheme of finite type over $\mathbb{Z}$ whose generic fibre is a reductive algebraic group over $\mathbb{Q}$. The Mumford–Tate conjecture states that $\mathtt{MT}(A)_{\mathbb{Z}_\ell} = \mathtt{G}_\ell(A)$ for every prime number ℓ. On the other hand, let x be a point on $\mathcal{A}_{g,n}$ corresponding to A, and let Y be the special closure of x; then $\mathtt{GMT}(Y) \cong \mathtt{MT}(A)$. As such, the Mumford–Tate conjecture predicts that the answer to the following question is ‘yes’:

Question. *Let A be a g-dimensional abelian variety over a number field $K \subset \mathbb{C}$. Does there exist a special subvariety S of $\mathcal{A}_{g,n}$ such that $\mathtt{GMT}(Y)_{\mathbb{Z}_\ell} \cong \mathtt{G}_\ell(A)$ for all prime numbers ℓ?*

By slightly altering the proof of theorem 8.1, we can prove the following converse to this question, and give an affirmative answer in the smallest unsolved case of the Mumford–Tate conjecture:

Theorem 8.22. *Let A be a g-dimensional principally polarised abelian variety over a number field $K \subset \mathbb{C}$, and let $n > 2$ be an integer. Then there exist at most finitely many special subvarieties Y of $\mathcal{A}_{g,n}$ such that $\mathtt{GMT}(Y)_{\mathbb{Z}_\ell} \cong \mathtt{G}_\ell(A)$ for all prime numbers ℓ. If A is of Mumford’s type (see definition 8.27) then at least one such Y exists.*

The structure of this part is as follows: The lengthy chapter 7 is dedicated to the proof of theorem 7.1; in chapter 8 we prove theorems 8.1 and 8.22. We let go of the notations and conventions of the previous part, with the exception that we will continue to use `Hom`, `Aut`, `Stab`, etc, for the schemes underlying Hom, Aut, Stab, etc. With the exception of section 8.2 all of the material is adapted mostly unchanged from [36].

Chapter 7

Integral models in representations

As in the introduction we let K be a number field or a p-adic field and R its ring of integers, and for a vector space V over K, an algebraic subgroup $G \subset \mathtt{GL}(V)$, and a lattice $\Lambda \subset V$, we let $\mathtt{mod}_G(\Lambda)$ be the closure of G in $\mathtt{GL}(\Lambda)$. The goal of this chapter is to prove the following theorem:

Theorem 7.1. *Let G be a connected reductive group over a number field or p-adic field K, and let V be a finite dimensional faithful representation of G. Let N be the scheme-theoretic normaliser of G in $\mathtt{GL}(V)$. Let $\mathscr{G}$ be a model of G. Then the lattices Λ in V such that $\mathtt{mod}_G(\Lambda) \cong \mathscr{G}$ are contained in at most finitely many $N(K)$-orbits.*

In a sense this is a generalisation of the statement that the class group of a number field is finite, see example 7.7. The strategy for the case that G is split and K is a local field is as follows. Let $\mathfrak{g}$ be the Lie algebra of G, then V is a faithful representation of G. If $\mathscr{G}$ is any model of G, then its Lie algebra $\mathfrak{G}$ is a lattice in $\mathfrak{g}$. The proof consists of the following steps:

1. We define a set of 'nice' lattices in $\mathfrak{g}$ (definition 7.28) and a set of 'nice' lattices in V (definition 7.35);
2. We show that the nice lattices in V form only finitely many orbits under a suitably chosen algebraic group (proposition 7.40);
3. We show that if $\mathscr{G}$ is the model corresponding to a lattice Λ, then we can give an upper bound to the distance from Λ to a 'nice' lattice in terms of the distance from $\mathfrak{G}$ to a nice lattice (proposition 7.46).

This upper bound allows us to prove that there are only finitely many $N(K)$-orbits corresponding to one model of $\mathscr{G}$. The proof of this is given in section 7.3. In section 7.4 we generalise this to nonsplit groups, and in section 7.5 we generalise it to number fields. For this last step we will need that for p-adic K under sufficiently nice assumptions there will only correspond one $N(K)$-orbit to the model $\mathscr{G}$.

7.1 Lattices, models, Hopf algebras and Lie algebras

In this section we will discuss a number of properties of models, and their relation to lattices in various vector spaces. Throughout we fix a number field or p-adic field K, along with its ring of integers R.

7.1.1 Models of reductive groups

Definition 7.2. Let G be a connected reductive algebraic group over K, and let T be a maximal torus of G.

1. A *model* of G is a flat group scheme $\mathscr{G}$ of finite type over R such that there exists an isomorphism $\varphi \colon \mathscr{G}_K \xrightarrow{\sim} G$. Such an isomorphism is called an *anchoring* of $\mathscr{G}$. The set of isomorphism classes of models of G is denoted $\mathrm{Mod}(G)$.

2. An *anchored model* of G is pair $(\mathscr{G}, \varphi)$ consisting of a model $\mathscr{G}$ of G and an anchoring $\varphi \colon \mathscr{G}_K \xrightarrow{\sim} G$. The set of isomorphism classes of anchored models of G is denoted $\mathrm{Mod}^{\mathrm{a}}(G)$.

3. A *model* of (G, T) is a pair $(\mathscr{G}, \mathscr{T})$ consisting of a model of G and a closed reduced subgroup scheme $\mathscr{T}$ of $\mathscr{G}$, for which there exists an isomorphism $\varphi \colon \mathscr{G}_K \xrightarrow{\sim} G$ such that $\varphi|_{\mathscr{T}_K}$ is an isomorphism from $\mathscr{T}_K$ to T. Such a φ is called an *anchoring* of $(\mathscr{G}, \mathscr{T})$. The set of isomorphism classes of models of (G, T) is denoted $\mathrm{Mod}(G, T)$.

Note that there are natural forgetful maps $\mathrm{Mod}^{\mathrm{a}}(G) \to \mathrm{Mod}(G, T) \to \mathrm{Mod}(G)$. Our use of the terminology 'model' may differ from its use in the literature; for instance, some authors consider the choice of an anchoring to be part of the data (hence their 'models' would be our 'anchored models'), or they may impose other conditions on the group scheme $\mathscr{G}$ over R; see for instance [10], [18] and [21]. Our choice of terminology is justified by the fact that our models are exactly those that arise from lattices in representations (see remark 7.8). This use of the word 'model' also differs from definition 2.11, but as mentioned in the introduction of this part we will drop all our notations from the previous part.

Definition 7.3. Let V be a K-vector space. A *lattice* in V is a locally free R-submodule of V that spans V as a K-vector space. The set of lattices in V is denoted $\mathrm{Lat}(V)$. If $H \subset \mathtt{GL}(V)$ is an algebraic subgroup, we write $\mathrm{Lat}_H(V)$ for the quotient $H(K)\backslash\mathrm{Lat}(V)$.

Remark 7.4. If V is finite dimensional, then an R-submodule $\Lambda \subset V$ is a lattice if and only if Λ is finitely generated and $K \cdot \Lambda = V$ (see [62, Tag 00NX]).

Let G be a connected reductive group over K, and let V be a finite dimensional faithful representation of G; we consider G as an algebraic subgroup of $\mathtt{GL}(V)$. Let Λ be a lattice in V. The identification $\Lambda_K = V$ induces a natural isomorphism

$$f_\Lambda \colon \mathtt{GL}(\Lambda)_K \xrightarrow{\sim} \mathtt{GL}(V).$$

Now let $\mathtt{mod}_G(\Lambda)$ be the Zariski closure of $f_\Lambda^{-1}(G)$ in $\mathtt{GL}(\Lambda)$; this is a model of G. If we let φ_Λ be the isomorphism $f_\Lambda|_{\mathtt{mod}_G(\Lambda)_K} : \mathtt{mod}_G(\Lambda)_K \xrightarrow{\sim} G$, then $(\mathtt{mod}_G(\Lambda), \varphi_\Lambda)$ is an anchored model of G. This gives us a map

$$\begin{aligned} \mathtt{mod}_G^{\mathrm{a}} \colon \mathrm{Lat}(V) &\to \mathrm{Mod}^{\mathrm{a}}(G) \\ \Lambda &\mapsto (\mathtt{mod}_G(\Lambda), \varphi_\Lambda). \end{aligned}$$

The compositions of $\mathtt{mod}_G^{\mathrm{a}}$ with the forgetful maps $\mathrm{Mod}^{\mathrm{a}}(G) \to \mathrm{Mod}(G,T)$ (for a maximal torus T of G) and $\mathrm{Mod}^{\mathrm{a}}(G) \to \mathrm{Mod}(G)$ are denoted $\mathtt{mod}_{G,T}$ and $\mathtt{mod}_G$, respectively.

Lemma 7.5. *Let G be a connected reductive group over K and let V be a faithful finite dimensional representation of G. Consider G as a subgroup of $\mathtt{GL}(V)$. Let $Z := \mathtt{Cent}_{\mathtt{GL}(V)}(G)$ be the scheme-theoretic centraliser of G in $\mathtt{GL}(V)$, and let $N := \mathtt{Norm}_{\mathtt{GL}(V)}(G)$ be the scheme-theoretic normaliser of G in $\mathtt{GL}(V)$. Let T be a maximal torus of G, and let $H := Z \cdot T \subset \mathtt{GL}(V)$.*

1. *The map $\mathtt{mod}_G^{\mathrm{a}} \colon \mathrm{Lat}(V) \to \mathrm{Mod}^{\mathrm{a}}(G)$ factors through $\mathrm{Lat}_Z(V)$.*
2. *The map $\mathtt{mod}_{G,T} \colon \mathrm{Lat}(V) \to \mathrm{Mod}(G,T)$ factors through $\mathrm{Lat}_H(V)$.*
3. *The map $\mathtt{mod}_G \colon \mathrm{Lat}(V) \to \mathrm{Mod}(G)$ factors through $\mathrm{Lat}_N(V)$.*

Proof. We only prove the first statement; the other two can be proven analogously. Let g be an element of $\mathrm{GL}(V)$. The map $\mathrm{inn}(g) \in \mathrm{Aut}(\mathtt{GL}(V))$ extends to an automorphism $\mathtt{GL}(\Lambda) \to \mathtt{GL}(g\Lambda)$ as in the following diagram:

$$\begin{array}{ccc}
\mathtt{GL}(\Lambda) & \xrightarrow[\sim]{(f_{g\Lambda} \circ \mathrm{inn}(g) \circ f_\Lambda^{-1})^{\mathrm{zar}}} & \mathtt{GL}(g\Lambda) \\
\uparrow & & \uparrow \\
\mathtt{GL}(\Lambda)_K & \xrightarrow[\sim]{f_{g\Lambda} \circ \mathrm{inn}(g) \circ f_\Lambda^{-1}} & \mathtt{GL}(g\Lambda)_K \\
\wr\downarrow f_\Lambda & & \wr\downarrow f_{g\Lambda} \\
\mathtt{GL}(V) & \xrightarrow[\sim]{\mathrm{inn}(g)} & \mathtt{GL}(V) \\
\uparrow & & \uparrow \\
G & \xrightarrow[\sim]{} & gGg^{-1}
\end{array}$$

This shows that $(\mathtt{mod}_G(\Lambda), \varphi_\Lambda) \cong (\mathtt{mod}_{gGg^{-1}}(g\Lambda), \mathrm{inn}(g)^{-1} \circ f_{g\Lambda}|_{\mathtt{mod}_{gGg^{-1}}(g\Lambda)_K})$ as anchored models of G. If g is an element of $Z(K)$ we find that as anchored models of G we have $(\mathtt{mod}_G(\Lambda), \varphi_\Lambda) \cong (\mathtt{mod}_G(g\Lambda), \varphi_{g\Lambda})$, as was to be proven. $\square$

Remark 7.6. Throughout the rest of this chapter we say that a map of sets is *finite* if it has finite fibres. In the terminology of the lemma above, theorem 7.1 then states that the map $\mathtt{mod}_G\colon \mathrm{Lat}_N(V) \to \mathrm{Mod}(G)$ is finite.

Example 7.7. Let F be a number field, and let $G = \mathrm{Res}_{F/\mathbb{Q}}(\mathbb{G}_\mathrm{m})$ be the Weil restriction of $\mathbb{G}_\mathrm{m}$ from F to $\mathbb{Q}$. Let V be the $\mathbb{Q}$-vector space F, together with its natural representation of G. Now let Λ be a lattice in V, and define the ring

$$A_\Lambda := \{x \in F \colon x\Lambda \subset \Lambda\};$$

this is an order in F. In this case one has $\mathtt{mod}_G(\Lambda) \cong \mathrm{Res}_{A_\Lambda/\mathbb{Z}}(\mathbb{G}_\mathrm{m})$ as group schemes over $\mathbb{Z}$. Now let Λ be such that $A_\Lambda = \mathscr{O}_F$. As an additive subgroup of F the lattice Λ can be considered as a fractional $\mathscr{O}_F$-ideal. Since in this case we have $N(\mathbb{Q}) = G(\mathbb{Q}) = F^\times$, the $N(\mathbb{Q})$-orbit of Λ corresponds to an element of the class group $\mathrm{Cl}(F)$. On the other hand, every element of $\mathrm{Cl}(F)$ corresponds to a $N(\mathbb{Q})$-orbit of lattices Λ in V satisfying $A_\Lambda = \mathscr{O}_F$. In other words, there is a bijective correspondence between $N(\mathbb{Q})$-orbits of lattices yielding the model $\mathrm{Res}_{\mathscr{O}_F/\mathbb{Z}}(\mathbb{G}_\mathrm{m})$ of G, and elements of the class group $\mathrm{Cl}(F)$. This shows that a model of G generally does not correspond to a single N-orbit of lattices. In this setting, theorem 7.1 recovers the well-known fact that $\mathrm{Cl}(F)$ is finite.

Remark 7.8. Let G be a (not necessarily connected) reductive group over K, and let $\mathscr{G}$ be a model of G. Then [22, Exp. VI.B, Prop. 13.2] tells us that there exists a free R-module Λ of finite rank such that $\mathscr{G}$ is isomorphic to a closed subgroup of $\mathtt{GL}(\Lambda)$. If we take $V = \Lambda_K$, we find that V is a faithful representation of G, and $\mathscr{G}$ is the image of Λ under the map $\mathtt{mod}_G\colon \mathrm{Lat}(V) \to \mathrm{Mod}(G)$. Hence every model of G arises from a lattice in some representation.

7.1.2 Hopf algebras and Lie algebras

Definition 7.9. Let G be a connected reductive group over K, and let $A := \mathcal{O}(G)$ be the Hopf algebra of G. An *order* of A is an R-subalgebra $\mathscr{A}$ of A of finite type such that $\mathscr{A}$ has the structure of an R-Hopf algebra with the comultiplication, counit, and coinverse of A, and such that $\mathscr{A}$ is a lattice in the K-vector space A.

If $\mathscr{A}$ is an order in A, then $(\mathrm{Spec}(\mathscr{A}), \mathrm{Spec}(A \xrightarrow{\sim} \mathscr{A}_K))$ is an anchored model of G, and this gives a bijection between the set of orders of A and $\mathrm{Mod}^\mathrm{a}(G)$. Analogously the set $\mathrm{Mod}(G)$ corresponds bijectively to the set of flat R-Hopf algebras $\mathscr{A}$ of finite type such that $\mathscr{A}_K \cong A$. If V is a faithful representation of G, and Λ is a lattice in V, we write $\mathrm{mod}_A(\Lambda)$ for the order of A corresponding to the anchored model $(\mathtt{mod}_G(\Lambda), \varphi_\Lambda)$. It is the image of the composite map of rings

$$\mathcal{O}(\mathtt{GL}(\Lambda)) \hookrightarrow \mathcal{O}(\mathtt{GL}(V)) \twoheadrightarrow A.$$

Let $\mathfrak{g}$ be the (K-valued points of the) Lie algebra of G. Let $\mathscr{G}$ be a model of G, and let $\mathfrak{G}$ be the (R-valued points of the) Lie algebra of $\mathfrak{G}$. Then $\mathfrak{g}$ is a K-vector space of dimension $\dim(G)$, and $\mathfrak{G}$ is a locally free R-module of rank $\dim(G)$. If φ is an anchoring of $\mathscr{G}$, then φ induces an embedding of R-Lie algebras $\operatorname{Lie}\varphi\colon \mathfrak{G} \hookrightarrow \mathfrak{g}$, and its image is a lattice in $\mathfrak{g}$. Suppose V is a faithful representation of G and $\Lambda \subset V$ is a lattice such that $\mathtt{mod}^{\mathrm{a}}_G(\Lambda) = (\mathscr{G}, \varphi)$. Then $(\operatorname{Lie}\varphi)(\mathfrak{G}) = \mathfrak{g} \cap \mathfrak{gl}(\Lambda)$ as subsets of $\mathfrak{gl}(V)$.

Example 7.10. We give an example that shows that $\mathtt{mod}_G\colon \operatorname{Lat}_N(V) \to \operatorname{Mod}(G)$ is generally not injective over local fields. Let K be the field $\mathbb{Q}_2$, and let G be the algebraic group $\mathtt{PGL}_2$ over K. The standard representation V of $\tilde{G} = \mathtt{SL}_{2,\mathbb{Q}_2}$ induces a representation of G on $W = \operatorname{Sym}^2(V)$. Let $E = \{e_1, e_2\}$ be the standard basis of V; this induces a basis $F = \{e_1^2, e_1e_2, e_2^2\}$ of W. Relative to this basis the representation is given as follows:

$$\begin{array}{ccc} \tilde{G} & \to & \mathtt{GL}(W) \\ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) & \mapsto & \begin{pmatrix} a^2 & ab & b^2 \\ 2ac & ad+bc & 2bd \\ c^2 & cd & d^2 \end{pmatrix}. \end{array}$$

Then $\mathcal{O}(\tilde{G}) = \mathbb{Q}_2[x_{11}, x_{12}, x_{21}, x_{22}]/(x_{11}x_{22} - x_{12}x_{21} - 1)$, and $A := \mathcal{O}(G)$ is the $\mathbb{Q}_2$-subalgebra of $\mathcal{O}(\tilde{G})$ generated by the coefficients of this representation, i.e. by the set

$$S = \left\{x_{11}^2, x_{11}x_{12}, x_{12}^2, 2x_{11}x_{21}, x_{11}x_{22} + x_{12}x_{21}, 2x_{12}x_{22}, x_{21}^2, x_{21}x_{22}, x_{22}^2\right\}.$$

Let Λ be the lattice generated by F; then $\operatorname{mod}_A(\Lambda)$ is the $\mathbb{Z}_2$-subalgebra of A generated by S. It contains $x_{11}x_{21} = x_{11}^2(x_{21}x_{22}) - x_{21}^2(x_{11}x_{12})$ and $x_{12}x_{22} = x_{22}^2(x_{11}x_{12}) - x_{12}^2(x_{21}x_{22})$, hence $\operatorname{mod}_A(\Lambda)$ is also generated as a $\mathbb{Z}_2$-algebra by

$$S' = \left\{x_{11}^2, x_{11}x_{12}, x_{12}^2, x_{11}x_{21}, x_{11}x_{22} + x_{12}x_{21}, x_{12}x_{22}, x_{21}^2, x_{21}x_{22}, x_{22}^2\right\}.$$

Now consider the basis $F' = \{e_1^2, 2e_1e_2, e_2^2\}$ of W, and let Λ' be the lattice in W generated by F'. Relative to this basis the representation is given by

$$\begin{array}{ccc} \tilde{G} & \to & \mathtt{GL}(W) \\ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) & \mapsto & \begin{pmatrix} a^2 & 2ab & b^2 \\ ac & ad+bc & bd \\ c^2 & 2cd & d^2 \end{pmatrix}. \end{array}$$

Analogous to the above we see that $\operatorname{mod}_A(\Lambda')$ is also generated by S', hence $\operatorname{mod}_A(\Lambda) = \operatorname{mod}_A(\Lambda')$ as $\mathbb{Z}_2$-subalgebras of A. Let $T \subset \mathtt{GL}(W)$ be the group of scalars; then the normaliser N of G is equal to the subgroup $T \cdot G$ of $\mathtt{GL}(W)$. We will show that $N(\mathbb{Q}_2) \cdot \Lambda$ and $N(\mathbb{Q}_2) \cdot \Lambda'$ are two different elements of $\operatorname{Lat}_N(V)$. Call a lattice $L \subset W$ *pure* if $L = c \cdot \operatorname{Sym}^2(M)$ for some lattice $M \subset V$ and some $c \in K^\times$. I claim that the pure lattices form a single orbit under the action of $N(\mathbb{Q}_2)$ on $\operatorname{Lat}(W)$. To see this, note that pure lattices from an orbit under the action of $\operatorname{GL}(V) \times T(\mathbb{Q}_2)$ on W. We get a short exact sequence

$$1 \to \mathbb{G}_{\mathrm{m}} \to \mathtt{GL}(V) \times T \to N \to 1,$$

where the first map is given by $x \mapsto \left(\left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right), x^{-2}\right)$. Taking Galois cohomology, we obtain an exact sequence

$$1 \to \mathbb{Q}_2^\times \to \operatorname{GL}(V) \times T(\mathbb{Q}_2) \to N(\mathbb{Q}_2) \to \mathrm{H}^1(\mathbb{Q}_2, \mathbb{G}_{\mathrm{m}}).$$

By Hilbert 90 the last term of this sequence is trivial; hence the image of the group $\mathrm{GL}(V) \times T(\mathbb{Q}_2)$ in $\mathtt{GL}(W)$ is equal to $N(\mathbb{Q}_2)$, and pure lattices form a single $N(\mathbb{Q}_2)$-orbit.

Let $M := \mathbb{Z}_2 \cdot e_1 \oplus \mathbb{Z}_2 \cdot e_2 \subset V$. Then Λ is equal to $\mathrm{Sym}^2(M)$, hence it is pure. Suppose Λ' is pure; then there exist $x = x_1e_1 + x_2e_2, y = y_1e_1 + y_2e_2$ and $c \in K^\times$ such that Λ' is generated by $\{cx^2, cxy, cy^2\}$. By changing c if necessary, we may assume that $x^2, xy, y^2 \in \Lambda'$. Since $x^2 = x_1^2e_1^2 + 2x_1x_2e_1e_2 + x_2e_2^2$ is an element of Λ', we see that $x_1, x_2 \in \mathbb{Z}_2$. The same is true for y_1 and y_2, hence $M' := \mathbb{Z}_2 \cdot x \oplus \mathbb{Z}_2 \cdot y \subset V$ is a sublattice of M. Then a straightforward calculation shows that

$$\begin{aligned}
\#(\Lambda/\Lambda') &= \det \begin{pmatrix} cx_1^2 & cx_1y_1 & cy_1^2 \\ 2cx_1x_2 & cx_1y_2 + cx_2y_1 & 2cy_1y_2 \\ cx_2^2 & cy_2y_2 & cy_2^2 \end{pmatrix} \\
&= c^3(x_1y_2 - x_2y_1)^3 \\
&= c^3 \det \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}^3 \\
&= c^3\#(M/M')^3.
\end{aligned}$$

On the other hand, from the definition of Λ and Λ' we see $\#(\Lambda/\Lambda') = 2$. This is a contradiction as 2 is not a cube in $\mathbb{Q}_2$, hence Λ' cannot be pure. Since Λ is pure, we find that $N(\mathbb{Q}_2) \cdot \Lambda$ and $N(\mathbb{Q}_2) \cdot \Lambda'$ are two different elements of $\mathrm{Lat}_N(V)$ that have the same image in $\mathrm{Mod}(G)$.

Definition 7.11. Suppose G is a split reductive group with a split maximal torus T. In that case there is exactly one model $(\mathscr{G}, \mathscr{T})$ of (G, T) such that $\mathscr{G}$ is reductive (i.e. smooth with reductive fibres) and such that $\mathscr{T}$ is a split fibrewise maximal torus of $\mathscr{G}$, see [22, Exp. XXIII, Cor. 5.2; Exp. XXV, Cor. 1.2]. This model is called the *Chevalley model* of (G, T). We also refer to $\mathscr{G}$ as the Chevalley model of G.

7.1.3 Lattices in vector spaces over p-adic fields

Suppose K is a p-adic field, and let ω be a uniformiser of K. Let V like before be a finite dimensional K-vector space, and let Λ, Λ' be two lattices in V. Then there exist integers n, m such that $\omega^n\Lambda \subset \Lambda' \subset \omega^m\Lambda$. If we choose n minimal and m maximal, then we call $d(\Lambda, \Lambda') := n - m$ the *distance* between Λ and Λ'. Let G be an algebraic subgroup of $\mathtt{GL}(V)$, and as before let $\mathrm{Lat}_G(V) = G(K)\backslash\mathrm{Lat}(V)$. We define a function

$$\begin{aligned}
d_G \colon \mathrm{Lat}_G(V) \times \mathrm{Lat}_G(V) &\to \mathbb{R}_{\geq 0} \\
(X, Y) &\mapsto \min_{(\Lambda,\Lambda') \in X \times Y} d(\Lambda, \Lambda').
\end{aligned}$$

The following lemma tells us that the name 'distance' is justified. Its proof is straightforward and therefore omitted.

Lemma 7.12. *Let V and G be as above. Suppose G contains the scalars in* $\mathtt{GL}(V)$*.*

1. *Let $X, Y \in \mathrm{Lat}_G(V)$ and let $\Lambda \in X$. Then $d_G(X,Y) = \min_{\Lambda' \in Y} d(\Lambda, \Lambda')$.*
2. *The map d_G is a distance function on $\mathrm{Lat}_G(V)$.*
3. *For every $r \in \mathbb{R}_{\geq 0}$ and every $Y \in \mathrm{Lat}_G(V)$ the open ball*

$$\Big\{X \in \mathrm{Lat}_G(V) : d_G(X,Y) < r\Big\}$$

   is a finite set. □

7.2 Representations of split reductive groups

As before let K be a number field or a p-adic field. In this section we will briefly review the representation theory of split reductive groups over K. Furthermore, we will prove some results on the associated representation theory of Lie algebras. We will assume all representations to be finite dimensional.

Let G be a connected split reductive group over K, and let $T \subset G$ be a split maximal torus. Furthermore, we fix a Borel subgroup $B \subset G$ containing T. Let $\Psi \subset \mathrm{X}^*(T)$ be the set of roots of G with respect to T (see [42, Thm. 22.44]); let $Q \subset \mathrm{X}^*(T)$ be the subgroup generated by Ψ. Associated to B we have a basis Δ^+ of Ψ such that every $\beta \in \Psi$ can be written as $\beta = \sum_{\alpha \in \Delta^+} m_\alpha \alpha$, with the m_α either all nonpositive integers or all nonnegative integers. This gives a decomposition $\Psi = \Psi^+ \sqcup \Psi^-$. Accordingly, if $\mathfrak{g}$ and $\mathfrak{t}$ are the Lie algebras of G and T, respectively, we get

$$\mathfrak{g} = \mathfrak{t} \oplus \mathfrak{n}^+ \oplus \mathfrak{n}^- := \mathfrak{t} \oplus \left(\bigoplus_{\alpha \in \Psi^+} \mathfrak{g}_\alpha\right) \oplus \left(\bigoplus_{\alpha \in \Psi^-} \mathfrak{g}_\alpha\right).$$

The following theorem gives a description of the irreducible representations of G. If V is a representation of G, we call the characters of T that occur in V the *weights* of V (with respect to T).

Theorem 7.13. (See [42, Th. 24.3], [40, 3.39], and [5, Ch. VIII, §6.1, Prop. 1]) *Let V be an irreducible representation of G.*

1. *There is a unique weight ψ of V, called the* highest weight *of V, such that V_ψ has dimension 1, and every weight of V is of the form $\psi - \sum_{\alpha \in \Delta^+} m_\alpha \alpha$ for constants $m_\alpha \in \mathbb{Z}_{\geq 0}$.*
2. *V is irreducible as a representation of the Lie algebra $\mathfrak{g}$.*
3. *V is generated by the elements obtained by repeatedly applying $\mathfrak{n}^-$ to V_ψ.*
4. *Up to isomorphism V is the only irreducible representation of G with highest weight ψ.* □

Corollary 7.14 (Schur's lemma)**.** *Let V be an irreducible representation of G. Then the natural inclusion $K \hookrightarrow \mathrm{End}_G(V)$ is an isomorphism.*

Proof. Every endomorphism of V has to send V_ψ to itself. By point 3 we find that an endomorphism of V is determined by its action on V_ψ, hence this gives us an injective map $\mathrm{End}_G(V) \hookrightarrow \mathrm{End}_K(V_\psi) = K$; this map is an isomorphism since it is the inverse of the inclusion $K \hookrightarrow \mathrm{End}_G(V)$. □

Remark 7.15. With G as above, let V be any representation of G. Then, because G is reductive, we know that V is a direct sum of irreducible representations of G. By theorem 7.13.1 we can canonically write $V = \bigoplus_{\psi \in \mathcal{D}} V_{(\psi)}$, where for $\psi \in \mathrm{X}^*(T)$ the subspace $V_{(\psi)}$ is the isotypical component of V with highest weight ψ (as a character of T), and $\mathcal{D}$ is the set of highest weights occuring in V. Furthermore, we can decompose every $V_{(\psi)}$ into T-character spaces, and we get a decomposition

$$V = \bigoplus_{\psi \in \mathcal{D}} \bigoplus_{\chi \in \mathrm{X}^*(T)} V_{(\psi),\chi}.$$

Let $U(\mathfrak{g})$ be the universal enveloping algebra of $\mathfrak{g}$. It obtains a Q-grading coming from the Q-grading of $\mathfrak{g}$; we may also regard this as a $\mathrm{X}^*(T)$-grading via the inclusion $Q \subset \mathrm{X}^*(T)$. If V is a representation of G, then the associated map $U(\mathfrak{g}) \to \mathrm{End}(V)$ is a homomorphism of $\mathrm{X}^*(T)$-graded K-algebras. Furthermore, from the Poincaré–Birkhoff–Witt theorem (see [24, 17.3, Cor. C]) it follows that there is a natural isomorphism of Q-graded K-algebras $U(\mathfrak{g}) \cong U(\mathfrak{n}^-) \otimes U(\mathfrak{t}) \otimes U(\mathfrak{n}^+)$, with the map from right to left given by multiplication. The following two results will be useful in the next section.

Theorem 7.16 (Jacobson density theorem)**.** *Let G be a split reductive group, and let $\mathfrak{g}$ be its Lie algebra. Let $V_1, \ldots, V_n$ be pairwise nonisomorphic irreducible representations of G. Then the induced map $U(\mathfrak{g}) \to \bigoplus_i \mathrm{End}(V_i)$ is surjective.*

Proof. This theorem is proven over algebraically closed fields in [17, Thm. 2.5] for representations of algebras in general (not just for universal enveloping algebras of Lie algebras). The hypothesis that K is algebraically closed is only used in invoking Schur's lemma, but this also holds in our situation, see corollary 7.14. □

Proposition 7.17. *Let V be an irreducible representation of G of highest weight ψ. Let χ be a weight of V. Then the maps*

$$U(\mathfrak{n}^-)_{\chi-\psi} \to \mathrm{Hom}_K(V_\psi, V_\chi),$$
$$U(\mathfrak{n}^+)_{\psi-\chi} \to \mathrm{Hom}_K(V_\chi, V_\psi)$$

are surjective.

Proof. From theorem 7.13.3 we know that $V = U(\mathfrak{n}^-) \cdot V_\psi$. Since $U(\mathfrak{n}^-) \to \mathrm{End}(V)$ is a homomorphism of $\mathrm{X}^*(T)$-graded K-algebras, this implies that $V_\chi = U(\mathfrak{n}^-)_{\chi-\psi} \cdot V_\psi$. Since

V_ψ is one-dimensional by theorem 7.13.1 this shows that $U(\mathfrak{n}^-)_{\chi-\psi} \to \mathrm{Hom}_K(V_\psi, V_\chi)$ is surjective.

For the surjectivity of the second map, let $f\colon V_\chi \to V_\psi$ be a linear map, and extend f to a map $\tilde{f}\colon V \to V$ by letting $\tilde{f}$ be trivial on all $V_{\chi'}$ with $\chi' \neq \chi$. Then $\tilde{f}$ is pure of degree $\psi-\chi$, and $\psi-\chi \in Q$ by theorem 7.13.1. By theorem 7.16 there exists a $u \in U(\mathfrak{g})_{\psi-\chi}$ such that the image of u in $\mathrm{End}(V)$ equals $\tilde{f}$. We know that $U(\mathfrak{g})$ is isomorphic to $U(\mathfrak{n}^-)\otimes U(\mathfrak{t})\otimes U(\mathfrak{n}^+)$; write $u = \sum_{i\in I} u_i^- \cdot t_i \cdot u_i^+$ with each u_i^-, t_i and u_i^+ of pure degree, such that each $u_i^- \cdot t_i \cdot u_i^+$ is of degree $\psi-\chi$. Let I' be the subset of I of the i for which u_i^+ is of degree $\psi-\chi$. Since only negative degrees (i.e. sums of nonpositive multiples of elements of Δ^+) occur in $U(\mathfrak{n}^-)$ and only degree 0 occurs in $U(\mathfrak{t})$, this means that u_i^- is of degree 0 for $i \in I'$; hence for these i the element u_i^- is a scalar. Now consider the action of u on V_χ. If $i \notin I'$, then the degree of u_i^+ will be greater than $\psi - \chi$, in which case we will have $u_i^+ \cdot V_\chi = 0$. For all $v \in V_\chi$ we now have

$$\begin{aligned}
\tilde{f}(v) &= u \cdot v \\
&= \left(\sum_{i\in I} u_i^- \cdot t_i \cdot u_i^+\right) \cdot v \\
&= \left(\sum_{i\in I'} u_i^- \cdot t_i \cdot u_i^+\right) \cdot v \\
&= \sum_{i\in I'} u_i^- \cdot t_i \cdot (u_i^+ \cdot v) \\
&= \sum_{i\in I'} u_i^- \psi(t_i)(u_i^+ \cdot v) \\
&= \left(\sum_{i\in I'} u_i^- \psi(t_i) u_i^+\right) \cdot v.
\end{aligned}$$

Because every factor u_i^- in this sum is a scalar, we know that $\sum_{i\in I'} u_i^- \psi(t_i) u_i^+$ is an element of $U(\mathfrak{n}^+)_{\chi-\psi}$, and it acts on V_χ as the map $f \in \mathrm{Hom}_K(V_\chi, V_\psi)$; hence the map $U(\mathfrak{n}^+)_{\psi-\chi} \to \mathrm{Hom}_K(V_\chi, V_\psi)$ is surjective. □

7.3 Split reductive groups over local fields

Throughout the rest of this chapter K is either a number field or a p-adic field, and R is its ring of integers. All representations of algebraic groups are assumed to be finite dimensional. The aim of this section is to prove the following theorem.

Theorem 7.18. *Let G be a split connected reductive group over K, and let V be a faithful representation of G. Regard G as a subgroup of $\mathrm{GL}(V)$, and let N be the scheme-theoretic normaliser of G in $\mathrm{GL}(V)$.*

1. *Suppose K is a p-adic field. Then the map $\mathtt{mod}_G \colon \mathrm{Lat}_N(V) \to \mathrm{Mod}(G)$ of lemma 7.5 is finite.*
2. *Suppose K is a number field. Then for all but finitely many finite places v of K there is at most one $N(K_v)$-orbit X of lattices in V_{K_v} such that $\mathtt{mod}_G(X)$ is the Chevalley model of G (see definition 7.11).*

The first point of this theorem is theorem 7.1 for split reductive groups over local fields. The second point is quite technical by itself, but we need this finiteness result to prove theorem 7.1 for number fields. Before we prove this theorem we will need to develop some theory of integral structures in representations of split reductive groups.

7.3.1 Lattices in representations

In this section we will introduce two important classes of lattices that occur in representations of split reductive groups. We will rely on much of the results and notations from section 7.2.

Notation 7.19. For the rest of this section, we fix the following objects and notation:

- a split connected reductive group G over K and a split maximal torus $T \subset G$;
- the Lie algebras $\mathfrak{g}$ and $\mathfrak{t}$ of G and T, respectively;
- the root system $\Psi \subset \mathrm{X}^*(T)$ of G with respect to T, and the subgroup Q of $\mathrm{X}^*(T)$ generated by Ψ;
- the image $\bar{T}$ of T in $G^{\mathrm{ad}} \subset \mathtt{GL}(\mathfrak{g})$;
- the decomposition $\mathfrak{g} = \mathfrak{t} \oplus \bigoplus_{\alpha \in \Psi} \mathfrak{g}_\alpha$;
- the basis of positive roots Δ^+ of Ψ associated to some Borel subgroup B of G containing T, the decompositions $\Psi = \Psi^+ \sqcup \Psi^-$ and $\mathfrak{g} = \mathfrak{t} \oplus \mathfrak{n}^+ \oplus \mathfrak{n}^-$;
- the Q-graded universal enveloping algebra $U(\mathfrak{g})$ of $\mathfrak{g}$;
- a faithful representation V of G and its associated inclusion $\mathfrak{g} \subset \mathfrak{gl}(V)$;
- the centraliser Z of G in $\mathtt{GL}(V)$, and the group $H = Z \cdot T \subset \mathtt{GL}(V)$;
- the decomposition $V = \bigoplus_{\psi \in \mathcal{D}} \bigoplus_{\chi \in \mathrm{X}^*(T)} V_{(\psi),\chi}$ (see remark 7.15);
- the projections $\mathrm{pr}_{(\psi),\chi} \colon V \to V_{(\psi),\chi}$ associated to the decomposition above.

Remark 7.20.

1. Since the set of characters of T that occur in the adjoint representation is equal to $\{0\} \cup \Psi$, the inclusion $\mathrm{X}^*(\bar{T}) \hookrightarrow \mathrm{X}^*(T)$ has image Q.

2. By corollary 7.14 the induced map $Z \to \prod_{\psi \in \mathcal{D}} \mathtt{GL}(V_{(\psi),\psi})$ is an isomorphism.

Definition 7.21. Let W be a K-vector space with a decomposition $W = \bigoplus_i W_i$. An R-submodule $M \subset V$ is called *split* with respect to this decomposition if one of the following equivalent conditions is satisfied:

1. $M = \bigoplus_i \mathrm{pr}_i M$;
2. $M = \bigoplus_i (W_i \cap M)$.

If M is split, we write $M_i := \mathrm{pr}_i M = W_i \cap M$.

We now define two classes of lattices that will become important later on. Since the Lie algebra $\mathfrak{g}$ is a K-vector space, we can consider lattices in $\mathfrak{g}$. For a vector space W over K, let $\mathrm{FLat}(W)$ be the set of lattices in W that are free as R-modules. Define the following sets:

$$\begin{aligned} \mathcal{L}^+ &:= \prod_{\alpha \in \Delta^+} \mathrm{FLat}(\mathfrak{g}_\alpha); \\ \mathcal{L}^- &:= \prod_{\alpha \in \Delta^+} \mathrm{FLat}(\mathfrak{g}_{-\alpha}); \\ \mathcal{J} &:= \prod_{\psi \in \mathcal{D}} \mathrm{FLat}(V_{(\psi),\psi}). \end{aligned}$$

As before, let $U(\mathfrak{n}^+)$ be the universal enveloping algebra of $\mathfrak{n}^+$. Let $L^+ = (L^+_\alpha)_{\alpha \in \Delta^+}$ be an element of $\mathcal{L}^+$, and let $\mathscr{U}_{L^+}$ be the R-subalgebra of $U(\mathfrak{n}^+)$ generated by the R-submodules $L^+_\alpha \subset \mathfrak{n}^+$. Define, for an $L^- \in \mathcal{L}^-$, the R-subalgebra $\mathscr{U}_{L^-} \subset U(\mathfrak{n}^-)$ analogously. Now let $L^+ \in \mathcal{L}^+$, $L^- \in \mathcal{L}^-$ and $J \in \mathcal{J}$ be as above. We define the following two R-submodules of V:

$$\begin{aligned} S^+(L^+, J) &:= \Big\{ x \in V : \mathrm{pr}_{(\psi),\psi}(\mathscr{U}_{L^+} \cdot x) \subset J_\psi \ \ \forall \psi \in \mathcal{D} \Big\}, \\ S^-(L^-, J) &:= \sum_{\psi \in \mathcal{D}} \mathscr{U}_{L^-} \cdot J_\psi \subset V. \end{aligned}$$

Note that the sum in the second equation is actually direct, since $\mathscr{U}_{L^-} \cdot J_\psi \subset V_{(\psi)}$ for all $\psi \in \mathcal{D}$. In the next proposition we use the symbol $\pm$ for statements that hold both for $+$ and $-$.

Proposition 7.22. *Let $L^+ \in \mathcal{L}^+$, $L^- \in \mathcal{L}^-$ and $J = (J_\psi)_{\psi \in \mathcal{D}}$.*

1. *$\mathscr{U}_{L^\pm}$ is a split lattice in $U(\mathfrak{n}^\pm)$ with respect to the Q-grading.*
2. *$S^\pm(L^\pm, J)$ is a split lattice in V with respect to the decomposition $V = \bigoplus_{\psi,\chi} V_{(\psi),\chi}$.*
3. *For all $\psi \in \mathcal{D}$ and all $\chi < \psi$ one has $S^\pm(L^\pm, J)_{(\psi),\psi} = J_\psi$. Furthermore, $S^+(L^+, J)$ (respectively $S^-(L^-, J)$) is the maximal (respectively minimal) split lattice Λ in V closed under the action of the L^+_α (respectively the L^-_α) such that $\Lambda_{(\psi),\psi} = J_\psi$ for all $\psi \in \mathcal{D}$.*

Proof.

1. It suffices to prove this for $\mathscr{U}_{L^+}$. Recall that $U(\mathfrak{n}^+)$ has a Q-grading coming from the Q-grading on $U(\mathfrak{g})$. Since $\mathscr{U}_{L^+}$ is generated by elements of pure degree, we see that $\mathscr{U}_{L^+}$ is split with respect to the Q-grading; hence it suffices to show that $\mathscr{U}_{L^+,\chi}$ is a lattice in $U(\mathfrak{n}^+)_\chi$ for all χ. Since each $\mathfrak{g}_\alpha$ is one-dimensional, the R-module L^+_α is free of rank 1; let x_α be a generator. Then the R-module $\mathscr{U}_{L^+,\chi}$ is generated by the finite set
$$\Big\{x_{\alpha_1}\cdot x_{\alpha_2}\cdots x_{\alpha_k} : k\in\mathbb{Z}_{\geq 0}, \sum_i \alpha_i = \chi\Big\}.$$
On the other hand, the Poincaré–Birkhoff–Witt theorem (see [24, 17.3, Cor. C]) tells us that the K-vector space $U(\mathfrak{n}^+)_\chi$ is also generated by this set; hence $\mathscr{U}_{L^+,\chi}$ is a lattice in $U(\mathfrak{n}^+)_\chi$, as was to be shown.

2. We start with $S^-(L^-,J)$. Since the action of $U(\mathfrak{n}^-)_\chi$ sends $V_{(\psi),\chi'}$ to $V_{(\psi),\chi+\chi'}$, we see that
$$S^-(L^-,J) = \bigoplus_{\psi\in\mathcal{D}}\bigoplus_{\chi\in Q}\mathscr{U}_{L^-,\chi}\cdot J_\psi = \bigoplus_{\psi\in\mathcal{D}}\bigoplus_{\chi\in Q} S^-(L^-,J)\cap V_{(\psi),\psi+\chi},$$
hence $S^-(L^-,J)$ is split. Since $\mathscr{U}_{L^-,\chi}$ is a finitely generated R-module spanning $U(\mathfrak{n}^-)_\chi$, and J^-_ψ is a finitely generated R-module spanning $V_{(\psi),\psi}$, we may conclude that $\mathscr{U}_{L^-,\chi}\cdot J^-_\psi$ is a finitely generated R-module spanning $U(\mathfrak{n}^-)_\chi\cdot V_{(\psi),\psi}$, which is equal to $V_{(\psi),\psi+\chi}$ by proposition 7.17. Hence $S^-(L^-,J)_{(\psi),\psi+\chi}$ is a lattice in $V_{(\psi),\psi+\chi}$, and since $S^-(L^-,J)$ is split this shows that it is a lattice in V.

   Now consider $S^+(L^+,J)$. Let $x\in V$, and write $x=\sum_{\psi,\chi}x_{(\psi),\chi}$ where every $x_{(\psi),\chi}$ is an element of $V_{(\psi),\chi}$. Then for every $\psi\in\mathcal{D}$ we have
$$\mathrm{pr}_{(\psi),\psi}(\mathscr{U}_{L^+}\cdot x) = \sum_{\chi\in Q}\mathrm{pr}_{(\psi),\psi}(\mathscr{U}_{L^+,\chi}\cdot x) = \sum_{\chi\in Q}\mathscr{U}_{L^+,\chi}\cdot x_{(\psi),\psi-\chi},$$
hence x is an element of $S^+(L^+,J)$ if and only if $x_{(\psi),\chi}$ is for all $\psi\in\mathcal{D}$ and all $\chi\in \mathrm{X}^*(T)$; this shows that $S^+(L^+,J)$ is split with respect to the decomposition $V=\bigoplus_{\psi,\chi}V_{(\psi),\chi}$. We now need to show that $S^+(L^+,J)_{(\psi),\chi}$ is a lattice in $V_{(\psi),\chi}$. Fix a χ and ψ, and choose a basis $f_1,\ldots,f_k$ of J_ψ; then $W_i := U(\mathfrak{g})\cdot f_i$ is an irreducible subrepresentation of $V_{(\psi)}$. We get a decomposition $V_{(\psi),\chi}=\bigoplus_i W_{i,\chi}$, and from the definition of $S^+(L^+,J)$ we get
$$S^+(L^+,J)_{(\psi),\chi} = \bigoplus_i S^+(L^+,J)_{(\psi),\chi}\cap W_{i,\chi},$$
so we need to show that for each i the R-module $S_{i,\chi} := S^+(L^+,J)_{(\psi),\chi}\cap W_{i,\chi}$ is a lattice in $W_{i,\chi}$. Fix an i, and let $e_1,\ldots,e_n$ be a basis of $W_{i,\chi}$. For $j\leq n$, let $\varphi_j\colon W_{i,\chi}\to W_{i,\psi}=K\cdot f_i$ be the linear map that sends e_j to f_i, and the other

$e_{j'}$ to 0. By proposition 7.17 there exists a $u_j \in U(\mathfrak{n}^+)$ such that u_j acts like φ_j on $W_{i,\chi}$. Since $\mathscr{U}_{L^+}$ is a lattice in $U(\mathfrak{n}^+)$ there exists a $r \in R$ such that $ru_j \in \mathscr{U}_{L^+}$ for all j. Then for all $x \in S_{i,\chi}$ one has $ru_j \cdot x \in Rf_i$ for all j, so x lies in the free R-submodule of $W_{i,\chi}$ generated by $r^{-1}e_1, \ldots, r^{-1}e_n$; hence $S_{i,\chi}$ is finitely generated. On the other hand, since $\mathscr{U}_{L^+,\psi-\chi}$ is finitely generated, for every $x \in W_{i,\chi}$ we get that $\mathscr{U}_{L^+,\psi-\chi} \cdot x$ is a lattice in $W_{i,\psi}$. As such we can find some $r' \in R$ such that $\mathscr{U}_{L^+,\psi-\chi} \cdot r'x \subset R \cdot f_i$; hence $S^+(L^+, J)_{(\psi),\chi,i}$ generates $W_{i,\chi}$ as a K-vector space, so $S_{i,\chi}$ is a lattice in $W_{i,\chi}$, as was to be shown.

3. Since $\mathscr{U}_{L^+,0} = \mathscr{U}_{L^-,0} = R$ we immediately get $S^+(L^+, J)_{(\psi),\psi} = J_\psi$ for all ψ. The other statement follows immediately from the definition of the modules $S^+(L^+, J)$ and $S^-(L^-, J)$. □

Remark 7.23. By proposition 7.22 we can define maps $S^\pm \colon \mathcal{L}^\pm \times \mathcal{J} \to \mathrm{Lat}(V)$.

Let $H = Z \cdot T$ as before. Since H normalises G, we see that H acts on G by conjugation. This gives us a representation $\varrho\colon H \to \mathtt{GL}(\mathfrak{g})$. Since Z acts trivially on G, we see that the image of H in $\mathtt{GL}(\mathfrak{g})$ is equal to $\bar{T}$. As such we see that the action of H on $\mathfrak{g}$ respects the decomposition $\mathfrak{g} = \mathfrak{t} \oplus \bigoplus_{\alpha \in \Psi} \mathfrak{g}_\alpha$.

Lemma 7.24. *The map $\varrho\colon H \twoheadrightarrow \bar{T}$ is surjective on K-points.*

Proof. The short exact sequence $1 \to Z \to H \to \bar{T} \to 1$ of algebraic groups induces a longer exact sequence of groups

$$1 \to Z(K) \to H(K) \to \bar{T}(K) \to \mathrm{H}^1(K, Z).$$

Since $\mathrm{H}^1(K, \mathtt{GL}_n)$ is trivial for every integer n and Z is isomorphic to a product of $\mathtt{GL}_n$s by remark 7.20.2, this implies that the map $H(K) \to \bar{T}(K)$ is surjective. □

Since the action of H on $\mathfrak{g}$ respects its decomposition into root spaces, we get an action of $H(K)$ on the sets $\mathcal{L}^\pm$. Furthermore, the representation $H \hookrightarrow \mathtt{GL}(V)$ respects the decomposition $V = \bigoplus_{\psi \in \mathcal{D}} V_{(\psi)}$. Since H centralises T, the action of H also respects the decomposition $V_{(\psi)} = \bigoplus_{\chi \in \mathrm{X}^*(T)} V_{(\psi),\chi}$; hence $H(K)$ acts on the set $\mathcal{J}$.

Proposition 7.25. *The maps $S^\pm \colon \mathcal{L}^\pm \times \mathcal{J} \to \mathrm{Lat}(V)$ are $H(K)$-equivariant, and the action of $H(K)$ on $\mathcal{L}^\pm \times \mathcal{J}$ is transitive.*

Proof. The Lie algebra action map $\mathfrak{g} \times V \to V$ is equivariant with respect to the action of $H(K)$ on both sides. From the definition of $S^\pm(L^\pm, J)$ it now follows that

$$S^\pm(h \cdot L^\pm, h \cdot J) = h \cdot S^\pm(L^\pm, J)$$

for all $h \in H(K)$. Now let $L_1^+, L_2^+ \in \mathcal{L}^+$ and $J_1, J_2 \in \mathcal{J}$. For every $\alpha \in \Delta^+$, let $x_\alpha \in K^\times$ be such that $L_{1,\alpha}^+ = x_\alpha L_{2,\alpha}^+$; the scalar x_α exists because $L_{1,\alpha}^+$ and $L_{2,\alpha}^+$ are free lattices in the same one-dimensional vector space. Since Δ^+ is a basis for $Q = \mathrm{X}^*(\bar{T})$ (see remark 7.20.1) there exists a unique $t \in \bar{T}(K)$ such that $\alpha(t) = x_\alpha$ for all $\alpha \in \Delta^+$. By lemma

7.24 there exists an $h \in H(K)$ such that $\varrho(h) = t$; then $h \cdot L_1^+ = L_2^+$. Since $Z(K)$ acts transitively on $\mathcal{J}$ by remark 7.20.2, there exists a $z \in Z(K)$ such that $z \cdot (h \cdot J_1) = J_2$. As z acts trivially on $\mathcal{L}^+$, we get $zh \cdot (L_1^+, J_1) = (L_2^+, J_2)$; this shows that $H(K)$ acts transitively on $\mathcal{L}^+ \times \mathcal{J}$. The proof for $\mathcal{L}^-$ is analogous. □

7.3.2 Chevalley lattices

In this subsection we consider lattices in the K-vector space $\mathfrak{g}$. We will define the set of Chevalley lattices in $\mathfrak{g}$. The distance (in the sense of lemma 7.12) between such a Chevalley lattice and the Lie algebra of a model of (G, T) (as lattices in $\mathfrak{g}$) will serve as a good measure of the 'ugliness' of the model, and this will allow us to prove finiteness results. We keep employing notation 7.19.

Let G^{der} be the derived group of G, and let T' be the identity component of $T \cap G^{\mathrm{der}}$. Let $\mathfrak{g}^{\mathrm{ss}}$ and $\mathfrak{t}'$ be the Lie algebras of G^{der} and T', respectively. The roots of G (with respect to T) induce linear maps $\mathrm{Lie}(\alpha)\colon \mathfrak{t}' \to K$, and these form the root system of the split semisimple Lie algebra $(\mathfrak{g}^{\mathrm{ss}}, \mathfrak{t}')$ in the sense of [5, Ch. VIII, §2]. Since the Killing form κ on $\mathfrak{t}'$ is nondegenerate by [24, Thm. 5.1] there exists a unique $t_\alpha \in \mathfrak{t}'$ such that $\kappa(t_\alpha, -) = \mathrm{Lie}(\alpha)$. Since $\kappa(t_\alpha, t_\alpha) \neq 0$ we may define $h_\alpha := \frac{2}{\kappa(t_\alpha, t_\alpha)} t_\alpha$; see [24, Prop. 8.3].

Definition 7.26. An element $x = (x_\alpha)_{\alpha \in \Psi}$ of $\prod_{\alpha \in \Psi} (\mathfrak{g}_\alpha \setminus \{0\})$ is called a *Chevalley set* if the following conditions are satisfied:

1. $[x_\alpha, x_{-\alpha}] = h_\alpha$ for all $\alpha \in \Psi$;
2. If α and β are two $\mathbb{R}$-linearly independent roots such that $\beta + \mathbb{Z}\alpha$ intersects Ψ in the elements $\beta - r\alpha, \beta - (r-1)\alpha, \ldots, \beta + q\alpha$, then $[x_\alpha, x_\beta] = 0$ if $q = 0$, and $[x_\alpha, x_\beta] = \pm(r+1) x_{\alpha+\beta}$ if $q > 0$.

There is a canonical isomorphism of K-vector spaces:

$$\begin{array}{rcl} K \otimes_{\mathbb{Z}} \mathrm{X}^*(T) & \xrightarrow{\sim} & \mathfrak{t}^\vee \\ 1 \otimes \alpha & \mapsto & \mathrm{Lie}(\alpha). \end{array}$$

Under this isomorphism, we can consider $\mathfrak{T}_0 := (R \otimes_{\mathbb{Z}} \mathrm{X}^*(T))^\vee$ as an R-submodule of the K-vector space $\mathfrak{t}$.

Lemma 7.27. *Let $\alpha \in \Phi$. Then $h_\alpha \in \mathfrak{T}_0$.*

Proof. It suffices to show that $\mathrm{Lie}(\lambda)(h_\alpha) \in \mathbb{Z}$ for all $\lambda \in \mathrm{X}^*(T)$. Since the action of $\lambda \in \mathrm{X}^*(T)$ on $\mathfrak{t}'$ only depends on its image in $\mathrm{X}^*(T')$, it suffices to prove this for semisimple G; this was done in in [25, 31.1]. □

Definition 7.28. A *Chevalley lattice* is an R-submodule of $\mathfrak{g}$ of the form

$$\mathfrak{C}(x) = \mathfrak{T}_0 \oplus \bigoplus_{\alpha \in \Psi} R \cdot x_\alpha,$$

where x is a Chevalley set. The set of Chevalley lattices is denoted $\mathcal{C}$.

Remark 7.29. It is clear that $\mathfrak{C}(x)$ is a finitely generated R-submodule of $\mathfrak{g}$ that generates $\mathfrak{g}$ as a K-vector space, hence it is indeed a lattice. The name comes from the fact that if G is adjoint, then $\{h_\alpha\}_{\alpha\in\Delta^+} \cup \{x_\alpha : \alpha \in \Psi\}$ is a *Chevalley basis* of $\mathfrak{g}$ in the sense of [24, Section 25.2], and the Lie algebra of the Chevalley model (for any anchoring of φ) is a Chevalley lattice in $\mathfrak{g}$ (see definition 7.11).

Lemma 7.30. *Let* $\mathrm{Aut}(G,T) := \{\sigma \in \mathrm{Aut}(G) : \sigma(T) = T\}$.

1. *There exists a Chevalley lattice in* $\mathfrak{g}$.
2. *Every Chevalley lattice is an* R*-Lie subalgebra of* $\mathfrak{g}$.
3. *Let* $\sigma \in \mathrm{Aut}(G,T)$*, and let* $\mathfrak{C} \in \mathcal{C}$*. Then the lattice* $\sigma(\mathfrak{C}) \subset \mathfrak{g}$ *is again a Chevalley lattice.*

Proof.

1. It suffices to show that a Chevalley set exists, for which we refer to [24, Thm. 25.2].
2. By definition we have $[x_\alpha, x_{-\alpha}] \in \mathfrak{T}_0$ and $[x_\alpha, x_\beta] \in R\cdot x_{\alpha+\beta}$ if $\alpha+\beta\neq 0$. Furthermore for $t \in \mathfrak{T}_0$ one has $[t, x_\alpha] = \mathrm{Lie}(\alpha)(t)\cdot x_\alpha \in R\cdot x_\alpha$ by definition of $\mathfrak{T}_0$.
3. The automorphism $\sigma \in \mathrm{Aut}(G,T)$ induces an automorphism $\bar\sigma$ of Ψ. Then σ maps $\mathfrak{g}_\alpha$ to $\mathfrak{g}_{\bar\sigma(\alpha)}$ and $\mathfrak{T}_0$ to $\mathfrak{T}_0$. Let x be a Chevalley set such that $\mathfrak{C} = \mathfrak{C}(x)$, and define $x' = (x'_\alpha)_{\alpha\in\Psi}$ by $x'_\alpha = \sigma(x_{\bar\sigma^{-1}(\alpha)})$. Since $\sigma(h_\alpha) = h_{\bar\sigma(\alpha)}$ this is again a Chevalley set, and $\sigma(\mathfrak{C}) = \mathfrak{C}(x')$. ☐

It is easily checked that the action of $H(K)$ on $\mathrm{Lat}(\mathfrak{g})$ sends the subset $\mathcal{C}$ to itself. Furthermore there are natural isomorphisms of $H(K)$-sets

$$f^\pm : \mathcal{C} \xrightarrow{\sim} \mathcal{L}^\pm \qquad (7.31)$$
$$\mathfrak{C} \mapsto (\mathfrak{C} \cap \mathfrak{g}_{\pm\alpha})_{\alpha\in\Delta^+}.$$

Since the action of $H(K)$ on $\mathcal{L}^\pm$ is transitive, we have shown:

Lemma 7.32. *The action of* $H(K)$ *on* $\mathcal{C}$ *is transitive.* ☐

Lemma 7.33. *Let* $\mathfrak{C} \in \mathcal{C}$ *be a Chevalley lattice and let* $\mathscr{U}_\mathfrak{C}$ *be the* R*-subalgebra of* $U(\mathfrak{g})$ *generated by* $\mathfrak{C}$*. Then* $\mathscr{U}_\mathfrak{C}$ *is split with respect to the* Q*-grading of* $U(\mathfrak{g})$*. The subalgebra* $\mathscr{U}_{\mathfrak{C},0} \subset U(\mathfrak{g})_0$ *does not depend on the choice of* $\mathfrak{C}$*.*

Proof. The fact that $\mathscr{U}_\mathfrak{C}$ is split follows from the fact that it is generated by elements of pure degree. Now let $\mathfrak{C}, \mathfrak{C}' \in \mathcal{C}$. Since $H(K)$ acts transitively on $\mathcal{C}$ and the action of H on $\mathcal{C}$ factors through $\bar T$, there exists a $t \in \bar T(K)$ such that $t\cdot\mathfrak{C} = \mathfrak{C}'$. Then $\mathscr{U}_{\mathfrak{C}'} = t\cdot\mathscr{U}_\mathfrak{C}$, where t acts on $U(\mathfrak{g})$ according to its Q-grading. In particular this shows that $\mathscr{U}_{\mathfrak{C},0} = \mathscr{U}_{\mathfrak{C},0}$. ☐

Lemma 7.34. *There exists an* $r \in R$ *such that for every Chevalley lattice* $\mathfrak{C}$*, every* $\psi \in \mathcal{D}$ *and every* $\chi \in \mathrm{X}^*(T)$*, the endomorphism* $r\cdot\mathrm{pr}_{(\psi),\chi}$ *of* V *lies in the image of the map* $\mathscr{U}_\mathfrak{C} \to \mathrm{End}(V)$*.*

Proof. Fix a $\psi_0 \in \mathcal{D}$ and a $\chi \in \mathrm{X}^*(T)$. For every $\psi \in \mathcal{D}$, let $W(\psi)$ be the irreducible representation of G of highest weight ψ. Let $f_{\psi_0,\chi} \in \bigoplus_{\psi \in \mathcal{D}} \mathrm{End}(W(\psi))$ be the element whose ψ_0-component is pr_χ and whose other components are 0. By theorem 7.16 there exists a $u_{\psi_0,\chi} \in U(\mathfrak{g})_0$ that acts as $f_{\psi_0,\chi}$ on $\bigoplus_{\psi \in \mathcal{D}} W(\psi)$; then $u_{\psi_0,\chi}$ acts as $\mathrm{pr}_{(\psi),\chi}$ on V. Let $\mathfrak{C}$ be a Chevalley lattice, and let $r \in R$ be such that $ru_{\psi_0,\chi} \in \mathscr{U}_{\mathfrak{C},0}$ for all $\psi_0 \in \mathcal{D}$ and all χ for which $V_{(\psi_0),\chi} \neq 0$. Then r satisfies the properties of the lemma for $\mathfrak{C}$. By Lemma 7.33 the element r works regardless of the choice of $\mathfrak{C}$, which proves the lemma. □

7.3.3 Chevalley-invariant lattices

In this section we consider lattices in V that are invariant under some Chevalley lattice in $\mathfrak{g}$. The main result is that up to $H(K)$-action only finitely many such lattices exist. As before we keep employing notation 7.19.

Definition 7.35. Let Λ be a lattice in V. We call Λ *Chevalley-invariant* if there exists a Chevalley lattice $\mathfrak{C} \subset \mathfrak{g}$ such that $\mathfrak{C} \cdot \Lambda \subset \Lambda$.

Lemma 7.36. *There exists a Chevalley-invariant lattice in V.*

Proof. This is proven for $K = \mathbb{Q}$ in [5, Ch. VIII, §12.8, Thm. 4]; note that for a Chevalley lattice $\mathfrak{C}$ the lattice $\mathfrak{C} \cap \mathfrak{t} = \mathfrak{T}_0$ is a *reseau permis* in the sense of [5, Ch. VIII, §12.6, Def. 1]. The proof given there also works for general K. Alternatively, one can use the classification of split reductive Lie algebras in [5, Ch. VIII, §4.3, Thm. 1 & §4.4, Thm. 1] and their representations in [5, Ch. VIII, §7.2, Thm. 1] to construct a model of the representation $\mathfrak{g} \hookrightarrow \mathfrak{gl}(V)$ over $\mathbb{Q}$, and use a Chevalley-invariant lattice in this model to obtain one in the original setting. □

Lemma 7.37. *The set of Chevalley-invariant lattices is invariant under the action of $H(K)$ on V.*

Proof. If Λ is closed under multiplication by a Chevalley lattice $\mathfrak{C}$ and h is an element of $H(K)$, then $h \cdot \Lambda$ is closed under multiplication by $h \cdot \mathfrak{C}$; hence this follows from lemma 7.32. □

Remark 7.38. Since $H(K)$ acts transitively on the set of Chevalley lattices, we see that for every Chevalley lattice $\mathfrak{C}$ there is a lattice in V closed under multiplication by $\mathfrak{C}$.

Lemma 7.39. *Let $\mathfrak{C}_0$ be a Chevalley lattice in $\mathfrak{g}$, and let $J_0 \in \mathcal{J}$. Let $L_0^+ = f^+(\mathfrak{C}_0)$ and $L_0^- = f^-(\mathfrak{C}_0)$ (see (7.31)). Let $\Lambda \subset V$ be a split Chevalley-invariant lattice such that $\Lambda_{(\psi),\psi}$ is a free R-module for all $\psi \in \mathcal{D}$. Then there exists an $h \in H(K)$ such that*

$$S^-(L_0^-, J_0) \subset h \cdot \Lambda \subset S^+(L_0^+, J_0).$$

Proof. Let $\mathfrak{C}$ be a Chevalley lattice in $\mathfrak{g}$ such that $\mathfrak{C} \cdot \Lambda \subset \Lambda$. Let $J = (\Lambda_{(\psi),\psi})_{\psi \in \mathcal{D}}$; by assumption it is an element of $\mathcal{J}$. Since $\mathcal{C}$ is isomorphic to $\mathcal{L}^+$ as $H(K)$-sets, by proposition 7.25 there exists an $h \in H(K)$ such that $h \cdot \mathfrak{C} = \mathfrak{C}_0$ and $h \cdot J = J_0$. Now let $\Lambda_0 = h \cdot \Lambda$; this is a split lattice satisfying $(\Lambda_0)_{(\psi),\psi} = J_{0,\psi}$ for all ψ. Furthermore, the lattice Λ_0 is closed under multiplication by Chevalley lattice $\mathfrak{C}_0$; in particular it is closed under the action of the $f^+(\mathfrak{C}_0)_\alpha = \mathfrak{C}_0 \cap \mathfrak{g}_\alpha$ and the $f^-(\mathfrak{C}_0)_\alpha = \mathfrak{C}_0 \cap \mathfrak{g}_{-\alpha}$, where $f^\pm$ is as in subsection 7.3.2. By proposition 7.22.3 we now get

$$S^-(L_0^-, J_0) \subset \Lambda_0 \subset S^+(L_0^+, J_0).$$

□

Proposition 7.40. *Suppose K is a p-adic field. Then there are only finitely many $H(K)$-orbits of Chevalley-invariant lattices.*

Proof. Let $\mathfrak{C}_0$, J_0, L_0^+ and L_0^- be as in the previous lemma. Let ω be a uniformiser of K. Let $m \in \mathbb{Z}_{\geq 0}$ be such that $\omega^m S^+(L_0^+, J_0) \subset S^-(L_0^-, J_0)$, and let $n \in \mathbb{Z}_{\geq 0}$ be such that for every Chevalley lattice $\mathfrak{C}$, every $\psi \in \mathcal{D}$ and every $\chi \in \mathrm{X}^*(T)$ the endomorphism $\omega^n \mathrm{pr}_{(\psi),\chi} \in \mathrm{End}(V)$ lies in the image of $\mathscr{U}_{\mathfrak{C}}$; such an n exists by lemma 7.34. Let P^+ be the $H(K)$-orbit of lattices of the form $S^+(L^+, J)$ (see proposition 7.25). Let X be an $H(K)$-orbit of Chevalley-invariant lattices. Let Λ be an element of X, and let $\mathfrak{C}$ be a Chevalley lattice such that Λ is closed under multiplication by $\mathfrak{C}$. Then Λ is closed under multiplication by $\mathscr{U}_{\mathfrak{C}}$, hence

$$\omega^n \bigoplus_{(\psi),\chi} \mathrm{pr}_{(\psi),\chi}\Lambda \subset \mathscr{U}_{\mathfrak{C}} \cdot \Lambda = \Lambda \subset \bigoplus_{(\psi),\chi} \mathrm{pr}_{(\psi),\chi}\Lambda. \tag{7.41}$$

Since $\mathfrak{C} = \bigoplus_\chi \mathfrak{C}_\chi$, we see that $\Lambda' := \bigoplus_{(\psi),\chi} \mathrm{pr}_{(\psi),\chi}\Lambda$ is also closed under multiplication by $\mathfrak{C}$. Then (7.41) tells us that $d(\Lambda, \Lambda') \leq n$ (where d is the distance function from subsection 7.1.3). Since K is a p-adic field, all locally free R-modules are in fact free, hence Λ' satisfies the conditions of lemma 7.39, and there exists an $h \in H(K)$ such that

$$S^-(L_0^-, J_0) \subset h \cdot \Lambda' \subset S^+(L_0^+, J_0);$$

hence $d(h \cdot \Lambda', S^+(L_0^+, J_0)) \leq m$. From this we get

$$\begin{aligned} d_H(X, P^+) &\leq d_H(X, H(K)\cdot\Lambda') + d_H(H(K)\cdot\Lambda', P^+) \\ &\leq d(\Lambda, \Lambda') + d_H(H(K)\cdot\Lambda', P^+) \\ &\leq n + d_H(H(K)\cdot\Lambda', P^+) \\ &\leq n + d(h\cdot\Lambda', S^+(L_0^+, J_0)) \\ &\leq n + m. \end{aligned}$$

This shows that all $H(K)$-orbits of Chevalley-invariant lattices lie within a ball of radius $n+m$ around P^+ in the metric space $(\mathrm{Lat}_H(V), d_H)$. By lemma 7.12.3 this ball is finite, which proves the proposition. □

Proposition 7.42. *Let K be a number field. Then for almost all finite places v of K there is exactly one $H(K_v)$-orbit of Chevalley-invariant lattices in $\mathrm{Lat}(V_{K_v})$.*

Proof. Fix a Chevalley lattice $\mathfrak{C} \subset \mathfrak{g}$ and a $J \in \mathcal{J}$, and let $L^\pm = f^\pm(\mathfrak{C})$. For a finite place v of K define $\mathfrak{C}_v := \mathfrak{C}_{R_v}$ and $J_v = (J_{\psi,R_v})_{\psi\in\mathcal{D}}$. Then $\mathfrak{C}_v$ is a Chevalley lattice in $\mathfrak{g}_{K_v}$, and we set

$L_v^\pm := f^\pm(\mathfrak{C}_v)$; then it follows from the definitions of $f^\pm$ and $S^\pm$ that $L_v^\pm = (L^\pm_{\alpha,R_v})_{\alpha\in\Delta^+}$ and

$$S^\pm(L_v^\pm, J_v) = S^\pm(L^\pm, J)_{R_v} \subset V_{K_v}.$$

This shows that $S^-(L_v^-, J_v) = S^+(L_v^+, J_v)$ for almost all v. Furthermore, let r be as in lemma 7.34; then $v(r) = 0$ for almost all v. Now let v be such that $S^-(L_v^-, J_v) = S^+(L_v^+, J_v)$ and $v(r) = 0$. Consider the proof of the previous proposition for the group G_{K_v} and its representation on V_{K_v}, taking $\mathfrak{C}_0 := \mathfrak{C}_v$ and $J_0 := J_v$. In the notation of that proof we get $m = n = 0$, hence $X = P^+$, and there is exactly one orbit of Chevalley-invariant lattices. □

7.3.4 Models of split reductive groups

In this section we apply our results about lattices in representations of Lie algebras to prove theorem 7.18. The strategy is to give a bound for the distance between a lattice Λ and a Chevalley-invariant lattice in V in terms of the distance between the Lie algebra of $\mathtt{mod}_G(\Lambda)$ and a Chevalley lattice in $\mathfrak{g}$. Combined with propositions 7.40 and 7.42 this will give the desired finiteness properties.

Notation 7.43. Let $(\mathscr{G}, \mathscr{T})$ be a model of (G, T), and let $\mathfrak{G}$ be the Lie algebra of $\mathscr{G}$. Let $\mathscr{U}_{\mathfrak{G},\varphi}$ be the R-subalgebra of $U(\mathfrak{g})$ generated by $(\mathrm{Lie}\,\varphi)(\mathfrak{G}) \subset \mathfrak{g}$. Let furthermore $\varrho\colon U(\mathfrak{g}) \to \mathrm{End}(V)$ be the homomorphism of K-algebras induced by the representation $\mathfrak{g} \to \mathfrak{gl}(V)$.

Lemma 7.44.

1. *Let Λ be a lattice in V, let $(\mathscr{G}, \varphi) = \mathtt{mod}^{\mathrm{a}}_G(\Lambda)$ be the anchored model of G associated to Λ, and let $\mathfrak{G}$ be the Lie algebra of $\mathscr{G}$. Then $\varrho(\mathscr{U}_{\mathfrak{G},\varphi})$ is a lattice in the K-vector space $\varrho(U(\mathfrak{g}))$.*

2. *Let $\mathfrak{C} \subset \mathfrak{g}$ be a Chevalley lattice, and let $\mathscr{U}_{\mathfrak{C}}$ be as in lemma 7.33. Then $\varrho(\mathscr{U}_{\mathfrak{C}})$ is a lattice in $\varrho(U(\mathfrak{g}))$.*

Proof.

1. The image of $\mathscr{U}_{\mathfrak{G},\varphi}$ under ϱ is contained in $\varrho(U(\mathfrak{g}))\cap\mathrm{End}(\Lambda)$; since $\mathrm{End}(\Lambda)$ is a lattice in $\mathrm{End}(V)$, we see that $\varrho(U(\mathfrak{g})) \cap \mathrm{End}(\Lambda)$ is a lattice in $\varrho(U(\mathfrak{g}))$; hence $\varrho(\mathscr{U}_{\mathfrak{G},\varphi})$ is finitely generated. On the other hand $\mathscr{U}_{\mathfrak{G},\varphi}$ generates $U(\mathfrak{g})$ as a K-vector space, hence $\varrho(\mathscr{U}_{\mathfrak{G},\varphi})$ is a lattice in $\varrho(U(\mathfrak{g}))$.

2. Let Λ be a lattice closed under multiplication by $\mathfrak{C}$, and let $(\mathscr{G}, \varphi)$ be its associated anchored model of G; then $\varrho(\mathscr{U}_{\mathfrak{C}})$ is an R-submodule of the lattice $\varrho(\mathscr{U}_{\mathfrak{G},\varphi})$ that generates $\varrho(U(\mathfrak{g}))$ as a K-vector space, i.e. a lattice in $\varrho(U(\mathfrak{g}))$. □

Lemma 7.45. *Let $(\mathscr{G}, \mathscr{T})$ be a model of (G, T). Let $\mathfrak{G}$ be the Lie algebra of $\mathscr{G}$. Then there is an $r \in R$ such that for every anchoring φ of $(\mathscr{G}, \mathscr{T})$ there exists a Chevalley lattice $\mathfrak{C}$ such that*

$$r \cdot \varrho(\mathscr{U}_{\mathfrak{G},\varphi}) \subset \varrho(\mathscr{U}_{\mathfrak{C}}) \subset r^{-1} \cdot \varrho(\mathscr{U}_{\mathfrak{G},\varphi}).$$

Proof. Fix a Chevalley lattice $\mathfrak{C}$ and an anchoring φ of $(\mathscr{G},\mathscr{T})$. By lemma 7.44 both $\varrho(\mathscr{U}_{\mathfrak{G},\varphi})$ and $\varrho(\mathscr{U}_{\mathfrak{C}})$ are lattices in $\varrho(U(\mathfrak{g}))$, hence there exists an $r_\varphi \in R$ such that $r_\varphi \varrho(\mathscr{U}_{\mathfrak{G},\varphi})) \subset \varrho(\mathscr{U}_{\mathfrak{C}}) \subset r_\varphi^{-1}\varrho(\mathscr{U}_{\mathfrak{G},\varphi})$. Let

$$\mathrm{Aut}(G,T) = \left\{\sigma \in \mathrm{Aut}(G) : \sigma(T) = T\right\}$$

as in lemma 7.30, and let $\mathtt{Aut}(G,T)$ be the underlying K-group scheme. There is a short exact sequence of algebraic groups over K

$$1 \to G^{\mathrm{ad}} \to \mathtt{Aut}(G) \to \Gamma \to 1$$

where Γ is the automorphism group scheme of the based root datum (Ψ,Δ^+); this is a finite étale group scheme. The kernel of the map $\mathtt{Aut}(G,T) \to \Gamma$ is the image of the normaliser $\mathtt{Norm}_G(T)$ in G^{ad}; its identity component is $\bar{T}$. Since Γ is finite and the index of $\bar{T}$ in $\ker(\mathtt{Aut}(G,T) \to \Gamma)$ is finite, we see that $\bar{T}(K)$ has finite index in $\mathrm{Aut}(G,T)$. Now let φ' be another anchoring of $(\mathscr{G},\mathscr{T})$. There exists a unique $\sigma \in \mathrm{Aut}(G,T)$ such that $\varphi' = \sigma\circ\varphi$. The automorphism σ also induces automorphisms of $\mathfrak{g}$ and $U(\mathfrak{g})$, which we will still denote by σ; by lemma 7.30 $\sigma(\mathfrak{C})$ is again a Chevalley lattice. Suppose σ is an inner automorphism corresponding to a $t \in \bar{T}(K)$. Then σ acts as $\chi(t)$ on $U(\mathfrak{g})_\chi$ for every $\chi \in Q$. Since ϱ is a homomorphism of $\mathrm{X}^*(T)$-graded algebras we get

$$\begin{aligned}
r_\varphi \cdot \varrho(\mathscr{U}_{\mathfrak{G},\varphi'}) &= r_\varphi \cdot \varrho(\mathscr{U}_{\mathfrak{G},\sigma\circ\varphi}) \\
&= r_\varphi \cdot \varrho(\sigma(\mathscr{U}_{\mathfrak{G},\varphi})) \\
&= r_\varphi \cdot \varrho(t\cdot \mathscr{U}_{\mathfrak{G},\varphi})) \\
&= r_\varphi \cdot t \cdot (\varrho(\mathscr{U}_{\mathfrak{G},\varphi})) \\
&\subset t\cdot \varrho(\mathscr{U}_{\mathfrak{C}}) \\
&= \varrho(\mathscr{U}_{\sigma(\mathfrak{C})}).
\end{aligned}$$

Similarly one shows $\varrho(\mathscr{U}_{\sigma(\mathfrak{C})}) \subset r_\varphi^{-1}\cdot \varrho(\mathscr{U}_{\mathfrak{G},\varphi'})$; hence the element $r_\varphi \in R$ only depends on the $\bar{T}(K)$-orbit of the anchoring φ. Since there are only finitely many such orbits, we can take r to be a common multiple of these r_φ. □

Proposition 7.46. *If K is a p-adic field, then the map $\mathtt{mod}_{G,T}\colon \mathrm{Lat}_H(V) \to \mathrm{Mod}(G,T)$ of lemma 7.5 is finite.*

Proof. Let $(\mathscr{G},\mathscr{T})$ be a model of (G,T), and let r be as in lemma 7.45. Let $\mathcal{P} \subset \mathrm{Lat}_H(V)$ be the set of $H(K)$-orbits of Chevalley-invariant lattices; this is a finite set by proposition 7.40. Let X be an $H(K)$-orbit of lattices in V such that $\mathtt{mod}_{G,T}(X) = (\mathscr{G},\mathscr{T})$. Let $\Lambda \in X$, and let φ be the anchoring of $(\mathscr{G},\mathscr{T})$ induced by Λ. Then Λ is closed under multiplication by $\varrho(\mathscr{U}_{\mathfrak{G},\varphi})$. Let C be a Chevalley lattice in $\mathfrak{g}$ such that $r^{-1}\varrho(\mathscr{U}_{\mathfrak{G},\varphi}) \subset \varrho(\mathscr{U}_{\mathfrak{C}}) \subset r\varrho(\mathscr{U}_{\mathfrak{G},\varphi})$, and let $\Lambda' = \varrho(\mathscr{U}_{\mathfrak{C}})\cdot\Lambda \subset V$. Since $\varrho(\mathscr{U}_{\mathfrak{C}})$ is a finitely generated submodule of $\mathrm{End}(V)$, we see that Λ' is a lattice in V that is closed under multiplication by C. Furthermore we see

$$\begin{aligned} r^{-1}\Lambda &= r^{-1}\varrho(\mathscr{U}_{\mathfrak{G},\varphi})\Lambda \\ &\subset \varrho(\mathscr{U}_{\mathfrak{C}})\Lambda \\ &= \Lambda' \\ &\subset r\varrho(\mathscr{U}_{\mathfrak{G},\varphi})\Lambda \\ &= r\Lambda, \end{aligned}$$

hence $d(\Lambda, \Lambda') \leq 2v(r)$, where v is the valuation on K. For the metric space $\mathrm{Lat}_H(V)$ this implies that X is at most distance $2v(r)$ from an element of $\mathcal{P}$. Since $\mathcal{P}$ is finite and balls are finite in this metric space, we see that there are only finitely many possibilities for X, which proves the proposition. □

Lemma 7.47. *Suppose K is a number field. Then for almost all finite places v of K there is exactly one $H(K_v)$-orbit X of lattices in V_{K_v} such that $\mathtt{mod}_{G_{K_v},T_{K_v}}(X)$ is the Chevalley model of (G_{K_v}, T_{K_v}).*

Proof. Let $(\mathscr{G}, \mathscr{T})$ be the Chevalley model of (G, T), let φ be some anchoring of $(\mathscr{G}, \mathscr{T})$, and let $\mathfrak{C} \subset \mathfrak{g}$ be a Chevalley lattice. Then $R_v \otimes_R (\mathrm{Lie}\ \varphi)(\mathfrak{G}) = R_v \otimes_R \mathfrak{C}$ as lattices in $\mathfrak{g}_{K_v}$ for almost all finite places v of K. Hence for these v, the Lie algebra of the Chevalley model of (G_{K_v}, T_{K_v}) is a Chevalley lattice via the embedding induced by the anchoring φ. However, two anchorings differ by an automorphism in $\mathrm{Aut}(G_{K_v}, T_{K_v})$. Since the action of $\mathrm{Aut}(G_{K_v}, T_{K_v})$ on $\mathrm{Lat}(\mathfrak{g}_{K_v})$ sends Chevalley lattices to Chevalley lattices by lemma 7.36.3, this means that for these v the Lie algebra of the Chevalley model will be a Chevalley lattice with respect to every anchoring. For these v, a lattice in V_{K_v} yielding the Chevalley model must be Chevalley-invariant; hence by discarding at most finitely many v we may assume by proposition 7.42 that there is at most one $H(K_v)$-orbit of lattices yielding the Chevalley model. On the other hand, any model of G will be reductive on an open subset of $\mathrm{Spec}(R)$, and any model of T will be a split torus on an open subset of $\mathrm{Spec}(R)$. This shows that any model of (G, T) is isomorphic to the Chevalley model over almost all R_v; hence for almost all v there is at least one lattice yielding the Chevalley model. □

Proof of theorem 7.18.

1. Let $\mathscr{G}$ be a given model of G. Let T be a split maximal torus of G, and choose a subgroup scheme $\mathscr{T} \subset \mathscr{G}$ such that $(\mathscr{G}, \mathscr{T})$ is a model of (G, T). Let Λ' be a lattice in V with model $\mathtt{mod}_{G,T}(\Lambda') = (\mathscr{G}', \mathscr{T}')$, and suppose there exists an isomorphism $\psi\colon \mathscr{G} \xrightarrow{\sim} \mathscr{G}'$. Then $\psi(\mathscr{T}_K)$ is a split maximal torus of $\mathscr{G}'_K$. Since all split maximal tori of a split reductive group are conjugate (see [61, Thm. 15.2.6]), there exists a $g \in \mathscr{G}'(K)$ such that $\psi(\mathscr{T}_K) = g\mathscr{T}'_K g^{-1}$. Then $\mathrm{inn}(g) \circ \psi$ is an isomorphism of models of (G, T) between $(\mathscr{G}, \mathscr{T})$ and $\mathtt{mod}_{G,T}(g\Lambda')$. By proposition 7.46 there are only finitely many $H(K)$-orbits yielding $(\mathscr{G}, \mathscr{T})$, so $g\Lambda'$ can only lie in finitely many $H(K)$-orbits; hence Λ' can only lie in finitely many $(G \cdot H)(K)$-orbits. Since

$G \cdot H = G \cdot Z$ is a subgroup of N, this shows that there are only finitely many $N(K)$-orbits in $\mathrm{Lat}(V)$ yielding the model $\mathscr{G}$ of G.

2. Let T be a split maximal torus of G. By lemma 7.47 for almost all finite places v of K there exists exactly one $H(K_v)$-orbit $Y_v \subset \mathrm{Lat}(V_{K_v})$ yielding the Chevalley model of (G_{K_v}, T_{K_v}); let v be such a place. Repeating the proof of the previous point, we see that $g\Lambda'$ has to lie in Y_v, hence Λ' has to lie in $(G \cdot Z)(K_v) \cdot Y_v$, and in particular in the single $N(K_v)$-orbit $N(K_v) \cdot Y_v$. □

7.4 Nonsplit reductive groups

The main goal of this section is to prove theorem 7.1 for local fields, as well as a stronger finiteness result à la theorem 7.18.2 needed to prove theorem 7.1 for number fields. We will make use of some Bruhat–Tits theory to prove one key lemma (7.56).

7.4.1 Bruhat–Tits buildings

In this subsection we give a very brief summary of the part of Bruhat–Tits theory that is revelant to our purposes; Bruhat–Tits theory will only play a role in the proof of lemma 7.56. The reader looking for an actual introduction to the theory is referred to [66] and [6]. If Δ is a simplicial complex, I denote its topological realisation by $|\Delta|$.

Theorem 7.48. (See [7, Cor. 2.1.6; Lem. 2.5.1; 2.5.2], [66, 2.2.1] and [6, Thm. VI.3A]) *Let G be a connected semisimple algebraic group over a p-adic field K. Then there exists a locally finite simplicial complex $\mathcal{I}(G, K)$, called the* Bruhat–Tits building of *G, with the following properties:*

1. *$\mathcal{I}(G, K)$ has finite dimension;*
2. *Every simplex is contained in a simplex of dimension $\dim(\mathcal{I}(G, K))$, and these maximal simplices are called* chambers*;*
3. *There is an action of $G(K)$ on $\mathcal{I}(G, K)$ that induces a proper and continuous action of $G(K)$ on $|\mathcal{I}(G, K)|$, where $G(K)$ is endowed with the p-adic topology;*
4. *The stabilisers of points in $|\mathcal{I}(G, K)|$ are compact open subgroups of $G(K)$;*
5. *$G(K)$ acts transitively on the set of chambers of $\mathcal{I}(G, K)$;*
6. *There is a metric d on $|\mathcal{I}(G, K)|$ invariant under the action of $G(K)$ that gives the same topology as its topological realisation.* □

Remark 7.49. Since the stabiliser of each point is an open subgroup of $G(K)$, the $G(K)$-orbits in $|\mathcal{I}(G, K)|$ are discrete subsets.

Corollary 7.50. *Let G be a connected semisimple algebraic group over a p-adic field K, let $C \subset |\mathcal{I}(G,K)|$ be a chamber, let $\bar{C} \subset |\mathcal{I}(G,K)|$ be its closure, and let $r \in \mathbb{R}_{>0}$. Then the subset V of $|\mathcal{I}(G,K)|$ given by*

$$V := \left\{ x \in |\mathcal{I}(G,K)| : d(x,\bar{C}) \leq r \right\}$$

is compact.

Proof. Since the metric of $|\mathcal{I}(G,K)|$ is invariant under the action of $G(K)$ and $G(K)$ acts transitively on the set of chambers, we see that every chamber has the same size. Since $\mathcal{I}(G,K)$ is locally finite this means that V will only meet finitely many chambers. The union of the closures of these chambers is compact, hence V, being a closed subset of this, is compact as well. □

Theorem 7.51. (See [59, Prop. 2.4.6; Cor. 5.2.2; Cor. 5.2.8]) *Let G be a connected semisimple algebraic group over a p-adic field K, and let L/K be a finite Galois extension.*

1. *The simplicial complex $\mathcal{I}(G,L)$ has a natural action of $\mathrm{Gal}(L/K)$;*
2. *The map $G(L)\times\mathcal{I}(G,L) \to \mathcal{I}(G,L)$ that gives the $G(L)$-action on $\mathcal{I}(G,L)$ is $\mathrm{Gal}(L/K)$-equivariant;*
3. *There is a canonical inclusion $\mathcal{I}(G,K) \hookrightarrow \mathcal{I}(G,L)^{\mathrm{Gal}(L/K)}$, which allows us to view $\mathcal{I}(G,K)$ as a subcomplex of $\mathcal{I}(G,L)$;*
4. *There is an $r \in \mathbb{R}_{>0}$ such that for every $x \in |\mathcal{I}(G,L)|^{\mathrm{Gal}(L/K)}$ there exists a point y in $|\mathcal{I}(G,K)|$ such that $d(x,y) \leq r$.* □

7.4.2 Compact open subgroups and quotients

Let G be an algebraic group over a p-adic field K, and let L be a finite Galois extension of K. Let U be a compact open subgroup of $G(L)$ that is invariant under the action of $\mathrm{Gal}(L/K)$. Then $G(L)/U$ inherits an action of $\mathrm{Gal}(L/K)$, and its set of invariants $(G(L)/U)^{\mathrm{Gal}(L/K)}$ has a left action of $G(K)$. The goal of this section is to show that, for various choices of G, K, L and U, the quotient $G(K)\backslash(G(L)/U)^{\mathrm{Gal}(L/K)}$ is finite. We will also show that it has cardinality 1 if we choose U suitably 'nice'.

Notation 7.52. Let G be an algebraic group over a p-adic field K, let L/K be a finite Galois extension over which G splits, and let U be a compact open subgroup of $G(L)$ (with respect to the p-adic topology) fixed under the action of $\mathrm{Gal}(L/K)$. Then we write $Q_G^{L/K}(U) := G(K)\backslash(G(L)/U)^{\mathrm{Gal}(L/K)}$.

The next lemma tells us that compact open subgroups often appear in the contexts relevant to us.

Lemma 7.53. (See [57, p. 134]) *Let G be an algebraic group over a p-adic field K, and let L be a finite field extension of K. Let $(\mathscr{G},\varphi)$ be an anchored model of G. Then $\varphi(\mathscr{G}(\mathscr{O}_L))$ is a compact open subgroup of $G(L)$ with respect to the p-adic topology.* □

Lemma 7.54. *Let G be an algebraic group over a p-adic field K, and let L/K be a finite Galois extension over which G splits. If $Q_G^{L/K}(U)$ is finite for some compact open Galois invariant $U \subset G(L)$, then it is finite for all such U.*

Proof. This follows from the fact that if U and U' are compact open Galois invariant subgroups of $G(L)$, then $U'' := U \cap U'$ is as well, and U'' has finite index in both U and U'. ☐

We will now prove that $Q_G^{L/K}(U)$ is finite for connected reductive G. To prove this we first prove it for tori and for semisimple groups, and then combine these results.

Lemma 7.55. *Let T be a torus over a p-adic field K, and let L be a finite Galois extension of K over which T splits. Let U be a compact open subgroup of $T(L)$. Then $Q_T^{L/K}(U)$ is finite.*

Proof. Choose an isomorphism $\varphi\colon T_L \xrightarrow{\sim} \mathbb{G}_{\mathrm{m},L}^d$. Then $T(L)$ has a unique maximal compact open subgroup, namely $\varphi^{-1}((\mathscr{O}_L^\times)^d)$; by lemma 7.54 it suffices to prove this lemma for $U = \varphi^{-1}((\mathscr{O}_L^\times)^d)$. Let f be the ramification index of L/K, and let t be a uniformiser of L such that $t^f \in K$. Now consider the homomorphism of abelian groups

$$\begin{aligned} F\colon \mathrm{X}_*(T) &\to T(L)/U \\ \eta &\mapsto \eta(t) \cdot U. \end{aligned}$$

For every cocharacter η the subgroup $\eta(\mathscr{O}_L^\times)$ of $T(L)$ is contained in U. This implies that for all $\eta \in \mathrm{X}_*(T)$ and all $\pi \in \mathrm{Gal}(L/K)$ one has

$$\begin{aligned} F(\pi \cdot \eta) &= (\pi \cdot \eta)(t) \cdot U \\ &= \pi(\eta(\pi^{-1}t))) \cdot U \\ &= \pi(\eta(t)) \cdot \pi\left(\eta\left(\frac{\pi^{-1}t}{t}\right)\right) \cdot U \\ &= \pi(\eta(t)) \cdot U \\ &= \pi(F(\eta)) \cdot U, \end{aligned}$$

since $\frac{\pi^{-1}t}{t} \in \mathscr{O}_L^\times$. This shows that F is Galois-equivariant. On the other hand φ induces isomorphisms of abelian groups $\mathrm{X}_*(T) \cong \mathbb{Z}^d$ and

$$T(L)/U \cong (L^\times/\mathscr{O}_L^\times)^d = \langle t \rangle^d.$$

In terms of these identifications the map F is given by

$$\mathbb{Z}^d \ni (x_1, \ldots, x_d) \mapsto (t^{x_1}, \ldots, t^{x_d}) \in \langle t \rangle^d \cong T(L)/U.$$

We see from this that F is an isomorphism of abelian groups with an action of $\mathrm{Gal}(L/K)$. Let $t \in T(L)/U$ be Galois invariant, and let $\eta = F^{-1}(t) \in \mathrm{X}_*(T)^{\mathrm{Gal}(L/K)}$; then η is a cocharacter that is defined over K. By definition we have $t^f \in K$, hence $F(f \cdot \eta) = \eta(t^f)$ is an element of $T(K)$. This shows that the abelian group

$$\mathrm{X}_*(T)^{\mathrm{Gal}(L/K)}/F^{-1}(T(K) \cdot U)$$

is annihilated by f. Since it is finitely generated, it is finite. Furthermore, the map F induces a bijection

$$\mathrm{X}_*(T)^{\mathrm{Gal}(L/K)}/F^{-1}(T(K)\cdot U) \xrightarrow{\sim} Q_T^{L/K}(U),$$

hence $Q_T^{L/K}(U)$ is finite. □

Lemma 7.56. *Let G be a (connected) semisimple group over a p-adic field K, and let L be a finite Galois extension over which G splits. Let U be a Galois invariant compact open subgroup of $G(L)$. Then $Q_G^{L/K}(U)$ is finite.*

Proof. By lemma 7.54 it suffices to show this for a chosen U. Let $\mathcal{I}(G,K)$ be the Bruhat–Tits building of G over K, and let $\mathcal{I}(G,L)$ be the Bruhat–Tits building of G over L. Choose a point $x \in |\mathcal{I}(G,K)| \subset |\mathcal{I}(G,L)|^{\mathrm{Gal}(L/K)}$; its stabiliser $U \subset G(L)$ is a Galois invariant compact open subgroup of $G(L)$ by theorems 7.48.4 and 7.51.2. Now we can identify $Q_G^{L/K}(U)$ with

$$G(K)\backslash(G(L)\cdot x)^{\mathrm{Gal}(L/K)},$$

so it suffices to show that this set is finite. Let $y \in (G(L)\cdot x)^{\mathrm{Gal}(L/K)}$, and let r be as in theorem 7.51.4. Then there exists a $z \in \mathcal{I}(G,K)$ such that $d(y,z) \leq r$. Now fix a chamber C of $\mathcal{I}(G,K)$, and let $g \in G(K)$ such that $gz \in \bar{C}$ (see theorem 7.48.5). Then $d(gy,\bar{C}) \leq r$, so gy lies in the set $D = \{v \in |\mathcal{I}(G,L)| : d(v,\bar{C}) \leq r\}$, which is compact by corollary 7.50. On the other hand the action of $G(L)$ on $|\mathcal{I}(G,L)|$ has discrete orbits by remark 7.49, so $G(L)\cdot x$ intersects D in only finitely many points. Hence there are only finitely many possibilities for gy, so $G(K)\backslash(G(L)\cdot x)^{\mathrm{Gal}(L/K)}$ is finite, as was to be shown. □

Proposition 7.57. *Let G be a connected reductive group over a p-adic field K, and let L be a finite Galois extension of K over which G splits. Let U be a Galois invariant compact open subgroup of $G(L)$. Then $Q_G^{L/K}(U)$ is finite.*

Proof. Let G' be the semisimple group G^{der}, and let G^{ab} be the torus G/G'. This gives us an exact sequence

$$1 \to G'(K) \to G(K) \xrightarrow{\psi} G^{\mathrm{ab}}(K) \to \mathrm{H}^1(G',K).$$

The image $\psi(U) \subset G^{\mathrm{ab}}(L)$ is compact. It is also open: if Z is the centre of G, then the map $\psi\colon Z \to G^{\mathrm{ab}}$ is an isogeny, and since $Z(L)\cap U$ is open in $Z(L)$, its image in G^{ab} is open as well. As such we know by lemma 7.55 that $Q_{G^{\mathrm{ab}}}^{L/K}(\psi(U))$ is finite. Furthermore, by [60, III.4.3] $\mathrm{H}^1(G',K)$ is finite, hence the image of $G(K)$ in $G^{\mathrm{ab}}(K)$ has finite index. If we let $G(K)$ act on $(G^{\mathrm{ab}}(L)/\psi(U))^{\mathrm{Gal}(L/K)}$ via ψ, we now find that the quotient set $G(K)\backslash(G^{\mathrm{ab}}(L)/\psi(U))^{\mathrm{Gal}(L/K)}$ is finite. The projection map

$$\psi\colon (G(L)/U)^{\mathrm{Gal}(L/K)} \to (G^{\mathrm{ab}}(L)/\psi(U))^{\mathrm{Gal}(L/K)}$$

is $G(K)$-equivariant, so we get a map of $G(K)$-quotients

$$Q_G^{L/K}(U) \to G(K)\backslash(G^{\mathrm{ab}}(L)/\psi(U))^{\mathrm{Gal}(L/K)}.$$

To show that $Q_G^{L/K}(U)$ is finite it suffices to show that for every $x \in Q_G^{L/K}(U)$ there exist at most finitely many $y \in Q_G^{L/K}(U)$ such that $\psi(x) = \psi(y)$ in the quotient set $G(K)\backslash(G^{\mathrm{ab}}(L)/\psi(U))^{\mathrm{Gal}(L/K)}$. Choose such an x and y, and choose a representative $\tilde{x}$ of x in $G(L)$. Then there exists a representative $\tilde{y}$ of y in $G(L)$ such that $\tilde{x} = \tilde{y}$ in $G^{\mathrm{ab}}(L)$; hence there is a $g' \in G'(L)$ such that $g'\tilde{x} = \tilde{y}$. Since $\tilde{x}U$ and $\tilde{y}U$ are Galois invariant, the element g' is Galois invariant in $G'(L)/(G'(L) \cap \tilde{x}U\tilde{x}^{-1})$; this makes sense because the compact open subgroup $G'(L) \cap \tilde{x}U\tilde{x}^{-1}$ of $G'(L)$ is Galois invariant. Furthermore the element y only depends on the choice of g' in

$$G'(K)\backslash\Big(G'(L)/(G'(L) \cap \tilde{x}U\tilde{x}^{-1})\Big)^{\mathrm{Gal}(L/K)} = Q_{G'}^{L/K}(G'(L) \cap \tilde{x}U\tilde{x}^{-1}).$$

Since this set is finite by lemma 7.56 there are only finitely many possibilities for y for a given x. This proves the proposition. □

The final proposition of this subsection is a stronger version of proposition 7.57 in the case that the compact open subgroup U comes from a 'nice' model of G. We need this to prove a stronger version of theorem 7.1 over local fields in the case that we have models over a collection of local fields coming from the places of some number field (compare theorem 7.18.2).

Proposition 7.58. *Let K be a p-adic field, and let $\mathscr{G}$ be a smooth group scheme over $\mathscr{O}_K$ whose generic fibre is reductive and splits over an unramified Galois extension L/K. Then $Q_{\mathscr{G}_K}^{L/K}(\mathscr{G}(\mathscr{O}_L))$ has cardinality 1.*

Proof. Let k be the residue fueld of K. Let $g \in \mathscr{G}(L)$ such that $g\mathscr{G}(\mathscr{O}_L)$ is Galois-invariant; we need to show that $g\mathscr{G}(\mathscr{O}_L)$ has a point defined over K. Since L/K is unramified, we see that $\mathrm{Gal}(L/K)$ is the étale fundamental group of the covering $\mathrm{Spec}(\mathscr{O}_L)/\mathrm{Spec}(\mathscr{O}_K)$. As such $g\mathscr{G}(\mathscr{O}_L)$ can be seen as the $\mathscr{O}_L$-points of a $\mathscr{G}$-torsor $\mathscr{B}$ over $\mathrm{Spec}(\mathscr{O}_K)$ in the sense of [41, III.4]. By Lang's theorem the $\mathscr{G}_k$-torsor $\mathscr{B}_k$ is trivial, hence $\mathscr{B}(k)$ is nonempty. Since $\mathscr{G}$ is smooth over $\mathscr{O}_K$, so is $\mathscr{B}$, and we can lift a point of $\mathscr{B}(k)$ to a point of $\mathscr{B}(\mathscr{O}_K)$. Hence $g\mathscr{G}(\mathscr{O}_L)$ has an $\mathscr{O}_K$-point, as was to be shown. □

7.4.3 Models of reductive groups

In this subsection we prove theorem 7.1 over local fields, plus a stronger statement for local fields coming from one number field; we need this to prove theorem 7.1 for number fields.

Theorem 7.59. *Let G be a connected reductive group over K. Let V be a faithful representation of G, and regard G as an algebraic subgroup of $\mathtt{GL}(V)$. Let N be the scheme-theoretic normaliser of G in $\mathtt{GL}(V)$.*

1. *Let K be a p-adic field. Then the map $\mathtt{mod}_G \colon \mathrm{Lat}_N(V) \to \mathrm{Mod}(G)$ of lemma 7.5 is finite.*

2. *Let K be a number field. Then there exists a finite Galois extension L of K over which G splits with the following property: For almost all finite places v of K there is exactly one $N(K_v)$-orbit X_v of lattices in V_{K_v} such that $\mathtt{mod}_{G_{K_v}}(X_v)_{\mathscr{O}_{L_w}}$ is the Chevalley model of G_{L_w} for all places w of L over v (see definition 7.11).*

Proof. As before, let N^0 and $\pi_0(N)$ be the identity group and component group of N, respectively.

1. Let L/K be a Galois extension over which G splits. Let R and S be the rings of integers of K and L, respectively. Then we have the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Lat}_{N^0}(V) & \xrightarrow{S \otimes_R -} & \mathrm{Lat}_{N^0}(V_L) \\ \downarrow & & \downarrow \\ \mathrm{Lat}_N(V) & \xrightarrow{S \otimes_R -} & \mathrm{Lat}_N(V_L) \\ \downarrow{\scriptstyle \mathtt{mod}_G} & & \downarrow{\scriptstyle \mathtt{mod}_{G_L}} \\ \mathrm{Mod}(G) & \xrightarrow{\mathrm{Spec} S \times_{\mathrm{Spec} R} -} & \mathrm{Mod}(G_L) \end{array}$$

By theorem 7.18.1 we know that the map on the lower right is finite. Furthermore, since N^0 is of finite index in N, we know that the maps on the upper left and upper right are finite and surjective. To show that the map on the lower left is finite, it now suffices to show that the top map is finite. Let Λ be a lattice in V. The $N^0(L)$-orbit of Λ_S in $\mathrm{Lat}(V_L)$ is a Galois-invariant element of $\mathrm{Lat}_{N^0}(V_L)$. As a set with an $N^0(L)$-action and a Galois action, this set is isomorphic to $N^0(L)/U$, where $U \subset N^0(L)$ is the stabiliser of Λ_S; this is a compact open Galois-invariant subgroup of $N^0(L)$. If $\Lambda' \in \mathrm{Lat}(V)$ is another lattice such that $\Lambda'_S \in N^0(L) \cdot \Lambda_S$, then Λ'_S corresponds to a Galois-invariant element of $N^0(L)/U$. By [68] we see that N^0 is reductive, hence $Q^{L/K}_{N^0}(U)$ is finite by proposition 7.57. This shows that, given Λ, there are only finitely many options for $N^0(K) \cdot \Lambda'$. Hence the top map of the above diagram is finite, as was to be shown.

2. Let L/K be finite Galois such that the map $N(L) \to \pi_0(N)(\bar{K})$ is surjective. Choose a lattice $\Lambda \in \mathrm{Lat}(V)$. Let $\mathscr{N}^0$ be the model of N^0 induced by Λ. Let $\mathscr{N}^0_v := \mathscr{N}^0_{R_v}$; this is the model of $N^0_{K_v}$ induced by $\Lambda_{R_v} \subset V_{K_v}$. For almost all v the R_v-group scheme $\mathscr{N}^0_v$ is reductive. Since G_L is split, for almost all places w of L the model of G_{L_w} associated to Λ_{S_w} is the Chevalley model. Furthermore, let $n_1, \ldots, n_r \in N(L)$ be a set of representatives of $\pi_0(N)(\bar{K})$; then for every place w of L we have

$$N(L_w) \cdot \Lambda_{S_w} = \bigcup_{i=1}^{r} N^0(L_w) n_i \cdot \Lambda_{S_w}.$$

For almost all w all the lattices $n_i \cdot \Lambda_{S_w}$ coincide, hence for those w we have $N(L_w) \cdot \Lambda_{S_w} = N^0(L_w) \cdot \Lambda_{S_w}$. Now let v be a finite place of K satisfying the following conditions:

- For every place w of L above v, the $N(L_w)$-orbit of lattices $N(L_w) \cdot \Lambda_{S_w}$ is the only orbit of lattices in V_{L_w} inducing the Chevalley model of G_{L_w};
- for every place w of L above v we have $N(L_w) \cdot \Lambda_{S_w} = N^0(L_w) \cdot \Lambda_{S_w}$;
- L is unramified over v;
- $\mathscr{N}_v^0$ is reductive.

The last three conditions hold for almost all v, and by theorem 7.18.2 the same is true for the first condition. Let us now follow the proof of the previous point, for the group G_{K_v} and its faithful representation V_{K_v}. The first two conditions tell us that $N^0(L_w) \cdot \Lambda_{S_w}$ is the only $N^0(L_w)$-orbit of lattices yielding the Chevalley model of G_{L_w} for every place w of L over v. By the last two conditions and proposition 7.58 we know that $Q_{N^0}^{L_w/K_v}(\mathscr{N}^0(S_w)) = 1$, hence there is only one $N^0(K_v)$-orbit of lattices that gets mapped to $N^0(L_w) \cdot \Lambda_{S_w}$. This is the unique $N^0(K_v)$-orbit of lattices in V_{K_v} yielding the Chevalley model of G_{L_w}; in particular there is only one $N(K_v)$-orbit of such lattices. □

7.5 Reductive groups over number fields

In this section we prove theorem 7.1 over number fields. We work with the topological ring of finite adèles $\mathbb{A}_{K,\mathrm{f}}$ over a number field K; let $\hat{R} \subset \mathbb{A}_{K,\mathrm{f}}$ be the profinite completion of the ring of integers R of K. If M is a free $\mathbb{A}_{K,\mathrm{f}}$-module of finite rank, we say that a *lattice* in M is a free $\hat{R}$-submodule that generates M as an $\mathbb{A}_{K,\mathrm{f}}$-module. The set of lattices in M is denoted $\mathrm{Lat}(M)$, and if G is a subgroup scheme of $\mathtt{GL}(M)$, we denote $\mathrm{Lat}_G(M) := G(\mathbb{A}_{K,\mathrm{f}})\backslash\mathrm{Lat}(M)$. If V is a finite dimensional K-vector space, then the map $\Lambda \mapsto \Lambda_{\hat{R}}$ gives a bijection $\mathrm{Lat}(V) \xrightarrow{\sim} \mathrm{Lat}(V_{\mathbb{A}_{K,\mathrm{f}}})$.

Lemma 7.60. *Let K be a number field, let G be a (not necessarily connected) reductive group over K, and let V be a finite dimensional faithful representation of G. Let $\mathscr{G}$ be a model of G.*

1. *$\mathscr{G}(\hat{R})$ is a compact open subgroup of $G(\mathbb{A}_{K,\mathrm{f}})$ in the adèlic topology;*
2. *The induced map $\mathrm{Lat}_G(V) \to \mathrm{Lat}_G(V_{\mathbb{A}_{K,\mathrm{f}}})$ is finite;*
3. *The map $\mathrm{Lat}_G(V_{\mathbb{A}_{K,\mathrm{f}}}) \to \prod_v \mathrm{Lat}_G(V_{K_v})$ is injective.*

Proof.

1. Let V be a faithful representation of G and let Λ be a lattice in V such that $\mathscr{G}$ is the model of G associated to Λ. Then $\mathscr{G}(\hat{R}) = G(\mathbb{A}_{K,\mathrm{f}}) \cap \mathrm{End}(\Lambda_{\hat{R}})$. Since $\mathrm{End}(\Lambda_{\hat{R}})$ is

open in $\operatorname{End}(V_{\mathbb{A}_{K,\mathrm{f}}})$, we see that $\mathscr{G}(\hat{R})$ is open in $G(\mathbb{A}_{K,\mathrm{f}})$. It is compact because it is the profinite limit of finite groups $\varprojlim \mathscr{G}(R/IR)$, where I ranges over the nonzero ideals of R.

2. Let Λ be a lattice in V, and let $\mathscr{G}$ be the model of G induced by Λ. Then the stabiliser of $\Lambda_{\hat{R}}$ in $G(\mathbb{A}_{K,\mathrm{f}})$ is equal to $\mathscr{G}(\hat{R})$, which by the previous point is a compact open subgroup of $G(\mathbb{A}_{K,\mathrm{f}})$. Then as a $G(\mathbb{A}_{K,\mathrm{f}})$-set we can identify $G(\mathbb{A}_{K,\mathrm{f}}) \cdot \Lambda_{\hat{R}}$ with $G(\mathbb{A}_{K,\mathrm{f}})/\mathscr{G}(\hat{R})$. By [4, Thm. 5.1] the set $G(K)\backslash G(\mathbb{A}_{K,\mathrm{f}})/\mathscr{G}(\hat{R})$ is finite; as such $G(\mathbb{A}_{K,\mathrm{f}}) \cdot \Lambda_{\hat{R}}$ consists of only finitely many $G(K)$-orbits of lattices in $\operatorname{Lat}(V_{\mathbb{A}_{K,\mathrm{f}}})$. Since the map $\operatorname{Lat}(V) \to \operatorname{Lat}(V_{\mathbb{A}_{K,\mathrm{f}}})$ is a $G(K)$-equivariant bijection, each of these orbits corresponds to one $G(K)$-orbit of lattices in V; hence there are only finitely many $G(K)$-orbits of lattices in V with the same image as Λ in $\operatorname{Lat}_G(V_{\mathbb{A}_{K,\mathrm{f}}})$, which proves that the given map is indeed finite.

3. Let Λ, Λ' be two lattices in $V_{\mathbb{A}_{K,\mathrm{f}}}$ whose images in $\prod_v \operatorname{Lat}_G(V_{K_v})$ are the same. Then for every v there exists a $g_v \in G(K_v)$ such that $g_v \cdot (\Lambda_{R_v}) = \Lambda'_{R_v}$. Since $\Lambda_{R_v} = \Lambda'_{R_v}$ for almost all v, we can take $g_v = 1$ for almost all v; hence $g \cdot \Lambda = \Lambda'$ for $g = (g_v)_v \in G(\mathbb{A}_{K,\mathrm{f}})$. □

Proof of theorem 7.1. The case that K is a p-adic field is proven in theorem 7.59.1, so suppose K is a number field. Then we have the following commutative diagram:

$$\begin{array}{ccccc}
\operatorname{Lat}_N(V) & \xrightarrow{\;f_1\;} & \operatorname{Lat}_N(V_{\mathbb{A}_{K,\mathrm{f}}}) & \xrightarrow{\;f_2\;} & \prod_v \operatorname{Lat}_N(V_{K_v}) \\
\big\downarrow \mathtt{mod}_G & & & & \big\downarrow \prod_v \mathtt{mod}_{G_{K_v}} \\
\operatorname{Mod}(G) & & \xrightarrow{\;\prod_v \operatorname{Spec}(R_v) \times_{\operatorname{Spec}(R)} -\;} & & \prod_v \operatorname{Mod}(G_{K_v})
\end{array}$$

Let L be as in theorem 7.59.2, and let R and S be the rings of integers of K and L, respectively. Let $\mathscr{G}$ be a model of G. Then for almost all finite places w of L the model $\mathscr{G}_{S_w}$ of G_{L_w} is its Chevalley model. By theorem 7.59.1 we know that for every finite place v of K there are only finitely many $N(K_v)$-orbits of lattices in V_{K_v} whose associated model is $\mathscr{G}_{R_v}$, and for almost all v there is exactly one such orbit. This shows that there are only finitely many elements of $\prod_v \operatorname{Lat}_N(V_{K_v})$ that map to $(\mathscr{G}_{R_v})_v$. Hence the map $\prod_v \mathtt{mod}_{G_{K_v}}$ on the right of the diagram above is finite; since f_1 and f_2 are finite as well by lemma 7.60, this proves the theorem. □

Remark 7.61. The proof of theorem 7.1 also shows that for every collection of models $(\mathscr{G}_v)_v$ of the G_v, there are at most finitely many lattices in V that yield that collection of models.

Chapter 8

Integral Mumford–Tate groups

Let g and n be integers with $g \geq 1$ and $n \geq 3$. Let $\mathcal{A}_{g,n}$ be the moduli space of principally polarised complex abelian varieties of dimension g with full level n structure, and let $\mathcal{X}_{g,n}$ be the universal abelian variety over $\mathcal{A}_{g,n}$. The singular cohomology of the fibres $\mathcal{X}_{g,n}$ gives a variation of integral Hodge structures on $\mathcal{A}_{g,n}$. If $Y \subset \mathcal{A}_{g,n}$ is a subvariety, then the *generic Mumford–Tate group* $\mathtt{GMT}(Y)$ of Y is the generic (integral) Mumford–Tate group of this variation of integral Hodge structures over Y. If Y is a special subvariety of $\mathcal{A}_{g,n}$, then $\mathtt{GMT}(Y)$ is the (integral) Mumford–Tate group of any point of which Y is the special closure.

For a special subvariety Y the group scheme $\mathtt{GMT}(Y)$ is an integral model of its generic fibre, which is a reductive algebraic group over $\mathbb{Q}$. While reductive groups over fields are well understood, generic integral Mumford–Tate groups are more complicated: there is no general classification of the models of a given rational reductive group, not even for tori (see [18]). On the other hand, the advantage of the integral group scheme $\mathtt{GMT}(Y)$ is that it carries more information than its generic fibre. This can be seen in [16, Thm. 4.1], where a lower bound is given on the size of the Galois orbit of a CM-point of a Shimura variety in terms of the reduction of its generic Mumford–Tate group at finite primes. In theorem 8.1, we present another instance of this phenomenon, by showing that up to a finite ambiguity a special subvariety Y of $\mathcal{A}_{g,n}$ is determined by $\mathtt{GMT}(Y)$. This is not generally true when we only consider its generic fibre, as this is invariant under Hecke correspondence. The main ingredient in proving this is theorem 7.1.

Let A be a g-dimensional abelian variety over a number field K, and for every prime number ℓ, let $\mathtt{G}_\ell(A)$ be its ℓ-adic Galois monodromy group (see definition 8.20); this is a flat group scheme of finite type over $\mathbb{Z}_\ell$. By adapting theorem 7.1 we can show that there exist at most finitely many special subvarieties Y such that $\mathtt{GMT}(Y)_{\mathbb{Z}_\ell} \cong \mathtt{G}_\ell(A)$ for all primes ℓ (see theorem 8.22). On the other hand, the Mumford–Tate conjecture (8.21) implies that at least one such Y exists. In theorem 8.22 we will show that in the smallest unsolved case of the Mumford–Tate conjecture this is indeed the case. This provides additional evidence for the Mumford–Tate conjecture.

8.1 Generic integral Mumford–Tate groups

Let g and $n > 2$ be positive integers, and let $\mathcal{A}_{g,n}$ be the moduli space of complex principally polarised abelian varieties of dimension g with full level n structure. Let $\mathcal{X}_{g,n}$ be the universal abelian variety over $\mathcal{A}_{g,n}$, and let $\mathcal{V}_{g,n}$ be the variation of integral Hodge structures in $\mathcal{A}_{g,n}$ for which $\mathcal{V}_{g,n,y} = \mathrm{H}^1(\mathcal{X}^{\mathrm{an}}_{g,n,y}, \mathbb{Z})$ for every $y \in \mathcal{A}_{g,n}(\mathbb{C})$. If $Y \subset \mathcal{A}_{g,n}$ is a special subvariety, then we can define its *generic (integral) Mumford–Tate group* $\mathtt{GMT}(Y)$ analogously to how one defines the generic rational Mumford–Tate group for a variation of rational Hodge structures as for instance in [45]. if $y \in Y$ is Hodge generic (i.e. its special closure is Y) then $\mathtt{GMT}(Y)$ is isomorphic to the Mumford–Tate group of the integral Hodge structure $\mathcal{V}_{g,n,y}$. The resulting integral group scheme is flat and of finite type over $\mathbb{Z}$, and its generic fibre is a reductive rational algebraic group. The aim of this section is to prove the following theorem:

Theorem 8.1. *Let g and n be positive integers with $n > 2$, and let $\mathscr{G}$ be a group scheme over $\mathbb{Z}$. Then there are at most finitely many special subvarieties Y of $\mathcal{A}_{g,n}$ such that $\mathtt{GMT}(Y) \cong \mathscr{G}$.*

Throughout this section, by a *symplectic representation* of an algebraic group G over a field K we mean a morphism of algebraic groups $G \to \mathtt{GSp}(V, \psi)$ for some symplectic K-vector space (V, ψ). By [31, Thm. 2.1(b)] the isomorphism class of a symplectic representation is uniquely determined by its underlying representation $G \to \mathtt{GL}(V)$. The structure of this section is as follows: in subsection 8.1.1 we prove a weaker version of theorem 8.1 concerning only the generic fibre $\mathtt{GMT}(Y)_{\mathbb{Q}}$ (see proposition 8.2), and in subsection 8.1.2 we use this, and the theory of integral models in representations from chapter 7, to prove theorem 8.1.

8.1.1 The rational case

The goal of this subsection is to prove the following proposition:

Proposition 8.2. *Let G be a reductive algebraic group over $\mathbb{Q}$. Then up to Hecke correspondence there are only finitely many special subvarieties Y of $\mathcal{A}_{g,n}$ such that $\mathtt{GMT}(Y)_{\mathbb{Q}} \cong G$.*

This is as far as we can get into proving theorem 8.1 without using integral information, as rational Mumford–Tate groups are invariant under Hecke correspondences. We first need to set up some notation before we get to the proof. For an algebraic group G over $\mathbb{Q}$ we write $G(\mathbb{R})^+$ for the identity component of the Lie group $G(\mathbb{R})$. We write $\mathbb{S}$ for the Deligne torus $\mathrm{Res}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_{\mathrm{m}}$. Let $\mathcal{H}_g$ be the g-dimensional Siegel space; then $(\mathtt{GSp}_{2g}, \mathcal{H}_g)$ is a Shimura datum. We fix a connected component $\mathcal{H}_g^+ \subset \mathcal{H}_g$.

Definition 8.3. A *reductive connected Shimura datum* is a pair (G, X^+) consisting of a connected reductive group G over $\mathbb{Q}$ and a $G(\mathbb{R})^+$-orbit X^+ of morphisms $\mathbb{S} \to G_{\mathbb{R}}$ such that the pair $(G, G(\mathbb{R}) \cdot X^+)$ is a Shimura datum.

A reductive connected Shimura datum differs from a connected Shimura datum in the sense of [44, Def. 4.4] in that we do not require G to be semisimple, and we look at morphisms $\mathbb{S} \to G_{\mathbb{R}}$ instead of maps $\mathbb{S}^1 \to G_{\mathbb{R}}^{\mathrm{ad}}$.

Definition 8.4. A *connected Shimura triple of rank* $2g$ is a triple (G, X^+, ϱ) consisting of:

- a reductive algebraic group G over $\mathbb{Q}$;
- a $G(\mathbb{R})^+$-orbit $X^+ \subset \mathrm{Hom}(\mathbb{S}, G_{\mathbb{R}})$ such that the pair (G, X^+) is a connected reductive Shimura datum;
- an injective morphism of algebraic groups $\varrho\colon G \hookrightarrow \mathtt{GSp}_{2g,\mathbb{Q}}$ such that $\varrho_{\mathbb{R}} \circ X^+ \subset \mathcal{H}_g^+$, and such that G is the generic Mumford–Tate group of X^+ under this embedding.

A *morphism of connected Shimura triples* $\sigma\colon (G, X^+, \varrho) \to (G', X'^+, \varrho')$ is a morphism $\sigma\colon G \to G'$ such that $\sigma_{\mathbb{R}} \circ X^+ \subset X'^+$ and such that $\sigma \circ \varrho = \varrho'$. The collection of isomorphism classes of connected Shimura triples of rank $2g$ is denoted $\mathcal{S}_{2g}$; the subset of connected Shimura triples whose first element is isomorphic to an algebraic group G is denoted $\mathcal{S}_{2g}(G)$. We let $\mathrm{GSp}_{2g}(\mathbb{Q})$ act on $\mathcal{S}_{2g}(G)$ on the right by the formula

$$(G, X^+, \varrho) \cdot a = (G, X^+, \mathrm{inn}(a^{-1}) \circ \varrho). \tag{8.5}$$

The reason to study these special triples is that every special subvariety of $\mathcal{A}_g$ comes from a special triple in the following sense: the Shimura variety $\mathcal{A}_{g,n}$ is a finite disjoint union of complex analytical spaces of the form $\Gamma\backslash\mathcal{H}_g^+$, where $\Gamma \subset \mathrm{GSp}_{2g}(\mathbb{Z})$ is a congruence subgroup, and $\mathcal{H}_g^+$ is a connected component of $\mathcal{H}_g^+$. For such a Γ, and a connected Shimura triple (G, X^+, ϱ) of rank $2g$, denote by $Y_\Gamma(G, X^+, \varrho)$ the image of $\varrho(X^+) \subset \mathcal{H}_g^+$ in $\Gamma\backslash\mathcal{H}_g^+$. This is a special subvariety of $\Gamma\backslash\mathcal{H}_g^+$, and all special subvarieties arise in this way. Furthermore, $\mathtt{GMT}(Y_\Gamma(G, X^+, \varrho))_{\mathbb{Q}}$ is isomorphic to G. If $Y = Y_\Gamma(G, X^+, \varrho)$ and Y' are two special subvarieties of $\Gamma\backslash\mathcal{H}_g^+$ that differ by a Hecke correspondence, then there exists an $a \in \mathrm{GSp}_{2g}(\mathbb{Q})$ such that $Y' = Y_\Gamma(G, X^+, \varrho) \cdot a$. Proposition 8.2 is now a direct consequence of the following result.

Proposition 8.6. *Let G be a connected reductive group over $\mathbb{Q}$. Then the cardinality of the quotient set $\mathcal{S}_{2g}(G)/\mathrm{GSp}_{2g}(\mathbb{Q})$ is finite.*

The rest of this subsection is dedicated to the proof of this proposition. We first prove some auxiliary results.

Lemma 8.7. *Let d be a positive integer. Let Π be a finite subgroup of $\mathrm{GL}_d(\mathbb{Z})$, and let $\eta_0 \in \mathbb{Z}^d$ be such that $\Pi \cdot \eta_0$ generates the rational vector space $\mathbb{Q}^d$. Then up to the action of $\mathrm{Aut}_\Pi(\mathbb{Z}^d)$ there are only finitely many elements $\eta \in \mathbb{Z}^d$ such that for all $\pi_1, \ldots, \pi_d \in \Pi$ we have*

$$\det(\pi_1 \cdot \eta_0, \ldots, \pi_d \cdot \eta_0) = \det(\pi_1 \cdot \eta, \ldots, \pi_d \cdot \eta). \tag{8.8}$$

Proof. Fix $\pi_1, \dots, \pi_d \in \Pi$ such that the $\pi_i \cdot \eta_0$ are $\mathbb{Q}$-linearly independent, and define the integer $C := \det(\pi_1 \cdot \eta_0, \dots, \pi_d \cdot \eta_0)$; then $C \neq 0$. Now let $\eta \in \mathbb{Z}^d$ be such that it satisfies (8.8). Then $\det(\pi_1 \cdot \eta, \dots, \pi_d \cdot \eta) = C \neq 0$, so the $\pi_i \circ \eta$ are $\mathbb{Q}$-linearly independent as well. If π is any element of Π, then there exist unique $c_i, c_i' \in \mathbb{Q}$ such that $\pi \cdot \eta_0 = \sum_i c_i(\pi_i \cdot \eta_0)$ and $\pi \cdot \eta = \sum_i c_i'(\pi_i \cdot \eta)$. Then we may calculate

$$\begin{aligned} c_i \cdot C &= \det(\pi_1 \cdot \eta_0, \dots, \pi_{i-1} \cdot \eta_0, \pi \cdot \eta_0, \pi_{i+1} \cdot \eta_0, \dots, \pi_d \cdot \eta_0) \\ &= \det(\pi_1 \cdot \eta, \dots, \pi_{i-1} \cdot \eta, \pi \cdot \eta, \pi_{i+1} \cdot \eta, \dots, \pi_d \cdot \eta) \\ &= c_i' \cdot C, \end{aligned}$$

hence $c_i = c_i'$ for all i. We find that for every collection of scalars $(x_\pi)_{\pi \in \Pi}$ in $\mathrm{Map}(\Pi, \mathbb{Q})$ we have

$$\sum_{\pi \in \Pi} x_\pi \cdot (\pi \cdot \eta_0) = 0 \Leftrightarrow \sum_{\pi \in \Pi} x_\pi \cdot (\pi \cdot \eta) = 0.$$

It follows that that there exists a unique Π-equivariant linear isomorphism $f_\eta \colon \mathbb{Q}^d \to \mathbb{Q}^d$ satisfying $f_\eta(\eta_0) = \eta$. Let Λ_η be the lattice in $\mathbb{Q}^d$ generated by $\Pi \cdot \eta$; then $f_\eta(\Lambda_{\eta_0}) = \Lambda_\eta$. Now let $\eta' \in \mathbb{Z}^d$ be another element satisfying (8.8); then $f_{\eta'} \circ f_\eta^{-1}$ is the unique Π-equivariant automorphism of $\mathbb{Q}^d$ that sends η to η'. This automorphism induces a Π-equivariant automorphism of $\mathbb{Z}^d$ if and only if $f_\eta^{-1}(\mathbb{Z}^d) = f_{\eta'}^{-1}(\mathbb{Z}^d)$ in $\mathbb{Q}^d$; hence $\mathrm{Aut}_\Pi(\mathbb{Z}^d)$-orbits of suitable η correspond bijectively to lattices of the form $f_\eta^{-1}(\mathbb{Z}^d)$ in $\mathbb{Q}^d$. Let C be as above; then $\Lambda_\eta \subset \mathbb{Z}^d \subset C^{-1}\Lambda_\eta$, hence $\Lambda_{\eta_0} \subset f_\eta^{-1}(\mathbb{Z}^d) \subset C^{-1}\Lambda_{\eta_0}$. Since there are only finitely many options for lattices between Λ_{η_0} and $C^{-1}\Lambda_{\eta_0}$, we conclude that there are only finitely many options for the $\mathrm{Aut}_\Pi(\mathbb{Z}^d)$-orbit of η. ☐

Lemma 8.9. *Let T be a torus over $\mathbb{Q}$, and let $\nu \colon \mathbb{G}_{\mathrm{m},\bar{\mathbb{Q}}} \to \mathtt{GSp}_{2g,\bar{\mathbb{Q}}}$ be a symplectic representation. Let S be the collection of pairs (η, ϱ), where $\eta \colon \mathbb{G}_{\mathrm{m},\bar{\mathbb{Q}}} \to T_{\bar{\mathbb{Q}}}$ is a cocharacter whose image is Zariski dense in the $\mathbb{Q}$-group T, and $\varrho \colon T \hookrightarrow \mathtt{GSp}_{2g,\mathbb{Q}}$ is a faithful symplectic representation, such that $\nu \cong \varrho_{\bar{\mathbb{Q}}} \circ \eta$ as symplectic representations of $\mathbb{G}_{\mathrm{m},\bar{\mathbb{Q}}}$. Define an action of $\mathrm{Aut}(T)$ on S by $\sigma \cdot (\eta, \varrho) = (\sigma_{\bar{\mathbb{Q}}} \circ \eta, \varrho \circ \sigma^{-1})$. Then $\mathrm{Aut}(T) \backslash S$ is finite.*

Proof. Let $X = \mathrm{X}_*(T)$ as a free abelian group with a Galois action, and identify $\mathrm{X}^*(T)$ with $X^\vee$ via the natural perfect pairing. Let Π be the image of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{GL}(X)$; this is a finite group. Now let $(\eta, \varrho) \in S$; then ϱ is given by a multiset $W \subset X^\vee$. The fact that ϱ is faithful and defined over $\mathbb{Q}$ implies that W generates $X^\vee$ as an abelian group and that W is invariant under the action of Π. Since the image of η is Zariski dense in T, we find that $X_{\mathbb{Q}}$ is generated by $\Pi \cdot \eta$. Now let d be the rank of X, and let $\pi_1, \dots, \pi_d \in \Pi$. Consider the homomorphism of abelian groups

$$\begin{aligned} \varphi_{\eta,(\pi_i)_i} \colon X^\vee &\to \mathbb{Z}^d \\ \lambda &\mapsto (\lambda(\pi_i \cdot \eta))_{i \leq d}. \end{aligned}$$

The isomorphism class of the representation ν is given by a multiset $\Sigma \subset \mathrm{X}^*(\mathbb{G}_{\mathrm{m}}) = \mathbb{Z}$. Since we require $\nu \cong \varrho_{\mathbb{Q}} \circ \eta$, we find that $W \circ \eta = \Sigma$ as multisets in $\mathbb{Z}$. Furthermore, W is

Galois-invariant, so $W \circ (\pi \cdot \eta) = \Sigma$ for all $\pi \in \Pi$. Let

$$m := \max\{|\sigma| : \sigma \in \Sigma \subset \mathbb{Z}\};$$

then the multiset $\varphi_{\eta,(\pi)_i}(W)$ in $\mathbb{Z}^d$ is contained in $[-m, m]^d$. Now choose an identification $X \cong \mathbb{Z}^d$, so that we may consider $\varphi_{\eta,(\pi_i)_i}$ as an element of $\mathrm{Mat}_d(\mathbb{Z})$; then $|\det(\varphi_{\eta,(\pi_i)_i})|$ is equal to the volume of the image of a fundamental parallellogram of $\mathbb{Z}^d$. Since $X^\vee$ is generated by W, this volume cannot exceed m^d, hence $|\det(\varphi_{\eta,(\pi_i)_i})| \leq m^d$ for all choices of the π_i. Hence if we let (ϱ, η) range over S there are only finitely many possibilities for the map

$$\begin{aligned} t_\eta \colon \Pi^d &\to \mathbb{Z} \\ (\pi_1, \ldots, \pi_d) &\mapsto \det(\varphi_{\eta,(\pi_i)_i}). \end{aligned}$$

By lemma 8.7 there are, up to the action of $\mathrm{Aut}(T) \cong \mathrm{Aut}_\Pi(X)$, only finitely many $\eta \in X$ yielding the same t_η; since the set of possible t_η is also finite, we see that there are only finitely many options for η (up to the $\mathrm{Aut}(T)$-action). Now fix such an η. For every $w \in W$ we need to have $w(\pi \cdot \eta) \in \Sigma$, for all $\pi \in \Pi$. Since $\Pi \cdot \eta$ generates $X_\mathbb{Q}$, there are only finitely many options for w, hence for the multiset W, since the cardinality of W has to be equal to $2g$. We conclude that up to the action of $\mathrm{Aut}(T)$ there are only finitely many possibilities for (η, ϱ). □

Lemma 8.10. *Let G be a connected reductive group over $\mathbb{Q}$, and let Z^0 be the identity component of its centre; let φ be the map $\mathrm{Aut}(G) \to \mathrm{Aut}(Z^0)$. Then $\varphi(\mathrm{Aut}(G))$ has finite index in $\mathrm{Aut}(Z^0)$.*

Proof. Let $H := Z^0 \cap G^{\mathrm{der}}$, and let $n := \#H$. If σ is an automorphism of Z^0 that is the identity on H, then we can extend σ to an automorphism $\tilde{\sigma}$ of G by having $\tilde{\sigma}$ be the identity on G^{der}; hence it suffices to show that the subgroup

$$\left\{\sigma \in \mathrm{Aut}(Z^0) \colon \sigma|_H = \mathrm{id}_H\right\} \subset \mathrm{Aut}(Z^0)$$

has finite index. Let $X = \mathrm{X}_*(Z^0)$. Let $\sigma \in \mathrm{Aut}(T)$, and consider σ as an element of $\mathrm{GL}(X)$. If σ maps to the identity in $\mathrm{Aut}_{\mathbb{Z}/n\mathbb{Z}}(X/nX)$, then σ is the identity on $Z^0[n]$, and in particular on H. Since $\mathrm{Aut}_{\mathbb{Z}/n\mathbb{Z}}(X/nX)$ is finite, the lemma follows. □

Lemma 8.11. *Let G be a connected reductive group over $\mathbb{Q}$, and let Z^0 be the identity component of its centre. Let ϱ_{cent} and ϱ_{der} be $2g$-dimensional symplectic representations of Z^0 and G^{der}. Then there are at most finitely many isomorphism classes of symplectic representations ϱ of G such that $\varrho|_{Z^0} \cong \varrho_{\mathrm{cent}}$ and $\varrho|_{G^{\mathrm{der}}} \cong \varrho_{\mathrm{der}}$ as symplectic representations of Z^0 and G^{der}, respectively.*

Proof. Let T' be a maximal torus of G^{der}; then the isomorphism classes of ϱ_{cent} and ϱ_{der} are given by multisets $\Sigma_{\mathrm{cent}} \subset \mathrm{X}^*(Z^0)$ and $\Sigma_{\mathrm{der}} \subset \mathrm{X}^*(T')$, both of cardinality $2g$. Let $T := Z^0 \cdot T' \subset G$, this is a maximal torus. A symplectic representation ϱ of G satisfying these conditions corresponds to a multiset $\Sigma \subset \mathrm{X}^*(T)$ of cardinality $2g$, such that Σ maps to Σ_{cent} in $\mathrm{X}^*(Z^0)$ and to Σ_{der} in $\mathrm{X}^*(T')$. Because

$$\mathrm{X}^*(T)_\mathbb{Q} = \mathrm{X}^*(Z^0)_\mathbb{Q} \oplus \mathrm{X}^*(T')_\mathbb{Q}$$

there are only finitely many options for Σ, as we obtain all of them by pairing elements of Σ_{cent} with elements of Σ_{der}. □

Proof of proposition 8.6. Let Ω be the sets of pairs (X^+, ϱ) such that (G, X^+, ϱ) is a special triple. The group $\mathrm{Aut}(G)$ acts on Ω by $\sigma \cdot (X^+, \varrho) := (\sigma_{\mathbb{R}} \circ X^+, \varrho \circ \sigma^{-1})$, and we may identify $\mathcal{S}_{2g}(G)$ with $\mathrm{Aut}(G)\backslash\Omega$. Furthermore, Ω has the same right action of $\mathrm{GSp}_{2g}(\mathbb{Q})$ as $\mathcal{S}_{2g}(G)$; we write $\bar{\Omega} := \Omega/\mathrm{GSp}_{2g}(\mathbb{Q})$. Since the left and right actions on Ω commute, we get an action of $\mathrm{Aut}(G)$ on $\bar{\Omega}$, and this identifies $\mathrm{Aut}(G)\backslash\bar{\Omega}$ with $\mathcal{S}_{2g}(G)/\mathrm{GSp}_{2g}(\mathbb{Q})$.

Consider the natural projection $Z^0 \times G^{\mathrm{der}} \to G$. This is an isogeny, and we let n be its degree. Let (X^+, ϱ) be an element of Ω. If x is an element of X^+, then the composite map

$$\mathbb{S} \xrightarrow{n} \mathbb{S} \xrightarrow{x} G_{\mathbb{R}}$$

factors uniquely through $Z^0_{\mathbb{R}} \times G^{\mathrm{der}}_{\mathbb{R}}$. Let x_{cent} and x_{der} be the associated maps from $\mathbb{S}$ to $Z^0_{\mathbb{R}}$ and $G^{\mathrm{der}}_{\mathbb{R}}$, respectively; then $X^+_{\mathrm{der}} := \{x_{\mathrm{der}} : x \in X^+\}$ is a $G^{\mathrm{der}}(\mathbb{R})^+$-orbit in $\mathrm{Hom}(\mathbb{S}, G^{\mathrm{der}}_{\mathbb{R}})$. Let $X^{+,\mathrm{ad}}$ be the image of X^+ under $\mathrm{Ad}\colon G \to G^{\mathrm{ad}}$; then $(G^{\mathrm{ad}}, X^{+,\mathrm{ad}})$ is a connected Shimura datum (in the sense of [39, Def. 4.4]). Furthermore $\mathrm{Ad} \circ X^+_{\mathrm{der}} = X^{+,\mathrm{ad}} \circ n$ as subsets of $\mathrm{Hom}(\mathbb{S}, G^{\mathrm{ad}}_{\mathbb{R}})$. Now let $\bar{\Omega}_{\mathrm{der}}$ be the set of all pairs $(Y^+, \bar{\sigma})$ satisfying:

- Y^+ is a $G^{\mathrm{der}}(\mathbb{R})^+$-orbit in $\mathrm{Hom}(\mathbb{S}, G^{\mathrm{der}}_{\mathbb{R}})$ such that $\mathrm{Ad} \circ Y^+ = X^{+,\mathrm{ad}} \circ n$ for some connected Shimura datum $(G^{\mathrm{ad}}, X^{+,\mathrm{ad}})$;
- $\bar{\sigma}$ is an isomorphism class of symplectic representations of G^{der} of dimension $2g$.

It follows from [11, Cor. 1.2.8] that, for a given G, there are only finitely many possibilities for $X^{+,\mathrm{ad}}$. Since $\mathrm{Ad}\colon G^{\mathrm{der}} \to G^{\mathrm{ad}}$ is an isogeny, there are only finitely many possibilities for Y^+. Furthermore a semisimple group has only finitely many symplectic representations of a given dimension, hence $\bar{\Omega}_{\mathrm{der}}$ is a finite set. Consider also the following set:

$$\Xi_{\mathrm{cent}} := \Big\{(\eta, \bar{\tau}) : \eta \in \mathrm{X}^*(Z^0), \bar{\tau} \text{ isom. class of sympl. rep. of } Z^0 \text{ of dim. } 2g\Big\}.$$

If $\mu\colon \mathbb{G}_{\mathrm{m},\mathbb{C}} \to \mathbb{S}_{\mathbb{C}}$ is the Hodge cocharacter, then there is a natural map

$$\begin{aligned} \varphi_{\mathrm{cent}}\colon \bar{\Omega} &\to \Xi_{\mathrm{cent}} \\ (X^+, \varrho) &\mapsto (x_{\mathrm{cent}} \circ \mu, \varrho|_{Z^0}) \end{aligned}$$

for some $x \in X^+$; this is well-defined because x_{cent} does not depend on the choice of x, and because $x_{\mathrm{cent},\mathbb{C}} \circ \mu\colon \mathbb{G}_{\mathrm{m},\mathbb{C}} \to Z^0_{\mathbb{C}}$, being a morphism of tori, is defined over $\bar{\mathbb{Q}}$. Let $\bar{\Omega}_{\mathrm{cent}}$ be the image of $\bar{\Omega}$ in Ξ_{cent}. We also have a map

$$\begin{aligned} \varphi_{\mathrm{der}}\colon \bar{\Omega} &\to \bar{\Omega}_{\mathrm{der}} \\ (X^+, \varrho) &\mapsto (X^+_{\mathrm{der}}, \varrho|_{G^{\mathrm{der}}}). \end{aligned}$$

Consider the product map $\varphi := \varphi_{\mathrm{cent}} \times \varphi_{\mathrm{der}}\colon \bar{\Omega} \to \bar{\Omega}_{\mathrm{cent}} \times \bar{\Omega}_{\mathrm{der}}$. An element $x \in X^+$ is determined by x_{cent} and x_{der}, so X^+ is determined by x_{cent} and X^+_{der}. Furthermore lemma

8.11 tells us that the isomorphism class of ϱ is determined, up to a finite choice, by the isomorphism classes of $\varrho|_{Z^0}$ and $\varrho|_{G^{\mathrm{der}}}$. As such we find that φ is finite. It is also $\mathrm{Aut}(G)$-equivariant, where $\mathrm{Aut}(G)$ works on the right hand side via the map

$$\mathrm{Aut}(G) \to \mathrm{Aut}(Z^0) \times \mathrm{Aut}(G^{\mathrm{der}}).$$

It follows that the induced map

$$\mathrm{Aut}(G)\backslash\bar{\Omega} \to \mathrm{Aut}(G)\backslash(\bar{\Omega}_{\mathrm{cent}} \times \bar{\Omega}_{\mathrm{der}})$$

is finite as well; to show that its domain is finite, it now suffices to show that its codomain is finite. To see this, let (X^+, ϱ) be an element of Ω, and let $x \in X^+$. Then the isomorphism class of $\varrho_{\mathbb{R}} \circ x$ is fixed; it is the symplectic representation of $\mathbb{S}$ corresponding to a polarised Hodge structure of type $\{(1,0),(0,1)\}$ of dimension $2g$. It follows that the isomorphism class of the representation $\varrho_{\mathbb{R}} \circ x_{\mathrm{cent}}$ of $\mathbb{S}$ is uniquely determined, hence there is only one possibility for the isomorphism class of the symplectic representation $\varrho_{\mathbb{C}} \circ x_{\mathrm{cent},\mathbb{C}} \circ \mu$ of $\mathbb{G}_{\mathrm{m},\mathbb{C}}$. Now choose x such that $x(\mathbb{S})$ is Zariski dense in G, which exists by our assumption that G is the generic Mumford–Tate group on X. Then the image of $x_{\mathrm{cent}} \circ \mu$ is Zariski dense in Z^0. Since there was only one possibility for $\varrho_{\mathbb{C}} \circ x_{\mathrm{cent},\mathbb{C}} \circ \mu$, lemma 8.9 now tells us that $\mathrm{Aut}(Z^0)\backslash\bar{\Omega}_{\mathrm{cent}}$ is finite. Since the image of $\mathrm{Aut}(G)$ in $\mathrm{Aut}(Z^0)$ has finite index by lemma 8.10 and $\bar{\Omega}_{\mathrm{der}}$ is finite, we conclude that $\mathrm{Aut}(G)\backslash(\bar{\Omega}_{\mathrm{cent}} \times \bar{\Omega}_{\mathrm{der}})$ is finite; this proves the proposition. □

8.1.2 The integral case

In this subsection we prove theorem 8.1. Recall that as a complex analytic space we can view $\mathcal{A}_{g,n}$ as a disjoint union of spaces of the form $\Gamma\backslash\mathcal{H}_g^+$, where Γ is a congruence subgroup of $\mathrm{GSp}_{2g}(\mathbb{Z})$. As before, for a connected Shimura triple (G, X^+, ϱ), let $Y_\Gamma(G, X^+, \varrho)$ be the image of $\varrho(X^+)$ in $\Gamma\backslash\mathcal{H}_g^+$. We call two special triples (G, X^+, ϱ) and (G', X'^+, ϱ) *equivalent under* Γ if

$$Y_\Gamma(G, X^+, \varrho) = Y_\Gamma(G', X', \varrho').$$

This holds if and only if there is a $\gamma \in \Gamma$ such that $(G, X^+, \varrho) \cong (G', X'^+, \varrho') \cdot \gamma$, where the action of $\Gamma \subset \mathrm{GSp}_{2g}(\mathbb{Q})$ on $\mathcal{S}_{2g}$ is as in (8.5). Let $\mathrm{Mod}(G)$ be the set of (integral) models of G as in definition 7.2. Using this notation we get a natural map

$$\mathtt{GMT}\colon \mathcal{S}_{2g}(G)/\Gamma \to \mathrm{Mod}(G)$$

by sending (G, X^+, ϱ) to the generic (integral) Mumford–Tate group of $Y_\Gamma(G, X^+, \varrho)$; note that this is the same as the generic Mumford–Tate group of X^+. We may also describe this map in the terminology of chapter 7, as follows: let $(G, X^+, \varrho) \in \mathcal{S}_{2g}(G)$. The standard representation $V := \mathbb{Q}^{2g}$ of $\mathtt{GSp}_{2g,\mathbb{Q}}$ has a lattice $\Lambda := \mathbb{Z}^{2g}$. Then $\mathtt{GMT}(G, X^+, \varrho) = \mathtt{mod}_{\varrho(G)}(\Lambda)$. We can also understand Hecke correspondences in this way: recall that special subvarieties equivalent to $Y_\Gamma(G, X^+, \varrho)$ under Hecke correspondence are of the form

$Y_\Gamma(G, X^+, \mathrm{inn}(a^{-1}) \circ \varrho)$ for some $a \in \mathrm{GSp}_{2g}(\mathbb{Q})$. For such a connected Shimura triple we get

$$\mathtt{GMT}(G, X^+, \mathrm{inn}(a^{-1}) \circ \varrho) = \mathtt{mod}_{a^{-1}\varrho(G)a}(\Lambda) = \mathtt{mod}_{\varrho(G)}(a\Lambda). \tag{8.12}$$

Furthermore, the map GMT defined above allows us to consider theorem 8.1 as a consequence of the following result:

Theorem 8.13. *Let G be a connected reductive group over $\mathbb{Q}$, and let $\Gamma \subset \mathrm{GSp}_{2g}(\mathbb{Z})$ be a congruence subgroup. Then the map* $\mathtt{GMT}\colon \mathcal{S}_{2g}(G)/\Gamma \to \mathrm{Mod}(G)$ *is finite.*

Proof of theorem 8.1 from theorem 8.13. The Shimura variety $\mathcal{A}_{g,n}$ is a finite disjoint union of connected Shimura varieties $\Gamma\backslash\mathcal{H}_g^+$. We need to show that for every Γ and for every group scheme $\mathscr{G}$ over $\mathbb{Z}$ there are only finitely many special subvarieties of $\Gamma\backslash\mathcal{H}_g^+$ whose generic Mumford–Tate group is isomorphic to $\mathscr{G}$. Let G be the generic fibre of $\mathscr{G}$; then every such special subvariety is of the form $Y_\Gamma(G, X^+, \varrho)$, for some (X^+, ϱ) such that $(G, X^+, \varrho) \in \mathcal{S}_{2g}(G)$. The theorem now follows from theorem 8.13. □

Let Γ be a congruence subgroup of $\mathrm{GSp}_{2g}(\mathbb{Z})$. Write $M(\Gamma) := \Gamma\backslash\mathcal{H}_g^+$; this is a real analytic space. If Γ is small enough, then $M(\Gamma)$ is a connected Shimura variety. Let $\hat{\mathcal{H}}_g^+$ be the subspace $\mathrm{GL}_{2g}(\mathbb{R}) \cdot \mathcal{H}_g^+$ of $\mathrm{Hom}(\mathbb{S}, \mathtt{GL}_{2g,\mathbb{R}})$, and let $\hat{\Gamma}$ be a congruence subgroup of $\mathrm{GL}_{2g}(\mathbb{Z})$ and define $\hat{M}(\hat{\Gamma}) := \hat{\Gamma}\backslash\hat{\mathcal{H}}_g^+$. This is a real analytic space, but for $g > 1$ it will not have the structure of a connected Shimura variety.

Lemma 8.14. *Let $\Gamma \subset \mathrm{GSp}_{2g}(\mathbb{Z})$ be a congruence subgroup, and let $\hat{\Gamma} \subset \mathrm{GL}_{2g}(\mathbb{Z})$ be a congruence subgroup containing Γ. Then the map of real analytic spaces $M(\Gamma) \to \hat{M}(\hat{\Gamma})$ is finite.*

Proof. It suffices to prove this for $\Gamma = \mathrm{GSp}_{2g}(\mathbb{Z})$ and $\hat{\Gamma} = \mathrm{GL}_{2g}(\mathbb{Z})$. For these choices of congruence subgroups we have (see [16, 4.3]):

$$\begin{aligned} M(\Gamma) &\cong \Big\{\text{princ. pol. Hodge structures of type } \{(0,1),(1,0)\} \text{ on } \mathbb{Z}^{2g}\Big\}/\cong, \\ \hat{M}(\hat{\Gamma}) &\cong \Big\{\text{Hodge structures of type } \{(0,1),(1,0)\} \text{ on } \mathbb{Z}^{2g}\Big\}/\cong, \end{aligned}$$

where in the first equation we consider isomorphisms of polarised Hodge structures, and in the second equation isomorphisms of Hodge structures. In this terminology the natural map $M(\Gamma) \to \hat{M}(\hat{\Gamma})$ is just forgetting the polarisation. By [38, Thm. 18.1] a polarisable $\mathbb{Z}$-Hodge structure of type $\{(0,1),(1,0)\}$ has only finitely many principal polarisations (up to automorphisms of polarised Hodge structures), from which the lemma follows. □

Proof of theorem 8.13. By proposition 8.6 it suffices to show that for every $\mathrm{GSp}_{2g}(\mathbb{Q})$-orbit B in $\mathcal{S}_{2g}(G)$ the map $\mathtt{GMT}\colon B/\Gamma \to \mathrm{Mod}(G)$ is finite. Let (G, X^+, ϱ) be an element of such a B, and let N be the scheme-theoretic normaliser of $\varrho(G)$ in $\mathtt{GSp}_{2g,\mathbb{Q}}$. Then as a right $\mathrm{GSp}_{2g}(\mathbb{Q})$-set we can identify B with $N(\mathbb{Q})\backslash\mathrm{GSp}_{2g}(\mathbb{Q})$, and under this identification we have

$$\begin{aligned} B/\Gamma &\xrightarrow{\sim} N(\mathbb{Q})\backslash\mathrm{GSp}_{2g}(\mathbb{Q})/\Gamma \\ (G, X^+, \varrho) \cdot a\Gamma &\mapsto N(\mathbb{Q})a\Gamma. \end{aligned} \tag{8.15}$$

Now let $V := \mathbb{Q}^{2g}$ be the standard representation of $\mathtt{GSp}_{2g,\mathbb{Q}}$, and let $\hat{N}$ be the scheme-theoretic normaliser of $\varrho(G)$ in $\mathtt{GL}_{2g,\mathbb{Q}}$. Furthermore, recall that $\mathrm{Lat}_{\hat{N}}(V)$ is the set of $\hat{N}(\mathbb{Q})$-orbits of lattices in V (see definition 7.3); by considering every lattice as $g \cdot \Lambda$ for $\Lambda := \mathbb{Z}^{2g}$ and $g \in \mathrm{GL}_{2g}(\mathbb{Q})$, we get a natural identification

$$\mathrm{Lat}_{\hat{N}}(V) \cong \hat{N}(\mathbb{Q})\backslash \mathrm{GL}_{2g}(\mathbb{Q})/\mathrm{GL}_{2g}(\mathbb{Z}).$$

From (8.12) we see that the map $\mathtt{GMT}\colon B/\Gamma \to \mathrm{Mod}(G)$ sends a double coset $N(\mathbb{Q})a\Gamma$, considered as an element of B/Γ via (8.15), to $\mathtt{mod}_G(a\Lambda)$. As such we can decompose $\mathtt{GMT}$ as a composite map

$$\begin{aligned} B/\Gamma &\xrightarrow{\sim} N(\mathbb{Q})\backslash \mathrm{GSp}_{2g}(\mathbb{Q})/\Gamma \\ &\twoheadrightarrow N(\mathbb{Q})\backslash \mathrm{GSp}_{2g}(\mathbb{Q})/\mathrm{GSp}_{2g}(\mathbb{Z}) && (8.16)\\ &\to \hat{N}(\mathbb{Q})\backslash \mathrm{GL}_{2g}(\mathbb{Q})/\mathrm{GL}_{2g}(\mathbb{Z}) && (8.17)\\ &\xrightarrow{\sim} \mathrm{Lat}_{\hat{N}}(V) \\ &\xrightarrow{\mathtt{mod}_G} \mathrm{Mod}(G). && (8.18)\end{aligned}$$

Since Γ is of finite index in $\mathrm{GSp}_{2g}(\mathbb{Z})$ we see that the map in (8.16) is finite. Furthermore, theorem 7.1 tells us that the map in (8.18) is finite, so it suffices to prove that the map in (8.17) is finite; denote this map by f. Let $\mathcal{Z}$ be the set of connected real analytic subspaces of $M(\mathrm{GSp}_{2g}(\mathbb{Z}))$, and let $\hat{\mathcal{Z}}$ be the set of connected real analytic subspaces of $\hat{M}(\mathrm{GL}_{2g}(\mathbb{Z}))$. Since the map $M(\mathrm{GSp}_{2g}(\mathbb{Z})) \to \hat{M}(\mathrm{GL}_{2g}(\mathbb{Z}))$ is finite by lemma 8.14, the induced map $z\colon \mathcal{Z} \to \hat{\mathcal{Z}}$ is finite as well. There are injective maps

$$\begin{aligned} \iota\colon N(\mathbb{Q})\backslash \mathrm{GSp}_{2g}(\mathbb{Q})/\mathrm{GSp}_{2g}(\mathbb{Z}) &\hookrightarrow \mathcal{Z} \\ \hat{\iota}\colon \hat{N}(\mathbb{Q})\backslash \mathrm{GL}_{2g}(\mathbb{Q})/\mathrm{GL}_{2g}(\mathbb{Z}) &\hookrightarrow \hat{\mathcal{Z}} \end{aligned}$$

where ι sends the class of $a \in \mathrm{GSp}_{2g}(\mathbb{Q})$ to the image of $a^{-1}\rho(X^+)a$ in $\mathrm{GSp}_{2g}(\mathbb{Z})\backslash\mathcal{H}_g^+$, and $\hat{\iota}$ sends the class of $a \in \mathrm{GL}_{2g}(\mathbb{Q})$ to the image of $a^{-1}\rho(X^+)a$ in $\mathrm{GL}_{2g}(\mathbb{Z})\backslash\hat{\mathcal{H}}_g^+$. Then $z \circ \iota = \hat{\iota} \circ f$, and since z is finite and $\iota, \hat{\iota}$ are injective, we see that f is finite; this proves the theorem. □

Remark 8.19. By applying remark 7.61 rather than theorem 7.1, we can also prove that for every collection $(\mathscr{G}_\ell)_\ell$ of group schemes over $\mathbb{Z}_\ell$, there exist only finitely many special subvarieties Y of $\mathcal{A}_{g,n}$ such that $\mathtt{GMT}(Y)_{\mathbb{Z}_\ell} \cong \mathscr{G}_\ell$ for all prime numbers ℓ.

8.2 Connection to the Mumford–Tate conjecture

Let K be a number field embedded in $\mathbb{C}$, and let A be a principally polarised abelian variety over K. Let $\mathtt{MT}(A)$ be the (integral) Mumford–Tate group of A; it is the smallest closed subgroup scheme of $\mathtt{GSp}(\mathrm{H}^1(A^{\mathrm{an}}_{\mathbb{C}}, \mathbb{Z}))$ through which s factors, where

$$s\colon \mathbb{S} \to \mathtt{GSp}(\mathrm{H}^1(A^{\mathrm{an}}_{\mathbb{C}}, \mathbb{R}))$$

is the morphism defining the polarised Hodge structure. On the other hand, for every prime number ℓ there is a natural action of $\mathrm{Gal}(\bar{K}/K)$ on the étale cohomology $\mathrm{H}^1_{\text{ét}}(A_{\bar{K}}, \mathbb{Z}_\ell)$ which fixes the polarisation up to a scalar.

Definition 8.20. Let A be an abelian variety over a number field K, and let ℓ be a prime number. Then the *ℓ-adic Galois monodromy group of A*, $\mathtt{G}_\ell(A)$, is defined as follows: its generic fibre $\mathtt{G}_\ell(A)_{\mathbb{Q}_\ell}$ is the unit component of the Zariski closure of the image of $\mathrm{Gal}(\bar{K}/K)$ in $\mathtt{GSp}(\mathrm{H}^1_{\text{ét}}(A_{\bar{K}}, \mathbb{Q}_\ell))$, and $\mathtt{G}_\ell(A)$ itself is the Zariski closure of $\mathtt{G}_\ell(A)_{\mathbb{Q}_\ell}$ in $\mathtt{GSp}(\mathrm{H}^1_{\text{ét}}(A_{\bar{K}}, \mathbb{Z}_\ell))$.

One reason for taking the unit component, rather than the entire Zariski closure, is that the unit component remains unchanged if we replace K by a finite extension. Via the comparison theorem there is a canonical isomorphism of free $\mathbb{Z}_\ell$-modules with a symplectic form $\mathrm{H}^1_{\text{ét}}(A_{\bar{K}}, \mathbb{Z}_\ell) \xrightarrow{\sim} \mathrm{H}^1(A^{\text{an}}_{\mathbb{C}}, \mathbb{Z})_{\mathbb{Z}_\ell}$. As such we can regard $\mathtt{MT}(A)_{\mathbb{Z}_\ell}$ and $\mathtt{G}_\ell(A)$ as subgroup schemes of the same group scheme $\mathtt{GSp}(\mathrm{H}^1_{\text{ét}}(A_{\bar{K}}, \mathbb{Z}_\ell))$. The Mumford–Tate conjecture now claims the following:

Conjecture 8.21 (Mumford–Tate conjecture)**.** *Let A be an abelian variety over a number field K. Then for every prime ℓ one has $\mathtt{MT}(A)_{\mathbb{Z}_\ell} = \mathtt{G}_\ell(A)$ as subgroup schemes of $\mathtt{GSp}(\mathrm{H}^1_{\text{ét}}(A_{\bar{K}}, \mathbb{Z}_\ell))$.*

The Mumford–Tate conjecture is usually formulated in terms of the generic fibres of these groups, but this is equivalent to the 'integral' statement above. In general, the Mumford–Tate conjecture is very much an open problem, with the smallest unproven case appearing in dimension 4 already; this concerns abelian fourfolds of Mumford's type, see definition 8.27. An overview of the progress on the Mumford–Tate conjecture for abelian varieties is given in [8]. The conjecture has also been stated, and proven in some cases, for smooth proper varieties in general; see for example [1] or independently [64], [65] for the case of K3 surfaces, or [46] for the case of varieties with $h^{2,0} = 1$.

An implicit consequence of the Mumford–Tate conjecture is that the group schemes $\mathtt{G}_\ell(A)$ are all compatible in the sense that they all come from the same group scheme over $\mathbb{Z}$. This implies, for example, that all $\mathtt{G}_\ell(A)_{\bar{\mathbb{Q}}_\ell}$ have the same root system, and that $\mathtt{G}_\ell(A)$ is a reductive group scheme over $\mathbb{Z}_\ell$ for $\ell \gg 0$. The compatibility between the algebraic groups $\mathtt{G}_\ell(A)_{\mathbb{Q}_\ell}$ has been studied in [34] and [54]. In this section, we study a related question:

Question. *Let $n > 2$ be an integer, and let $g := \dim(A)$. Does there exist a special subvariety Y of $\mathcal{A}_{g,n}$ such that $\mathtt{GMT}(Y)_{\mathbb{Z}_\ell} \cong \mathtt{G}_\ell(A)$ for all prime numbers ℓ?*

It should be noted that if the Mumford–Tate conjecture is true, and x is a point on $\mathcal{A}_{g,n}$ corresponding to A, then the special closure of x provides a positive answer to question 8.2; hence a positive answer to this question provides additional evidence for the Mumford–Tate conjecture. Our main goal is to prove the following theorem. On one hand, it shows that the Y satisfying the conditions of question 8.2 are limited. On the other hand, it provides a positive answer to this question in the smallest unsolved case of the Mumford–Tate conjecture.

Theorem 8.22. *Let A be a g-dimensional principally polarised abelian variety over a number field*

$K \subset \mathbb{C}$, and let $n > 2$ be an integer. Then there exist at most finitely many special subvarieties Y of $\mathcal{A}_{g,n}$ such that $\mathtt{GMT}(Y)_{\mathbb{Z}_\ell} \cong \mathtt{G}_\ell(A)$ for all prime numbers ℓ. If A is of Mumford's type (see definition 8.27) then at least one such Y exists.

Without loss of generality we may replace K by a finite extension, and we will do so over the course of the proof. Roughly speaking the proof of the second part of this theorem is as follows: first, we classify groups of Mumford's type over a given field by means of quaternion algebras. Since quaternion algebras are determined by their local invariants, we can 'glue' the $\mathtt{G}_\ell(A)_{\mathbb{Q}_\ell}$ to a $\mathbb{Q}$-group G. The final step is to combine the integral structures in each $\mathtt{G}_\ell(A)$ to find an integral model of G.

8.2.1 Groups of Mumford's type and quaternion algebras

In this section we define groups of Mumford's type, and we classify them by means of quaternion algebras. For this we need to generalise the concept of quaternion algebras, and several of their characteristics, to étale algebras over a given field.

Definition 8.23. Let k be a field, and let E be an étale algebra over k. Suppose $E = \prod_i E_i$, where each E_i is a field extension of k. A *quaternion algebra* over E is an (non-commutative) E-algebra D such that each $D_i := E_i \otimes_E D$ is a quaternion algebra over E_i. The set of isomorphism classes of quaternion algebras over E is denoted $\mathrm{Quat}(E)$.

Suppose E is an étale algebra over a field k of rank n, and let D be a quaternion algebra over E. Let $\mathrm{Cores}_{E/k}(D)$ be the *corestriction* of D from E to k as defined in [33, 2.3]; this is a central simple algebra over k of dimension 2^n. There is a natural 'norm' homomorphism of groups

$$\mathrm{Nm}\colon D^\times \to \mathrm{Cores}_{E/k}(D)^\times$$

That can be interpreted as a morphism of algebraic groups if we consider both the domain and the codomain as algebraic groups over k (see [48, §4]). If k is algebraically closed the norm map is described as follows: Since every central simple algebra over k is a matrix algebra, we have $D^\times \cong \mathrm{GL}_2(k)^n$ and $\mathrm{Cores}_{E/k}(D)^\times \cong \mathrm{GL}_{2^n}(k)$ (also as algebraic groups over k). The map

$$\mathrm{Nm}\colon \mathrm{GL}_2(k)^n \to \mathrm{GL}_{2^n}(k) \tag{8.24}$$

is the representation of $\mathrm{GL}_2(k)^n$ obtained by taking the tensor product of the standard representation of its n factors.

We say that $\mathrm{Cores}_{E/k}(D)$ is *trivial* if it is isomorphic (as a k-algebra) to $\mathrm{Mat}_{2^n}(k)$; denote the subset of quaternion algebras with trivial corestriction by $\mathrm{Quat}_0(E)$. The following classification of quaternion algebras over étale algebras is a straightforward consequence of the 'regular' classification of quaternion algebras over local fields and number fields; see for example [53, §18] and [30]. For a number field k we denote the set of places of k by $\mathrm{S}(k)$.

Lemma 8.25. *Let k be a field, and let $E = \prod_i E_i$ be an étale algebra over k, where each E_i is a finite field extension of k.*

1. *Suppose k is a local field of characteristic 0; then there is a natural bijection*

$$\psi_E \colon \mathrm{Quat}(E) \xrightarrow{\sim} \bigoplus_i \tfrac{1}{2}\mathbb{Z}/\mathbb{Z}$$

whose image consists of all sequences $(d_i)_i$ such that $d_i = 0$ for all i with $E_i = \mathbb{C}$. This map sends $\mathrm{Quat}_0(E)$ to the subset of all $(d_i)_i \in \bigoplus_i(\frac{1}{2}\mathbb{Z}/\mathbb{Z})$ satisfying $\sum_i d_i = 0$. For a quaternion algebra D one has $E_i \otimes_E D \cong \mathrm{Mat}_2(E_i)$ if and only if the corresponding sequence satisfies $d_i = 0$; if $d_i = \frac{1}{2}$, then $E_i \otimes_E D$ is the unique nonsplit quaternion algebra over E_i.

2. *Suppose k is a number field, and suppose E is a field extension of k. Then the natural map*

$$\left(\prod_{w \in \mathrm{S}(E)} \psi_{E_w}\right) : \mathrm{Quat}(E) \to \prod_{w \in \mathrm{S}(E)} (\tfrac{1}{2}\mathbb{Z}/\mathbb{Z})$$

is injective, and its image equals the set of sequences $(d_w)_w$ satisfying $d_w = 0$ for almost all v, $d_w = 0$ if $E_w \cong \mathbb{C}$, and $\sum_w d_w = 0$. This map sends $\mathrm{Quat}_0(E)$ to the subset of all $(d_w)_w$ such that for every $v \in \mathrm{S}(k)$ one has $\sum_{w|v} d_w = 0$. □

Remark 8.26. Let k be a number field, and let E be a field extension of k. Since for every place v of k one has $k_v \otimes_k E \cong \prod_{w|v} E_w$, lemma 8.25 tells us that the natural map

$$\begin{array}{rcl} \mathrm{Quat}(E) & \to & \prod_{v \in \mathrm{S}(k)} \mathrm{Quat}(k_v \otimes_k E) \\ D & \mapsto & (k_v \otimes_k D)_v \end{array}$$

is injective and sends $\mathrm{Quat}_0(E)$ into the product of the $\mathrm{Quat}_0(k_v \otimes_k E)$.

We will use these algebraic objects to classify the algebraic groups we are interested in.

Definition 8.27. Let k be a field, let G be an algebraic group over k, and let V be a faithful representation of G. We say that (G, V) is *of Mumford's type* if the following three conditions are satisfied:

1. $\mathrm{Lie}(G)$ has a one dimensional centre $\mathfrak{c}$;
2. $\mathrm{Lie}(G)_{\bar{k}} \cong \mathfrak{c}_{\bar{k}} \oplus \mathfrak{sl}_{2,\bar{k}}^3$;
3. $\mathrm{Lie}(G)_{\bar{k}}$ acts on $V_{\bar{k}}$ by the tensor product of the standard representations C, V_1, V_2, V_3 of $\mathfrak{c}_{\bar{k}}$ and the factors $\mathfrak{sl}_{2,\bar{k}}$, respectively.

The set of isomorphism classes of triples of Mumford's type over k is denoted $\mathrm{Mum}(k)$. We say that an abelian variety A over a number field K is *of Mumford's type* if one (or equivalently all, see [50, Lem. 1.3]) of the pairs $(\mathtt{G}_\ell(A)_{\mathbb{Q}_\ell}, \mathrm{H}^1_{\text{ét}}(A_{\bar{K}}, \mathbb{Q}_\ell))$ is of Mumford's type over $\mathbb{Q}_\ell$.

The abelian varieties A over a number field K of Mumford's type are extensively studied in [50] and [51]. Our first task is to classify $\mathrm{Mum}(k)$. To do this, we define a *EQ-pair over k* to be a pair (E, D), where E is an étale algebra of rank 3 over k, and D is a quaternion algebra over E with trivial corestriction to k. The set of isomorphism classes of EQ-pairs over k is denoted $\mathrm{EQ}(k)$. For a field k we can define a map

$$\Psi_k \colon \mathrm{Mum}(k) \to \mathrm{EQ}(k) \tag{8.28}$$

as follows: let (G, V) be of Mumford's type over k. Let G' be the derived group of G, and let $\tilde{G}'$ be the universal cover of G'; then $\tilde{G}'_{\bar{k}} \cong \mathtt{SL}^3_{2,\bar{k}}$. Its three simple factors form a $\mathrm{Gal}(\bar{k}/k)$-set of cardinality 3, and as such it corresponds to an étale k-algebra E; then $\tilde{G}' \cong \mathrm{Res}_{E/k} B$, where B is a form of $\mathtt{SL}_{2,E}$. As is the case over fields, the forms of $\mathtt{SL}_2$ over E are in a one-to-one correspondence to quaternion algebras over E. The fact that G' has a faithful 8-dimensional representation implies that the quaternion algebra D corresponding to B has a trivial corestriction; we now define $\Psi_k(G, V) := (E, D)$.

Lemma 8.29. *Let k be a field. Then the map Ψ_k of (8.28) is a bijection. It is compatible with field extensions of k.*

Proof. Let $(E, D) \in \mathrm{EQ}(k)$. Then (8.24) tells us that $\mathrm{Nm}(D^\times) \subset \mathrm{Cores}_{E/k}(D)^\times \cong \mathrm{GL}_8(k)$ is of Mumford's type (together with the standard representation V of $\mathrm{GL}_8(k)$), when considered as an algebraic group over k. One can check that this is the inverse of Ψ_k, and that both these maps are compatible with field extensions of k. □

Remark 8.30. In our definition of Ψ_k we find the étale algebra E from the $\mathrm{Gal}(\bar{k}/k)$-set of simple factors in $\tilde{G}'$. We can also find E directly from G as follows: let T be a maximal torus of G defined over k. Then there exist $\chi, \varrho_1, \varrho_2, \varrho_3 \in \mathrm{X}^*(T)_\mathbb{Q}$ such that the characters of T present in V are those of the form $\chi \pm \varrho_1 \pm \varrho_2 \pm \varrho_3$, and the Galois action on $\mathrm{X}^*(T)$ is given by a Galois action on the set $\{\pm\varrho_i : i \leq 3\}$. From the latter, we get an action of $\mathrm{Gal}(\bar{k}/k)$ on $\{\{\pm\varrho_1\}, \{\pm\varrho_2\}, \{\pm\varrho_3\}\}$, and this is the $\mathrm{Gal}(\bar{k}/k)$-set corresponding to E. It does not depend on the choice of T.

We need one more lemma on étale algebras that will be useful later on.

Lemma 8.31. *Let Γ be a topological group, and let X and Y be two discrete sets of cardinality 3 with a continuous Γ-action. Suppose that there is a dense subset $S \subset \Gamma$ such that for every $s \in S$ there is an isomorphism of $\langle s \rangle$-sets $X \cong Y$. Then $X \cong Y$ as Γ-sets.*

Proof. For every s the action of s on X is trivial if and only if the action of s on Y is trivial as well. Let $\mathrm{Bij}(X)$ denote the group of permutations of X. Since S is dense in Γ this means that the kernels of the maps $\varrho_X : \Gamma \to \mathrm{Bij}(X)$ and $\varrho_Y : \Gamma \to \mathrm{Bij}(X)$ are the same. We may divide out this kernel and assume without loss of generality that the actions are faithful. In this case Γ is finite, so $S = \Gamma$. Upon choosing identifications $X \cong \{1, 2, 3\} \cong Y$ we get two subgroups $\varrho_X(\Gamma), \varrho_Y(\Gamma) \subset S_3$, and we need to prove that these two subgroups are conjugate. However, since ϱ_X and ϱ_Y are injective, these two subgroups have the same cardinality, and in S_3 subgroups are determined, up to conjugation, by their cardinality. □

Corollary 8.32. *Let k be a number field, and let E and F be two étale algebras of rank 3 over k. Suppose that $E_{k_v} \cong F_{k_v}$ as k_v-algebras for every finite place v of k. Then $E \cong F$ as k-algebras.*

Proof. Let X and Y be the $\mathrm{Gal}(\bar{k}/k)$-sets corresponding to E and F, respectively. For every finite place v of k, choose an embedding $\bar{k} \hookrightarrow \bar{k}_v$; this induces an injection $\mathrm{Gal}(\bar{k}_v/k_v) \hookrightarrow \mathrm{Gal}(\bar{k}/k)$. By Čebotarëv's density theorem the images of these injections form a dense subset (see [67]). Furthermore, by the assumption the $\mathrm{Gal}(\bar{k}_v/k_v)$-sets are isomorphic for every v. We can now use lemma 8.31 to find that E and F are isomorphic. □

8.2.2 Proof of theorem 8.22

From this point onwards we consider an abelian variety A over a number field K such that A is of Mumford's type. For each prime number ℓ we set $\mathscr{G}_\ell := \mathtt{G}_\ell(A)$. We let G_ℓ be the generic fibre of $\mathscr{G}_\ell$, and we define $V_\ell := \mathrm{H}^1_{\text{ét}}(A_{\bar{K}}, \mathbb{Q}_\ell)$. Let $(E_\ell, D_\ell) \in \mathrm{EQ}(\mathbb{Q}_\ell)$ be the pair corresponding to the pair (G_ℓ, V_ℓ) via the map $\Psi_{\mathbb{Q}_\ell}$ of (8.28).

Lemma 8.33. *There is a unique étale algebra E over $\mathbb{Q}$ such that $\mathbb{Q}_\ell \otimes_{\mathbb{Q}} E \cong E_\ell$ for all ℓ. This E is a totally real number field.*

Proof. Let S be the set of all finite places v of K for which the Frobenius torus T_v exists (see [9, 3.b]); this is a subset of $\mathrm{S}(K)$ of Dirichlet density 1. This T_v is a torus over $\mathbb{Q}$, and it comes equipped with a canonical representation W_v. By replacing S by a subset of density 1 if needed, we may assume that there exists an identification of $\mathbb{Q}_\ell$-vector spaces $W_{v,\mathbb{Q}_\ell} \cong V_\ell$ such that $T_{v,\mathbb{Q}_\ell}$ is a maximal torus of G_ℓ, for every prime number ℓ different from the characteristic of v (see [9, Cor. 3.8]). By remark 8.30 there exist $\chi, \varrho_1, \varrho_2, \varrho_3 \in \mathrm{X}^*(T_v)_{\mathbb{Q}}$ such that the characters of T present in W_v are those of the form $\chi \pm \varrho_1 \pm \varrho_2 \pm \varrho_3$. Let E be the étale $\mathbb{Q}$-algebra corresponding to the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-set $\{\{\pm\varrho_1\}, \{\pm\varrho_2\}, \{\pm\varrho_3\}\}$; this does not depend on the choice of v. Now let ℓ be a prime number not equal to the characteristic of v. Since $T_{v,\ell}$ is isomorphic to a maximal torus of G_ℓ, remark 8.30 tells us that $E_\ell \cong \mathbb{Q}_\ell \otimes_{\mathbb{Q}} E$ for all ℓ. Since for every ℓ we can find a $v \in S$ whose characteristic does not equal ℓ, this is actually true for every ℓ. Furthermore, E is the unique étale $\mathbb{Q}$-algebra with this property by corollary 8.32. Since G_ℓ^{der} is $\mathbb{Q}_\ell$-simple for infinitely many ℓ by [54, Thm. 5.13(b)], we see that E_ℓ is a field for infinitely many ℓ; hence E is a field. To prove that E is in fact totally real, let κ_v be the residue field of the place v, and let A_v be the reduction of A at v; this is an abelian variety over κ_v. After replacing K by a finite extension if necessary, we know by [49, Thm. 2.2] that A_v is an ordinary abelian variety for v in a set of Dirichlet density 1. Let $\mathrm{W}(\kappa_v)$ be the ring of Witt vectors of κ_v. Since A_v is an ordinary abelian variety we can consider its canonical lift A_v^{can}, which the unique lift of A_v to $\mathrm{W}(\kappa_v)$ for which the natural map $\mathrm{End}(A_v^{\mathrm{can}}) \to \mathrm{End}(A_v)$ is a bijection. Choose any embedding $\mathrm{W}(\kappa_v) \hookrightarrow \mathbb{C}$; then $\mathtt{MT}(A_{v,\mathbb{C}}^{\mathrm{can}})_{\mathbb{Q}} \cong T_v$, and the two representations W_v and $\mathrm{H}^1(A_{v,\mathbb{C}}^{\mathrm{can,an}}, \mathbb{Q})$ of this algebraic group are isomorphic. Then $\mathtt{MT}(A_v^{\mathrm{can}}, \mathbb{C})_{\mathbb{Q}} \sim \mathtt{Hdg}(A_{v,\mathbb{C}}^{\mathrm{can}})_{\mathbb{Q}} \times \mathbb{G}_{\mathrm{m},\mathbb{Q}}$, where $\mathtt{Hdg}(A_{v,\mathbb{C}}^{\mathrm{can}})$ is the (integral) Hodge group of the Hodge structure $\mathrm{H}^1(A_{v,\mathbb{C}}^{\mathrm{can,an}}, \mathbb{Z})$. Then $T' := \mathtt{Hdg}(A_{v,\mathbb{C}}^{\mathrm{can}})_{\mathbb{Q}} \cap T$ is a maximal torus of the algebraic group $\mathtt{Hdg}(A^{\mathrm{can}}_{v,\mathbb{C}})_{\mathbb{Q}}$, and the rational vector space $\mathrm{X}^*(T')_{\mathbb{Q}}$ can now be identified (in the terminology of remark 8.30) as

$$\mathrm{X}^*(T')_{\mathbb{Q}} = \mathrm{X}^*(T)_{\mathbb{Q}}/\langle\chi\rangle.$$

Since $\mathtt{Hdg}(A^{\mathrm{can}}_{v,\mathbb{C}})(\mathbb{R})$ is a compact Lie group, we see that complex conjugation acts as -1 on the $\mathrm{X}^*(T')_{\mathbb{Q}}$. For the Galois action on $\{\pm\varrho_i : i \leq 3\}$ this means that complex conjugation sends each ϱ_i to $-\varrho_i$. It follows that the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-set $\{\{\pm\varrho_1\}, \{\pm\varrho_2\}, \{\pm\varrho_3\}\}$ is trivial, hence E is totally real. □

Lemma 8.34. *There exists a special subvariety Y of $\mathcal{A}_{g,4}$ such that $\mathtt{MT}(Y)_{\mathbb{Q}_\ell} \cong \mathtt{G}_\ell(A)_{\mathbb{Q}_\ell}$ for all prime numbers ℓ.*

Proof. Let E be as in lemma 8.34, and choose an isomorphism $\mathbb{Q}_\ell \otimes_{\mathbb{Q}} E \cong E_\ell$ for every prime number ℓ. Furthermore, choose an isomorphism $\mathbb{R} \otimes_{\mathbb{Q}} E \cong \mathbb{R}^3$. These isomorphisms give us isomorphisms $E_\ell \cong \prod_{w|\ell} E_w$ and $\mathbb{R}^3 \cong \prod_{w|\infty} E_w$. For every finite place w of E, let $D_w := E_w \otimes_{E_\ell} D_\ell$, where ℓ is such that $w \mid \ell$. Define $D_\infty := \mathbb{H} \times \mathbb{H} \times \mathrm{M}_2(\mathbb{R})$ as a quaternion algebra over $\mathbb{R}^3$, and for every infinite place w of E define $D_w := E_w \otimes_{\mathbb{R}^3} D_\infty$. For each $w \in \mathrm{S}(E)$ we let $d_w \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ be the invariant corresponding to D_w. Since each D_ℓ has a trivial corestriction to $\mathbb{Q}_\ell$, lemma 8.25 shows that $\sum_{w|\ell} d_w = 0$ for all ℓ. Furthermore our definition of D_∞ implies $\sum_{w|\infty} d_w = 0$. By [34, Thm. 3.2], the group G_ℓ is quasi-split for almost all ℓ. In the notation of the definition of the map $\Psi_{\mathbb{Q}_\ell}$ of (8.28) this implies that $\tilde{G}'_\ell \cong \mathrm{Res}_{E_\ell/\mathbb{Q}_\ell}\mathrm{SL}_2$, hence $d_w = 0$ for almost all w. By lemma 8.25 the sequence $(d_w)_w$ now corresponds to a quaternion algebra D over E whose corestriction to $\mathbb{Q}$ is trivial. The construction from [48] now yields a special curve on $\mathcal{A}_{g,4}$ with the desired property. □

Remark 8.35. The quaternion algebra D constructed in the proof of 8.34 is not unique and depends on the chosen isomorphisms $\mathbb{Q}_\ell \otimes_{\mathbb{Q}} E \cong E_\ell$. However, the chosen isomorphism does not matter if all the invariants over ℓ are equal to 0, hence there will only be finitely many possibilities for D.

Proof of theorem 8.22. The first statement is a direct consequence of remark 8.19. For the second statement, let Y be as in lemma 8.34, and let $B := \mathtt{GMT}(S)_{\mathbb{Q}}$; then Y is the image of an embedding of Shimura varieties, corresponding to an injective morphism of algebraic groups $\varrho\colon B \hookrightarrow \mathtt{GSp}_{2g}$ that induces a morphism of Shimura varieties $(B, X) \to (\mathtt{GSp}_{2g}, \mathcal{H}_g)$. Consider B as a subgroup of $\mathtt{GSp}_{2g}$ via this injection. Let $V = \mathbb{Q}^8$ be the standard symplectic representation of $\mathtt{GSp}_{2g}$, and let $\Lambda \subset V$ be the lattice $\mathbb{Z}^8$. Then by assumption $B_{\mathbb{Q}_\ell} \cong G_\ell$. Furthermore, for $\ell \gg 0$ we find that $\mathtt{mod}_B(\Lambda)_{\mathbb{Z}_\ell}$ and $\mathscr{G}_\ell$ are isomorphic; they are both isomorphic to the quotient of the product $\mathbb{G}_{\mathrm{m},\mathbb{Z}_\ell} \times \mathrm{Res}_{(\mathbb{Z}_\ell \otimes \mathscr{O}_E)/\mathbb{Z}_\ell}\mathrm{SL}_2$ by its subgroup

$$\Big\{(x, y) \in \mu_2(\mathbb{Z}_\ell) \times \mu_2(\mathbb{Z}_\ell \otimes \mathscr{O}_E) : x \cdot \mathrm{N}_{E_{\mathbb{Q}_\ell}/\mathbb{Q}_\ell}(y) = 1\Big\},$$

where $\mathrm{N}_{(\mathbb{Q}_\ell \otimes E)/\mathbb{Q}_\ell}\colon (\mathbb{Q}_\ell \otimes E)^\times \to \mathbb{Q}_\ell^\times$ is the regular norm map from Galois theory. Let L be the finite set of ℓ for which $\mathtt{mod}_B(\Lambda)_{\mathbb{Z}_\ell} \ncong \mathscr{G}_\ell$. For each of $\ell \in L$, choose an isomorphism

$\varphi_\ell \colon V_{\mathbb{Q}_\ell} \xrightarrow{\sim} V_\ell$ of symplectic $\mathbb{Q}_\ell$-vector spaces that identifies $B_{\mathbb{Q}_\ell}$ and G_ℓ, and let $M_\ell := \varphi_\ell^{-1}(\mathrm{H}^1_{\text{ét}}(A_{\bar{K}}, \mathbb{Z}_\ell))$. Let $M \subset V$ be the lattice such that $M_{\mathbb{Z}_\ell} = M_\ell$ for all $\ell \in L$, and $M_{\mathbb{Z}_\ell} = \Lambda_{\mathbb{Z}_\ell}$ otherwise; then $\mathtt{mod}_B(M)_{\mathbb{Z}_\ell} \cong \mathscr{G}_\ell$ for all ℓ. Let $g \in \mathrm{GSp}_{2g}(\mathbb{Q})$ be such that $g\Lambda = M$. Then $\mathrm{inn}(g^{-1}) \circ \varrho$ is a morphism of Shimura data $(B, X) \to (\mathtt{GSp}_{2g}, \mathcal{H}_g)$, and any irreducible component of the image of X in $\mathcal{A}_{4,n}$ is a special subvariety that satisfies the conditions of the theorem. □

Bibliography

[1] Yves André. On the Shafarevich and Tate conjectures for hyperkähler varieties. *Mathematische Annalen*, 305(1):205–248, 1996.

[2] Pierre Berthelot, Lawrence Breen, and William Messing. *Théorie de Dieudonné cristalline II*, volume 930 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin & Heidelberg, Germany, 1982.

[3] Pierre Berthelot and William Messing. Théorie de Dieudonné cristalline III: théorèmes d'équivalence et de pleine fidélité. In *The Grothendieck Festschrift*, pages 173–247. Birkhäuser, Boston, United States, 2007.

[4] Armand Borel. Some finiteness properties of adele groups over number fields. *Publications Mathématiques de l'IHÉS*, 16:5–30, 1963.

[5] Nicholas Bourbaki. *Groupes et algèbres de Lie: Chapitres 7 et 8*. Eléments de Mathématique. Springer-Verlag, Berlin & Heidelberg, Germany, 2006.

[6] Kenneth S. Brown. *Buildings*. Springer-Verlag, New York City, United States, 1989.

[7] François Bruhat and Jacques Tits. Groupes réductifs sur un corps local. *Publications Mathématiques de l'IHÉS*, 41(1):5–251, 1972.

[8] Victoria Cantoral Farfán. A survey around the Hodge, Tate and Mumford–Tate conjectures for abelian varieties, 2016. Preprint, available at `https://arxiv.org/abs/1602.08354`.

[9] Wenchen Chi. ℓ-adic and λ-adic representations associated to abelian varieties defined over number fields. *American Journal of Mathematics*, 114(2):315–353, 1992.

[10] Brian Conrad. Non-split reductive groups over $\mathbb{Z}$, 2011. Available at `http://math.stanford.edu/~conrad/papers/redgpZsmf.pdf`.

[11] Pierre Deligne. Variétés de Shimura: interprétation modulaire, et techniques de construction de modeles canoniques. In *Automorphic forms, representations and L-functions: Symposium in Pure Mathematics held at Oregon State University, July 11-August 5, 1977, Cor-*

vallis, Oregon, volume 33, part 1 of *Proceedings of Symposia in Pure Mathematics*, pages 247–289, Providence, United States. American Mathematical Society, 1979.

[12] Michel Demazure. *Lectures on p-divisible groups*, volume 302 of *Lecture Notes in Mathematics*. Springer Verlag, Berlin & Heidelberg, Germany, 2006.

[13] Michel Demazure and Peter Gabriel. *Groupes algébriques. Tome 1: Géométrie algébrique, généralités, groupes commutatifs*. North Holland Publishing Company, Amsterdam, the Netherlands, 1970.

[14] Bangming Deng, Jie Du, Brian Parshall, and Jianpan Wang. *Finite dimensional algebras and quantum groups*, volume 150 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, United States, 2008.

[15] François Digne and Jean Michel. *Representations of finite groups of Lie type*, volume 21 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, United Kingdom, 1991.

[16] Bas Edixhoven and Andrei Yafaev. Subvarieties of Shimura varieties. *Annals of Mathematics*, 157(2):621–645, 2003.

[17] Pavel Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, and Elena Yudovina. *Introduction to representation theory*, volume 59 of *Student Mathematical Library*. American Mathematical Society, Providence, United States, 2011.

[18] Tat'yana Vladimirovna Fomina. Integral forms of linear algebraic groups. *Mathematical Notes*, 61(3):346–351, 1997. Translated by A.I. Shtern from: Целые формы линейных алгебраических групп. *Математические заметки*, 61(3):424-430, 1997.

[19] Ofer Gabber and Adrian Vasiu. Dimensions of group schemes of automorphisms of truncated Barsotti–Tate groups. *International Mathematics Research Notices*, 2013:4285–4333, 2013.

[20] Jean Giraud. *Cohomologie non abélienne*, volume 179 of *Grundlehren der mathematischen Wissenschaften*. Springer Verlag, Berlin & Heidelberg, Germany, 1966.

[21] Benedict H. Gross. Groups over $\mathbb{Z}$. *Inventiones mathematicae*, 124:263–279, 1996.

[22] A. Grothendieck and M. Demazure, editors. *Schémas en groupes (SGA 3)*. Société Mathématique de France, Paris, 1970. Séminaire de Géométrie Algébrique du Bois Marie 1962–64. Un séminaire dirigé par M. Demazure et A. Grothendieck avec la collaboration de M. Artin, J.E. Bertin, P. Gabriel, M. Raynaud, J.P. Serre.

[23] Alexandre Grothendieck. *Groupes de Barsotti–Tate et cristaux de Dieudonné*. Séminaire de mathématiques superieures. Presses de l'Université de Montréal, Montréal, Canada, 1974.

[24] James E. Humphreys. *Introduction to Lie algebras and representation theory*, volume 9 of *Graduate Texts in Mathematics*. Springer-Verlag, New York City, United States, 1972.

[25] James E. Humphreys. *Linear algebraic groups*, volume 21 of *Graduate Texts in Mathematics*. Springer-Verlag, New York City, United States, 1975.

[26] Aise Johan de Jong. The moduli spaces of principally polarized abelian varieties with $\Gamma_0(p)$-level structure. *Journal of Algebraic Geometry*, 2:667–688, 1993.

[27] Aise Johan de Jong. Crystalline Dieudonné module theory via formal and rigid geometry. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 82(1):5–96, 1995.

[28] Leonard William King and Reginald Campbell Thompson. *The sculptures and inscription of Darius the Great on the rock of Behistûn in Persia*. British Museum, Department of Egyptian and Assyrian Antiquities, London, United Kingdom, 1907.

[29] Mark Kisin. Integral models for Shimura varieties of abelian type. *Journal of the American Mathematical Society*, 23(4):967–1012, 2010.

[30] Ernst Kleinert. On the restriction and corestriction of algebras over number fields. *Communications in Algebra*, 36(9):3217–3223, 2008.

[31] Friedrich Knop. Classification of multiplicity free symplectic representations. *Journal of Algebra*, 301(2):531–553, 2006.

[32] Hanspeter Kraft. *Kommutative algebraische p-Gruppen (mit Anwendungen auf p-divisible Gruppen und abelsche Varietäten)*. Sonderforschungsbereich Bonn, Bonn, Germany, 1975. Unpublished manuscript.

[33] Daniel Krashen. Corestrictions of algebras and splitting fields. *Transactions of the American Mathematical Society*, 362(9):4781–4792, 2010.

[34] Michael Larsen and Richard Pink. Abelian varieties, ℓ-adic representations, and ℓ-independence. *Mathematische Annalen*, 302(1):561–579, 1995.

[35] Yves Laszlo and Martin Olsson. The six operations for sheaves on Artin stacks II: adic coefficients. *Publ. math. IHÉS*, 107(1):169–210, 2008.

[36] Milan Lopuhaä-Zwakenberg. Integral models of reductive groups and integral Mumford–Tate groups, 2017. Preprint, available at `https://arxiv.org/abs/1711.10587`.

[37] Milan Lopuhaä-Zwakenberg. The zeta function of stacks of G-zips and truncated Barsotti–Tate groups, 2017. Preprint, available at `https://arxiv.org/abs/1710.09487`.

[38] James S. Milne. Abelian varieties. In *Arithmetic geometry*, pages 103–150. Springer-Verlag, New York City, NY, 1986.

[39] James S. Milne. Introduction to Shimura varieties, 2004. Available at www.jmilne.org/math/.

[40] James S. Milne. Lie algebras, algebraic groups, and Lie groups, 2013. Available at www.jmilne.org/math/.

[41] James S. Milne. *Etale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 2016.

[42] James S. Milne. *Algebraic Groups*, volume 170 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, United Kingdom, 2017.

[43] Ben Moonen. Group schemes with additional structures and Weyl group cosets. In Carel Faber, Gerard van der Geer, and Frans Oort, editors, *Moduli of abelian varieties (Texel Island, 1999)*. Volume 195, Progress in Mathematics, pages 255–298. Birkhäuser, Basel, Switzerland, 2001.

[44] Ben Moonen. A dimension formula for Ekedahl-Oort strata. *Annales de l'Institut Fourier*, 54(3):666–698, 2004.

[45] Ben Moonen. An introduction to Mumford–Tate groups, 2004. Available at https://www.math.ru.nl/~bmoonen/.

[46] Ben Moonen. On the Tate and Mumford–Tate conjectures in codimension 1 for varieties with $h^{2,0} = 1$. *Duke Mathematical Journal*, 166(4):739–799, 2017.

[47] Ben Moonen and Torsten Wedhorn. Discrete invariants of varieties in positive characteristic. *International Mathematics Research Notices*, 2004(72):3855–3903, 2004.

[48] David Mumford. A note of Shimura's paper "Discontinuous groups and abelian varieties". *Mathematische Annalen*, 181(4):345–351, 1969.

[49] Rutger Noot. Abelian varieties – Galois representations and properties of ordinary reduction. *Compositio Mathematica*, 97(1):161–172, 1995.

[50] Rutger Noot. Abelian varieties with ℓ-adic Galois representation of Mumford's type. *Journal fur die Reine und Angewandte Mathematik*, 519:155–170, 2000.

[51] Rutger Noot. On Mumford's families of abelian varieties. *Journal of Pure and Applied Algebra*, 157(1):87–106, 2001.

[52] Frans Oort. A stratification of a moduli space of abelian varieties. In Carel Faber, Gerard van der Geer, and Frans Oort, editors, *Moduli of abelian varieties (Texel Island, 1999)*. Volume 195, Progress in Mathematics, pages 345–416. Birkhäuser, Basel, Switzerland, 2001.

[53] Richard S. Pierce. *Associative Algebras*. Springer, New York City, United States and Heidelberg/Berlin, Germany, 1982.

[54] Richard Pink. ℓ-adic algebraic monodromy groups, cocharacters, and the Mumford–Tate conjecture. *Journal für die reine und angewandte Mathematik*, 495:187–237, 1998.

[55] Richard Pink, Torsten Wedhorn, and Paul Ziegler. Algebraic zip data. *Documenta Mathematica*, 16:253–300, 2011.

[56] Richard Pink, Torsten Wedhorn, and Paul Ziegler. F-zips with additional structure. *Pacific Journal of Mathematics*, 274(1):183–236, 2015.

[57] Vladimir Petrovich Platonov and Andrei Stepanovich Rapinchuk. *Algebraic groups and number theory*, volume 139 of *Pure and Applied Mathematics*. Academic Press, San Diego, United States, 1994. Translated by Rachel Rowen from: *Алгебраические группы и теория чисел*. Nauka, Moscow, Soviet Union, 1991.

[58] Maxwell Rosenlicht. Questions of rationality for solvable algebraic groups over nonperfect fields. *Annali di matematica pura ed applicata*, 62(1):97–120, 1963.

[59] Guy Rousseau. *Immeubles des groupes réductifs sur les corps locaux*. Université Paris XI, UER Mathématique, 1977.

[60] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer Verlag, Berlin & Heidelberg, Germany, 1997.

[61] Tonny Albert Springer. *Linear algebraic groups* (2nd edition). Modern Birkhäuser Classics. Birkhäuser, Basel, Switzerland, 1998.

[62] The Stacks Project Authors. Stacks project. `http://stacks.math.columbia.edu`, 2018.

[63] Shenghao Sun. L-series of Artin stacks over finite fields. *Algebra & Number Theory*, 6(1):47–122, 2012.

[64] Sergei G. Tankeev. K3 surfaces over number fields and the Mumford–Tate conjecture. *Mathematics of the USSR – Izvestiya*, 37(1):191–208, 1991. Translated by N. Koblitz: Поверхности типа K3 над числовыми полями и гипотеза Мамфорда–Тейта. *Известия Российской академии наук, серия математическая*, 54(4):846-861, 1990.

[65] Sergei G. Tankeev. K3 surfaces over number fields and the Mumford–Tate conjecture II. *Mathematics of the USSR – Izvestiya*, 59(3):619–646, 1995. Translated by C.J. Shaddock: Поверхности типа K3 над числовыми полями и гипотеза Мамфорда–Тейта. II. *Известия Российской академии наук, серия математическая*, 59(3):179-206, 1995.

[66] Jacques Tits. Reductive groups over local fields. In *Automorphic forms, representations and L-functions: Symposium in Pure Mathematics held at Oregon State University, July 11-August 5, 1977, Corvallis, Oregon*, volume 33, Part 1 of *Proceedings of Symposia in Pure Mathematics*, pages 247–289, Providence, United States. American Mathematical Society, 1979.

[67] Nikolaj Tschebotareff. Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. *Mathematische Annalen*, 95(1):191–228, 1926.

[68] user27056. Is the normalizer of a reductive subgroup reductive? 2012. URL: `https://mathoverflow.net/questions/114243/is-the-normalizer-of-a-reductive-subgroup-reductive` (visited on 10/29/2017).

[69] Adrian Vasiu. Level m stratifications of versal deformations of p-divisible groups. *Journal of Algebraic Geometry*, 17:599–641, 2008.

[70] Torsten Wedhorn. The dimension of Oort strata of Shimura varieties of PEL-type. In Carel Faber, Gerard van der Geer, and Frans Oort, editors, *Moduli of abelian varieties (Texel Island, 1999)*. Volume 195, Progress in Mathematics, pages 441–471. Birkhäuser, Basel, Switzerland, 2001.

[71] Chao Zhang. Ekedahl–Oort strata for good reductions of Shimura varieties of Hodge type. *Canadian Journal of Mathematics*, 70:451–480, 2018.

Index

Samenvatting

"'Wat is het nut van een boek,' dacht Alice, 'zonder tekeningen en gesprekken?'"
Lewis Carroll, *Alice in Wonderland*, 1865

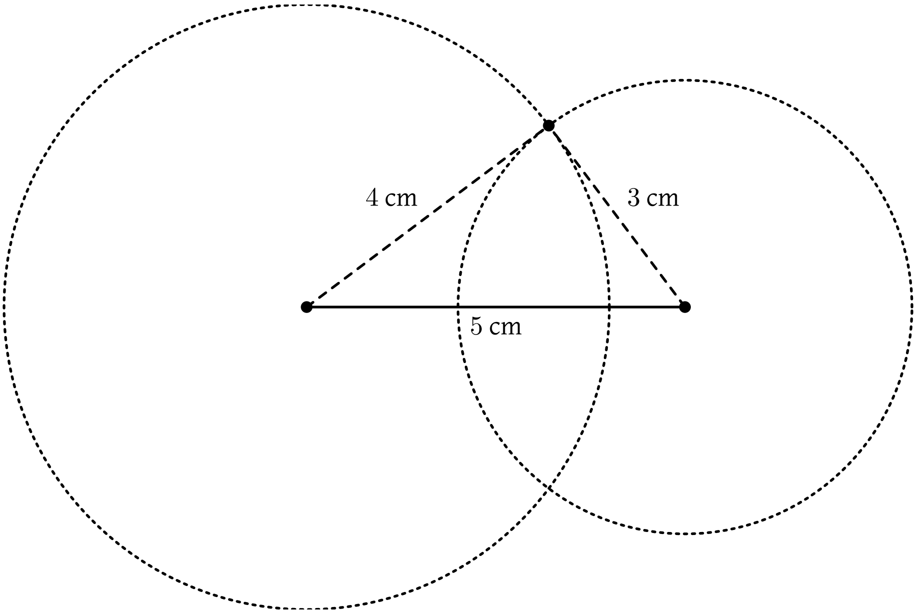
Deze samenvatting is geschreven onder de aanname dat iedereen die de algebraïsche meetkunde genoeg beheerst om een gedetailleerde, technische Nederlandse samenvatting van dit proefschrift te begrijpen, ook het Engels voldoende beheerst om uit hoofdstukken 0, 1 en 6 een goede indruk te krijgen wat er in dit proefschrift staat. Deze inleiding is dan ook bedoeld om de geïnteresseerde leek te laten proeven aan het soort wiskunde waarmee ik me de afgelopen vier jaar bezig heb gehouden.

Vertaald naar het het Nederlands is de titel van dit proefschrift *Moduli van abelse variëteiten via lineair-algebraïsche groepen*. Naar mijn mening is het eerste woord in deze titel het belangrijkst; hieronder zal ik dan ook proberen uit te leggen wat het begrip *moduliruimte* inhoudt aan de hand van een voorbeeld.

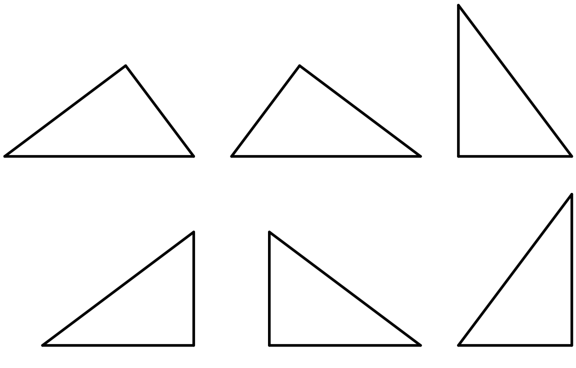
Driehoeken

In dit proefschrift bestudeer ik een aantal verschillende meetkundige objecten. Deze objecten zijn vaak lastig te visualiseren, omdat ze van een hogere dimensie zijn dan mensen zich voor kunnen stellen (de 'kleinste' objecten die ik bekijk zijn al vierdimensionaal). Om het toch een beetje begrijpelijk te houden, ga ik het in dit hoofdstuk hebben over meetkundige figuren waar de meeste mensen wat meer ervaring mee hebben, namelijk driehoeken. In een later hoofdstukje kom ik terug op hoe je als wiskundige meetkunde kan doen met dingen die je je moeilijk voor kunt stellen.

Op de middelbare school zullen veel mensen geleerd hebben hoe je een driehoek kunt construeren. Dit gaat als volgt: Stel dat je een driehoek met zijden van 3, 4 en 5 cm wil construeren. Dan begin je bijvoorbeeld door een lijnstuk van 5 cm te tekenen. Vervolgens teken je (met een passer) een cirkel met een straal van 4 cm met als middelpunt het ene eindpunt van je lijnstuk, en een cirkel met straal 3 cm met als middelpunt het andere eindpunt van je lijnstuk. Daarna kies je één van de twee snijpunten van de twee cirkels uit, en daar trek je vanuit de eindpunten lijnen naar. Deze constructie kun je zien in het plaatje hieronder:

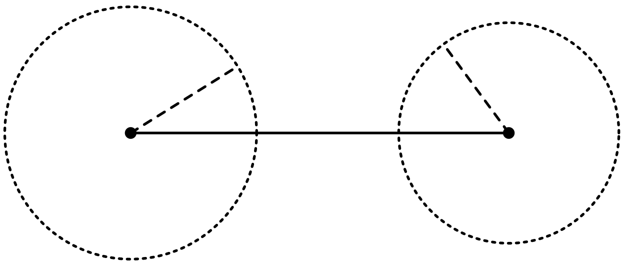


Zo kun je elke driehoek construeren, als je maar de zijden a, b en c gegeven krijgt. Op deze constructie is wel wat aan te merken. In het plaatje hieronder staan de driehoeken die we hadden gekregen door de afstanden 3 cm, 4 cm en 5 cm in een andere volgorde te gebruiken:



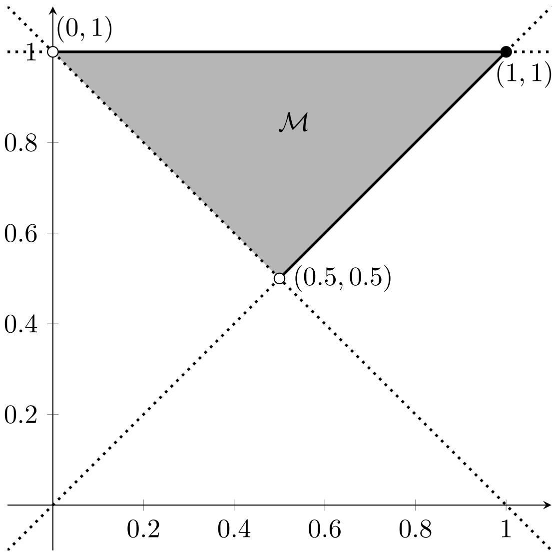
Zoals je ziet krijgen we eigenlijk steeds dezelfde driehoek, maar dan gedraaid en mogelijk gespiegeld. Ook als we in plaats daarvan een driehoek met zijden 30, 40, en 50 cm hadden genomen had het eigenlijk niet uitgemaakt; we hadden dezelfde driehoek gekregen, maar dan 10 keer zo groot.

Een driehoek wordt dus gegeven door de lengtes van zijn zijden a, b en c. Door te draaien en te spiegelen kunnen we aannemen dat deze op grootte geordend zijn, dat wil zeggen $a \leq b \leq c$. Door de driehoek te vergroten of te verkleinen kunnen we aannemen dat $c = 1$ cm; als we een willekeurige driehoek hebben, dan kunnen we die vergroten of verkleinen totdat de langste zijde 1 cm lang is. We nemen dus aan dat $a \leq b \leq 1$. Nu is het zo dat niet elke keuze van a en b een driehoek oplevert: als a en b te kort zijn, dan lukt het niet om zoals hierboven een driehoek te construeren, omdat de cirkels elkaar niet snijden, zoals in het plaatje hieronder:



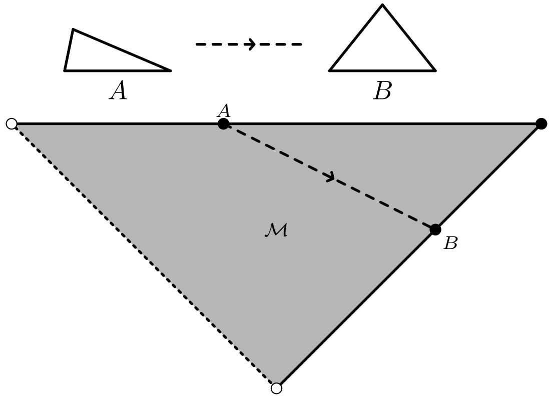
Er bestaat een driehoek met lengtes a, b en 1 cm dan en slechts dan als $a+b \geq 1$ cm. Kortom, we kunnen elke vorm driehoek krijgen door een driehoek te maken met zijden a, b en 1 cm, en er geldt $a \leq b \leq 1$ cm, en $a + b \geq 1$ cm. Laten we nu kijken hoe we deze informatie op een goede manier 'op kunnen slaan'. We kunnen het platte vlak nemen, en een assenstelsel kiezen met coördinaten x en y. Hierin kunnen we het gebied afbakenen van alle punten (x, y) waarvoor geldt $x \leq y \leq 1$ en $x + y > 1$. Dit gebied noemen we $\mathcal{M}$, en we kunnen dit zien in het plaatje[1] op de volgende pagina.

[1]Ik sta mezelf hier een beetje Engelse notatie toe door kommagetallen met een punt te schrijven, omdat $(0.5, 0.5)$ duidelijker is dan $(0, 5, 0, 5)$.

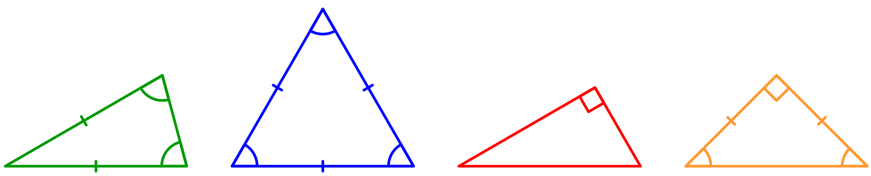


De bovenzijde en de rechterzijde van de driehoek horen wel bij $\mathcal{M}$, maar de linkerzijde niet: de linkerzijde zijn namelijk punten waarvoor geldt $x + y = 1$, en één van de voorwaarden voor $\mathcal{M}$ is dat $x + y > 1$. Omdat we de ongelijkheden die $\mathcal{M}$ definiëren slim hebben gekozen, correspondeert ieder punt (x, y) van $\mathcal{M}$ met een driehoek, namelijk een driehoek met zijden van lengte x cm, y cm en 1 cm. Zo correspondeert het punt $(0.6, 0.8)$ in $\mathcal{M}$ met een driehoek met zijden van 0.6 cm, 0.8 cm en 1 cm (of een driehoek met zijden van 6, 8 en 10 cm, omdat we mogen vergroten en verkleinen). Aan de andere kant kunnen we voor elke driehoek een punt van $\mathcal{M}$ vinden die ermee correspondeert, en dus kunnen we zeggen dat $\mathcal{M}$ de verzameling van alle driehoeken *classificeert*. Tegelijkertijd is het zo dat $\mathcal{M}$ zelf een meetkundig object is: het is een driehoek (met een missende zijde) in het xy-vlak.

Zo'n meetkundig object waarbij elk punt staat voor een ander meetkundig object wordt een *moduliruimte* genoemd, en deze spelen een belangrijke rol in de algebraïsche meetkunde. Wat moduliruimten zo belangrijk maakt, is dat één enkel meetkundig object, de moduliruimte, informatie bevat over oneindig veel meetkundige objecten. Zo kunnen we iets te weten komen over *alle* driehoeken, en hun onderlinge relaties, door het ene object $\mathcal{M}$ te bestuderen. Ik sluit dit hoofdstukje af met twee voorbeelden van hoe we de meetkunde van $\mathcal{M}$ kunnen gebruiken om driehoeken te bestuderen. Ten eerste, als we twee driehoeken A en B hebben, zoals in het plaatje hieronder, dan kunnen we in $\mathcal{M}$ een pad maken tussen de punten die corresponderen met A en B. Door over dit pad te lopen kunnen we driehoek A geleidelijk vervormen tot driehoek B: een punt halverwege het pad correspondeert met een driehoek die qua vorm 'halverwege' ligt tussen driehoek A en driehoek B. Voor driehoeken is dit misschien niet zo bijzonder, maar het kunnen vervormen van wiskundige objecten is een belangrijk trucje in de algebraïsche meetkunde, en moduliruimten geven een manier om dat te doen.

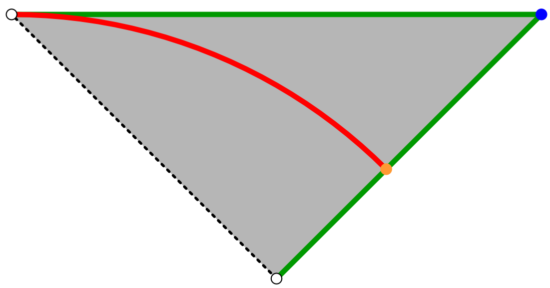


Ten tweede is het mogelijk om eigenschappen van een driehoek af te lezen aan de hand van de positie van het punt op $\mathcal{M}$ dat met die driehoek correspondeert. In het plaatje hieronder staan een aantal driehoeken met bijzondere eigenschappen:



De groene driehoek is *gelijkbenig*, dat wil zeggen dat hij twee even grote zijden en twee even grote hoeken heeft. De blauwe driehoek is *gelijkzijdig*: alle hoeken zijn even groot en alle zijden zijn even groot. De rode driehoek is *rechthoekig*: deze heeft een hoek van 90 graden. Tot slot is de oranje driehoek zowel rechthoekig als gelijkbenig. Het blijkt dat deze eigenschappen van driehoeken terug te vinden zijn in de moduliruimte $\mathcal{M}$. In het plaatje hieronder zijn de punten van $\mathcal{M}$ die op de twee groene lijnen liggen precies de punten die corresponderen met gelijkbenige driehoeken. Op dezelfde manier kunnen we ook gelijkzijdigheid (blauw), rechthoekigheid (rood), en de combinatie van rechthoekigheid en gelijkbenigheid (oranje) terugzien als meetkundige figuren in $\mathcal{M}$; zie de figuur op de volgende pagina.[2]

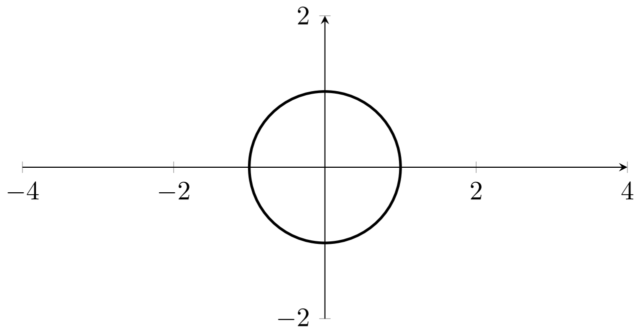
[2]Opgave voor mensen met een wiskundige achtergrond: laat zien dat de rode boog het deel van de cirkel met straal 1 en middelpunt $(0, 0)$ is dat in $\mathcal{M}$ bevat is.



Dit waren maar kleine voorbeelden van wat moduliruimten zijn, en wat voor handige eigenschappen ze hebben. Hoewel dit proefschrift niet over driehoeken gaat, maar over ingewikkeldere meetkundige objecten genaamd *abelse variëteiten* is het principe hetzelfde: Er bestaat een moduliruimte van abelse variëteiten, en we kunnen alle abelse variëteiten in één keer bestuderen door de meetkunde van deze moduliruimte beter te begrijpen.

Meetkunde in hogere dimensies

De abelse variëteiten waar dit proefschrift over gaat, zijn weliswaar meetkundige objecten, maar niet helemaal in dezelfde betekenis als de driehoeken die hierboven besproken zijn. Een eerste verschil is dat deze abelse variëteiten vaak hoger-dimensionaal zijn; de abelse variëteiten die ik in sectie 8.2 bespreek zijn vierdimensionaal, maar voor de rest gaat dit proefschrift over abelse variëteiten van elke dimensie. Hoe kun je meetkunde doen als je in een ruimte werkt die zoveel dimensies heeft dat je het niet voor je kunt zien? Dit kunnen we laten zien aan de hand van een voorbeeld. Neem de cirkel in het xy-vlak met middelpunt $(0, 0)$ en straal 1:



Zoals sommigen wel op de middelbare school geleerd hebben, kunnen we deze cirkel ook beschrijven met een vergelijking: De punten op de cirkel zijn namelijk alle punten (x, y) waarvoor geldt

$$x^2 + y^2 = 1.$$

Het mooie is nu dat we de cirkel ook kunnen bestuderen aan de hand van deze vergelijking. Om een voorbeeld te geven, een cirkel heeft de eigenschap dat elke (rechte) lijn een cirkel hoogstens in twee punten snijdt. Het blijkt dat dit te maken heeft met het feit dat de vergelijking hierboven alleen kwadraten bevat, en een kwadratische vergelijking hoogstens twee oplossingen heeft. Op deze manier kunnen we meetkundige eigenschappen van de cirkel bestuderen door de algebraïsche eigenschappen van de vergelijking te bestuderen. Het mooie is nu dat we dit nu ook kunnen toepassen op andere vergelijkingen, zoals

$$x^2 + y^2 + z^2 + v^2 + w^2 = 1.$$

Dit is een vergelijking in vijf variabelen, en we kunnen het dus beschouwen als een vergelijking die een meetkundig object in de vijfdimensionale $xyzvw$-ruimte definieert. Hoewel we ons deze ruimte en dit object moeilijk voor kunnen stellen, kunnen we alsnog zijn meetkundige eigenschappen *berekenen* aan de hand van deze vergelijking. Hoewel abelse variëteiten gegeven worden door meerdere (en ingewikkeldere) vergelijkingen, is het principe hetzelfde. Een tweede voordeel van deze aanpak is dat we dit soort vergelijkingen ook kunnen opstellen in andere 'getallensystemen' dan gebruikelijk. De x en y in de definitie van de cirkel zijn *reële getallen*, dat wil zeggen alle getallen die je van de middelbare school kent (positief en negatief, met eventueel oneindig veel cijfers achter de komma). Er worden in de wiskunde een hoop andere getallensystemen gebruikt dan de reële getallen, en op deze manier kunnen we ook in deze getallensystemen meetkunde doen. Een belangrijk voorbeeld hiervan zijn *eindige getallensystemen*: omdat deze 'klein' zijn vergeleken met de oneindig grote getallensystemen die meestal gebruikt worden, zijn ze relatief makkelijk om mee te werken, en hierdoor spelen ze een belangrijke rol in de theoretische wiskunde. Ze hebben ook praktische toepassingen: de meetkundige eigenschappen van abelse variëteiten in eindige getallensystemen spelen een belangrijke rol in de cryptografie.

Waar gaat dit proefschrift over?

In dit proefschrift probeer ik de moduliruimten van abelse variëteiten te beschrijven. Abelse variëteiten zijn meetkundige objecten die een belangrijke rol spelen in de algebraïsche meetkunde, aan de ene kant omdat ze veel symmetrie hebben en daardoor makkelijk te bestuderen zijn, en aan de andere kant omdat ze overal opduiken, van de getaltheorie tot de cryptografie. Abelse variëteiten blijken, net zoals driehoeken hierboven, moduliruimten te hebben, en door deze moduliruimten te bestuderen kunnen we meer over abelse variëteiten te weten komen.

Ik beschrijf moduliruimten van abelse variëteiten aan de hand van *lineair-algebraïsche groepen*. Lineair-algebraïsche groepen zijn wiskundige objecten uit de *lineaire algebra*. Dit is een vakgebied dat niet alleen in de wiskunde, maar zo ongeveer in alle bètavakken erg belangrijk is, omdat je er snel en eenvoudig berekeningen mee kunt doen in multidimensionale ruimten.

Door eigenschappen van moduliruimten te vertalen naar lineair-algebraïsche groepen, kunnen meetkundige eigenschappen van deze moduliruimten ontdekt worden doordat we ze expliciet uit kunnen rekenen.

Dit proefschrift bestaat uit twee delen die los van elkaar gelezen kunnen worden. In beide delen bestudeer ik een beschrijving van moduliruimten van abelse variëteiten in termen van lineair-algebraïsche groepen. Deze beschrijvingen waren eerder bedacht door andere wiskundigen, en ik probeer ze te verbeteren om er nieuwe resultaten mee te kunnen vinden. Het eerste deel gaat over moduliruimten over eindige getallensystemen. In deze context zijn de moduliruimten zelf ook 'eindig', en ik gebruik de beschrijving die ik heb verbeterd om een telformule te vinden die uitdrukt hoe groot deze moduliruimten zijn. Het tweede deel gaat over een manier om eigenschappen van deelruimten van moduliruimten uit te drukken in lineair-algebraïsche groepen. Ik verbeter deze beschrijving met behulp van de getaltheorie, en ik laat zien dat deze verbeterde beschrijving een stuk meer informatie over de moduliruimte geeft.

Acknowledgements

Doing research in algebraic geometry for four years, and turning this research into this Ph.D. thesis, has been a fantastic experience. There are a number of people whose support has been invaluable over these four years, and I would like to thank these people in the following pages.

Ben, thank you for being my supervisor, and for doing such a great job at it. You pointed me towards two beautiful areas of mathematics to explore in these four years. Your superb attention to detail and desire to see the bigger picture has had a great impact on me as a reseacher. At any time I could come into your office to discuss mathematics, teaching, or anything else, and I have felt supported every time.

I would like to thank Gert Heckman, Bas Edixhoven, Arno Kret, Lenny Taelman, and Torsten Wedhorn for taking place in the manuscript commmittee for this thesis.

Johan, thank you for being my office and train mate for three years. Our many discussions on everything from algebraic geometry to linguistics, politics and typography both formed a nice break from research, and helped this research in many ways. Your approach to mathematics by knowing at least something about seemingly everything, while always finding something new to learn, has been inspirational.

I would like to thank my fellow mathematical Ph.D. students in Nijmegen, for making our offices feel like home. Frank, Julius, Ruben, thank you for organising board game get-togethers, the canonical leisure activity for mathematicians. Bert, thank you for being a driving force behind the Ph.D. community. Henrique, thank you for introducing us to the concept of coffee discussions, and for reminding me that the question is often more important than the answer. I would like to thank all of you, and the others that have not been mentioned by name, for all the interesting discussions.

I want to thank all my colleagues in Nijmegen for creating a friendly atmosphere, in which there was always someone around to discuss any question I might have about any area of mathematics. I also thank Astrid and Greta, for their secretarial support.

My friends and family, there are too many of you to mention individually, but our contact, through board games, computer games, linguistics, movie nights, boat trips and many other ways, has made my non-mathematical life wonderful over the last four years. Thank you all very much!

Opa en oma, bedankt voor al jullie liefde en steun in deze vier jaar, en voor jullie trots in alles wat ik bereik. Ook al is dit proefschrift moeilijk voor jullie te volgen, ik ben dankbaar dat ik met jullie mijn eerste 'wiskundige' stappen heb kunnen zetten.

Finally I want to thank my wife, Ilse-Marie. The positive impact your love and support has on me cannot be overstated. Thank you for giving me a home with which no mathematics, linguistics or computer science can compete.

Curriculum Vitae

Milan Lopuhaä was born on April 25, 1990 in Amsterdam. In 1993 his family moved to Driehuis, where he spent the rest of his childhood. He graduated *cum laude* from the Gymnasium Felisenum in Velsen-Zuid in 2008. From 2008 to 2011 he pursued a BSc in mathematics at Leiden University, which he obtained *cum laude*. In this time, he also moved to Leiden, where he met his future wife, Ilse-Marie Zwakenberg. From 2009 to 2012 he also pursued a BA in comparative Indo-European linguistics, which he obtained *cum laude*. In 2014 he graduated from Leiden University with an MSc in mathematics *summa cum laude*, focused on geometry, algebra and number theory, and a research MA in linguistics *cum laude*, focused on comparative Indo-European linguistics. From 2014 to 2018 he pursued a Ph.D. in mathematics, specifically algebraic geometry, at Radboud University Nijmegen, supervised by Prof. Ben Moonen. In 2014, Ilse-Marie and he moved to Utrecht, and they married in 2017. Starting in 2018 he will work as a postdoctoral researcher in computer science at Eindhoven University of Technology.