Heights on commutative algebraic groups

Revised version

Master's thesis presented at the University of Freiburg
Mathematical Institute
by Clara Otte
Winter semester 2022/2023

Supervisor: Prof. Dr. Annette Huber-Klawitter

Contents

Introduction

This master's thesis looks at the behaviour of heights on connected commutative algebraic groups under taking integral multiples. In diophantine geometry the height is a measure of algebraic complexity of an algebraic number.

The starting point for the topic of this thesis was a lecture given by my advisor Prof. Dr. Huber-Klawitter on the Analytic Subgroup Theorem by Gisbert Wüstholz in the winter semester of 2020/2021. The Analytic Subgroup Theorem is a result in transcendental number theory. It implies several previous statements in this area like Baker's Theorem and can among other things be used to show transcendence of the logarithm $\log \alpha$ of an algebraic number $\alpha \neq 0, 1$.

The proof of the theorem given by Wüstholz in [Wüs89] uses heights on connected commutative algebraic groups to show that some differential operators must vanish at a given collection of points.

For a given commutative connected algebraic group G defined over $\overline{\mathbb{Q}}$ the inequalities needed for this are of the form

$$h([n]g) \leq c_1 n^{c_2}(h(g) + 1) + c_3, \tag{1}$$

$$h(g) \leq c_4 n^{c_5}(h([n]g) + 1) + c_6 \tag{2}$$

for points $g \in G(\overline{\mathbb{Q}})$ as well as integers $n \in \mathbb{Z}$ or $\mathbb{Z} \setminus \{0\}$ respectively. The notation $[n]$ is used for the multiplication-by-n-morphism.

In proving inequalities of shape (1) and (2) there are three different approaches in the literature.
One is trying to define canonical heights with regard to multiplication. This idea is used in [SC79]. This thesis applies this in Lemma 2.3.5 to the special cases of abelian and semiabelian varieties to obtain versions of both height estimates. The constants for both estimates only depend on the height function and the group.
Another approach is using the behaviour of the morphism of translation by a group element g. This is utilised in [SC79] to get an estimate similar to inequality (1) where one of the constants has a dependency on the point g. This estimate has the shape

$$h([n]g) \leq c_1 n^2 + c_2$$

with the constant c_1 depending on the point g. This is discussed in Theorem 2.4.13 of this thesis.
The third approach is employed in [Wüs89] for the second inequality. For this approach the multiplication-by-n-morphism is represented by some collection of polynomials on the group. This representation is then used show the inequalities. Depending on how explicitly

these polynomials are given, the quality of constants in the estimates changes. In the case of a general connected commutative algebraic group one gets estimates depending on the prime factorisation of n. In this thesis this is discussed in Proposition 2.4.1 for the first inequality and Proposition 2.5.5 for the second inequality. In the case of a linear group the multiplication-by-n-morphism can be explicitly given. This is done for both inequalities in [Hub21] and leads to estimates with constants which only depend on the group and the specific height function chosen. In this thesis this is Lemma 2.3.10.

The original proof of the Analytic Subgroup Theorem by Gisbert Wüstholz in [Wüs89] uses the inequalities shown in Proposition 2.0 in [Wüs89] and Proposition 5 in [SC79]. These are Theorem 2.4.13 and Proposition 2.5.5 in this thesis.

Inequalities of greater generality are stated by Alan Baker and Gisbert Wüstholz in section 6.8 of "Logarithmic Forms and Diophantine Geometry" ([BW08]). The two authors explain the steps necessary to prove the Analytic Subgroup Theorem and claim, but do not prove, that on any commutative connected algebraic group G defined over $\overline{\mathbb{Q}}$ height estimates of the form

$$h([n]g) \leq c_1 n^2 h(g) + c_2,$$
$$h(g) \leq c_3 n^{c_4} (h([n]g) + 1)$$

hold for the logarithmic height h associated to some very ample divisor D. Here g is a point in $G(\overline{\mathbb{Q}})$ and $[n]$ denotes the multiplication by $n \in \mathbb{Z}$. In contrast to the inequalities proven in this thesis, the constants $c_1, \ldots, c_4 \geq 0$ only depend on G and the divisor D.

Even though more general statements than proven in this thesis may hold, it aims to be a resource for the different height estimates on a connected commutative algebraic group.

Structure of the thesis

This thesis is structured into two chapters. The first chapter is concerned with the algebraic and geometric background needed to formulate and prove the height estimates. The second chapter covers the construction of a completion of a connected commutative algebraic group and the height estimates.

Section 1.1 gives a short introduction to divisors, linear systems and their associated maps as well as the notion of (relatively) ample divisors and a version of the Enriques-Severi-Zariski Lemma. This will later be used to define heights on varieties.

K-rational points of varieties are discussed in section 1.2.

Section 1.3 discusses the definition of algebraic groups, the special cases of abelian varieties and linear group varieties as well as the Theorem of Chevalley on the general structure of commutative algebraic groups.

Afterwards heights on projective space, varieties and polynomials are defined in section 1.4. The notions of the Weil height machine on an arbitrary projective smooth variety and the Néron-Tate height on an abelian variety are introduced. Additionally, this section formulates some inequalities for heights on projective spaces which are needed later.

In the first section 2.1 of the second chapter the completion of an algebraic group and a specific completion which is used in [SC79] are explained.

Section 2.2 looks at the relationship of the height estimates if the height differs with the help of a lemma in [SC79].

The special cases of the height estimates on linear algebraic groups, semiabelian varieties and algebraic groups which are a product of an abelian variety and a linear algebraic group are discussed in section 2.3.

Section 2.4 covers versions of inequality (1) in the general setting. One is dependent on prime factorisations while the other, which is covered in [SC79], is dependent on points.

Lastly, section 2.5 considers the version of inequality (2) in the general setting as done in [Wüs89].

Acknowledgements

I want to thank my advisor Professor Dr. Huber Klawitter for her support and help with this thesis. I also want to thank Professor Dr. Habegger of the University of Basel for answering my questions and his help in understanding and proving the Proposition 2.5.5. Additionally, I am grateful to Sören Andres, Paul Meffle, Charlotte Oldenburg and Tatjana Stiefken for their feedback on this thesis.

Chapter 1

Background

In this thesis a variety X is viewed as a reduced separable scheme of finite type over an algebraically closed field K. Its structure sheaf is denoted as $\mathcal{O}_X$. If X is irreducible, its function field is denoted as $K(X)$. The notation $K[X]$ is sometimes alternatively used for its ring of coordinates. An open subset of a variety is meant to be open in the Zariski topology. Most notations used are analogous to [Har77].

The letter K generally denotes a number field or $\overline{\mathbb{Q}}$. The algebraic closure of a field K is written as $\overline{K}$.

Homogeneous coordinates of a projective K-space are written as $[x_0 : \ldots : x_n] \in \mathbb{P}^n_K$. This might sometimes be shortened to $[x]$. If f and g are polynomials $[f : g]$ is intended to mean the (nonzero) coefficients of f and g viewed as points of some projective space. The subscript K in $\mathbb{P}^n_K$ will sometimes be omitted if the field of definition should be clear from the context. In general, this will then be the projective space defined over $\overline{\mathbb{Q}}$.

If a group G is a subgroup of some other group H the notation $G \leq H$ is used.

1.1 Maps and Divisors

The aim of this section is to see how a map $\phi : X \to \mathbb{P}^n_K$ from a projective variety over an algebraically closed field K can be assigned to an object on X. This object is depending on the viewpoint equivalently a linear equivalence class of divisors, an invertible $\mathcal{O}_X$-sheaf or an isomorphism class of line bundles.

This becomes relevant in section 1.4.3, where divisors are used to construct heights on varieties.

The main sources for this subsection are [Har77], [Mum76], [Sha13a] and [HS00].

In this whole section let X, Y denote smooth irreducible varieties over some algebraically closed field K of characteristic zero.

1.1.1 Definition of divisors

In the following subsection different definitions of divisors are introduced. While they are not equivalent in general, they coincide for smooth projective irreducible varieties, the situation in which they are needed for this thesis. Since for proving different statements some notions of divisor are more convenient than others several constructions will be introduced here.

Sources for this section are [Har77], [Sha13a] and [Sha13b].

Definition 1.1.1 ([Har77], Definition p.130)**.** Let X be a smooth irreducible variety. A *prime divisor* on X is a closed subvariety of codimension one. The free abelian group generated by the prime divisors on X is denoted as $\mathrm{Div}(X)$. Its elements are called *Weil divisors*.

Remark 1.1.2. Any smooth irreducible variety viewed as a scheme satisfies the conditions needed in [Har77] for the definition of Weil divisors. A variety is reduced, therefore an irreducible variety is an integral scheme. It is also separated and any smooth variety is regular [GW10, Remark 6.33] hence also regular in codimension one.

Definition 1.1.3 ([Har77], first Definition p.158)**.** The *support* of a Weil divisor $D = \sum_{i\in I} n_i Y_i \in \mathrm{Div}(X)$ is the union $\mathrm{Supp}(D) := \bigcup_{\substack{i\in I \\ n_i\neq 0}} Y_i$.

Remark 1.1.4. The group of Weil divisors on X is partially ordered with the following relation. Let $D = \sum n_i Y_i$ and $E = \sum m_j Y_j$ be divisors on X and define

$$D \leq E \iff n_i \leq m_i \ \forall Y_i \subset X \text{ subvarieties of codimension one.}$$

Definition 1.1.5 ([Har77], Definitions p.131)**.** Let X be a smooth irreducible variety and $f \in K(X)^*$ an invertible element of the function field of X. The *principal divisor* associated to f is

$$(f) = \sum v_{Y_i}(f) Y_i.$$

Here v_Y is the valuation defined on $K(X)$ by the discrete valuation ring $\mathcal{O}_{X,Y_i}$. If it is ambiguous whether a principal divisor (f) should be viewed as a divisor on X or some other variety, the notation $(f)_X$ will be employed.

Proposition 1.1.6 ([Har77], Paragraph after the first Definition p.131)**.** *The principal divisors form a subgroup of the group of divisors.*

Definition 1.1.7 ([Har77], Definitions p.131)**.** Two divisors are called *linearly equivalent* if they only differ by a principal divisor. The group $\mathrm{Cl}(X)$ of all divisors divided by the subgroup of principal divisors is called the *divisor class group* of X.

Definition 1.1.8 ([Har77], Definition p.141)**.** Let X be a smooth irreducible variety. A *Cartier divisor* is a global section of the sheaf $\mathcal{K}^*/\mathcal{O}^*$. Here $\mathcal{K}$ denotes the constant sheaf associated to $K(X)$ and $\mathcal{K}^*$ is the sheaf of its invertible elements. The abelian group $\mathrm{CaDiv}(X)$ of global sections of $\mathcal{K}^*/\mathcal{O}^*$ is called the *group of Cartier divisors*.

Remark 1.1.9. Even though the group structure on the group of Cartier divisors comes from the multiplication in $K(X)$, the group $\mathrm{CaDiv}(X)$ will in the following be denoted additively.

Remark 1.1.10 ([Sha13a], fourth paragraph p.153)**.** The above definition implies that a Cartier divisors D can be represented by a collection $\{U_i, f_i\}_{i\in I}$. Here I is some index set, the $U_i \subset X$ are an open cover of X and the $f_i \in K(U_i)^*$ are such that for any $i, j \in I$ with $U_i \cap U_j \neq \emptyset$ the quotient $\frac{f_i}{f_j}$ restricted to $U_i \cap U_j$ is an element of $\mathcal{O}(U_i \cap U_j)^*$. For two Cartier divisors $D = \{U_i, f_i\}_{i\in I}$ and $E = \{V_j, g_j\}_{j\in J}$ their sum $D + E$ can be represented by $\{U_i \cap V_j, f_i g_j\}_{i\in I,\ j\in J}$. The neutral element is represented by $\{X, 1\}$.

Definition 1.1.11 ([Har77], Definition p.141, compare Corollary II.6.14 for the definition of the Cartier class group)**.** A Cartier divisor is called *principal* if it is equivalent to a Cartier divisor of the form $\{X, f\}$. Two Cartier divisors are called *linearly equivalent* if they only differ by a principal divisor. The group $\mathrm{CaCl}(X)$ of Cartier divisors modulo principal Cartier divisors is called the *Cartier class group* of X.

Remark 1.1.12. The principal Cartier divisors, analogously to the case of Weil divisors in Definition 1.1.1, form a subgroup of the Cartier divisors. This follows from the definition and the preceding remark, since for $f, g \in K(X)^*$

$$\{X, f\} + \{X, g\} = \{X, fg\}$$

and $\{X, f^{-1}\}$ are principal divisors.

Definition 1.1.13 ([Sha13a], fifth paragraph p.153)**.** The *support* of a Cartier divisor $D = \{U_i, f_i\}_{i\in I}$ is defined as the closed set of all $x \in X$ such that if $x \in U_i$ the point x is a zero or a singularity of f_i.

Definition 1.1.14 ([Sha13b], third paragraph of section 1.4 on p.63)**.** Let X be a smooth irreducible variety. A *line bundle* L over X is a vector bundle of rank one.

Proposition 1.1.15 ([Sha13b], [Sha13b], compare section 1.4 on p.63)**.** *The line bundles over a smooth irreducible variety form a commutative group with the group operation being the tensor product. The neutral element is the trivial line bundle* $X \times \mathbb{A}^1$. *This induces a group structure on the set of line bundles up to isomorphism.*

Definition 1.1.16 ([Har77], fifth paragraph of Definitions p.109)**.** Let X be a smooth irreducible variety. An *invertible sheaf* on X is a locally free $\mathcal{O}_X$-module of rank one.

Proposition 1.1.17 ([Har77], Proposition II.6.12)**.** *The invertible sheaves on a smooth irreducible variety* X *form a group* $\mathrm{Pic}(X)$ *with regard to the tensor product of* $\mathcal{O}_X$*-modules.*

Definition 1.1.18 ([Sha13b], Definition p.84)**.** Let $\mathcal{F}$ be an invertible sheaf on a smooth irreducible variety X. The support $\mathrm{Supp}(\mathcal{F})$ of $\mathcal{F}$ is the complement $X \setminus W$, where $W = \bigcap_{\substack{U \subset X \text{ open} \\ \mathcal{F}(U)=0}} U$.

Theorem 1.1.19 ([Har77], Proposition II.6.11, Proposition II.6.15 and [Sha13b], Theorem 6.3 in the first Chapter)**.** *Let X be a smooth irreducible variety. The group of line bundles up to isomorphisms,* $\mathrm{Cl}(X)$, $\mathrm{CaCl}(X)$ *and* $\mathrm{Pic}(X)$ *are isomorphic via homomorphism induced by the following maps*

a) Let $D = \{U_i, f_i\}_{i \in I}$ be a Cartier divisor. The Weil divisor associated to D is

$$\sum v_{Y_j}(f_i) Y_j$$

where U_i is an open subset such that $Y_j \cap U_i \neq \emptyset$.

b) Let $D = \{U_i, f_i\}_{i \in I}$ be a Cartier divisor. The invertible sheaf $\mathcal{L}(D)$ associated to D is the $\mathcal{O}_X$-submodule of $\mathcal{K}$ generated by

$$U_i \mapsto \frac{1}{f_i} \mathcal{O}_X(U_i).$$

c) Let $D = \{U_i, f_i\}_{i \in I}$ be a Cartier divisor. The line bundle $L(D)$ associated to D is the bundle which has local trivialisations $U_i \times \mathbb{A}^1 \to U_i$ and transition functions

$$\begin{aligned} \phi_{ij} : (U_i \cap U_j) \times \mathbb{A}^1 &\to (U_i \cap U_j) \times \mathbb{A}^1 \\ (x, \lambda) &\mapsto \left(x, \lambda \cdot \left(f_i f_j^{-1}\right)(x)\right). \end{aligned}$$

Proof. The first isomorphism is Proposition II.6.11 in [Har77]. The proposition is applicable since any smooth variety is regular (Remark 1.1.2) and any regular local ring is a unique factorisation domain ([Mat70], Theorem 48 p.142).
The second isomorphism is Proposition II.6.15 in [Har77]. That proposition is applicable since any variety is reduced, therefore an irreducible variety has the structure of an integral scheme.
The third isomorphism is discussed in Theorem 6.3 of [Sha13b]. □

Example 1.1.20. Let $X = \mathbb{P}^n$ defined over $\overline{\mathbb{Q}}$ for some $n \in \mathbb{N}_{>0}$. It can be viewed as $\mathrm{Proj}\, \overline{\mathbb{Q}}[x_0, \ldots, x_n]$. Let $D = \left\{\{x_i \neq 0\}, \frac{x_0}{x_i}\right\}_{0 \leq i \leq n}$. The Weil divisor associated to this Cartier divisor is the hyperplane $H_0 = \{x_0 = 0\}$.
The line bundle associated to D has local trivialisations $\{x_i \neq 0\} \times \mathbb{A}^1$ and transitions functions $\phi_{i,j} = \frac{x_i}{x_j}$. Such a line bundle is called a *hyperplane bundle.*
The sheaf associated to D is the $\mathcal{K}(\mathbb{P}^n)$ subsheaf generated by $\frac{1}{x_i}\mathcal{O}_X(\{x_i \neq 0\})$. It is called *Serre's twisting sheaf* and denoted as $\mathcal{O}(1)$

From now on this text uses the conventions of Weil divisors for the group of divisors and divisors modulo principal divisors, that is $\mathrm{Div}(X)$ for the divisors on a variety X and $\mathrm{Cl}(X)$ for divisors modulo principal divisors.

Proposition 1.1.21 ([Har77], Proposition II.6.4)**.** *Let $n \in \mathbb{N}_{>0}$. The group $\mathrm{Cl}(\mathbb{P}^n)$ is isomorphic to $\mathbb{Z}$. An isomorphism $\mathrm{Cl}(\mathbb{P}^n) \to \mathbb{Z}$ is given by*

a) $[H] \mapsto 1$ *in the case of Weil divisors, where H is some hyperplane*

b) $\left[\left\{\{x_i \neq 0\}, \frac{x_0}{x_i}\right\}_{0 \le i \le n}\right] \mapsto 1$ *in the case of Cartier divisors, where $x_0, \dots, x_n$ is a choice of coordinates for the projective space*

c) $\mathcal{O}(1) \mapsto 1$ *in the case of invertible sheaves, where $\mathcal{O}(1)$ is Serre's twisting sheaf.*

d) $H \mapsto 1$ *in the case of line bundles, where H is the hyperplane bundle*

respectively.

Proof. In Proposition II.6.4 of [Har77] this is shown in the case of Weil divisors. Theorem 1.1.19 and Example 1.1.20 imply the map in case of Cartier divisors, line bundles and invertible sheaves. □

Lemma 1.1.22 ('Enriques-Severi-Zariski ', [HS00] Theorem A.3.2.5 and [Mum76] compare Theorem 6.10)**.** *Let $X \subset \mathbb{P}^n$ be a smooth projective irreducible variety. There exists some $d_0 \in \mathbb{N}$ such that for all $d \ge d_0$ the linear system of degree d hypersurface sections is complete. This means that every effective divisor D on X which is linearly equivalent to d-times a hyperplane section is cut out by a polynomial F of degree d, i.e. $D = (F)_X$.*

1.1.2 From maps into $\mathbb{P}^n$ to divisors

Definition 1.1.23 ([HS00], compare Definition p.40)**.** Let $\psi : X \to Y$ be a morphism of smooth irreducible varieties. Let $D = \{U_i, f_i\}_{i \in I} \in \mathrm{Div}(Y)$ be a divisor such that $\psi(X) \not\subset \mathrm{Supp}(D)$. Then the *pullback* of D is defined as $\psi^* D = \{\psi^{-1}(U_i), f_i \circ \psi\}_{i \in I}$.

Lemma 1.1.24 ('Moving Lemma', [HS00], compare A.2.2.5)**.** *Let $\psi : X \to Y$ be a morphism of smooth irreducible varieties.*

a) Let $D \sim \widetilde{D} \in \mathrm{Div}(Y)$ be two linearly equivalent divisors such that $\psi(X) \not\subset \mathrm{Supp}(D) \cup \mathrm{Supp}(\widetilde{D})$. Then $\psi^* D \sim \psi^* \widetilde{D}$ as divisors on X.

b) Let $D \in \mathrm{Div}(Y)$ be a divisor. Then there exists a divisor $\widetilde{D} \in \mathrm{Div}(Y)$ such that $\widetilde{D} \sim D$ and $\psi(X) \not\subset \mathrm{Supp}(D)$.

Corollary 1.1.25 ([HS00], Proposition A.2.2.6)**.** *Let* $\psi : X \to Y$ *be a morphism of smooth irreducible varieties. There is a well defined group homomorphism* $\psi^* : \mathrm{CaCl}(Y) \to \mathrm{CaCl}(X)$ *which is induced by the pullback of divisors defined in Definition 1.1.23. This map is also called* pullback*.*

Proof. Part b) of Lemma 1.1.24 implies that in any linear equivalence class $[D] \in \mathrm{CaCl}(Y)$ there exists some divisor $\widetilde{D} \in [D]$ such that $\psi^*\left(\widetilde{D}\right)$ is a well defined divisor in $\mathrm{Div}(X)$. Part a) of the Moving Lemma implies that $[\psi^*\widetilde{D}]$ is independent of the choice $\widetilde{D}$. Hence

$$\begin{aligned} \psi^* : \mathrm{CaCl}(Y) &\to \mathrm{CaCl}(X) \\ [D] &\mapsto [\psi^* D] \end{aligned}$$

is well defined.
This map is also a homomorphism. Let $D := \{(W_i, f_i)\}_{i \in I}$ and $E := \{(V_j, g_j)\}_{j \in J}$ be two Cartier divisors on Y such that $\psi(X) \not\subset \mathrm{Supp}(D)$ and $\psi(X) \not\subset \mathrm{Supp}(E)$. One calculates

$$\begin{aligned} \psi^*(D + E) &= \psi^*(\{(W_i \cap V_j, f_i g_j)\}_{(i,j) \in I \times J}) \\ &= \{(\psi^{-1}(W_i \cap V_j), (f_i g_j) \circ \psi)\}_{(i,j) \in I \times J} \\ &= \{(\psi^{-1}(W_i) \cap \psi^{-1}(V_j), (f_i \circ \psi) \cdot (g_j \circ \psi))\}_{(i,j) \in I \times J} \\ &= \{(\psi^{-1}(W_i), f_i \circ \psi)\}_{i \in I} + \{\psi^{-1}(V_j), g_j \circ \psi)\}_{j \in J} = \psi^* D + \psi^* E. \end{aligned}$$

□

Construction 1.1.26. Let $\phi : X \to \mathbb{P}^n$ be a morphism of smooth irreducible varieties. The *divisor class of X associated to ϕ* is $\phi^*([H])$ for some hyperplane $H \subset \mathbb{P}^n$.

Remark 1.1.27. Geometrically, the divisor class $\phi^*([H])$ is the class of a divisor D which is cut out by the preimage of $H' \cap \phi(X)$ under ϕ, where H' is a hyperplane of $\mathbb{P}^n$ such that $\phi(X)$ is not contained in H'.

1.1.3 From divisors to maps into $\mathbb{P}^n$

Let X be a smooth irreducible variety defined over $K = \overline{\mathbb{Q}}$.

Definition 1.1.28 ([Har77], first Definition p.157)**.** Let $D \in \mathrm{Div}(X)$ be a divisor. The *complete linear system of D* is the subset $|D| \subset \mathrm{Div}(X)$ of divisors which are effective and linearly equivalent to D.

Remark 1.1.29. This definition implies that a complete linear system is only dependent on the linear equivalence class of the divisor.

Remark 1.1.30 ([Har77], first Definition p.157)**.** For an invertible sheaf this corresponds to the space of global sections modulo $K(X)^*$. This implies that $|D|$ has the structure of a projective space.

Proposition 1.1.31 ([Har77], compare first Definition p.157)**.** *Let $D \in \mathrm{Div}(X)$ be a divisor. The system $|D|$ can equivalently be regarded as the subset $L(D) \subset K(X)$ of functions f such that*

$$(f) + D \geq 0$$

modulo $K(X)^*$.

Proof. This follows directly from the definition since for any effective divisor E linearly equivalent to D the difference $E - D$ must be principal, that is $E - D = (f)$ for some $f \in K(X)^*$ and $(f) + D = (E - D) + D = E \geq 0$. Since the principal divisor of two functions $f, g \in K(X)^*$ such that $\frac{f}{g} \in K^*$ is the same, the second claim follows. □

Definition 1.1.32 ([Har77], second Definition p.157)**.** A subset $L \subset \mathrm{Div}(X)$ is called a *linear system* if it is a projective subspace of some complete linear system. The *dimension* of L as a linear system is defined as the dimension of L as a projective space.

Lemma 1.1.33 ([HS00], Corollary A.3.2.7)**.** *Let X be a projective smooth irreducible variety and $D \in \mathrm{Div}(X)$. Then the dimension of $|D|$ is finite.*

Definition 1.1.34 ([HS00], second Definition p.51)**.** A linear system L on X is called *basepoint free* if $\bigcap_{D \in L} \mathrm{Supp}(D) = \emptyset$. A point $x \in \bigcap_{D \in L} \mathrm{Supp}(D)$ is called a *basepoint* of L. A divisor D is *basepoint free* if its complete linear system $|D|$ is basepoint free.

Construction 1.1.35 ([HS00], compare Definition p.51 and Exercise A.3.5)**.** Let $D \in \mathrm{Div}(X)$ be a basepoint free divisor such that $\dim L(D) < \infty$. The *map associated* to D is the projective map $\phi_D : X \to \mathbb{P}^n$ defined by mapping a point $x \in X$ as

$$x \mapsto [\phi_0(x) : \ldots : \phi_n(x)].$$

Here $\phi_0, \ldots, \phi_n \in K(X)$ are a basis of the linear system $|D|$. This is a priori a rational map defined on the open set, where no ϕ_i has singularities and not all ϕ_i vanish simultaneously. Let $x \in X$ be any point. View D as a Cartier divisor $\{U_i, f_i\}_{i \in I}$. Let $x \in U_{i_0}$ for some $i_0 \in I$. In this case $\phi_0 \cdot f_{i_0}, \ldots, \phi_n \cdot f_{i_0}$ are in $\mathcal{O}_X(U_{i_0})$. If they all simultaneously vanished at $x \in U_{i_0}$, any linear combination would also vanish at x. Any effective divisor linearly equivalent to D restricted to U_{i_0} is a principal divisor associated to a linear combination of $\phi_0 \cdot f_{i_0}, \ldots, \phi_n \cdot f_{i_0}$. Therefore if all those functions would vanish in a point $x' \in U_{i_0}$ that point would be contained in the support of any effective divisor linearly equivalent to D. This means that x' is a basepoint, but the base locus of $|D|$ is empty by assumption. Hence the map

$$y \mapsto [\phi_0 f_{i_0}(y) : \ldots : \phi_n f_{i_0}(y)]$$

is a morphism in an open neighbourhood of x. It defines the same rational map as ϕ_D. Therefore ϕ_D has a continuation as a morphism on X.

Lemma 1.1.36 ([Har77], compare Theorem 7.1 and Remark 7.8.1, [HS00] compare Theorem A.3.1.6)**.** *Let X be a smooth irreducible variety over K. There exists a bijection between the following sets:*

a) The set of linear systems L of dimension n which are basepoint free on X.

b) The set of morphism $\phi : X \to \mathbb{P}^n$ such that $\phi(X)$ is not contained in any hyperplane of $\mathbb{P}^n$ up to projective automorphisms in $\mathrm{PGL}_{n+1}(K)$.

Proof. In Theorem II.7.1 in [Har77] the author proves that there is an one-to-one correspondence between morphisms from a variety into projective space and sets of global sections of invertible sheaves $\mathcal{L}$ on X which generate the sheaf $\mathcal{L}$. Applying Remark II.7.8.1 in [Har77] implies that this is equivalent to a correspondence between sets of generators of linear systems without basepoints on X and morphism from X into some projective space. To get the result of the lemma one uses the map suggested in Remark II.7.8.1 of [Har77]. It maps each basepoint free linear system to the map associated to one of its bases as a vector space V. Since two bases can be transformed into one another by linear homomorphism $A \in \mathrm{GL}(V)$, the maps associated to two different bases of a linear system only vary by some projective automorphism (in the sense of a morphism in $\mathrm{PGL}_{n+1}(K)$). It is left to show that this associates every basepoint free linear system to a map whose image is not contained in any hyperplane and that conversely every such map can be generated by the basis of a linear system. Therefore assume that $\phi : X \to \mathbb{P}^n$ is the map associated to some linear system L and its image is contained in some hyperplane $H \subset \mathbb{P}^n$. This hyperplane is the vanishing locus of some linear polynomial, i.e. there exists some nontrivial linear relation

$$\sum_{i=0}^{n} \lambda_i y_i \circ \phi(x) = 0 \qquad \forall x \in X$$

for a given choice $y_0, \ldots, y_n$ of coordinates of $\mathbb{P}^n$. Hence the sections $\phi^*(y_0), \ldots, \phi^*(y_n)$ fulfil the same relation and are linearly dependent. This concludes the proof. □

Remark 1.1.37. The version of the previous lemma that can be found in [HS00] as Theorem A.3.1.6 seems to contain a slight inaccuracy.

The theorem claims that there is a bijection between linear systems without fixed components (linear systems L such that there is no effective divisor D_0 such that $D \geq D_0$ for any $D \in L$ [compare HS00, third Definition p.51]) and morphisms into projective space not contained in hyperplanes. But these linear systems should be in correspondence with rational maps, while morphisms are in correspondence with basepoint free divisors.

An easy example why morphisms cannot be in correspondence with linear systems without fixed components is the rational map

$$\mathbb{P}^2 \to \mathbb{P}^1$$
$$[x_0 : x_1 : x_2] \mapsto [x_0 : x_1]$$

It is surjective, therefore not contained in any hyperplane. The linear system which it is associated to is generated by the hyperplanes $\{x_0 \neq 0\}$ and $\{x_1 \neq 0\}$. Their intersection has codimension two, therefore this linear system does not have any fixed component. But the map is not a morphism at $[0 : 0 : 1]$.

It is unclear to me, whether the authors aimed to present the bijection for rational maps or for morphisms. For this thesis I decided to present the version with morphisms.

The statement for rational maps can be found in Theorem 6.8 of [Mum76] for varieties defined over $\mathbb{C}$.

Remark 1.1.38. The maps used in the proof of Lemma 1.1.36 are analogous to the ways in which in Construction 1.1.26 and Construction 1.1.35 maps were associated to divisors and vice versa.

1.1.4 Ample, very ample and relatively ample divisors

Let X be a smooth irreducible variety defined over $K = \overline{\mathbb{Q}}$.

Definition 1.1.39 ([HS00], Definition p.52)**.** A divisor D on a $\overline{\mathbb{Q}}$-variety X is called *very ample*, if there is an $n \in \mathbb{N}_{>0}$ and an immersion $i : X \to \mathbb{P}^n$ such that $i^*\mathcal{O}(1)$ is isomorphic to the sheaf associated to D. A divisor D is called *ample* if some positive multiple nD is very ample.

Remark 1.1.40. If D is an divisor on a projective variety X, then this is equivalent to $|D|$ defining an immersion by Construction 1.1.35.

Remark 1.1.41 ([Har77], compare Remark II.5.16.1)**.** If an irreducible variety X is projective there will always be very ample divisors on that variety. This is the case since by definition X can be embedded into projective space. The divisor class associated to this morphism by Construction 1.1.26 must now be very ample by Lemma 1.1.36. Any very ample divisor is basepoint free, since it defines a morphism into projective space.

If the divisors are viewed as invertible sheaves a more direct definition of ample can be given. In the case of varieties that definition is equivalent to the one above by Theorem II.7.6 in [Har77].

Definition 1.1.42 ([Har77], Definition p.153 and Theorem 7.6)**.** An invertible sheaf $\mathcal{L}$ on X is *ample* if for any coherent sheaf $\mathcal{F}$ on X there is some integer $n_0 \geq 0$ such that for all $n \geq n_0$ the sheaf $\mathcal{F} \otimes \mathcal{L}$ is generated by its global sections.

Proposition 1.1.43 ([Har77], Example 7.4.2)**.** *If X is an affine irreducible variety, any divisor D on X is ample.*

Lemma 1.1.44 ([HS00], Proposition A.3.2.4)**.** *Let $\phi : X \to Y$ be a morphism of projective irreducible varieties. Let $D \in \mathrm{Div}(Y)$ be basepoint free. If $\phi^* D$ is well defined it is a basepoint free divisor of X.*

Lemma 1.1.45 ([HS00], compare Theorem A.3.2.3)**.** *Let X be a projective irreducible variety and $D, E \in \mathrm{Div}(X)$ such that E is very ample*

a) There exists some $n \in \mathbb{N}$ such that $D + nE$ is basepoint free.

b) If D is basepoint free then $D + E$ is very ample.

Corollary 1.1.46. *Let X be a projective irreducible variety and $D \in \mathrm{Div}(X)$. Then there exists basepoint free (and even very ample) divisors $E_1, E_2 \in \mathrm{Div}(X)$ such that*

$$D = E_1 - E_2.$$

Proof. Let $H \in \mathrm{Div}(X)$ be any very ample divisor. By points a) and b) of the previous lemma there exists some $n \in \mathbb{N}$ such that $D + nH$ is very ample. Point b) implies that also nH is very ample. Defining $E_1 := D + nH$ and $E_2 := nH$ gives the desired decomposition. □

Definition 1.1.47 ([Staa], compare Definition 29.37.1 and Lemma 29.37.4 (3))**.** Let X, Y be irreducible varieties and $\phi : X \to Y$ a morphism. An invertible sheaf $\mathcal{F}$ on X is called *ϕ-relatively ample* if there exists an affine open covering $\{U_i\}_{i \in I}$ of Y such that $\mathcal{F}$ restricted to $\phi^{-1}(U_i)$ is ample.

Remark 1.1.48. While the definition of ample used in Stacks is slightly different than the one used in Hartshorne, which is used in this thesis, they agree in the setting of irreducible varieties due to Proposition 28.26.13 (7) of [Stab].

Lemma 1.1.49 ([Staa], Lemma 29.37.7)**.** *Let X, Y be irreducible varieties and $\phi : X \to Y$ a morphism. Let $\mathcal{F}$ be an invertible sheaf on X and $\mathcal{G}$ an invertible sheaf on Y which is ϕ-relatively ample. There exists some $n \in \mathbb{N}_{>0}$ such that*

$$\mathcal{F} \otimes \phi^* \mathcal{G}^{\otimes n}$$

is ample.

1.2 K-rational points of varieties

The analytic subgroup theorem looks at properties of commutative algebraic groups. To define those in the generality required for the height estimates it is necessary to look at the structure of varieties over arbitrary number fields. This section aims to give a short outline of the necessary algebraic geometry to be able to do so. The main sources in this section are [GW10] and [Bor91].

Let K be a subfield of $\overline{\mathbb{Q}}$. Any variety in this chapter is defined over $\overline{\mathbb{Q}}$.

Definition 1.2.1. A *K-structure* on a variety X defined over $\overline{\mathbb{Q}}$ is a K-scheme X_K of finite type over K which is reduced and separable such that

$$X_K \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\overline{\mathbb{Q}}) \cong X.$$

Definition 1.2.2. Let X be a variety defined over $\overline{\mathbb{Q}}$ together with a K-structure X_K. A subvariety $Y \subset X$ is *defined over* K if there is a K-subscheme $Y_K \subset X_K$ reduced, separable and of finite type over K such that

$$Y_K \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\overline{\mathbb{Q}}) \cong Y.$$

Definition 1.2.3. Let X, Y be two $\overline{\mathbb{Q}}$-varieties. A morphism $\phi : X \to Y$ is *defined over* K if for X_K a K-structure on X and Y_K a K-structure on Y there exist a K-morphism $\phi_K : X_K \to Y_K$ and $\phi_K \times_{\mathrm{Spec}(K)} \overline{\mathbb{Q}} \cong \phi$.

Remark 1.2.4. The three preceding definitions are reformulations of constructions done in [Bor91] sections AG.11 and AG.12.2.

The K-structure on a variety is a more general formulation of the idea that for an affine variety V over $\overline{\mathbb{Q}}$ for which the associated ideal $I_V \subset \overline{\mathbb{Q}}[X_1, \dots, X_n]$ can be generated by polynomials $f_1, \dots, f_m$ defined over some number field K there is a scheme over K associated to

$$K[X_1, \dots, X_n]/(f_1, \dots, f_m)$$

whose base extension by $\overline{\mathbb{Q}}$ is V.

Definition 1.2.5 ([GW10], compare definition in the first paragraph of section (5.1) on page 118)**.** Let X be a variety defined over $\overline{\mathbb{Q}}$ which has a K-structure X_K. A *K-rational point* of X is a morphism from $\mathrm{Spec}(K) \to X_K$. The set of K-rational points of X will be denoted as $X(K)$.

The notion of a K-rational point is the more general formulation of the closed points of an affine variety X which have coordinates in K. The morphisms $\mathrm{Spec}(K) \to X$ correspond to the K-algebra morphisms

$$K[X_1, \dots, X_n]/(f_1, \dots, f_m) \to K.$$

Any such morphism gives a point in the variety with coordinates $(x_1, \dots, x_n) \in \mathbb{A}^n_K$ and vice versa, since

$$K[X_1, \dots, X_n]/(f_1, \dots, f_m) \otimes_K \overline{\mathbb{Q}} = \overline{\mathbb{Q}}[X_1, \dots, X_n]/(f_1, \dots, f_m)$$

and any K-algebra homomorphism is completely determined by its images for a set of generators. In this case these are $X_1, \dots, X_n$.

Example 1.2.6. The affine line $\mathbb{A}^1_K$ associated to $K[X]$ is a K-structure on $\mathbb{A}^1_{\overline{\mathbb{Q}}}$. Its K-rational points are all closed points in $\mathbb{A}^1_K$. Therefore $\mathbb{A}^1_{\overline{\mathbb{Q}}}(K)$ can be associated to the points of K.

Example 1.2.7. The affine variety defined by the ideal $(X_1X_2 - 1) \subset \overline{\mathbb{Q}}[X_1, X_2]$ is a K-variety, since $X_1X_2 - 1 \in \mathbb{Q}[X_1, X_2] \subset K[X_1, X_2]$. Its K-rational points can be associated to the vanishing locus of $X_1X_2 - 1$ in $\mathbb{A}^2_K$ since every such tuple of coordinates defines a morphism

$$K[X_1, X_2]/(X_1X_2 - 1) \to K.$$

By projecting to either X_1 or X_2 the set of K-rational points can also be associated to $\mathbb{A}^1_K \setminus \{0\}$.

1.3 Commutative algebraic groups

This section aims to be a short introduction to commutative algebraic groups. It will mainly follow [Spr98] and [Bor91] for the first subsection and the definition of linear algebraic groups, [Mum70] for abelian varieties and [Mil15] for Chevalley's theorem.

1.3.1 General definitions

In the following K will denote a subfield of $\overline{\mathbb{Q}}$ and G will be a variety defined over $\overline{\mathbb{Q}}$.

Definition 1.3.1 ([Spr98], 2.1.1)**.** An *algebraic group* is a variety G defined over $\overline{\mathbb{Q}}$ and a choice of morphisms called multiplication μ and inverse ι

$$\mu : G \times G \to G \qquad\qquad \iota : G \to G$$

and a $\overline{\mathbb{Q}}$-point $e \in X(\overline{\mathbb{Q}})$ called the neutral element, such that μ, ι and e give the $\overline{\mathbb{Q}}$-points of G the structure of a group.
An algebraic group such that the group structure is commutative is called a *commutative algebraic group.*

Definition 1.3.2 ([Spr98], 2.1.1)**.** A *morphism* of algebraic groups is a morphism which is a group homomorphism and a morphism of varieties.

Definition 1.3.3 ([Spr98], 2.1.1)**.** If the algebraic group G has a K-structure, $e \in X$ is a K-rational point and the morphisms μ and ι are defined over K, then G is a *K-group.*

Proposition 1.3.4 ([Spr98], 2.1.1)**.** *If G is a K-group, the set $G(K)$ has a group structure induced by the structure on G.*

Proof. The set $G(K)$ is equal to the set $\mathrm{Mor}(\mathrm{Spec}(K), G)$. Since G has a group structure it induces a group structure on $\mathrm{Mor}(\mathrm{Spec}(K), G)$ and therefore on $G(K)$. □

Definition 1.3.5 ([Spr98], 2.1.1)**.** A morphism $\phi : G \to H$ of algebraic groups is a *K-morphism* if G and H have a K-structure and ϕ is defined over K as a morphism.

To emphasise the fact that the algebraic groups considered in this thesis will be commutative they will be, if not stated otherwise, denoted additively. That is as an algebraic group

$$(G, 0_G, +).$$

There will be some exceptions to this rule if the group operation for a specific group coincides with an operation which is generally denoted multiplicatively. These will be stated explicitly. The notation $[n]_G$, or $[n]$ if there will not be any confusion about the group, will denote the multiplication by n, i.e.

$$\begin{aligned} [n]_G : G &\to G. \\ g &\mapsto \underbrace{g + \ldots + g}_{n \text{ times}} \end{aligned}$$

Definition 1.3.6 ([Spr98], 2.1.1)**.** Let G be an algebraic group. A *closed subgroup* H of G is a closed subset of G (in the Zariski topology) which is also a subgroup with regards to the group structure on G.

Remark 1.3.7. A closed subgroup H of an algebraic group G is again an algebraic group and the inclusion morphism $H \hookrightarrow G$ is a group homomorphism ([Spr98] 2.1.1).

There can be subgroups of G which do not have the structure of a variety as the following example shows.

Example 1.3.8. Let $G = \mathbb{A}^1_{\overline{\mathbb{Q}}} \setminus \{0\}$ and choose an embedding of $\overline{\mathbb{Q}}$ into the complex numbers. The subset $\mathbb{S}^1_{\overline{\mathbb{Q}}} = \{x \in \overline{\mathbb{Q}}^* \mid x \cdot \overline{x} = 1\}$ is a subgroup of G. Here $\overline{x}$ denotes the complex conjugation of x. Since all proper Zariski-closed subsets of G are finite, $\mathbb{S}^1_{\overline{\mathbb{Q}}}$ is not closed in the Zariski topology. Therefore $\mathbb{S}^1_{\overline{\mathbb{Q}}}$ is a subgroup but not a closed subgroup of G.

The definition of a subgroup also extends analogously to the definitions above to K-algebraic groups.

Definition 1.3.9 ([Spr98], 2.1.1)**.** Let G be an algebraic group which is defined over K. A *K-subgroup* of G is a subgroup $H \leq G$ such that H is a closed K-subvariety of G.

The added structure provided by the group operation has some implications on the underlying variety.

Proposition 1.3.10 ([Spr98], compare Proposition 2.2.1)**.** *The underlying variety of an algebraic group G is irreducible iff it is connected.*

Proof. The implication irreducible to connected holds for any variety.
For the converse one can use points (i) and (ii) of Proposition 2.2.1 in [Spr98], which state that there is a unique irreducible component G^0 of G which contains the identity element and that this irreducible component is a subgroup of G. This is also the unique connected component of G containing 0_G.
So $G^0 = G$ if G is connected and therefore the variety underlying G is irreducible in this case. □

Proposition 1.3.11 ([Bor91], Proposition I.1.2)**.** *Any algebraic group is smooth.*

Lemma 1.3.12 ([Bor91], I.1.4 and [Spr98], Proposition 2.2.5)**.** *Let $\phi : G \to H$ be a morphism of algebraic groups. Then*

a) $\phi(G)$ *is a closed subgroup of* H*.*

b) $\ker(\phi)$ *is a normal and closed subgroup of* G*.*

If G and H are K-groups and the morphism ϕ is defined over K then $\phi(G)$ is a K-subgroup of H.

1.3.2 Abelian varieties

As stated in the introduction of the section, this subsection will mainly be following [Mum70].

This subsection is again looking at algebraic groups defined over $\overline{\mathbb{Q}}$. The letter K will again denote a subfield of $\overline{\mathbb{Q}}$.

Definition 1.3.13 ([Mum70], Definition on p.39)**.** An algebraic group whose underlying variety is irreducible and complete is called an *abelian variety.*

This definition especially implies that all abelian varieties are connected.

Proposition 1.3.14 ([Mum70], p.41 (ii))**.** *Any abelian variety is commutative.*

The condition of completeness also leads to an interaction of line bundles with the group operation.

Definition 1.3.15 ([HS00], Corollary A.7.2.5)**.** Let A be an abelian variety. A divisor or line bundle L is called *symmetric* if

$$L \cong [-1]_A^* L.$$

It is called *antisymmetric* if

$$L^{-1} \cong [-1]_A^* L.$$

Lemma 1.3.16 ('Law of the Cube', [Mum70], Corollary 3 p.59)**.** *Let A be an abelian variety. For any $n \in \mathbb{Z}$ and any line bundle L the following holds*

$$[n]_A^* L \sim L^{\left(\frac{n^2+n}{2}\right)} \otimes ([-1]_A^* L)^{\left(\frac{n^2-n}{2}\right)}.$$

Corollary 1.3.17. *If L is a symmetric line bundle on an abelian variety A, then*

$$[n]_A^* L \sim L^{n^2}.$$

If L is an antisymmetric line bundle, then

$$[n]_A^* L \sim L^n.$$

Proof. For a symmetric line bundle one has $[-1]^* L \sim L$. Therefore an easy explicit calculation gives

$$\begin{aligned} [n]_A^* L &\overset{1.3.16}{\sim} L^{\left(\frac{n^2+n}{2}\right)} \otimes ([-1]_A^* L)^{\left(\frac{n^2-n}{2}\right)} \\ &\sim L^{\left(\frac{n^2+n}{2}\right)} \otimes L^{\left(\frac{n^2-n}{2}\right)} \\ &= L^{\left(\frac{n^2+n+n^2-n}{2}\right)} \\ &= L^{n^2}. \end{aligned}$$

An analogous computation using $[-1]_A^* L \sim L^{-1}$ gives the result for antisymmetric line bundles. □

Regarding the line bundles as divisors one gets the following equivalent result.

Corollary 1.3.18. *Let D be a divisor on the abelian variety A. If D is symmetric, i.e. $[-1]_A^* D \sim D$, then*

$$[n]_A^* D \sim n^2 D.$$

If D is antisymmetric , i.e. $[-1]_A^* D \sim -D$, then

$$[n]_A^* D \sim nD.$$

Proposition 1.3.19 ([Mum70], Proposition p.64)**.** *Let A be an abelian variety of dimension g and $n \in \mathbb{N}_{>0}$. Then*

$$A_n := \ker([n]_A) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}.$$

Corollary 1.3.20. *Let A be an abelian variety of dimension g and $n \in \mathbb{N}_{>0}$. If A is defined over K then*

$$|\{a \in A(K)|\ [n]_A a = 0_A\}|$$

divides n^{2g}.

Proof. This follows from the preceding proposition combined with the facts that $A(K)$ and $\ker([n]_A)$ are subgroups of A. This implies that

$$\{a \in A(K)|\ [n]_A a = 0_A\} = A(K) \cap \ker([n]_A) \leq \ker([n]_A)$$

is a group. Now Lagrange's theorem implies the statement. □

1.3.3 Linear algebraic groups

Next to abelian varieties another class of algebraic groups are linear algebraic groups.

Just like the previous subsections, this subsection is again looking at algebraic groups defined over $\overline{\mathbb{Q}}$. The letter K will again denote a subfield of $\overline{\mathbb{Q}}$.

The literature used for this section is [Spr98] and [Bor91].

Definition 1.3.21 ([Spr98], 2.1.1)**.** An algebraic group whose underlying variety is affine is called a *linear algebraic group.*

Unlike abelian varieties a linear algebraic group don not have to be commutative.

Example 1.3.22 ([Bor91], compare with I.1.6 (2))**.** Let $n \geq 1$. The group

$$(\mathrm{GL}_n(\overline{\mathbb{Q}}), \cdot)$$

(with $\cdot$ denoting the matrix multiplication) has a structure of an algebraic group. It is given by taking the matrix entries $(X_{i,j})_{1\leq i,j\leq n}$ and the inverse of the determinant $D^{-1} = \det((X_{i,j})_{1\leq i,j,\leq n})^{-1}$ as coordinates of the affine space $\mathbb{A}^{n^2+1}_{\overline{\mathbb{Q}}}$. The rational points $\mathrm{GL}_n(\overline{\mathbb{Q}})$ can now be identified with the following closed subvariety of $\mathbb{A}^{n^2+1}_{\overline{\mathbb{Q}}}$

$$\left\{(X_{1,1},\ X_{1,2}, \ldots,\ X_{n,n},\ D^{-1}) \in \mathbb{A}^{n^2+1}_{\overline{\mathbb{Q}}}\ \middle|\ \det((X_{i,j})_{1\leq i,j,\leq n})) \cdot D^{-1} - 1 = 0\right\} \subset \mathbb{A}^{n^2+1}_{\overline{\mathbb{Q}}}.$$

This is an affine variety, since it is a closed subvariety of an affine variety.
The multiplication and inversion of $\mathrm{GL}_n(\overline{\mathbb{Q}})$ are each given by polynomial equations for each coordinate

$$\mu : \mathrm{GL}_n(\overline{\mathbb{Q}}) \times \mathrm{GL}_n(\overline{\mathbb{Q}}) \to \mathrm{GL}_n(\overline{\mathbb{Q}})$$
$$(((X_{i,j})_{1\leq i,j\leq n},\ D_X^{-1}), ((Y_{i,j})_{1\leq i,j\leq n},\ D_Y^{-1})) \mapsto \left(\left(\sum_{k=1}^{n} X_{i,k}Y_{k,j}\right)_{1\leq i,j\leq n},\ D_X^{-1}D_Y^{-1}\right)$$

$$\iota : \mathrm{GL}_n(\overline{\mathbb{Q}}) \to \mathrm{GL}_n(\overline{\mathbb{Q}})$$
$$((X_{i,j})_{1\leq i,j\leq n},\ D^{-1}) \mapsto \left(\left((-1)^{i+j}D^{-1}\det\left((X_{l,m})_{\substack{1\leq l,m\leq n\\ l\neq i,\ m\neq j}}\right)\right)_{1\leq i,j\leq n},\ \det((X_{i,j})_{1\leq i,j\leq n})\right).$$

Hence they are morphisms of varieties. This algebraic structure is compatible with the group structure and makes $\mathrm{GL}_n(\overline{\mathbb{Q}})$ a linear algebraic group. But for $n \geq 2$ this group structure is not commutative. These groups are called *general linear groups.*

In the case $n = 1$ this group is given the following name.

Definition 1.3.23 ([Bor91], Example I.1.6 (2))**.** The linear algebraic group $\mathrm{GL}_1(\overline{\mathbb{Q}})$ is called *multiplicative group.* It will generally be denoted as $(\mathbb{G}_m, \cdot, 1)$.

The affine line $\mathbb{A}^1_{\overline{\mathbb{Q}}}$ can also be given a group structure compatible with its algebraic structure by the addition on $\overline{\mathbb{Q}}$.

$$\begin{aligned}\mu : \mathbb{A}^1_{\overline{\mathbb{Q}}} \times \mathbb{A}^1_{\overline{\mathbb{Q}}} &\to \mathbb{A}^1_{\overline{\mathbb{Q}}}\\ (X, Y) &\mapsto X + Y\\ \iota : \mathbb{A}^1_{\overline{\mathbb{Q}}} &\to \mathbb{A}^1_{\overline{\mathbb{Q}}}\\ X &\mapsto -X\end{aligned}$$

This group as well has its own name.

Definition 1.3.24 ([Bor91], Example I.1.6 (1))**.** The affine line $\mathbb{A}^1_{\overline{\mathbb{Q}}}$ with the group structure defined above is called the *additive group.* It is generally denoted as $(\mathbb{G}_a, +, 0)$.

Remark 1.3.25. The multiplicative group as well as the additive group are defined over any field $\mathbb{Q} \subset K \subset \overline{\mathbb{Q}}$. Their K-rational points can be associated with $K \setminus \{0\}$ and K respectively, since they have a K-structure defined by $K[X, X^{-1}]$ and $K[X]$.

Definition 1.3.26 ([Spr98], 3.4.1)**.** An algebraic group V such that for some $l \in \mathbb{N}_0$

$$V \cong \mathbb{G}_a^l$$

is called a *vector group.*

Definition 1.3.27 ([Spr98], 3.2.1)**.** An algebraic group T is called a torus if there is some $l \in \mathbb{N}_0$ such that

$$T \cong \mathbb{G}_m^l.$$

It can be shown that up to isomorphism every linear algebraic group is a subgroup of a general linear group.

Lemma 1.3.28 ([Spr98], Theorem 2.3.7)**.** *Any linear algebraic group defined over a field K is isomorphic to a closed subgroup of $\mathrm{GL}_n(K)$ for some $n \in \mathbb{N}_{>0}$.*

This allows to transplant definitions like unipotent and semi-simple into the setting of linear algebraic groups.

Definition 1.3.29 ([Spr98], 2.4.1)**.** Let $L \subset \mathrm{GL}_n(K)$ be a linear algebraic group. An element $g \in L$ is called *unipotent* if there exists some $m \in \mathbb{N}_{>0}$ such that

$$(g - 1_{\mathrm{GL}_n(K)})^m = 0_{\mathrm{Mat}_n(K)}.$$

An element $h \in L$ is called *semi-simple* if it is diagonisable as a matrix over the algebraic closure $\overline{K}$ of K.

This generalises to automorphisms over vector spaces of arbitrary dimension in the following way.

Definition 1.3.30 ([Spr98], 2.4.7)**.** Let W be an arbitrary K-vector space. An endomorphism f of W is said to be *locally unipotent* if its restriction to any finite dimensional f-invariant subspace is unipotent. Analogously f is said to be *locally semi-simple* if its restriction to any f-invariant finite dimensional sub vector space is semi-simple.

For any linear algebraic K-group L right multiplication by $g \in L$ is a group isomorphism. Since the underlying variety is affine morphisms from L to L can be associated with K-algebra morphisms on the coordinate ring $K[L]$ ([Bor91], I.1.5). So the right multiplication by g defines a K-vector space morphism $\rho_g : K[L] \to K[L]$, which we can use to define semi-simple and unipotent for arbitrary linear algebraic groups and a Jordan decomposition of elements in L.

Proposition 1.3.31 ('Jordan Decomposition', [Spr98], 2.4.8 and [Bor91], Theorem 4.4)**.** *For $g \in L$, where L a linear K-group, there are unique elements $g_u \in L$ called the* unipotent part *and $g_s \in L$ called the* semi-simple part *of L, such that*

$$g = g_u g_s = g_s g_u$$
$$(\rho_g)_u = \rho_{g_u}, \qquad (\rho_g)_s = \rho_{g_s}.$$

If L is a subgroup of some $\mathrm{GL}_n(K)$, then this coincides with the notion of unipotent and semi-simple defined above. The unipotent part g_u as well as the semi-simple part g_s are again defined over K.

Definition 1.3.32 ([Spr98], 2.4.8)**.** An element $g \in L$ is called *unipotent* if it is equal to its unipotent part g_u. The element is called *semi-simple* if it is equal to its semi-simple part g_s.

Since the notions of unipotent and semi-simple part are compatible with group homomorphisms, this implies that these definitions are compatible with the ones for subgroups of general linear groups ([Spr98], 2.4.9).

Definition 1.3.33 ([Spr98], 2.4.11)**.** A linear algebraic group U is called a *unipotent group* if all its elements are unipotent.

Definition 1.3.34 ([Bor91], I.4.5)**.** A linear algebraic group L is called a *semi-simple group* if all its elements are semi-simple.

An example of a unipotent group is a vector group.

Example 1.3.35. Let $V = \mathbb{G}_a(K)^n$ be a vector group over a number field K. Then the following embedding makes V a unipotent subgroup of $\mathrm{GL}_{n+1}(K)$

$$\phi : V \to \mathrm{GL}_{n+1}(K)$$
$$(v_1, \ldots, v_n) \mapsto \begin{pmatrix} 1 & v_1 & 0 & \ldots & \ldots & 0 \\ 0 & 1 & v_2 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & \ldots & 0 & 1 & v_n \\ 0 & \ldots & \ldots & \ldots & 0 & 1 \end{pmatrix}.$$

So any vector group is unipotent.

Theorem 1.3.36 ([Spr98], 3.1.1, 3.1.2 and [Bor91], I.4.5, I.4.6 and Theorem I.4.7)**.** *Let L be a connected commutative linear algebraic group over a number field K. The unipotent elements L_u and the semi-simple elements L_s of L each form a connected closed subgroup of L. The map induced by the multiplication on L*

$$\mu : L_u \times L_s \to L$$

is an isomorphism of algebraic groups.
After some finite field K'/K extension L_u is isomorphic to a vector group and L_s is isomorphic to a split torus. So one gets

$$L \cong \mathbb{G}_a^{l_a} \times \mathbb{G}_m^{l_m}$$

for some $l_a,\ l_m \in \mathbb{N}_0$ as K'-groups.

Proof. The first statement is Theorem I.4.6 in [Bor91]. The idea behind the proof is to embed L into some general linear group. Then use a generalisation of the fact that when two endomorphisms commute they can be triagonalised simultaneously together with the only unipotent semi-simple morphism being the identity morphism.
The second statement can be found in the book by Springer. For the unipotent part this is [Spr98] Lemma 14.3.2 in combination with any module over a field being free (compare [Spr98] 3.3.1). The statement on the semi-simple part is using part (b) of the proposition in I.4.6 [Bor91], which states that any set of commuting endomorphisms can be diagonalised over the field extension by the eigenvalues of the endomorphisms. To obtain such a field extension it is sufficient to adjoin finitely many elements, since the K-vector space of semi-simple endomorphisms contained in $\mathrm{GL}_n(K)$ is finitely generated and any endomorphism has only finitely many eigenvalues over the algebraic closure. So there is such a field extension which is a finite extension. □

Proposition 1.3.37. *In the group $\mathbb{G}_a$ the kernel of the morphism $[n]_{\mathbb{G}_a}$ is trivial. In $\mathbb{G}_m$ the kernel of $[n]_{\mathbb{G}_m}$ has n elements if K is algebraically closed. If K is not algebraically closed $|\ker[n]_{\mathbb{G}_m}|$ divides n.*

Proof. For $\mathbb{G}_a$ this is the claim that multiplication by n in a field is injective.
For $\mathbb{G}_m$ the claim is that a field contains either all n-th roots of unity or their number divides n and every algebraically closed field contains all roots of unity. □

Corollary 1.3.38. *Let $L \cong \mathbb{G}_a^{l_a} \times \mathbb{G}_m^{l_m}$, $\dim L = l_a + l_m =: d$ be a split commutative linear group. Then for any $x \in L$ and $n \in \mathbb{Z}$ the cardinality of $[n]_L^{-1}(\{x\})$ divides n^d.*

Proof. The preceding proposition implies that the cardinality of the kernel of $[n]_L$ divides n^d. Since $[n]_L$ is a group homomorphism the cardinality of the preimage is the same everywhere which implies the corollary. □

1.3.4 Chevalley's theorem

In general, a smooth connected algebraic group over a number field will be an extension of an abelian variety by an affine variety. This is the structure theorem for algebraic groups by Chevalley.

Definition 1.3.39 ([Mil15], compare Definition 1.48 and the paragraph following it)**.** A *short exact sequence* of algebraic groups is a sequence

$$0 \to G' \xrightarrow{i} G \xrightarrow{p} G'' \to 0$$

such that i is an isomorphism onto the kernel of p and p is surjective. One also says G is an extension of G'' by G'.

Remark 1.3.40. The script [Mil15] uses a more general definition of algebraic groups. What in this thesis is called an algebraic group is called a group variety in [Mil15].

Theorem 1.3.41 ([Mil13], compare Theorem 5.1)**.** *Let G be an algebraic K-group with K being a subfield of $\overline{\mathbb{Q}}$. Then G is a unique extension of an abelian variety A by a normal linear algebraic group L which is a subgroup of G*

$$0 \to L \xrightarrow{i} G \xrightarrow{p} A \to 0.$$

This construction commutes with extension of the base field K.

Corollary 1.3.42. *Let K be a subfield of $\overline{\mathbb{Q}}$ and G a connected commutative algebraic K-group. Then there exists a finite field extension K'/K and $l_a,\ l_m \in \mathbb{N}_0$ such that G is the following extension of algebraic groups*

$$0 \to \mathbb{G}_a^{l_a} \times \mathbb{G}_m^{l_m} \xrightarrow{i} G \xrightarrow{p} A \to 0.$$

Proof. This follows from combining the decomposition in Theorem 1.3.41 and the one in Theorem 1.3.36 combined with the fact that the decomposition in Theorem 1.3.41 is compatible with change of the base field. □

Proposition 1.3.43. *Let K be a subfield of $\overline{\mathbb{Q}}$ and G a connected commutative algebraic K-group. Then for any $g \in G$ the number of preimages of the multiplication-by-n-morphism $[n]_G$ of g divides $n^{2 \dim G}$.*

Proof. Without loss of generality assume that the linear part L of G is split over K. Let $g \in G$ be some point and $g_1, \dots, g_m$ its preimages under $[n]_G$. Since the projection map $p : G \to A$ commutes with the group operations, the number of elements in $\{p(g_1), \dots, p(g_m)\}$ divides $n^{2 \dim A}$. We want to know how many of the $g_1, \dots, g_m$ have the same image under p. Assume $g_1, \dots, g_c$ are all mapped to the same $a \in A$ by p. Then all the differences $l_j := g_1 - g_j$ for $1 \leq j \leq c$ must be in the kernel of p and therefore in the image of i. The l_j are n torsion elements of G, since $[n]_G l_j = [n]_G(g_1 - g_j) = g - g = 0$. Combining Corollary 1.3.38 with the fact that i is an injective map gives that the number of preimages of 0_G under $[n]_G$ in $i(L)$ divides $n^{\dim L}$. The only thing left to note is now that if a' is some other element in A such that $[n]_A a' = p(g)$, at least c of the $g_1, \dots, g_m$ must map to a'. Hence c divides m and therefore m must divide $n^{2 \dim A} \cdot n^{\dim L}$ and thus also $n^{2 \dim G}$. □

Another way to regard this exact sequence is to say that G is a *L-torsor* over A or *principal L-bundle over A*. This first needs some definitions.

Definition 1.3.44 ([Spr98], 2.3.1)**.** Let G be an algebraic group. A variety X defined over $\overline{\mathbb{Q}}$ is called a *G-space* if it has a G-action which is given by a morphism. This means there is a morphism of varieties

$$\cdot : G \times X \to X$$

such that for all $h, g \in G$ and $x \in X$

$$\cdot(g, \cdot(h, x)) = \cdot(g + h, x), \qquad\qquad \cdot(0_G, x) = x.$$

If G, X and the action are defined over some field $K \subset \overline{\mathbb{Q}}$ then X is a G-space over K.

In the following text the notation $g \cdot x$ is used for $\cdot(g, x)$.

Definition 1.3.45 ([Spr98], 2.3.1)**.** Let G be an algebraic group. A *morphism between G-spaces* X and Y is a morphism $\phi : X \to Y$ of varieties such that for all $g \in G$ and all $x \in X$

$$\phi(g \cdot x) = g \cdot \phi(x).$$

Definition 1.3.46 ([BSU13], Definition 6.1.1)**.** Let L be an affine algebraic group. A *principal L-bundle* or *torsor* is a morphism of varieties $p : X \to Y$ such that

a) p is faithfully flat.

b) X is an L-space with action α and p is invariant under this action.

c) The following diagram is cartesian

$$\begin{array}{ccc} L \times X & \xrightarrow{\mathrm{pr}_2} & X \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle p} \\ X & \xrightarrow{p} & Y \end{array}.$$

Here pr_2 is the projection on the second coordinate.

Remark 1.3.47. Let $p : X \to Y$ and $p' : X' \to Y'$ be principal L-bundles. Any map $f : X \to X'$ of L-spaces induces a unique map $f^L : Y \to Y'$ such that $p' \circ f = f^L \circ p$, since p is a quotient ([BSU13] p.77 paragraph after point (iv) and [MFK94] Proposition 0.1). Such maps f are called L-equivariant and define morphisms between L-principal bundles. If there are L-bundles $p : X \to Y$, $p' : X' \to Y'$ and $p'' : X'' \to Y''$ and L-space morphisms $f : X \to X'$, $g : X' \to X''$, one has $(g \circ f)^L = g^L \circ f^L$. This is a consequence of the big square in the following commutative diagram commuting, if both smaller ones do, together with the factoring of a map through the quotient being unique.

$$\begin{array}{ccccc} X & \xrightarrow{f} & X' & \xrightarrow{g} & X'' \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle p'} & & \downarrow{\scriptstyle p''} \\ Y & \xrightarrow{f^L} & Y' & \xrightarrow{g^L} & Y'' \end{array}.$$

Uniqueness of the factorisation also implies that $(id_X)^L = id_Y$.

Proposition 1.3.48 ([Mil15], compare 2-1, 5.61)**.** *Let G be an algebraic group and L and A as in Theorem 1.3.41. Then G is an L-principal bundle over A.*

Proof. The morphism p is faithfully flat by Remark 1.28 in [Mil15]. The linear group L acts on G by

$$\begin{aligned} \cdot : L \times G &\to G \\ (l, g) &\mapsto g + i(l). \end{aligned}$$

The map p is invariant under this action since $\ker(p) = i(L)$. It is left to show that

$$\begin{aligned} L \times G &\to G \times_A G \\ (l, g) &\mapsto (g + i(l), g) \end{aligned}$$

is an isomorphism of varieties. This map is a well defined morphism since for any $g \in G$ and $l \in L$ the equality $p(g + i(l)) = p(g)$ holds. This has an inverse map as a map of sets

$$\begin{aligned} G \times_A G &\to L \times G \\ (g', g) &\mapsto (i^{-1}(g' - g), g) \end{aligned}$$

and as such is a bijective map. But since the fibre product $G \times_A G$ can be viewed as a closed subset of $G \times G$ this map is also a morphism of varieties. So this is an isomorphism $L \times G \cong G \times_A G$. It can be seen that the induced map of sets

$$L(K) \times G(K) \to G(K) \times_{A(K)} G(K)$$

for any field of definition K of G is also bijective with an analogous reasoning. □

Definition 1.3.49 ([BSU13], paragraph after the Example on p.77)**.** Let L be an affine algebraic group and $p : X \to Y$ a principal L-bundle and Z an L-space. Then a variety W with a morphism $q : X \times Z \to W$ and $p_Z : W \to Y$ such that

$$\begin{array}{ccc} X \times Z & \xrightarrow{\mathrm{pr}_1} & X \\ \downarrow{\scriptstyle q} & & \downarrow{\scriptstyle p} \\ W & \xrightarrow{p_Z} & Y \end{array}$$

is cartesian is called an *associated bundle.* In the following text the associated bundle will also be denoted as $X \times^L Z$.

Remark 1.3.50. This construction makes $q : X \times Z \to X \times^L Z$ a G-bundle with regards to the diagonal action of L on $X \times Z$ defined as

$$\begin{aligned} L \times (X \times Z) &\to X \times Z \\ (l, (x, z)) &\mapsto (l \cdot x, l^{-1} \cdot z) \end{aligned}$$

([BSU13], paragraph after the example on p.77). Therefore $X \times^L Z$ is a quotient of $X \times Z$ by the diagonal action. Let $X' \times^L Z'$ be an L-bundle associated to $p' : X' \to Y'$. Due to the universal property of the quotient any morphism $f : X \times Z \to X' \times Z'$ of L-spaces with regards to the diagonal action defines a morphism of the associated bundles. If one has $f_1 : X \to X'$ and $f_2 : Z \to Z'$ maps of L-spaces with their respective action, then their product $f_1 \times f_2 : X \times Z \to X' \times Z'$ will be a map of L-spaces with the diagonal action. Hence each such map defines a morphism $f_1 \times^L f_2$ of associated bundles.

1.4 Heights

A height function is intended to be a way to measure algebraic complexity of an algebraic number and to be a generalisation of the normal absolute value on $\mathbb{Z}$.

The following is a survey of the material needed to do the height estimate in later chapters. It is mainly taken from chapters 1 to 5 of Part B in [HS00].

In the following section let K always denote an algebraic number field.

1.4.1 Heights on projective space

The set of non-trivial places of K will be denoted as M_K. The subset of archimedian and nonarchimedian places will be written as M_K^0 and M_K^∞ respectively.

Remark 1.4.1. Every absolute value $|\cdot|$ in M_K^0 is normalised such that its restriction to $\mathbb{Q}$ agrees with the standard archimedian absolute value on $\mathbb{Q}$, that is for any $x \in \mathbb{Q}$

$$|x| = \max\{x, -x\}.$$

If $|\cdot|$ is an absolute value in M_K^∞ then it is normalised such that its restriction to $\mathbb{Q}$ is one of the standard p-adic absolute values. This means that if $p \in \mathbb{N}_{>0}$ is a prime such that $|p| \leq 1$, then the normalisation of $|\cdot|$ is chosen such that

$$|p| = \frac{1}{p}.$$

Definition 1.4.2 ([Lan94], Corollary 1 Part II §1)**.** Let $\nu \in M_K$ be a place. The *local degree* d_ν is defined as

$$d_\nu := \begin{cases} [K_\nu : \mathbb{Q}_p] & \nu \in M_K^0 \text{ corresponding to a prime ideal } \mathfrak{p}|(p) \\ [K_\nu : \mathbb{R}] & \nu \in M_K^\infty. \end{cases}$$

Here K_ν denotes the completion of K with respect to the absolute value ν.

For any number field K and any finite algebraic field extension L/K there is the following degree formula

Lemma 1.4.3 ('Degree Formula', [Lan94], Corollary 1 Part II §1). *It holds that*

$$\sum_{\substack{\omega \in M_L \\ \omega|_K = \nu}} [L_\omega : K_\nu] = [L : K].$$

In the case of $K = \mathbb{Q}$ and L a number field this formula implies

$$\sum_{\substack{\nu \in M_L^0 \\ \nu | p}} d_\nu = [L : \mathbb{Q}] \qquad \sum_{\nu \in M_L^\infty} d_\nu = [L : \mathbb{Q}].$$

These places also fulfil the following product formula.

Lemma 1.4.4 (Product formula, [HS00], Proposition B.1.2). *For a number field K and $a \in K \setminus \{0\}$ one has*

$$\prod_{\nu \in M_K} |a|_\nu^{d_\nu} = 1.$$

Definition 1.4.5 ([HS00], Definition p.176). Let $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ be a point with projective coordinates $[p_0 : \ldots : p_n]$, such that $p_0, \ldots, p_n \in K$ for a number field K.
The *absolute multiplicative height* of P on the projective space $\mathbb{P}^n(\overline{\mathbb{Q}})$ is defined as

$$H(P) := \left(\prod_{\nu \in M_K} \max\{|p_0|_\nu, \ldots |p_n|_\nu\}^{d_\nu} \right)^{\frac{1}{[K:\mathbb{Q}]}}.$$

The *absolute logarithmic height* or *absolute height* of P on the projective space $\mathbb{P}^n(\overline{\mathbb{Q}})$ is defined as

$$h(P) := \log H(P) = \frac{1}{[K : \mathbb{Q}]} \sum_{\nu \in M_K} d_\nu \log \max\{|p_0|_\nu, \ldots |p_n|_\nu\}.$$

Lemma 1.4.6 ([HS00], compare Lemma B.2.1). *The absolute height is well defined and induces the following height maps:*

$$\begin{aligned} H : \mathbb{P}^n(\overline{\mathbb{Q}}) &\to [1, \infty) \\ P &\mapsto H(P) \\ h : \mathbb{P}^n(\overline{\mathbb{Q}}) &\to [0, \infty) \\ P &\mapsto h(P) \end{aligned}$$

Remark 1.4.7. If it is not obvious which projective space a height function h is associated to a subscript $h_{\mathbb{P}^n}$ is added.

Definition 1.4.8 ([HS00], Definition p.171)**.** The *(logarithmic) height* on $\overline{\mathbb{Q}}$ or *affine height* is defined as the projective height of the point $[1 : a] \in \mathbb{P}^1(\overline{\mathbb{Q}})$

$$h(a) := h([a : 1]) \qquad \forall a \in \overline{\mathbb{Q}}.$$

Proposition 1.4.9 ([HS00], Proposition B.2.6 (b))**.** *Let*

$$\begin{aligned} S_{n,m} : \mathbb{P}^n \times \mathbb{P}^m &\to \mathbb{P}^N \\ ([x], [y]) &\mapsto [x_0y_0 : x_0y_1 : \ldots : x_ny_m] \end{aligned}$$

be the Segre embedding. For any $[x] \in \mathbb{P}^n$ and $[y] \in \mathbb{P}^m$

$$h_{\mathbb{P}^N}\left(S_{n,m}([x], [y])\right) = h_{\mathbb{P}^n}([x]) + h_{\mathbb{P}^m}([y]).$$

1.4.2 Some inequalities for heights on projective spaces

Lemma 1.4.10. *Let $P = [x_0 : \ldots : x_n]$, $Q = [y_0 : \ldots : y_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$. Let h be the height function associated to that choice of coordinates. If the pointwise product and sum respectively of P and Q is well defined, then*

$$\begin{aligned} h([x_0 + y_0 : \ldots : x_n + y_n]) &\le \log 2 + h([x_0 : \ldots : x_n : y_0 : \ldots : y_n]) \\ h([x_0y_0 : \ldots : x_ny_n]) &\le h([x_0 : \ldots : x_n]) + h([y_0 : \ldots : y_n]). \end{aligned}$$

Proof. Let K be a number field such that $x_0, \ldots, x_n, y_0, \ldots, y_n \in K$, then

$$\begin{aligned} h([x_0 + y_0 : \ldots : x_n + y_n]) &= \frac{1}{[K : \mathbb{Q}]} \sum_{\nu \in M_K} d_\nu \log \max_{i=1,\ldots,n} |x_i + y_i|_\nu \\ &\le \frac{1}{[K : \mathbb{Q}]} \left(\sum_{\nu \in M_K^0} d_\nu \log \max_{i=1,\ldots,n} \max\{|x_i|_\nu,\ |y_i|_\nu\} \right. \\ &\qquad \left. + \sum_{\nu \in M_K^\infty} d_\nu \log \max_{i=1,\ldots,n} 2 \max\{|x_i|_\nu, |y_i|_\nu\} \right) \\ &= \frac{1}{[K : \mathbb{Q}]} \left(\sum_{\nu \in M_K} d_\nu \log \max_{i=1,\ldots,n} \{|x_i|_\nu, |y_i|_\nu\} + \sum_{\nu \in M_K^\infty} d_\nu \log 2 \right) \\ &= h([x_0 : \ldots : x_n : y_0 : \ldots : y_n]) + \frac{\sum_{\nu \in M_K^\infty} d_\nu}{[K : \mathbb{Q}]} \log 2 \\ &\overset{1.4.3}{=} h([x_0 : \ldots : x_n : y_0 : \ldots : y_n]) + \frac{[K : \mathbb{Q}]}{[K : \mathbb{Q}]} \log 2 \\ &= h([x_0 : \ldots : x_n : y_0 : \ldots : y_n]) + \log 2, \end{aligned}$$

$$\begin{aligned}
h([x_0 \cdot y_0 : \ldots : x_n \cdot y_n]) =& \frac{1}{[K:\mathbb{Q}]} \sum_{\nu \in M_K} d_\nu \log \max_{i=1,\ldots,n} |x_i y_i|_\nu \\
=& \frac{1}{[K:\mathbb{Q}]} \sum_{\nu \in M_K} d_\nu \log \max_{i=1,\ldots,n} |x_i|_\nu |y_i|_\nu \\
\leq& \frac{1}{[K:\mathbb{Q}]} \sum_{\nu \in M_K} d_\nu \log \left(\max_{i=1,\ldots,n} |x_i|_\nu \max_{j=1,\ldots,n} |y_j|_\nu \right) \\
=& \frac{1}{[K:\mathbb{Q}]} \left(\sum_{\nu \in M_K} d_\nu \log \max_{i=1,\ldots,n} |x_i|_\nu + \sum_{\nu \in M_K} d_\nu \log \max_{j=1,\ldots,n} |y_j|_\nu \right) \\
=& h([x_0 : \ldots : x_n]) + h([y_0 : \ldots : y_n]).
\end{aligned}$$

□

Remark 1.4.11. Since the projective point $[x_0 + y_0 : \ldots : x_n + y_n]$ depends on the chosen representatives $[x_0 : \ldots : x_n]$ and $[y_0 : \ldots : y_n]$ of the points P and Q, the first inequality will as well depend on those choices. Since the projective point $[x_0 y_0 : \ldots : x_n y_n]$ is independent of those choices, the latter inequality is as well.

Remark 1.4.12. Both inequalities generalise if one has more summands or factors respectively. Assume there are points $\left[x_0^{(1)} : \ldots : x_n^{(1)}\right], \ldots, \left[x_0^{(m)} : \ldots : x_n^{(m)}\right] \in \mathbb{P}^n(\overline{\mathbb{Q}})$ such that their pointwise sum or product is a well defined point in $\mathbb{P}^n$. For the first inequality one has

$$h\left(\left[\sum_{i=1}^m x_0^{(i)} : \ldots : \sum_{i=1}^m x_n^{(i)}\right]\right) \leq h\left(\left[x_0^{(1)} : \ldots : x_n^{(1)} : \ldots : x_0^{(m)} : \ldots : x_n^{(m)}\right]\right) + \log m.$$

This uses that for any absolute value $|\cdot|$ on a number field which contains $x_0^{(1)}, \ldots, x_n^{(m)}$

$$\max_{1 \leq j \leq n} \left\{ \left| \sum_{i=1}^m x_j^{(i)} \right| \right\} \leq m \max_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \left\{ \left| x_j^{(i)} \right| \right\}$$

holds. Then the calculations can be done analogously to Lemma 1.4.10.
For the second inequality one has

$$h\left(\left[\prod_{i=1}^m x_0^{(i)} : \ldots : \prod_{i=1}^m x_n^{(i)}\right]\right) \leq \sum_{i=1}^m h\left(\left[x_0^{(i)} : \ldots : x_n^{(i)}\right]\right)$$

and this follows from a repeated application of the inequality in the case of two factors.

Corollary 1.4.13. *For any $n \in \mathbb{Z}$ and $x, y \in \overline{\mathbb{Q}}$*

$$h(nx) \leq h(x) + \log |n|_\infty \tag{1.1}$$
$$h(x+y) \leq h(x) + h(y) + \log 2 \tag{1.2}$$
$$h(x^n) = |n|_\infty h(x) \tag{1.3}$$
$$h(x \cdot y) \leq h(x) + h(y). \tag{1.4}$$

Here $|\cdot|_\infty$ refers to the normal absolute value on $\mathbb{Z}$.

Proof. Let K be a number field such that $x, y \in K$. We first proof the fourth inequality:

$$h(x \cdot y) = h([x \cdot y : 1]) = h([x \cdot y : 1 \cdot 1]) \overset{1.4.10}{\leq} h([x : 1]) + h([y : 1]) = h(x) + h(y)$$

Let $n \in \mathbb{Z}$ be any integer. Then the following holds:

$$h([n : 1]) = \sum_{p \text{ prime}} \log \max\{|n|_{\nu_p}, 1\} + \log \max\{|n|_\infty, 1\} = \log \max\{|n|_\infty, 1\} = \log |n|_\infty$$

Here ν_p denotes the place in $\mathbb{Q}$ associated to the prime number p. Therefore if $y = n$

$$h(nx) \leq h(x) + \log |n|_\infty.$$

This proves the first inequality.
The proof of the second inequality also works analogously to Lemma 1.4.10. It holds that

$$\begin{aligned}
h(x+y) &= h([x+y : 1]) \\
&= \frac{1}{[K : \mathbb{Q}]} \left(\sum_{\nu \in M_K^0} d_\nu \log \max\{|x+y|_\nu, 1\} + \sum_{\nu \in M_K^\infty} d_\nu \log \max\{|x+y|_\nu, 1\} \right) \\
&\leq \frac{1}{[K : \mathbb{Q}]} \left(\sum_{\nu \in M_K^0} d_\nu \log \max\{|x|_\nu |y|_\nu, 1\} + \sum_{\nu \in M_K^\infty} d_\nu \log \left(2 \max\{|x|_\nu, |y|_\nu, 1\}\right) \right) \\
&\leq \frac{1}{[K : \mathbb{Q}]} \sum_{\nu \in M_K} d_\nu \log \left(\max\{|x|_\nu, 1\} \max\{|y|_\nu, 1\}\right) + \log 2 \\
&= h([x : 1]) + h([y : 1]) + \log 2 \\
&= h(x) + h(y) + \log 2.
\end{aligned}$$

The " $\leq$ "-inequality of the third equality follows from a successive application of the fourth inequality. To see that even equality holds one proceeds as in the proof of the second inequality in Lemma 1.4.10 but uses that for any absolute value $|\cdot|$

$$\max\{|x^n|, 1\} = \max\{|x|^n, 1\} = (\max\{|x|, 1\})^n = (\max\{|x|, 1\})^{|n|}$$

holds if $n \geq 0$. If $n < 0$, one uses

$$\max\{|x^n|, 1\} = \max\{|x|^n, 1\} = |x|^n \max\{|x|^{-n}, 1\} = |x|^n \left(\max\{|x|^{-1}, 1\}\right)^{|n|_\infty}.$$

The product formula Lemma 1.4.4 now implies that

$$h(x^n) = |n|_\infty h(x) + n \sum_{\nu \in M_K} d_\nu \log |x|_\nu = |n|_\infty h(x) + 0 = |n|_\infty h(x).$$

□

Proposition 1.4.14. *Let $[x_0 : \ldots : x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$ for some choice of coordinates. Let h be the height function associated to that choice of coordinates. Assume that $x_0 \neq 0$. Then*

$$h([x_0 : \ldots : x_n]) \leq \sum_{i=1}^{n} h([x_0 : x_i]) \leq n h([x_0 : \ldots : x_n]).$$

Proof. If $x_0 \neq 0$ one has

$$h([x_0 : \ldots : x_n]) = h\left(\left[1 : \frac{x_1}{x_0} : \ldots : \frac{x_n}{x_0}\right]\right)$$
$$h([x_0 : x_i]) = h\left([1 : \frac{x_i}{x_0}]\right) \qquad 1 \leq i \leq n.$$

Let K be a number field containing $x_0, \ldots, x_n$ and $|\cdot|$ any absolute value on this number field. Then

$$\max_{1\leq i\leq n} \left\{\left|\frac{x_i}{x_0}\right|, |1|\right\} = \max_{1\leq i\leq n} \left\{\left|\frac{x_i}{x_0}\right|, 1\right\} \leq \prod_{i=1}^{n} \max\left\{\left|\frac{x_i}{x_0}\right|, 1\right\}.$$

This implies the first inequality.
For any $1 \leq i \leq n$ and any absolute value $|\cdot|$ on K one has

$$\max\{|x_0|, |x_i|\} \leq \max_{0\leq j\leq n} \{|x_j|\}.$$

Therefore

$$h([x_0 : x_i]) \leq h([x_0 : \ldots : x_n])$$

for any $1 \leq i \leq n$ and

$$\sum_{i=1}^{n} h([x_0 : x_i]) \leq n h([x_0 : \ldots : x_n]).$$

□

Proposition 1.4.15. *Let $[1 : x_1 : \ldots : x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$ and $[1 : y_1 : \ldots : y_m] \in \mathbb{P}^m(\overline{\mathbb{Q}})$ for some choice of coordinates. Then*

$$h([1:x_1:\ldots:x_n:1:y_1:\ldots:y_m]) \leq h([1:x_1:\ldots:x_n]) + h([1:y_1:\ldots:y_m])$$
$$h([1:x_1:\ldots:x_n]) + h([1:y_1:\ldots:y_m]) \leq 2h([1:x_1:\ldots:x_n:1:y_1:\ldots:y_m]).$$

Proof. This works analogously to Proposition 1.4.14. Let K be a number field containing $x_1, \ldots, x_n, y_1, \ldots, y_m$ and let $|\cdot|$ be any absolute value on this number field. Then

$$\max_{\substack{1\leq i\leq n\\1\leq j\leq m}} \{|x_i|, |y_j|, |1|\} = \max_{\substack{1\leq i\leq n\\1\leq j\leq m}} \{|x_i|, |y_j|, 1\} \leq \max_{1\leq i\leq n} \{|x_i|, 1\} \max_{1\leq j\leq m} \{|y_j|, 1\}.$$

This implies the first inequality.
The second follows since

$$h([1 : x_1 : \ldots : x_n]) \leq h([1 : x_1 : \ldots : x_n : 1 : y_1 : \ldots : y_m])$$
$$h([1 : y_1 : \ldots : y_m]) \leq h([1 : x_1 : \ldots : x_n : 1 : y_1 : \ldots : y_m])$$

analogously to Proposition 1.4.14. □

1.4.3 Heights on varieties

Let X be an irreducible projective variety over $\overline{\mathbb{Q}}$.

Definition 1.4.16 ([HS00], Definition p.183)**.** Let $\phi : X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}$ be a morphism. The *(absolute logarithmic) height of X relative to ϕ* is defined as

$$\begin{aligned} h_\phi : X(\overline{\mathbb{Q}}) &\to [0, \infty) \\ P &\mapsto h(\phi(P)). \end{aligned}$$

Here $h : \mathbb{P}^n(\overline{\mathbb{Q}}) \to [0, \infty)$ is the absolute height on the projective space $\mathbb{P}^n(\overline{\mathbb{Q}})$.

Proposition 1.4.17 ([HS00], Theorem B.2.5)**.** *Let $\phi : \mathbb{P}^n_{\overline{\mathbb{Q}}} \to \mathbb{P}^m_{\overline{\mathbb{Q}}}$ be a rational map, which is given locally on some open set by the homogeneous degree $d \in \mathbb{N}$ polynomials $\phi_0, \dots, \phi_m$. Then for all $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ such that not all ϕ_i vanish in P*

$$h(\phi(P)) \leq dh(P) + O(1).$$

Here $O(1)$ is a bounded function only dependent on n, d and ϕ.
If P is an element in a subvariety $X \subset \mathbb{P}^n_{\overline{\mathbb{Q}}}$ and the ϕ_i vanish nowhere simultaneously on X one has

$$h(\phi(P)) = dh(P) + O(1).$$

In this case $O(1)$ depends again on n, d and ϕ but also on the subvariety X.

Theorem 1.4.18 ([HS00], Theorem B.3.1)**.** *Let $\phi : X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}$, $\psi : X \to \mathbb{P}^m_{\overline{\mathbb{Q}}}$ be morphisms associated to the same Divisor on X. Then*

$$h_\phi(P) = h_\psi(P) + O(1) \qquad \forall P \in X(\overline{\mathbb{Q}})$$

$O(1)$ is independent of P but depends on ϕ and ψ.

This now enables constructing the following families of heights defined up to bounded functions on projective varieties.

Theorem 1.4.19 ('Height Machine (Weil)', [HS00], Theorem B.3.2)**.** *Let X be a smooth variety defined over a number field K. Then there exists*

$$\begin{aligned} h_X : \mathrm{Div}(X) &\to \{\text{functions } X(\overline{\mathbb{Q}}) \to \mathbb{R}\} \\ D &\mapsto h_{X,D} \end{aligned}$$

such that

a) (Normalisation) For H the divisor associated to a hyperplane in $\mathbb{P}^n(\overline{\mathbb{Q}})$ and $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ one has

$$h_{\mathbb{P}^n,H}(P) = h_{\mathbb{P}^n}(P) + O(1) \qquad P \in \mathbb{P}^n(\overline{\mathbb{Q}}).$$

b) (Functoriality) For a morphism $f : X \to Y$ of smooth K-varieties and $D \in \mathrm{Div}(Y)$ one has

$$h_{X,\phi^*D}(P) = h_{Y,D}(\phi(P)) \qquad \forall P \in X(\overline{\mathbb{Q}}).$$

c) (Additivity) For $D, E \in \mathrm{Div}(X)$

$$h_{X,D+E}(P) = h_{X,D}(P) + h_{X,E}(P) + O(1) \qquad \forall P \in X(\overline{\mathbb{Q}}).$$

d) (Linear equivalence) For $D, E \in \mathrm{Div}(X)$ such that D and E are linearly equivalent

$$h_{X,D}(P) = h_{X,E}(P) + O(1) \qquad \forall P \in X(\overline{\mathbb{Q}}).$$

e) (Positivity) For $D \in \mathrm{Div(X)}$ effective and B the base locus of $|D|$

$$h_{X,D}(P) \geq O(1) \qquad \forall P \in (X \setminus B)(\overline{\mathbb{Q}}).$$

f) (Uniqueness) A height function $h_{X,D}$ is up to $O(1)$ determined by normalization, functoriality for embeddings and additivity.

The idea behind proving this theorem is the following. If a divisor $D \in \mathrm{Div}(X)$ is basepoint free (or alternatively very ample), then D defines a morphism $\phi_D : X \to \mathbb{P}^n$. In this case the height that the height machine associates to the divisor D is defined as the height h_{ϕ_D} relative to the map ϕ_D. Any divisor E on a projective variety can be written as the difference of two basepoint free divisors. The height associated to E will be defined as the difference of the heights associated to two such basepoint free divisors. Now Proposition 1.4.17 and Theorem 1.4.18 can be used to check that the construction is well defined and that it has the desired properties. Since there is a choice to be made in the divisors used for the definition as well as in the coordinates chosen for an embedding associated to a basepoint free divisor, this definition will only determine h_X up to bounded functions.
The details of the proof can be found in [HS00] (Theorem B.3.2).

Remark 1.4.20. If it is clear from the context to which variety X the Theorem 1.4.19 is applied to, the notation $h_{X,D}$ for a given divisor $D \in \mathrm{Div}(X)$ is shortened to h_D.

Remark 1.4.21 ([HS00], compare Theorem B.3.6)**.** Using the uniqueness property in the preceding theorem induces a function

$$\begin{aligned} h_X : \mathrm{Div}(X) &\to \{\text{functions } X(\overline{\mathbb{Q}}) \to \mathbb{R}\}/\{\text{bounded functions}\} \\ D &\mapsto h_{X,D} \end{aligned}$$

uniquely determined by the analogous properties of normalisation, functoriality and additivity.
The linear equivalence property implies that this function is constant on divisor classes so Theorem 1.4.19 also induces a function

$$\begin{aligned} \mathrm{Cl}(X) &\to \{\text{functions } X(\overline{\mathbb{Q}}) \to \mathbb{R}\}/\{\text{bounded functions}\} \\ [D] &\mapsto h_{X,D} \end{aligned}$$

uniquely determined by the analogous formulations of normalisation, functoriality and additivity.

Remark 1.4.22. The functions $O(1)$ appearing in the height machine depend on the variety, the divisor and the morphism, but are independent of the choice of points in the variety. Therefore the second point in the height machine can be phrased in the following way. Let ϕ, X, Y and D be as in point (b) of Theorem 1.4.19. Then there exists some constant $C := C(f, X, Y, D) \in \mathbb{R}_{\geq 0}$ such that for any $P \in X(\overline{\mathbb{Q}})$

$$|h_{X,\phi^* D}(P) - h_{Y,D}(\phi(P))| \leq C.$$

Remark 1.4.23. In the following text sometimes the notation

$$h \sim h'$$

used in [SC79] will be used to denote two height function h and h' which only differ by some bounded function $O(1)$.

Corollary 1.4.24 ([HS00], compare Theorem B.3.6)**.** *Let X be a smooth variety over a number field K. Then there exists*

$$\begin{aligned} h_X : \mathrm{Cl}(X) &\to \{\textit{functions } X(\overline{\mathbb{Q}}) \to \mathbb{R}\}/O(1) \\ D &\mapsto h_{X,D}. \end{aligned}$$

Lemma 1.4.25 ([SC79], Lemme 3)**.** *Let X be an irreducible projective variety and ϕ and ψ morphisms*

$$\phi : X \to \mathbb{P}^N \qquad\qquad \psi : X \to \mathbb{P}^M,$$

such that ϕ is a closed immersion. Then

$$h_\psi \leq C_1 + C_2 h_\phi$$

for some $C_1,\ C_2 \in \mathbb{R}$ and $C_1 \neq 0$.

Proof. Since ϕ^{-1} exists as a rational map and $\phi(X)$ is a variety one has the following morphism of varieties

$$\psi \circ \phi^{-1} : \phi(X) \subset \mathbb{P}^N \to \mathbb{P}^M.$$

This is locally given by polynomials. The Weil height on $\phi(X)$ viewed as subvariety of the projective space is the height h_ϕ on X. One has that if in a neighbourhood of $x \in X(\overline{\mathbb{Q}})$ the rational map $\psi \circ \phi^{-1}$ is given by a family of homogeneous polynomials F of the same degree, then

$$h_\psi(x) = h_{\phi(X)}((\psi \circ \phi^{-1})(x)) \leq \deg(F) h_\phi(x) + O(1).$$

Since the variety $\phi(X)$ is quasi-compact a finite subset of such neighbourhoods cover $\phi(X)$. If one takes the maximum of $\deg F$ and bounds C for the absolute value of $O(1)$ associated to these open neighbourhoods, one gets the constants C_1 and C_2 respectively. With this the claim follows. □

Corollary 1.4.26. *Let X be an irreducible projective variety defined over $\overline{\mathbb{Q}}$, D a divisor on X which is linearly equivalent to a basepoint-free one and E a divisor on X linear equivalent to a very ample one. Then there are λ, μ such that for any $x \in X$*

$$h_D(x) \leq \mu h_E(x) + \lambda.$$

Proof. If D is a basepoint free divisor, its associated height is the same as the height h_{ϕ_D} of one of its associated maps into projective space. So the claim holds if D is basepoint free and E is very ample by the preceding Lemma 1.4.25. In the general case let $D' \sim D$ be basepoint free and $E' \sim E$ be very ample and the statement holds with constants λ' and μ'. The fourth point of Theorem 1.4.19 implies that there are constants $C_1,\ C_2$ such that for any $x \in X(\overline{\mathbb{Q}})$

$$h_D(x) \leq h_{D'}(x) + C_1 \qquad\qquad h_{E'}(x) \leq h_E(x) + C_2.$$

Hence

$$\begin{aligned} h_D(x) &\leq h_{D'}(x) + C_1 \leq \mu' h_{E'}(x) + \lambda' + C_1 \\ &\leq \mu' h_E(x) + \mu' C_2 + \lambda' + C_1 \\ &=: \mu h_E(x) + \lambda \end{aligned}$$

with $\mu := \mu'$ and $\lambda := \mu' C_2 + \lambda' + C_1$. □

1.4.4 Heights on abelian varieties

Heights on abelian varieties have the additional property that they are (up to some bounded function depending on the variety and divisor) quadratic with respect to the group law. This is section B.3 and B.4 in [HS00].

Proposition 1.4.27 ([HS00], Corollary B.3.4 (a))**.** *For an abelian variety A defined over K and a divisor $D \in \mathrm{Div}(A)$ the following formula holds for all $P \in A(\overline{\mathbb{Q}})$ and $m \in \mathbb{Z}$*

$$h_{A,D}([m]_A P) = \frac{m^2+m}{2} h_{A,D}(P) + \frac{m^2-m}{2} h_{A,D}([-1]P) + O(1).$$

The proof uses the law of the cube, which is Lemma 1.3.16.

For a divisor D whose divisor class is symmetric (as in Definition 1.3.15) the formula of the proposition simplifies to

$$h_{A,D}([m]P) = m^2 h_{A,D}(P) + O(1).$$

Here $O(1)$ depends on A, D and m. Furthermore the height fulfills the parallelogram equality for all $P, Q \in A(\overline{\mathbb{Q}})$ up to some bounded function dependent on D, A and the group law on A

$$h_{A,D}(P+Q) + h_{A,D}(P-Q) = 2h_{A,D}(P) + 2h_{A,D}(Q) + O(1).$$

So the height relative to a symmetric divisor is a quadratic form up to some bounded function.

For antisymmetric divisors something similar happens,

$$h_{A,D}([m]P) = m h_{A,D}(P) + O(1)$$

with $O(1)$ dependent on A, D and m. Here the height can be viewed as linear up to some bounded function. For all $P, Q \in A(\overline{K})$

$$h_{A,D}(P+Q) = h_{A,D}(P) + h_{A,D}(Q) + O(1)$$

with $O(1)$ again dependent on D, A and the group law on A.

This allows one to construct a canonical height with respect to a multiplication morphism for symmetric and antisymmetric divisors respectively. The construction works analogously to the construction of a Néron-Tate height on a variety relative to a divisor and a function (compare to [HS00], Theorem B.4.1). But it turns out that the resulting height is independent of the choice of m for the multiplication.

Theorem 1.4.28 ('Néron, Tate', [HS00], Theorem 5.1)**.** *Let A be an abelian variety defined over a number field K and $D \in \mathrm{Div}(A)$ a divisor of symmetric divisor class. Then there exists a unique height function which only depends on the divisor class of D*

$$\hat{h}_{A,D} : A(\overline{\mathbb{Q}}) \to \mathbb{R}$$

such that $\hat{h}_{A,D}$ is a quadratic form, i.e.

a) $\hat{h}_{A,D} = h_{A,D} + O(1)$

b) $\hat{h}_{A,D} \circ [m] = m^2 \hat{h}_{A,D}$

c) $\hat{h}_{A,D}(P+Q) + \hat{h}_{A,D}(P-Q) = 2\hat{h}_{A,D}(P) + 2\hat{h}_{A,D}(Q) \qquad \forall P, Q \in A(\overline{\mathbb{Q}})$.

For an antisymmetric divisor the analogous construction gives the following theorem.

Theorem 1.4.29 ([HS00], Theorem 5.5)**.** *Let A be an abelian variety defined over a number field K and $D \in \mathrm{Div}(A)$ a divisor of antisymmetric divisor class. Then there exists a unique height function only dependent on the divisor class of D*

$$\hat{h}_{A,D} : A(\overline{\mathbb{Q}}) \to \mathbb{R}$$

such that $\hat{h}_{A,D}$ is a linear form, i.e.

1. $\hat{h}_{A,D} = h_{A,D} + O(1)$

2. $\hat{h}_{A,D}(P+Q) = \hat{h}_{A,D}(P) + \hat{h}_{A,D}(Q) \qquad \forall P, Q \in A(\overline{\mathbb{Q}})$.

Splitting an arbitrary divisor into its symmetric and antisymmetric parts allows one to construct a canonical height for that divisor, which has a unique linear and quadratic part. This leads to the following generalisation of the previously constructed heights for symmetric and antisymmetric divisors respectively.

Lemma 1.4.30 ([HS00], Theorem B.5.6)**.** *Let A be an abelian variety defined over a number field K and $D \in \mathrm{Div}(A)$ a divisor. For any divisor class associated to such a D there exists a unique height function*

$$\hat{h}_{A,D} : A(\overline{\mathbb{Q}}) \to \mathbb{R}$$

such that $\hat{h}_{A,D}$ agrees with the canonical height constructed in the previous theorems if D is a symmetric or antisymmetric divisor and

a) For any $D \in \mathrm{Div}(A)$: $\hat{h}_{A,D}(0) = 0$

b) For any $D,\ E \in \mathrm{Div}(A)$: $\hat{h}_{A,D+E} = \hat{h}_{A,D} + \hat{h}_{A,E}$

c) For any $D \in \mathrm{Div}(A)$ there is a unique quadratic form q_D and a unique linear form l_D such that

$$\hat{h}_{A,D} = q_D + l_D$$

which can be obtained by the height functions

$$q_D = \frac{1}{2}\hat{h}_{A,D+[-1]^*D} \qquad\qquad l_D = \frac{1}{2}\hat{h}_{A,D-[-1]^*D}.$$

A consequence of this lemma is that up to something bounded, every logarithmic height on an abelian variety is quadratic with respect to the group law.

Corollary 1.4.31. *Let A be an abelian variety defined over a number field K and $D \in \mathrm{Div}(A)$ a divisor. Let the height associated to D be $h_{A,D}$ and let $\hat{h}_{A,D}$ be the canonical height associated with D as in the previous lemma. Then*

$$h_{A,D} = \hat{h}_{A,D} + O(1).$$

In particular any height on an abelian variety associated to a divisor behaves up to some bounded function quadratic with respect to the group law.

Proof. Let $D \in \mathrm{Div}(A)$ be a divisor. Then

$$2D \sim (D + [-1]^* D) + (D - [-1]^* D) \tag{1.5}$$

is a decomposition of $2D$ into a symmetric and an antisymmetric divisor. This leads to

$$\begin{aligned}
2h_{A,D} &\overset{1.4.19\,(3)}{=} h_{A,D+D} + O(1) \\
&= h_{A,2D} + O(1) \\
&\overset{(1.5)}{=} h_{A,(D+[-1]^*D)+(D-[-1]^*D)} + O(1) \\
&\overset{1.4.19\,(c)}{=} h_{A,D+[-1]^*D} + h_{A,D-[-1]^*D} + O(1) \\
&= \hat{h}_{A,D+[-1]^*D} + \hat{h}_{A,D-[-1]^*D} + O(1) \\
&= 2\left(\frac{1}{2}\hat{h}_{A,D+[-1]^*D} + \frac{1}{2}\hat{h}_{A,D-[-1]^*D}\right) + O(1) \\
&\overset{1.4.30}{=} 2\hat{h}_{A,D} + O(1).
\end{aligned}$$

Therefore

$$h_{A,D} = \hat{h}_{A,D} + O(1).$$

□

1.4.5 Heights on polynomials

Definition 1.4.32 ([HS00], section B.7 on p.224 and Remark B.7.0 on p.225)**.** Let K be a number field, ν an absolute value on K and $f = \sum a_\alpha X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in K[X_1, \ldots, X_n]$ a polynomial. The *Gauss norm* of f is defined as

$$|f|_\nu = \max_\alpha |a_\alpha|_\nu.$$

The *logarithmic height* of the polynomial is defined as

$$h(f) = \frac{1}{[K : \mathbb{Q}]} \sum_{\nu \in M_K} d_\nu \log |f|_\nu.$$

Remark 1.4.33. This is the same as the height of the coefficients of f taken as a projective point and thus also independent of the choice of field of definition K. This follows again from the product formula in Lemma 1.4.4.
Therefore two polynomials which only differ by a scalar in K have the same height.

Proposition 1.4.34 ('Gelfand's inequality', [HS00], Proposition B.7.3)**.** *Let there be integers $d_1, \ldots, d_m \in \mathbb{N}_{\geq 1}$ and algebraic polynomials $f_1, \ldots, f_r \in \overline{\mathbb{Q}}[X_1, \ldots, X_m]$ such that $\deg_{X_i}(f_1, \ldots f_r) \leq d_i$ for any $i \in \{1, \ldots, m\}$, then*

$$\sum_{i=1}^{r} h(f_i) \leq h(f_1 \cdots f_r) + d_1 + \ldots + d_m.$$

Proposition 1.4.35 (compare [HS00] Proposition B.7.3 (a))**.** *Let there be polynomials $f_1, \ldots, f_r \in \overline{\mathbb{Q}}[X_1, \ldots, X_m]$ and $d_1, \ldots, d_m \in \mathbb{N}_{\geq 1}$ such that $\deg_{X_i}(f_1, \ldots f_r) \leq d_i$ for any $i \in \{1, \ldots, m\}$, then*

$$h(f_1 \cdots f_r) \leq \sum_{i=1}^{r} \left(h(f_i) + (\deg f_i + m) \log 2 \right).$$

Proof. We proceed analogously to the proof of Proposition B.7.3 (a) in [HS00] and only change the definition of the height of a polynomial.

Each coefficient of $f_1 \cdots f_r$ is a sum of a products $a_1 \cdots a_r$ where a_i is a coefficient of f_i. The number of non-zero summands for the coefficient of a monomial $X_1^{E_1} \cdots X_m^{E_m}$ for $E_1 + \ldots + E_m = \deg(f_1 \cdots f_r)$ is at most

$$\prod_{i=1}^{m} \binom{E_i + r - 1}{r - 1}.$$

This holds since the number of r-partitions of E_i is $\binom{E_i+r-1}{r-1}$. We want to estimate this product. For this we use the following claim.

Claim. *Let $n, m \in \mathbb{N}_0$ and $n \geq m$. Then*

$$\binom{n}{m} \leq 2^n. \tag{1.6}$$

Proof. One shows that $\sum_{m=0}^{n} \binom{n}{m} = 2^n$. This follows by induction on n.
$\mathbf{n = 0}$:

$$\sum_{m=0}^{0} \binom{0}{m} = \binom{0}{0} = 1 = 2^0$$

$\mathbf{n \geq 1}$: Assume the claim holds for a given $n \geq 0$.

$$\begin{aligned}
\sum_{m=0}^{n+1} \binom{n+1}{m} &= \binom{n+1}{0} + \sum_{m=1}^{n} \binom{n+1}{m} + \binom{n+1}{n+1} \\
&= 1 + \sum_{m=1}^{n} \left(\binom{n}{m-1} + \binom{n}{m} \right) + 1 \\
&= \binom{n}{0} + \sum_{m=1}^{n} \binom{n}{m} + \sum_{m=0}^{n-1} \binom{n}{m} + \binom{n}{n} \\
&= 2 \sum_{m=0}^{n} \binom{n}{m} \\
&\overset{IH}{=} 2 \cdot 2^n \\
&= 2^{n+1}
\end{aligned}$$

□

Therefore

$$\prod_{i=1}^{m} \binom{E_i + r - 1}{r-1} \leq \prod_{i=1}^{m} 2^{E_i + r - 1} = 2^{\sum_{i=1}^{r} E_i + m(r-1)} = 2^{\deg(f_1 \cdots f_r) + m(r-1)}$$

Using Remark 1.4.33 we can view the polynomials as projective points and apply the two inequalities of Lemma 1.4.10 to pullout the sums and products of coefficients of the f_i. This leads to

$$\begin{aligned}
h(f_1 \cdots f_r) &\leq \sum_{i=1}^{r} h(f_i) + \log \left(\prod_{i=1}^{m} \binom{E_i + r - 1}{r-1} \right) \\
&\leq \sum_{i=1}^{r} h(f_i) + \log 2^{\deg(f_1 \cdots f_r) + m(r-1)} \\
&= \sum_{i=1}^{r} h(f_i) + (\deg(f_1 \cdots f_r) + m(r-1)) \log 2 \\
&= \sum_{i=1}^{r} h(f_i) + \left(\sum_{i=1}^{r} (\deg(f_i) + m) \right) \log 2 \\
&= \sum_{i=1}^{r} (h(f_i) + (\deg(f_i) + m) \log 2) .
\end{aligned}$$

□

Chapter 2

Heights and height estimates on commutative connected algebraic groups

Let G be a commutative connected algebraic group. To obtain heights on G one could try to use the height machine. But G is in general not a complete variety, therefore the theorem is not applicable. The following sections will construct a completion $\overline{G}$ of G and divisors on this completion.

2.1 Completion of a connected commutative algebraic group

2.1.1 The completion of L

In this section let L be an affine algebraic group defined over some number field K. Assume without loss of generality that

$$L \cong \mathbb{G}_a^{l_a} \times \mathbb{G}_m^{l_m}$$

for some $l_a, l_m \in \mathbb{N}_0$ over K. This can be done because of Theorem 1.3.36. The goal of this section is to find a projective variety $\overline{L}$ which is a completion of L, that is $L \subset \overline{L}$ is dense. The construction done here is the same as in [SC79] section 1.2.

Proposition 2.1.1 ([SC79], 1.2)**.** *The variety $\overline{L} := (\mathbb{P}^1)^{l_a+l_m}$ is a completion of L. This is a smooth and connected variety.*

Proof. The projective line $\mathbb{P}^1$ is a completion of $\mathbb{G}_a$ and $\mathbb{G}_m$ by the inclusion

$$\begin{aligned} \mathbb{A}^1 &\to \mathbb{P}^1 \\ x &\mapsto [x : 1] \end{aligned}$$

Since L is isomorphic to a product of copies of $\mathbb{G}_a$ and $\mathbb{G}_m$ the statement follows. The projective line $\mathbb{P}^1$ is smooth and connected, therefore so is $\overline{L}$. □

The completion of $\mathbb{G}_a$ and $\mathbb{G}_m$ as the projective space $\mathbb{P}^1$ will be denoted by $\overline{\mathbb{G}}_a$ and $\overline{\mathbb{G}}_m$ respectively.

Proposition 2.1.2. *The variety $\overline{L}$ has an L-action which agrees with the group law on L.*

Proof. Since L and $\overline{L}$ are products this can be proved by checking the statement for each factor $\mathbb{G}_a \subset \mathbb{P}^1$ and $\mathbb{G}_m \subset \mathbb{P}^1$. In the additive case there is the addition map

$$\begin{aligned} \mathbb{G}_a \times \mathbb{G}_a &\to \mathbb{G}_a \\ ([x : 1], [y : 1]) &\mapsto [x + y : 1]. \end{aligned}$$

By rewriting this, one sees that the map can be regularly continued to $\mathbb{G}_a \times \mathbb{P}^1$ as

$$\begin{aligned} \mathbb{G}_a \times \mathbb{P}^1 &\to \mathbb{P}^1 \\ ([x : 1], [y_0 : y_1]) &\mapsto [xy_1 + y_0 : y_1]. \end{aligned}$$

In the multiplicative case the group law is given as

$$\begin{aligned} \mathbb{G}_m \times \mathbb{G}_m &\to \mathbb{G}_m \\ ([x : 1], [y : 1]) &\mapsto [xy : 1]. \end{aligned}$$

which has a continuation to $\mathbb{G}_m \times \mathbb{P}^1$ by

$$\begin{aligned} \mathbb{G}_m \times \mathbb{P}^1 &\to \mathbb{P}^1 \\ ([x : 1], [y_0 : y_1]) &\mapsto [xy_0 : y_1]. \end{aligned}$$

□

Proposition 2.1.3 ([SC79], Proposition 2)**.** *Let $n \in \mathbb{Z} \setminus \{0\}$. Then the multiplication-by-n-morphism $[n]_L$ on L has a continuation $[n]_{\overline{L}}$ as a morphism on $\overline{L}$.*

Proof. This can again be checked on the level of factors, since the multiplication-by-n-morphism is defined by multiplication-by-n on every factor. On the factors the continuations are

$$\begin{aligned} [n]_{\overline{\mathbb{G}}_a} : \mathbb{P}^1 &\to \mathbb{P}^1 \\ [x_0 : x_1] &\mapsto [nx_0 : x_1] \end{aligned}$$

and

$$\begin{aligned} [n]_{\overline{\mathbb{G}}_m} &: \mathbb{P}^1 \to \mathbb{P}^1 \\ [x_0 : x_1] &\mapsto \begin{cases} [x_0^n : x_1^n] & n \geq 0 \\ [x_0^{-n} : x_1^{-n}] & n < 0. \end{cases} \end{aligned}.$$

Therefore a continuation on $\overline{L}$ exists. □

For $1 \leq i \leq l_a + l_m$ let pr_i denote the projection of $\overline{L}$ to its i-th factor. These projection maps are compatible with the L-action on $\overline{L}$ in the sense that for $l \in L$ and $x \in \overline{L}$

$$\mathrm{pr}_i(l \cdot x) = \mathrm{pr}_i(l) \cdot \mathrm{pr}_i(x).$$

On the left hand side one has L operating on $\overline{L}$ and on the right hand side $\mathbb{G}_a$ or $\mathbb{G}_m$ acting on $\mathbb{P}^1$ as in the proof of Proposition 2.1.2. Define divisors

$$L'_a = [1:0], \qquad\qquad L'_m = [0:1] + [1:0]$$

in $\mathbb{P}^1$. They are the divisors associated to the subvarieties $\mathbb{P}^1 \setminus \mathbb{G}_a$ and $\mathbb{P}^1 \setminus \mathbb{G}_m$ respectively. Then the subvarieties

$$L_i := \begin{cases} \mathrm{pr}_i^{-1}(L'_a) & 1 \leq i \leq l_a \\ \mathrm{pr}_i^{-1}(L'_m) & l_a < i \leq l_a + l_m \end{cases}$$

are divisors in $\overline{L}$. Define the divisor L_∞ as

$$L_\infty := \bigcup_{i=1}^{l_a+l_m} L_i.$$

By definition, the divisor L_∞ agrees with the closed subvariety $\overline{L} \setminus L$ of $\overline{L}$.

Lemma 2.1.4. *The divisor L_∞ is invariant under the action of L on $\overline{L}$ and a very ample divisor.*

Proof. To prove the first point one shows that any divisor L_i is invariant under the action of L. But for this it suffices to show that the divisors L'_a and L'_m are invariant under the action of $\mathbb{G}_a$ and $\mathbb{G}_m$ respectively, since the projections are compatible with the group action of L. We get the orbits

$$\{[x \cdot 0 + 1 : 0 \cdot 1] |\ x \in \mathbb{G}_a\} = \{[1:0]\} = L'_a$$

for L'_a and

$$\begin{aligned} \{[x \cdot 0 : 1] |\ x \in \mathbb{G}_m\} &= \{[0:1]\}, \\ \{[x \cdot 1 : 0] |\ x \in \mathbb{G}_m\} &= \{[1:0]\} \end{aligned}$$

for the elements of L'_m and thus the L'_m are $\mathbb{G}_m$-invariant. So all L_i are L-invariant and therefore L_∞ is L-invariant.
To prove the second part of the statement, one constructs the embedding into projective space associated to the divisor. For a component $\overline{\mathbb{G}}_a \cong \mathbb{P}^1$ the corresponding divisor L_a limited to this component is by construction just the divisor associated to the point $[1:0]$. The map associated to this divisor is the identity map on $\mathbb{P}^1$

$$\begin{aligned}\xi_a : \overline{\mathbb{G}}_a &\to \mathbb{P}^1,\\ [x_0 : x_1] &\mapsto [x_0 : x_1].\end{aligned}$$

For a component $\overline{\mathbb{G}}_m \cong \mathbb{P}^1$ the corresponding divisor L_m on this component is the sum of points $[1:0]$ and $[0:1]$. This divisor has the associated linear system $L(D) = \langle 1, \frac{x_0}{x_1}, \frac{x_1}{x_0}\rangle_K$ if x_0, x_1 are the coordinates on $\mathbb{P}^1$. It is therefore associated to the following embedding:

$$\begin{aligned}\xi_m : \overline{\mathbb{G}}_m &\to \mathbb{P}^2\\ [x_0 : x_1] &\mapsto [x_0x_1 : x_0^2 : x_1^2].\end{aligned}$$

Composing ξ_a and ξ_m with the Segre-embedding sufficiently often gives an embedding ϕ of $\overline{L}$ into $\mathbb{P}^{2^{l_a}3^{l_m}-1}$. If this space has coordinates $z_0, \ldots, z_{2^{l_a}3^{l_m}}$ the divisor L_∞ is the pullback of the hyperplane $\{z_0 = 0\}$:

$$\begin{aligned}\phi^*(\{z_0 = 0\}) &= \{x_0^{(1)} \cdots x_0^{(l_a)} x_0^{(l_a+1)} x_1^{(l_a+1)} \cdots x_0^{(l_a+l_m+1)} x_1^{(l_a+l_m+1)} = 0\},\\ &= \bigcup_{i=1}^{l_a+l_m} \{x_0^{(i)} = 0\} \cup \bigcup_{i=1}^{l_m} \{x_1^{(l_a+i)} = 0\} \subset \left(\mathbb{P}^1\right)^{l_a+l_m}.\end{aligned}$$

Here $x_0^{(i)}$ and $x_1^{(i)}$ for $1 \le i \le l_a + l_m$ denote the x_0 and x_1 coordinate of the i-th factor of $\overline{L}$. Hence the divisor L_∞ is very ample. □

2.1.2 Constructing an associated bundle

The following statements are a slightly more detailed version of section 2 'Gefaserte Objekte' in [Wüs84] and subsection 1.3 in [SC79].

Lemma 2.1.5 ([Ros56], Theorem 10)**.** *Let G be an algebraic group and*

$$0 \to L \xrightarrow{i} G \xrightarrow{p} A \to 0$$

the decomposition as in Theorem 1.3.41. Then there exists a rational section s of p. If G is defined over a field $K \subset \overline{\mathbb{Q}}$, then s is also defined over K.

Proof. The Theorem 10 in the paper [Ros56] by Rosenlicht states that such a section exists if

- L is connected and solvable
- L acts on G in such a way that the map $p : G \to A$ is the natural map of L-orbits.

Every commutative group is solvable and since G is connected L is also connected (by Theorem 1.3.41). So the first condition holds. The second point is the restatement of the exact sequence done in Proposition 1.3.48, thus such a section exists.
If G is defined over K, Theorem 1.3.41 states that also L and A as well as i and p are defined over K. With Theorem 1.3.41 this implies that the action of L on G is defined over K as well. Therefore the theorem in [Ros56] implies that the section s is defined over K. □

Lemma 2.1.6. *Let G, A, L, p and i be as in the previous lemma. There exists a covering $U_1, \dots, U_n$ of open subsets of A such that*

$$p^{-1}(U_i) \cong L \times U_i$$

by some L-equivariant morphism such that

$$\begin{array}{ccc} p^{-1}(U_i) & \longrightarrow & L \times U_i \\ & \searrow^{p} & \downarrow{\scriptstyle pr_2} \\ & & U_i \end{array} .$$

Proof. By the previous Lemma 2.1.5 there is some rational section

$$s : A \to G.$$

Let $U \subset A$ be an open subset of A such that $s|_U$ is regular. Then there is an isomorphism

$$\begin{aligned} p^{-1}(U) &\xrightarrow{\sim} p^{-1}(0_A) \times s(U) \\ h &\mapsto (h - s(p(h)), s(p(h))) \end{aligned}$$

with its inverse being the addition on G. On the other hand

$$\begin{aligned} p^{-1}(0_A) \times s(U) &\xrightarrow{\sim} L \times U \\ (g_1, g_2) &\mapsto (i^{-1}(g_1), p(g_2)). \end{aligned}$$

This uses that $i(L) = p^{-1}(0_A)$ and s is a section. This leads to the following isomorphism

$$\begin{aligned} \phi_U : p^{-1}(U) &\xrightarrow{\sim} L \times U \\ h &\mapsto (i^{-1}(h - s(p(h))), p(h)) \\ i(l) + s(u) &\leftarrow\!\shortmid (l, u) \end{aligned}$$

where in the second component it is used that s is a section and therefore $p(s(p(h))) = p(h)$. L acts on both $p^{-1}(U)$ and $L \times U$. On $p^{-1}(U)$ this action is induced by the action of L on G. Consider

$$\begin{aligned} L \times p^{-1}(U) &\to p^{-1}(U) \\ (l, g) &\mapsto i(l) + g. \end{aligned}$$

This is well defined since p is L-invariant. The action on $L \times U$ is the following

$$\begin{aligned} L \times (L \times U) &\to (L \times U) \\ (l', (l, u)) &\mapsto (l + l', u). \end{aligned}$$

The map defined above is equivariant under these L-actions. It also makes the following diagram commute

$$\begin{array}{ccc} p^{-1}(U) & \xrightarrow{\phi_U} & L \times U \\ & \searrow^{p} & \downarrow \mathrm{pr}_2 \\ & & U \end{array} .$$

Let now $a \in U$ be fixed, choose $b \in A$ arbitrary and $g \in p^{-1}(a - b)$. Then

$$s_b := \tau_{-g} \circ s \circ \tau_{a-b}$$

is a rational section of p. Here τ denotes the translation morphism. The section s_b is regular on an open neighbourhood $U_b = \tau_{b-a}(U)$ of b, since for any $a' \in U_b$

$$\begin{aligned} p \circ s_b(a') &= p(s(a' + a - b) - g) \\ &\overset{a' \in U_b}{=} p(s(a' + a - b)) + p(-g) \\ &= a' + a - b - a + b \\ &= a'. \end{aligned}$$

Analogous to the case above one gets an L-equivariant morphism

$$\begin{aligned} \phi_{U_b} : p^{-1}(U_b) &\to L \times U_b \\ h &\mapsto (i^{-1}(h - s_b(p(h))), p(h)) \end{aligned}$$

such that

$$\begin{array}{ccc} p^{-1}(U_b) & \xrightarrow{\phi_{U_b}} & L \times U_b \\ & \searrow^{p} & \downarrow \mathrm{pr}_2 \\ & & U_b \end{array}$$

commutes. Since A is quasi-compact, a finite number of such neighbourhoods U_b cover A. Let them be called $U_1, \dots, U_n$ each with a corresponding section s_i regular on U_i and local trivialisations

$$\phi_i : p^{-1}(U_i) \to L \times U_i.$$

Let $U_i, U_j \in \{U_1, \dots, U_n\}$. The preimage $p^{-1}(U_i \cap U_j)$ can be viewed as a subset of $p^{-1}(U_i)$ as well as $p^{-1}(U_j)$ using the isomorphisms from above. This leads to the following gluing function

$$\begin{aligned} \phi_{i,j} := (\phi_i \circ \phi_j^{-1})|_{(U_i \cap U_j)} : L \times (U_i \cap U_j) &\to L \times (U_i \cap U_j) \\ (l, u) &\mapsto (l + i^{-1}(s_i(u) - s_j(u)), u) \end{aligned}$$

which is also L-equivariant. □

Proposition 2.1.7 ([Wüs84], Beispiel 1 p.179)**.** *Let G, A, L, p and i be as in the previous lemma and let X be an L-space. Then the associated bundle $G \times^L X$ over A exists.*

Proof. Let $\{U_1, \dots, U_n\}$ be a cover of A, which leads to a cover of G as in the previous corollary with transition function

$$\begin{aligned} \phi_{i,j} : L \times (U_i \cap U_j) &\to L \times (U_i \cap U_j) \\ (l, u) &\mapsto (g_{i,j}(u)(l), u) \end{aligned}$$

where each $g_{i,j}(u)$ is an L-equivariant map. Since the $g_{i,j}$ are functions associated to gluing together G from subvarietes they form a cocycle i.e. for any $i, j, k \in \{1, \dots, n\}$

$$g_{i,j} = g_{j,i} \qquad\qquad g_{i,k} = g_{j,k} \circ g_{i,j}.$$

Now one defines W as the variety obtained by gluing patches

$$U_i \times X$$

with the functions

$$\begin{aligned} \psi_{i,j} : (U_i \cap U_j) \times X &\to (U_i \cap U_j) \times X \\ (u, x) &\mapsto (u, g_{i,j}(0_L) \cdot x). \end{aligned}$$

Since the $g_{i,j}$ form a cocycle, the $\psi_{i,j}$ form one as well and the variety W is well defined. Define

$$q : G \times X \to W$$

by defining it locally as

$$\begin{aligned} (U_i \times L) \times X &\to U_i \times X \\ (u, l, x) &\mapsto (u, x) \end{aligned}$$

and

$$p_X : W \to A$$

by defining it locally as

$$\begin{aligned} U_i \times X &\to A \\ (u, x) &\mapsto u. \end{aligned}$$

Since any point (u, l, x) is uniquely determined by (u, x) and (u, l), the diagram

$$\begin{array}{ccc} (U_i \times L) \times X & \xrightarrow{\mathrm{pr}_1 \times \mathrm{pr}_3} & (U_i \times X) \\ \downarrow q & & \downarrow p \\ (U_i \times L) & \xrightarrow{p_X} & U_i \end{array}$$

is cartesian for any open set U_i and therefore

$$\begin{array}{ccc} G \times X & \xrightarrow{\mathrm{pr}_1} & G \\ \downarrow q & & \downarrow p \\ W & \xrightarrow{p_X} & A \end{array}$$

is cartesian. So $W = G \times^L X$ is the associated bundle. □

2.1.3 The completion of an arbitrary commutative connected algebraic group

This subsection is also following [Ser97] subsection 1.3 and [Wüs84] section I.1.3. Let G be a commutative connected algebraic group defined over a number field K with decomposition

$$0 \to L \xrightarrow{i} G \xrightarrow{p} A \to 0$$

by Theorem 1.3.41. Assume without loss of generality that

$$L \cong \mathbb{G}_a^{l_a} \times \mathbb{G}_m^{l_m}$$

with $l_a,\ l_m \in \mathbb{N}_0$ as in Theorem 1.3.36.

Proposition 2.1.8 ([Wüs84], I.1.3, [SC79], 1.3)**.** *Let $\overline{L}$ be as in Proposition 2.1.1. Then there exists a complete variety $\overline{G}$ such that $G \hookrightarrow \overline{G}$ is a dense open subset. Moreover there exists a morphism $\overline{p} : \overline{G} \to A$ which agrees with p on G and whose fibres are isomorphic to $\overline{L}$. The variety $\overline{G}$ is also smooth and connected.*

Proof. Take $\overline{G} := G \times^L \overline{L}$ as in Lemma 2.1.7. To show that the variety $\overline{G}$ is complete one can view it as $\overline{\mathbb{Q}}$-scheme. In this setting $\overline{G}$ is complete if the map

$$\overline{G} \to \mathrm{Spec}(\overline{\mathbb{Q}})$$

is proper. So we can apply the valuative criterion for properness to this map ([Har77], Theorem II.4.7). We already know that $\overline{L}$ and A are complete. Choose affine coverings $U_i = \mathrm{Spec}(B_i)$ of $\overline{L}$ and $V_j = \mathrm{Spec}(C_j)$ of A such that $\overline{G}$ is locally isomorphic to $U_i \times V_j$. Let K' be an arbitrary field and $R \overset{\iota}{\hookrightarrow} K'$ a valuation ring. Let the following diagram

$$\begin{array}{ccc} \mathrm{Spec}(K') & \longrightarrow & \overline{G} \\ \downarrow{\scriptstyle \iota^\sharp} & & \downarrow \\ \mathrm{Spec}(R) & \longrightarrow & \mathrm{Spec}(\overline{\mathbb{Q}}) \end{array} .$$

commute. The image of $\mathrm{Spec}(K')$ lies in some affine patch $U_i \times V_j$ of $\overline{G}$ and can be specified by giving an image of $\mathrm{Spec}(K')$ in $\overline{L}$ and an image of $\mathrm{Spec}(K')$ in A. This leads to the commutative diagrams

$$\begin{array}{ccc} \mathrm{Spec}(K') & \longrightarrow & U_i \\ \downarrow{\scriptstyle \iota^\sharp} & & \downarrow \\ \mathrm{Spec}(R) & \longrightarrow & \mathrm{Spec}(\overline{\mathbb{Q}}) \end{array} \qquad \begin{array}{ccc} \mathrm{Spec}(K') & \longrightarrow & V_j \\ \downarrow{\scriptstyle \iota^\sharp} & & \downarrow \\ \mathrm{Spec}(R) & \longrightarrow & \mathrm{Spec}(\overline{\mathbb{Q}}) \end{array} .$$

The completeness of $\overline{L}$ and A now implies

$$\begin{array}{ccc} \mathrm{Spec}(K') & \longrightarrow & U_i \\ \downarrow{\scriptstyle \iota^\sharp} & \overset{\exists!}{\nearrow} & \downarrow \\ \mathrm{Spec}(R) & \longrightarrow & \mathrm{Spec}(\overline{\mathbb{Q}}) \end{array} \qquad \begin{array}{ccc} \mathrm{Spec}(K') & \longrightarrow & V_j \\ \downarrow{\scriptstyle \iota^\sharp} & \overset{\exists!}{\nearrow} & \downarrow \\ \mathrm{Spec}(R) & \longrightarrow & \mathrm{Spec}(\overline{\mathbb{Q}}) \end{array} . \tag{2.1}$$

Therefore there exists a map $\mathrm{Spec}(R) \to U_i \times V_j$ such that the diagram commutes

$$\begin{array}{ccc} \mathrm{Spec}(K') & \longrightarrow & \overline{G} \\ \downarrow{\scriptstyle \iota^\sharp} & \overset{\exists}{\nearrow} & \downarrow \\ \mathrm{Spec}(R) & \longrightarrow & \mathrm{Spec}(\overline{\mathbb{Q}}) \end{array}$$

and hence $\overline{G}$ is complete.

Assume there was a second map $\phi : \mathrm{Spec} R \to \overline{G}$ making the diagram

$$\begin{array}{ccc} \mathrm{Spec}(K') & \longrightarrow & \overline{G} \\ \downarrow{\scriptstyle \iota^\sharp} & \overset{\phi}{\nearrow} & \downarrow \\ \mathrm{Spec}(R) & \longrightarrow & \mathrm{Spec}(\overline{\mathbb{Q}}) \end{array}$$

commute. Since the $U_a \times V_b$ cover $\overline{G}$, the map ϕ also defines a morphism $\phi : \mathrm{Spec} R \to U_{i'} \times V_{j'}$ for some i', j' such that

$$\begin{array}{ccc} \mathrm{Spec}(K') & \longrightarrow & U_{i'} \times V_{j'} \\ \downarrow{\scriptstyle \iota^\sharp} & \overset{\phi}{\nearrow} & \downarrow \\ \mathrm{Spec}(R) & \longrightarrow & \mathrm{Spec}(\overline{\mathbb{Q}}) \end{array}$$

and ergo

$$\begin{array}{ccc} \mathrm{Spec}(K') & \longrightarrow & U_{i'} \subset \overline{L} \\ \downarrow{\scriptstyle \iota^\sharp} & \nearrow & \downarrow \\ \mathrm{Spec}(R) & \longrightarrow & \mathrm{Spec}(\overline{\mathbb{Q}}) \end{array} \qquad \begin{array}{ccc} \mathrm{Spec}(K') & \longrightarrow & V_{j'} \subset A \\ \downarrow{\scriptstyle \iota^\sharp} & \nearrow & \downarrow \\ \mathrm{Spec}(R) & \longrightarrow & \mathrm{Spec}(\overline{\mathbb{Q}}) \end{array} .$$

The varieties $\overline{L}$ and A are both proper, therefore $\mathrm{pr}_{U_{i'}} \circ \phi : \mathrm{Spec}(R) \to U_{i'} \hookrightarrow \overline{L}$ and $\mathrm{pr}_{V_{j'}} \circ \phi : \mathrm{Spec}(R) \to V_{j'} \hookrightarrow A$ define the same maps as in the diagrams in Equation (2.1). Therefor ϕ must agree with the map constructed above, hence this map is the unique morphism to make the diagram commute and $\overline{G}$ is separated.
Therefore $\overline{G}$ is proper as a scheme over $\overline{\mathbb{Q}}$, hence a complete variety.
The group G is dense in this variety, since locally

$$V_j \times L \hookrightarrow V_j \times \overline{L}$$

maps onto a dense subset. Since $\overline{L}$ is smooth, any patch

$$V_j \times \overline{L}$$

is smooth and therefore $\overline{G}$ is a smooth variety. The morphism $\overline{p}$ can be taken as the morphism $p_{\overline{L}}$ from the construction of the associated bundle. This construction also implies that its fibres are isomorphic to $\overline{L}$. □

Remark 2.1.9. If one uses Remark 1.3.50, the inclusion $G \hookrightarrow \overline{G}$ constructed above is the morphism induced by the map $id_G \times \iota : G \times L \to G \times \overline{L}$. Here $\iota : L \to \overline{L}$ denotes the inclusion of L in $\overline{L}$.

Proposition 2.1.10 ([SC79], Proposition 2)**.** *The multiplication-by-n-morphism* $[n]_G$ *has a continuation as a morphism* $[n]_{\overline{G}}$ *on* $\overline{G}$ *for any* $n \in \mathbb{Z}$*.*

Proof. By Proposition 2.1.3 we already know that the multiplication on $\overline{L}$ can be continued to an L-equivariant morphism $[n]_{\overline{L}} : \overline{L} \to \overline{L}$. The morphism $[n]_G : G \to G$ is also L-equivariant and hence $[n]_G \times [n]_{\overline{L}} : G \times \overline{L} \to G \times \overline{L}$ is equivariant with regards to the diagonal action of L on the product.
Remark 1.3.50 now implies that there is a morphism $[n]_{\overline{G}} := [n]_G \times^L [n]_{\overline{L}}$.
It is left to show that this morphism is a continuation of $[n]_G$. Remark 2.1.9 implies that $id_G \times^L \iota : G \hookrightarrow \overline{G}$ is the inclusion of G in $\overline{G}$. One has

$$\begin{aligned}(id_G \times \iota_L) \circ ([n]_G \times [n]_L) &= [n_G] \times (\iota \circ [n]_L)\\ &\overset{2.1.3}{=} [n_G] \times ([n]_{\overline{L}} \circ \iota)\\ &= ([n]_G \times [n]_{\overline{L}}) \circ (id_G \times \iota_L)\,.\end{aligned}$$

Therefore

$$\left(id_G \times^L \iota\right) \circ \left([n]_G \times^L [n]_L\right) = \left([n]_G \times^L [n]_{\overline{L}}\right) \circ \left(id_G \times^L \iota\right).$$

If we define an L-action on L by the addition $l \cdot \hat{l} = \hat{l} + l$, we get that we can view G as the associated bundle $G \times^L L$ and $\alpha : G \times L \to G$ is an L-bundle with regards to the diagonal action. Here α denotes the action of L on G. The diagram

$$\begin{array}{ccc} G \times L & \xrightarrow{[n]_G \times [n]_L} & G \times L \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha} \\ G & \xrightarrow{[n]_G} & G \end{array}$$

commutes. Hence $[n]_G \times^L [n]_L = [n]_G$ and

$$\begin{array}{ccc} G & \xrightarrow{[n]_G} & G \\ \downarrow & & \downarrow \\ \overline{G} & \xrightarrow{[n]_{\overline{G}}} & \overline{G} \end{array}$$

commutes. This means that $[n]_{\overline{G}}$ is an continuation of $[n]_G$. □

Proposition 2.1.11 ([SC79], compare Lemme 1)**.** *Let* $g_0 \in G$ *and* τ_{g_0} *the translation by* g_0 *on* G*. Then this morphism extends to an* L*-equivariant morphism on* $\overline{G}$*.*

Proof. We proceed similarly to the previous proposition. The map $\tau_{g_0} \times id_{\overline{L}} : G \times \overline{L} \to G \times \overline{L}$ is L-equivariant with regards to the diagonal action of L on $G \times \overline{L}$. Therefore it induces a map $\tau_{g_0} \times^L id_{\overline{L}} : \overline{G} \to \overline{G}$. The map $\tau_{g_0} \times id_{\overline{L}}$ commutes with $id_G \times \iota$ defined as in Remark 2.1.9, that is

$$(\tau_{g_0} \times id_{\overline{L}}) \circ (id_G \times \iota) = (id_G \times \iota) \circ (\tau_{g_0} \times id_L),$$

additionally

$$\begin{array}{ccc} G \times L & \xrightarrow{\tau_{g_0} \times id_L} & G \times L \\ \Big\downarrow \alpha & & \Big\downarrow \alpha \\ G & \xrightarrow{\quad \tau_{g_0} \quad} & G \end{array}$$

commutes. Here α denotes the action of L on G. Like in the previous proposition, the map α defines an L-bundle with regards to the diagonal action of L on the product. By uniqueness of the factorisation through a quotient, $\tau_{g_0} = \tau_{g_0} \times^L id_L$. Just like in Proposition 2.1.10, the morphism $\tau_{g_0} \times^L id_{\overline{L}}$ is therefore a continuation of τ_{g_0}. □

2.1.4 Divisors on the completion $\overline{G}$

This part of the thesis follows subsections 1.4 and 1.5 of [SC79].

In this subsection the aim is to show that there is a very ample divisor on $\overline{G}$ which can later be used to define a height function on $\overline{G}$.

Proposition 2.1.12 ([Wüs84], I.1.3, [SC79], first paragraph of 1.4)**.** *Let $\overline{L}$ and $\overline{G}$ be as in Proposition 2.1.8 and $L_\infty \subset \overline{L}$ the divisor from Lemma 2.1.4. Then there exists an effective divisor $G_\infty \subset \overline{G}$ which is the fibre bundle over A with fibre L_∞.*

Proof. Let the collection $V_i \times \overline{L}$ with transition functions $\psi_{i,j}$ be as in the construction of $\overline{G}$. Consider the sets $V_i \times L_\infty$. Since L_∞ is invariant under L-action (by Lemma 2.1.4), the function

$$\begin{aligned} \psi_{i,j}|_{(V_i \cap V_j) \times L_\infty} : (V_i \cap V_j) \times L_\infty &\to (V_i \cap V_j) \times L_\infty \\ (u, d) &\mapsto (u, g_{i,j}(0_L) \cdot d) \end{aligned}$$

is well defined. Therefore all the $V_i \times L_\infty$ glue to a subvariety of G_∞ of $\overline{G}$, which is the set $\overline{G} \setminus G$. This subvariety is closed and of codimension 1, since it has these properties in every open subset $V_i \times \overline{L}$ of $\overline{G}$. So G_∞ is a divisor on $\overline{G}$. It is also effective, since L_∞ is an effective divisor. □

Proposition 2.1.13 ([SC79], Proposition 1)**.** *For $D \in \mathrm{Div}(A)$ ampleand $a, b \in \mathbb{N}_{>0}$ sufficiently large the following divisor is very ample:*

$$D_{a,b} := a\overline{p}^* D + bG_\infty.$$

Proof. By Lemma 2.1.4 it is already known that L_∞ is a very ample divisor. This can be used to show that G_∞ is relatively ample with regard to $\overline{p} : \overline{G} \to A$. For this choose again a covering $\{U_i\}_{i \in I}$ of A such that $\overline{p}^{-1}(U_i) \cong U_i \times \overline{L}$. Without loss of generality we can assume that all those open sets U_i are affine. Since U_i is affine all of its divisors are ample by Proposition 1.1.43. In particular the trivial divisor on U_i is ample. Since any multiple of the trivial divisor is again the trivial divisor it is also very ample. On the preimage $\overline{p}^{-1}(U_i) \cong U_i \times \overline{L}$ the divisor G_∞ is of the form $U_i \times L_\infty$.
This divisor is very ample on $U_i \times \overline{L}$. To see this choose $f_0, \dots, f_n$ in the linear system of the trivial divisor on U_i which define an embedding into projective space. If $U_i \cong \mathrm{Spec}(K[x_1, \dots, x_c]/(P_1, \dots, P_r))$ one such choice can be $1, x_1, \dots, x_c$. Choose $e_0, \dots, e_m$ as a basis of the linear system of L_∞ on $\overline{L}$. These correspond to embeddings

$$F : U_i \to \mathbb{P}^n \qquad\qquad E : \overline{L} \to \mathbb{P}^m$$
$$u \mapsto [f_0(u) : \dots : f_n(u)] \qquad\qquad l \mapsto [e_0(l) : \dots : e_m(l)].$$

Any of the functions f_j and e_k extend to elements of the linear system of $U_i \times L_\infty$ by

$$f'_j((u, l)) := f_j(u) \qquad \text{and} \qquad e'_k((u, l)) := e_k(u).$$

All products $f'_j e'_k$ are also in the linear system of $U_i \times L_\infty$. The $f'_j e'_k$ are a collection of rational functions on $U_i \times \overline{L}$. This collection defines an embedding

$$S_{n,m} \circ (F \times E) \colon U_i \times \overline{L} \to \mathbb{P}^s$$
$$(u, l) \mapsto [f'_0((u, l))e'_0((u, l)) : f'_0((u, l))e'_1((u, l)) : \dots : f'_n((u, l))e'_m((u, l))]$$

where $S_{n,m}$ denotes the Segre embedding. Therefore the pullback of $\mathcal{O}(1)$ under this map is isomorphic to $U_i \times L_\infty$ and $U_i \times L_\infty$ is very ample, hence ample.

For $D \in \mathrm{Div}(A)$ ample Proposition 1.1.49 implies that for $a \in \mathbb{N}_{>0}$ sufficiently large the divisor $G_\infty + a\overline{p}^* D$ is ample.

□

Corollary 2.1.14 ([SC79], Corollaire p.193)**.** *There are $(a, b) \in \mathbb{N}_{>0} \times \mathbb{N}_{>0}$ such that $D_{a,b}$ is very ample, which gives $\overline{G}$ the structure of a projective variety.*

Proof. Because $D_{a,b}$ is ample for some $a, b > 0$, some k-th multiple of it is very ample (by Definition 1.1.42). Thus let (ka, kb), $k \in \mathbb{N}$ be a tuple, such that the map relative to $D_{(ka,kb)}$ is a closed immersion.

□

Remark 2.1.15. While in the construction here only the divisor D is varied the previous theorems would hold analogously if L_∞ is replaced with a different very ample divisor on $\overline{L}$. This is discussed in [FL84], [FH85] and [Wüs84]. The dimension of the projective space in which $D_{a,b}$ embeds can be calculated depending on G_∞ and D. This is done in Theorem 6.4 in [FH85].

That the variety $\overline{G}$ is projective allows to use the theory developed in the theorem on the Weil height machine 1.4.19.

Proposition 2.1.16 ([SC79], Corollaire and Remarque 2 (iii) p.193)**.** *There exist $a, b \in \mathbb{N}_{>0}$ such that $D_{a,b}$ is very ample and has the following property. View $\overline{G}$ as a subvariety of some $\mathbb{P}^N$ via the embedding associated to $D_{a,b}$. Then any effective divisor E linearly equivalent to $mD_{a,b}$ for some $m \in \mathbb{N}_{>0}$ is the divisor of zeros of some nonzero polynomial φ of degree m in the coordinates of $\mathbb{P}^N$.*

Proof. Using the previous corollary let $\widetilde{a}, \widetilde{b} \in \mathbb{N}_{>0}$ be such that $D_{\widetilde{a},\widetilde{b}}$ is very ample. Then $\overline{G} \subset \mathbb{P}^N$ is a smooth and therefore normal projective variety. The Enriques-Severi-Zariski-Lemma 1.1.22 implies that there is some $m_0 \in \mathbb{N}_{>0}$ with the property that there is a homogeneous polynomial ψ of degree m such that $\operatorname{div} \psi = E'$ for all $m \geq m_0$ and any effective divisor E' on X which is linearly equivalent to m-times a hyperplane section. The m_0-uple embedding of $\mathbb{P}^N \to \mathbb{P}^M$ makes $\overline{G}$ a projective normal subvariety of $\mathbb{P}^M$ such that the Enriques-Severi-Zariski-Lemma holds with $m_0' = 1$. Since the pullback of divisors under the m_0-uple embedding corresponds to multiplying the divisor by m_0 this embedding of $\overline{G}$ is induced by

$$m_0 D_{\widetilde{a},\widetilde{b}} = D_{m_0\widetilde{a},m_0\widetilde{b}}.$$

Take $a := d_0\widetilde{a}$ and $b := d_0\widetilde{b}$. Since under this embedding any hyperplane section on $\overline{G}$ is linearly equivalent to $D_{a,b}$ this gives the desired result. □

Proposition 2.1.17 ([SC79], Corrolaire 1)**.** *If D is a symmetric divisor on A, then there exists some effective divisor Z_n in $\overline{G}$ dependent on $n \in \mathbb{Z} \setminus \{0\}$ such that*

$$[n]^*_{\overline{G}}(D_{a,b}) \sim n^2 D_{a,b} - bZ_n.$$

Proof. If L is trivial, the divisor G_∞ is trivial and $\overline{G} \cong A$ as well as $D_{a,b} = aD$. Therefore the claim follows from Lemma 1.3.16 and Z_n is trivial for every n.
Assume now that L is nontrivial. First one considers the pullbacks of the components of $D_{a,b}$. On a component $\overline{\mathbb{G}}_a \cong \mathbb{P}^1$ of $\overline{L}$ with coordinates $x_0,\ x_1$ one has:

$$[n]^*_{\overline{\mathbb{G}}_a}(L_a') = [n]^*_{\overline{\mathbb{G}}_a}\{x_0 = 0\} = \{nx_0 = 0\} = L_a'.$$

On $\overline{\mathbb{G}}_m \cong \mathbb{P}^1$ with coordinates $x_0,\ x_1$ one has:

$$[n]^*_{\overline{\mathbb{G}}_m}(L'_m) = [n]^*_{\overline{\mathbb{G}}_m}\{x_0x_1 = 0\} = \{x_0^n x_1^n = 0\} = |n|L'_m.$$

Let $\overline{L} \cong \mathbb{G}_a^{l_a} \times \mathbb{G}_m^{l_m}$ for $l_a,\ l_m \in \mathbb{N}_0$. Denote by G^i_∞ the component of G_∞ associated to L_i for $1 \leq i \leq l_a + l_m$. Here L_i is the divisor on $\overline{L}$ as defined before Lemma 2.1.4. If $l_a \neq 0$, this implies

$$\begin{aligned} [n]^*_{\overline{G}} G^i_\infty &= G^i_\infty && 1 \leq i \leq l_a, \\ [n]^*_{\overline{G}} G^i_\infty &= G^i_\infty |n| && l_a < i \leq l_a + l_m, \end{aligned}$$

because of the definition of G_∞ via gluing of L_∞. If $l_a = 0$ the first line is just omitted. On the abelian variety A the divisor D can be chosen such that it is of symmetric divisor class, meaning $D \sim [-1]^*_A D$. Since p is a homomorphism, it commutes with multiplication by n. Thus by the properties of the pullback it follows that:

$$[n]_A D \sim n^2 D,$$
$$[n]^*_{\overline{G}} \overline{p}^* D = ([n]^*_{\overline{G}} \circ \overline{p}^*)(D) = (p \circ [n]_{\overline{G}})^*(D) = ([n]_A \circ \overline{p})^*(D) \sim \overline{p}^*(n^2 D) = n^2 \overline{p}^* D.$$

Combining these facts one gets:

$$\begin{aligned} [n]^*_{\overline{G}}(D_{a,b}) = a[n]^*_{\overline{G}}\overline{p}^* D + b[n]^*_{\overline{G}} G_\infty &\sim an^2\overline{p}^* D + b\left(\sum_{i=1}^{l_a} G^i_\infty + |n| \sum_{j=l_a+1}^{l_m+l_a} G^j_\infty\right) \\ &\sim an^2\overline{p}^* D + b\left(\sum_{i=1}^{l_a} G^i_\infty + |n| \sum_{j=l_a+1}^{l_m+l_a} G^j_\infty + n^2 G_\infty - n^2 G_\infty\right) \\ &= n^2(a\overline{p}^* D + bG_\infty) - b\overbrace{\left(\sum_{i=1}^{l_a}(n^2 - |n|)G^i_\infty + \sum_{j=l_a+1}^{l_m+l_a}(n^2-1)G^j_\infty\right)}^{Z_n}. \end{aligned}$$

□

Remark 2.1.18. The support of the divisor Z_n is contained in G_∞ for any $n \in \mathbb{Z} \setminus \{0\}$. The preceding proposition also shows, that the different components of $D_{a,b}$ behave differently under pullback by $[n]_{\overline{G}}$. For $n \in \mathbb{Z} \setminus \{0\}$ one has

$$[n]^*_{\overline{G}}(\overline{p}^* D) = n^2(\overline{p}^* D)$$

while the part of G_∞ coming from the completion of the vector subgroup of L stays unchanged under pullback

$$[n]^*_{\overline{G}}\left(\sum_{i=1}^{l_a} G^i_\infty\right) = \left(\sum_{i=1}^{l_a} G^i_\infty\right)$$

and the part of G_∞ coming from the completion of the torus subgroup of L stays scales with the absolute value of n

$$[n]^*_{\overline{G}}\left(\sum_{i=l_a+1}^{l_a+l_m} G^i_\infty\right) = |n|\left(\sum_{i=l_a+1}^{l_a+l_m} G^i_\infty\right).$$

.

Lemma 2.1.19 ([SC79], Corollaire 2)**.** *Let $n \in \mathbb{Z}\setminus\{0\}$ and $a, b \in \mathbb{N}_{>0}$ such that $D_{a,b}$ is very ample. For this lemma view $\overline{G}$ as a subset of some $\mathbb{P}^N$ through the embedding defined by $D_{a,b}$. Let $X_0, \ldots, X_N$ be the coordinates obtained by the embedding into $\mathbb{P}^N$. In this case the multiplication-by-n-morphism $[n]_{\overline{G}}$ can be represented by*

$$\begin{aligned}\varphi^{(n)} : \overline{G} &\to \overline{G}\\ [x] &\mapsto [\varphi_0^{(n)}([x]) : \ldots : \varphi_N^{(n)}([x])]\end{aligned}$$

such that every $\varphi_i^{(n)}$ is a homogeneous polynomial of degree n^2 in $X_0, \ldots, X_N$ on the open subset G.

Proof. By Lemma 1.1.36 the divisor $D_{a,b}$ defines an embedding of $\overline{G}$ into $\mathbb{P}^N$ that is not completely contained in any hyperplane of $\mathbb{P}^N$. So for all hyperplanes $H_i := \{X_i = 0\}$ the intersection with $\overline{G} \subset \mathbb{P}^N$ defines a divisor on $\overline{G}$ linearly equivalent to $D_{a,b}$. By the functoriality of the pullback one has:

$$\begin{aligned}H_{i,n} := [n]^*_{\overline{G}} H_i \sim [n]^*_{\overline{G}} D_{a,b} &\sim n^2 D_{a,b} - bZ_n\\ \iff H_{i,n} + bZ_n &\sim n^2 D_{a,b}.\end{aligned}$$

Since H_i is an effective divisor, so is $H_{i,n}$ and therefore $H_{i,n} + bZ_n$ as well. According to Corollary 2.1.16 there exists a polynomial $\varphi_i^{(n)}$ homogeneous of degree n^2 such that

$$H_{i,n} + bZ_n = (\varphi_i^{(n)})_{\overline{G}}.$$

The base locus of this set of the $H_{i,n} + bZ_n$ is

$$\bigcap_{i=1}^{N}(H_{i,n} + bZ_n) = Z_n$$

since the intersection of all H_i is empty and therefore the intersection of all $H_{i,n}$ must be empty too. But this implies that on $\overline{G}$ the polynomials $\varphi_i^{(n)}$ all vanish at the same time only on $Z_n \subset G_\infty$. So $\varphi := [\varphi_0^{(n)} : \ldots : \varphi_N^{(n)}]$ is regular on all of $G = \overline{G} \setminus G_\infty$. If $|n| \geq 2$ the polynomials of φ vanish simultaneously on all of G_∞, since in those cases the support of Z_n is all of G_∞. The $\varphi_i^{(n)}$ can without loss of generality be chosen, such that the equality

$$\frac{\varphi_i^{(n)}}{\varphi_j^{(n)}} = [n]^*_{\overline{G}}\left(\frac{X_i}{X_j}\right)$$

holds, since

$$\left(\frac{\varphi_i^{(n)}}{\varphi_j^{(n)}}\right)_{\overline{G}} = \left(\varphi_i^{(n)}\right)_{\overline{G}} - \left(\varphi_j^{(n)}\right)_{\overline{G}} = (H_{i,n} - bZ_n) - (H_{j,n} - bZ_n)$$

$$= H_{i,n} - H_{j,n} = ([n]_{\overline{G}}^* X_i)_{\overline{G}} - ([n]_{\overline{G}}^* X_j)_{\overline{G}} = \left(\frac{[n]_{\overline{G}}^* X_i}{[n]_{\overline{G}}^* X_j}\right)_{\overline{G}} = [n]_{\overline{G}}^* \left(\frac{X_i}{X_j}\right)_{\overline{G}}.$$

Thus $\varphi = [n]_{\overline{G}}$ on G. □

2.2 The dependence of the estimates on the chosen height function

This section looks at which role the chosen height on the completion $\overline{G}$ of an algebraic group G plays in proving inequalities. If the chosen height function is for example the height associated to a constant morphism, every point of G will have the same height. As a consequence both inequalities hold trivially. But this does not mean that the inequalities have to hold for other heights.

One way to find different heights on $\overline{G}$ is the theorem of the Weil height machine 1.4.19. The aim of this section is to show that if any of the two inequalities holds for the height associated to a very ample divisor, it will hold for any height associated to a very ample divisor constructed in the height machine. If both inequalities hold for the height associated to a very ample divisor, they will hold for any divisor constructed in the height machine.

In this section G will always be a connected commutative algebraic group defined over $\overline{\mathbb{Q}}$ or a number field K. The variety $\overline{G}$ will denote its completion constructed in Proposition 2.1.8.

Lemma 2.2.1. *Let D be a very ample divisor on $\overline{G}$. Assume one of the inequalities*

$$h_D(g) \leq c_1 n^{c_2}(h_D([n]g) + c_3) + c_4,$$
$$h_D([n]g) \leq c_5 n^{c_6}(h_D(g) + c_7) + c_8$$

holds for $g \in G(\overline{\mathbb{Q}})$ and $n \in \mathbb{Z} \setminus \{0\}$ and the height h_D with constants c_i, for $1 \leq i \leq 8$, depending on some of G, D, g and n. Let E be another very ample divisor in $\mathrm{Div}(\overline{G})$. Then an inequality of the same form holds for h_E and the constants c_i' in this inequality are dependent on D, E and any of G, g and n if the inequality for h_D dependent on the same parameter. The constants c_2' and c_6' can be chosen the same as c_2 and c_6.

Proof. The Corollary 1.4.26 implies that there are constants C_D, C'_D, C_E, C'_E each dependent on both D and E such that for all $g \in G(\overline{\mathbb{Q}})$

$$h_D(g) \leq C_D h_E(g) + C'_D,$$
$$h_E(g) \leq C_E h_D(g) + C'_E.$$

In case of the first inequality this leads to

$$\begin{aligned}
h_E(g) &\leq C_E h_D(g) + C'_E \\
&\leq C_E \left(c_1 n^{c_2}(h_D([n]g) + c_3) + c_4\right) + C'_E \\
&\leq C_E \left(c_1 n^{c_2}(C_D h_E([n]g) + C'_D + c_3) + c_4\right) + C'_E \\
&= C_E \max(1, C_D) c_1 n^{c_2} \left(h_E([n]g) + (C'_D + c_3)\right) + (C_E c_4 + C'_E).
\end{aligned}$$

Therefore the constants can be chosen as $c'_1 = C_E \max(1, C_D) c_1$, $c'_2 = c_2$, $c_3 = C'_D + c_3$ and $c_4 = C_E c_4 + C'_E$.
For the second inequality the process works analogously.

□

Corollary 2.2.2. *Assume that in the situation of the previous lemma both inequalities hold for $n \in \mathbb{Z} \setminus \{0\}$. Let $E \in \mathrm{Div}(\overline{G})$ be an arbitrary divisor. Then both inequalities hold for h_E with the same constraints on the constants as in Lemma 2.2.1 except that c'_2 and c'_6 can take the possible values c_2, c_2^{-1}, c_6^{-1} and c_6.*

Proof. If $E \in \mathrm{Div}(\overline{G})$ is an arbitrary divisor there are very ample divisors E_1, E_2 such that $E = E_1 - E_2$ and $h_E = h_{E_1} - h_{E_2} + O(1)$. Let $C > 0$ be a constant such that $|O(1)| \leq C$. The first inequality in Lemma 2.2.1 implies that there are constants $c_1, \ldots, c_8$ for given $n \in \mathbb{Z} \setminus \{0\}$ such that for any $g \in G(\overline{\mathbb{Q}})$

$$h_{E_1}(g) \leq c_1 n^{c_2}(h_{E_1}([n]g) + c_3) + c_4,$$
$$h_{E_2}([n]g) \leq c_5 n^{c_6}(h_{E_2}(g) + c_7) + c_8.$$

This implies

$$h_{E_2}(g) \geq c_5^{-1} n^{-c_6} \left(h_{E_2}([n]g) - c_8\right) - c_7 \tag{2.2}$$

and therefore

$$\begin{aligned}
h_E(g) &\leq h_{E_1}(g) - h_{E_2}(g) + C \\
&\leq c_1 n^{c_2}(h_{E_1}([n]g) + c_3) + c_4 - h_{E_2}(g) + C \\
&\overset{(2.2)}{\leq} c_1 n^{c_2}(h_{E_1}([n]g) + c_3) + c_4 - \left(c_5^{-1} n^{-c_6} \left(h_{E_2}([n]g) - c_8\right) - c_7\right) + C \\
&\leq \left(\max\left\{c_1, c_5^{-1}\right\} n^{\max\{c_2, -c_6\}}\right) \left(h_{E_1}([n]g) - h_{E_2}([n]g) + (c_3 + c_8)\right) + (c_4 + c_7 + C) \\
&\leq \left(\max\left\{c_1, c_5^{-1}\right\} n^{\max\{c_2, -c_6\}}\right) \left(h_E([n]g) + C + (c_3 + c_8)\right) + (c_4 + c_7 + C).
\end{aligned}$$

Thus the constants can be chosen as $c_1' = \max\left\{c_1, c_5^{-1}\right\}$, $c_2' = \max\{c_2, -c_6\}$, $c_3' = c_3 + c_8 + C$ and $c_4' = c_4 + c_7 + C$.
The proof in case of the second inequality works analogously. □

Remark 2.2.3. If one looks at the inequalities while excluding $n = 0$, the following reductions of parameters can be done. If $c_3' = c_3 + |c_4|$ as for example in Corollary 2.2.2, then the constant c_4 can be chosen as one. For $c_1' := \max\{c_1 c_3, 1\}$ the constant c_3 can be chosen equal to one in the first inequality. The analogous statements hold for the second inequality. Both statements also hold if n is replaced by $|n|$.

Remark 2.2.4. Both the lemma and the corollary also hold if $\mathbb{Z}$ or $\mathbb{Z} \setminus \{0\}$ is replaced with some subset of $\mathbb{Z}$ or $\mathbb{Z} \setminus \{0\}$ respectively.

2.3 The height inequalities in special cases

2.3.1 The inequalities if G is an extension of an abelian variety by a torus

This section looks at how the construction of a canonical height can be done similarly to the case of abelian varieties if G is the extension of an abelian variety by a torus. To do this one uses the construction of a canonical height from sections B.4 and B.5 in [HS00].

In this section G will be a commutative connected algebraic group defined over some number field K or $\overline{\mathbb{Q}}$. The group G is assumed to be the extension of an abelian variety A by a linear group L that is a torus, i.e. $L \cong \mathbb{G}_m^t,\ t \in \mathbb{N}_0$, defined over $\overline{\mathbb{Q}}$. The variety $\overline{G}$ will be its completion as constructed in Proposition 2.1.8. The divisor G_∞ will be the divisor associated to the complement $\overline{G} \setminus G$ as in Proposition 2.1.12.

Definition 2.3.1 ([Hub21], Definition 9.16)**.** An algebraic group G is called a *semiabelian variety* if it is the extension of an abelian variety by a torus.

Proposition 2.3.2 ([HS00], analogous to Theorem B.5.1 (a) and (b) and compare [SC79] paragraph 2.2 (1))**.** *There is a canonical height h_∞ on $\overline{G}$ associated to the height h_{G_∞} such that for any $g \in \overline{G}(\overline{\mathbb{Q}})$ and $n \in \mathbb{Z}$*

$$h_\infty([n]g) = |n| h_\infty(g).$$

Proof. If the linear group is trivial, the height h_{G_∞} is trivial and can therefore be chosen as h_∞.
If L is not trivial, then this proof completely emulates the construction of a canonical height on abelian varieties (Lemma 1.4.30). The Remark 2.1.18 implies that for any $n \in \mathbb{Z} \setminus \{0\}$

$$[n]^* G_\infty \sim |n| G_\infty.$$

Choose $n = 2$. A canonical height $\hat{h}$ on $\overline{G}$ associated to the multiplication-by-two-morphism [2] can be constructed as

$$\hat{h}(g) = \lim_{n\to\infty} \frac{1}{2^n} h_{G_\infty}([2^n]g) \qquad \forall g \in \overline{G}(\overline{\mathbb{Q}}).$$

This construction can be found in Theorem B.4.1 of [HS00] and leads to a height that differs from h_{G_∞} only by a bounded function. To show that this height has the desired behaviour under integer multiplication one looks at

$$\begin{aligned}\hat{h}([l]g) &= \lim_{n\to\infty} \frac{1}{2^n} h_{G_\infty}([2^n l]g)\\ &\overset{1.4.19(2)}{=} \lim_{n\to\infty} \frac{1}{2^n}(|l| h_{G_\infty}([2^n]g) + O(1))\\ &= |l|\hat{h}(g) + \lim_{n\to\infty} \frac{O(1)}{2^n}\\ &= |l|\hat{h}(g)\end{aligned}$$

for arbitrary $l \in \mathbb{Z}$. Therefore the choice $h_\infty = \hat{h}$ has the desired properties. □

Remark 2.3.3. This construction would not work if L were not a torus, since on $\mathbb{G}_a$ the pullback of the divisor L'_a under multiplication with an integer $n \neq 0$ is

$$[n]^* L'_a \sim L'_a.$$

But the construction of the canonical height can only be applied to divisors D and morphisms $\varphi : \overline{G} \to \overline{G}$ for which

$$\varphi^* D \sim \alpha D$$

for $\alpha > 1$.

Proposition 2.3.4 ([HS00], analogous to Theorem B.5.1 (a) and (b))**.** *Let D be an ample symmetric divisor on A. Then there is a canonical height h_q associated to the height h_{p^*D} such that for any $g \in G(\overline{\mathbb{Q}})$ and $n \in \mathbb{Z}$*

$$h_q([n]g) = n^2 h_q(g).$$

Proof. The proof of Proposition 2.1.17 in section 2.1.4 implies that

$$[n]^*(p^* D) \sim n^2 p^* D.$$

Now the proof again can be done completely analogous to the construction of a canonical height on an abelian variety (Theorem 1.4.29) and Proposition 2.3.2. I have therefore omitted it. □

Lemma 2.3.5. *Let G be a commutative algebraic group defined over $\overline{\mathbb{Q}}$ which is the extension of an abelian variety A by a torus L. Let h be the height associated to a divisor $D_{a,b}$ as in Proposition 2.1.14. Then there exist constants c_1, c_2, c_3 independent of n and g such that for any $n \in \mathbb{Z} \setminus \{0\}$ and $g \in G(\overline{\mathbb{Q}})$*

$$\begin{aligned} h([n]g) &\leq c_1 n^2 (h(g) + 1) + c_2, \\ h(g) &\leq h([n]g) + c_3. \end{aligned}$$

Proof. Due to the additivity of the Weil height machine there is

$$h := h_{D_{a,b}} = h_{aG_\infty + bp^* D} = a h_{G_\infty} + b h_{p^* D} + O(1).$$

The bounded function $O(1)$ only depends on $\overline{G}$ and $D_{a,b}$. Let h_∞ and h_q be the canonical heights constructed in Proposition 2.3.2 and Proposition 2.3.4 respectively. Then there exists a bounded function $O(1)'$ dependent on $\overline{G}$ and $D_{a,b}$ such that

$$h = a h_\infty + b h_q + O(1)'.$$

Let C' be a constant such that $|O(1)'| \leq C'$. Therefore for any $g \in G(\overline{\mathbb{Q}})$ and $n \in \mathbb{Z}$

$$\begin{aligned} h([n]g) &\leq a h_\infty([n]g) + b h_q([n]g) + C' \\ &= a|n| h_\infty(g) + b n^2 h_q(g) + C' \\ &\leq n^2 \left(a h_\infty(g) + b h_q(g) \right) + C' \\ &\leq n^2 \left(h(g) + C' \right) + C' \\ &\leq \max\{C', 1\} n^2 \left(h(g) + 1 \right) + C', \\ h([n]g) &\geq h_\infty([n]g) + b h_q([n]g) - C' \\ &= a|n| h_\infty(g) + b n^2 h_q(g) - C' \\ &\geq h_\infty(g) + b h_q(g) - C' \\ &\geq h(g) - 2C' \\ \implies h(g) &\leq h([n]g) + 2C'. \end{aligned}$$

Hence the constants can be chosen as $c_1 = \max(C', 1)$, $c_2 = C'$ and $c_3 = 2C'$. □

Remark 2.3.6. The first inequality also holds for $n = 0$ if the constant c_2 is modified to $c_2' = \max\{h(0_G), c_2\}$.

Corollary 2.3.7. *Let G be defined as in the previous lemma and E be an arbitrary divisor on $\overline{G}$. There exist constants $c_1, \ldots, c_4$ independent of n and g such that for any $n \in \mathbb{Z} \setminus \{0\}$ and $g \in G(\overline{\mathbb{Q}})$*

$$\begin{aligned} h([n]g) &\leq c_1 n^2 (h(g) + 1) + c_2, \\ h(g) &\leq c_3 (h([n]g) + 1) + c_4. \end{aligned}$$

Proof. This is a direct consequence of Corollary 2.2.2. □

2.3.2 The inequalities if G is a linear group

This subsection aims to elaborate the calculations already done in Lemma 6.8 of [Hub21].

Proposition 2.3.8 ([Hub21], compare Lemma 6.8)**.** *Let h denote the height on $\overline{\mathbb{Q}}$. Then for all $g \in \mathbb{G}_a(\overline{\mathbb{Q}})$ and $n \in \mathbb{Z} \setminus \{0\}$*

$$\begin{aligned} h([n]g) &\leq |n|(h(g)+1), \\ h(g) &\leq |n|(h([n]g)+1). \end{aligned}$$

Proof. By Corollary 1.4.13 in the heights section

$$\begin{aligned} h([n]g) &\leq h(g) + \log|n| \\ &\leq |n|(h(g)+1), \\ h(g) &= h\left(\frac{[n]g}{n}\right) \\ &\leq h([n]g) + h\left(\frac{1}{n}\right) \\ &= h([n]g) + \log|n| \\ &\leq |n|\left(h([n]g)+1\right). \end{aligned}$$

□

Proposition 2.3.9 ([Hub21], compare Lemma 6.8)**.** *Let h denote the height on $\overline{\mathbb{Q}}$. Then for all $g \in \mathbb{G}_m(\overline{\mathbb{Q}})$ and $n \in \mathbb{Z}$*

$$h([n]g) = |n|h(g).$$

Proof. This is Corollary 1.4.13 (3). □

Let now L be an arbitrary nontrivial linear group defined over the field K. If $K = \overline{\mathbb{Q}}$ then

$$L \cong \mathbb{G}_a^{l_a} \times \mathbb{G}_m^{l_m}$$

for some $l_a, l_m \in \mathbb{N}_0$. If K is a number field this holds in some finite extension of K. Therefore it can be assumed without loss of generality that the linear group also has the form of such a product over the number field K. This means L can be completed as in Proposition 2.1.1

$$L \hookrightarrow \left(\mathbb{P}^1\right)^{l_a+l_m}.$$

Let h denote the height induced on L by the Segre embedding

$$\left(\mathbb{P}^1\right)^{l_a+l_m} \hookrightarrow \mathbb{P}^{2^{l_a+l_m}-1}.$$

This is the map associated to the divisor $\sum_{i=1}^{l_a+l_m} \mathrm{pr}_i^*([1:0])$ with $\mathrm{pr}_i : \overline{\mathbb{G}}_a^{l_a} \times \overline{\mathbb{G}}_m^{l_m} \to \overline{\mathbb{G}}_a$ for $1 \leq i \leq l_a$ and $\mathrm{pr}_i : \overline{\mathbb{G}}_a^{l_a} \times \overline{\mathbb{G}}_m^{l_m} \to \overline{\mathbb{G}}_m$ for $l_a < i \leq l_a + l_m$ being the projection on the i-th component of $\overline{L}$.

Lemma 2.3.10. *Let $L \cong \mathbb{G}_a^{l_a} \times \mathbb{G}_m^{l_m}$ be a linear group defined over $\overline{\mathbb{Q}}$. Then there exists some constant C only dependent on L such that for all $g \in L(\overline{\mathbb{Q}})$ and $n \in \mathbb{Z} \setminus \{0\}$*

$$\begin{aligned} h([n]g) &\leq n(h(g) + C), \\ h(g) &\leq n(h([n]g) + C). \end{aligned}$$

If $E \in \mathrm{Div}(\overline{L})$ is a different divisor there are constants $c_1, \ldots, c_4$ dependent on L and E such that

$$\begin{aligned} h([n]g) &\leq c_1 n(h(g) + 1) + c_2, \\ h(g) &\leq c_3 n(h([n]g) + 1) + c_4 \end{aligned}$$

for any $g \in L(\overline{\mathbb{Q}})$ and $n \in \mathbb{Z} \setminus \{0\}$.

Proof. Let $g = (g_1, \ldots, g_{l_a+l_m}) \in \mathbb{G}_a^{l_a} \times \mathbb{G}_m^{l_m}$. By Proposition 1.4.9 the properties of the Segre embedding imply

$$h(g) = \sum_{i=1}^{l_a+l_m} h(g_i)$$

with the heights on the right hand side denoting the affine height. Therefore

$$\begin{aligned} h([n]g) &= h((ng_1, \ldots, ng_s, (g_{l_a+1})^n, \ldots, (g_{l_a+l_m})^n)) \\ &= \sum_{i=1}^{l_a} h(ng_i) + \sum_{j=1}^{l_m} h((g_{l_a+j})^n) \\ &\leq |n| \left(\sum_{i=1}^{l_a} (h(g_i) + 1) + \sum_{j=1}^{l_m} h(g_{l_a+j}) \right) \\ &\leq |n|(h(g) + l_a). \end{aligned}$$

Propositions 2.3.8 and 2.3.9 are used in the third line. Hence C can be chosen to equal l_a. The second inequality is calculated in the same way

$$\begin{aligned} h(g) &= h((g_1, \ldots, g_{l_a}, g_{l_a+1}, \ldots, g_{l_a+l_m})) \\ &= \sum_{i=1}^{l_a} h(g_i) + \sum_{j=1}^{l_m} h(g_{l_a+j}) \\ &\leq |n| \left(\sum_{i=1}^{l_a} (h(ng_i) + 1) + \sum_{j=1}^{l_m} h(g_{l_a+j}) \right) \\ &\leq |n|(h(ng) + l_a) \\ &= |n|(h(g) + C). \end{aligned}$$

The second statement is a consequence of Corollary 2.2.2. □

Remark 2.3.11. If a different completion of L is chosen then the constant C can be chosen to be equal to 1 for factors $n \in \mathbb{N}_0$. Let

$$L \cong \mathbb{G}_a^{l_a} \times \mathbb{G}_m^{l_m}$$

over the field $\overline{\mathbb{Q}}$. Another way to complete L is to first embed it into $\mathbb{A}_{\overline{\mathbb{Q}}}^{l_a+l_m}$ which has completion $\mathbb{P}_{\overline{\mathbb{Q}}}^{l_a+l_m}$. Since this makes L a dense open subset of $\mathbb{A}_{\overline{\mathbb{Q}}}^{l_a+l_m}$ there is a completion

$$\begin{aligned} L \cong \mathbb{G}_a^{l_a} \times \mathbb{G}_m^{l_m} &\to \mathbb{P}_{\overline{\mathbb{Q}}}^{l_a+l_m} \\ (g_1, \ldots, g_{l_a+l_m}) &\mapsto [g_1 : \ldots : g_{l_a+l_m} : 1]. \end{aligned}$$

The projective height on $\mathbb{P}_{\overline{\mathbb{Q}}}^{l_a+l_m}$ induces a height function on L. This height will be denoted as $\widetilde{h}$. For any absolute value $|\cdot|$ the following holds:

$$\begin{aligned} \max_{\substack{1\leq i\leq l_a \\ 1\leq j\leq l_m}} \{|ng_i|, |g_{l_a+j}^n|, 1\} &\leq \max\{|n|, 1\} \max_{\substack{1\leq i\leq l_a \\ 1\leq j\leq l_m}} \{|g_i|, |g_{l_a+j}|^n, 1\} \\ &\leq \max\{|n|, 1\} \max_{\substack{1\leq i\leq l_a \\ 1\leq j\leq l_m}} \{|g_i|, |g_{l_a+j}|, 1\}^n, \end{aligned} \tag{2.3}$$

$$\begin{aligned} \max_{\substack{1\leq i\leq l_a \\ 1\leq j\leq l_m}} \{|g_i|, |g_{l_a+j}|, 1\} &\leq \max\left\{|n|^{-1}, 1\right\} \max_{\substack{1\leq i\leq l_a \\ 1\leq j\leq l_m}} \{|ng_i|, |g_{l_a+j}|, 1\} \\ &\leq \max\left\{|n|^{-1}, 1\right\} \max_{\substack{1\leq i\leq l_a \\ 1\leq j\leq l_m}} \{|ng_i|, |g_{l_a+j}|^n, 1\}. \end{aligned} \tag{2.4}$$

Let $g = (g_1, \dots, g_{l_a+l_m}) \in L(\overline{\mathbb{Q}})$ be a point, then

$$\begin{aligned}
\widetilde{h}([n]g) &= h_{\mathbb{P}^{l_a+l_m}}([ng_1 : \dots : ng_{l_a} : g^n_{l_a+1} : \dots : g^n_{l_a+l_m} : 1]) \\
&= \frac{1}{[K:\mathbb{Q}]} \sum_{\nu \in M_K} d_\nu \log \max_{\substack{1 \le i \le l_a \\ 1 \le j \le l_m}} \{|ng_i|, |g^n_{l_a+j}|, 1\} \\
&\overset{(2.3)}{\le} \frac{1}{[K:\mathbb{Q}]} \sum_{\nu \in M_K} d_\nu \log \max\{|n|, 1\} \max_{\substack{1 \le i \le l_a \\ 1 \le j \le l_m}} \{|g_i|, |g_{l_a+j}|, 1\}^n \\
&= \log |n| + |n| \widetilde{h}(g) \\
&\le |n|(\widetilde{h}(g) + 1), \\
\widetilde{h}(g) &= h_{\mathbb{P}^{l_a+l_m}}([g_1 : \dots : g_{l_a} : g_{l_a+1} : \dots : g_{l_a+l_m} : 1]) \\
&= \frac{1}{[K:\mathbb{Q}]} \sum_{\nu \in M_K} d_\nu \log \max_{\substack{1 \le i \le l_a \\ 1 \le j \le l_m}} \{|g_i|, |g_{l_a+j}|, 1\} \\
&\overset{(2.4)}{\le} \frac{1}{[K:\mathbb{Q}]} \sum_{\nu \in M_K} d_\nu \log \max\left\{|n|^{-1}, 1\right\} \max_{\substack{1 \le i \le l_a \\ 1 \le j \le l_m}} \{|ng_i|, |g_{l_a+j}|^n, 1\} \\
&\le \log |n| + \widetilde{h}([n]g) \\
&\le |n|(\widetilde{h}([n]g) + 1).
\end{aligned}$$

This is the completion used in [Hub21].

2.3.3 The inequalities if G is the product of an abelian variety and a linear group

All this section does is to combine the height estimates on a linear group and the height estimates on an abelian variety to show the following inequalities in the special case of G being a product of an abelian variety and a linear group.

Lemma 2.3.12. *Let G be a connected commutative algebraic group, L a linear algebraic group and A an abelian variety all defined over $\overline{\mathbb{Q}}$ such that $G \cong L \times A$. For any height constructed on $\overline{G}$ with the Weil height machine the following inequalities hold. Let $g \in G(\overline{\mathbb{Q}})$ and $n \in \mathbb{Z} \setminus \{0\}$*

$$\begin{aligned}
h([n]g) &\le c_1 n^2 (h(g) + 1) + c_2, \\
h(g) &\le c_3 n^2 (h([n](g) + 1) + c_4.
\end{aligned}$$

The constants c_1, c_2, c_3, c_4 only depend on G and the divisor.

Proof. As stated in Corollary 2.2.2 it is sufficient to show both height estimates in the case of the height associated to a very ample divisor.
Let D be a very ample symmetric divisor on A which embeds A into some $\mathbb{P}^N$ and let E be the divisor of points at infinity associated to the embedding of $\overline{L}$ in $\mathbb{P}^{2^{\dim L}-1}$ used in Lemma 2.3.10. Let $p_L : \overline{G} \to \overline{L}$ and $p_A : \overline{G} \to A$ be the respective projections. The divisor $F = p_L^* E + p_A^* D$ is associated to the embedding

$$\overline{G} = \overline{L} \times A \hookrightarrow \mathbb{P}^N \times \mathbb{P}^{2^{l_a+l_m}-1} \overset{\text{Segre}}{\hookrightarrow} \mathbb{P}^{(N+1)2^{l_a+l_m}-1}.$$

Therefore $h_F = h_{p_L^* E} + h_{p_A^* D}$ and the claim follows from Lemma 2.3.5 and Lemma 2.3.10 together with the functoriality of the height. The explicit calculations can be done analogously to Lemma 2.3.5. □

2.4 The first height inequality on an arbitrary commutative connected algebraic group

In this whole section let G be a commutative connected algebraic group defined over $\overline{\mathbb{Q}}$. Let $\overline{G}$ be the completion of G as in Proposition 2.1.8 and let

$$0 \to \overline{L} \overset{i}{\to} \overline{G} \overset{p}{\to} A \to 0$$

be the decomposition of $\overline{G}$ associated to the decomposition of G into a linear group L and an abelian variety A. The multiplication-by-n-morphism on $\overline{G}$ will be denoted as $[n]_G$. Fix $D_{a,b}$ the very ample divisor on $\overline{G}$ as in the Corollaries 2.1.16 and 2.1.14.

2.4.1 The inequality dependent on prime factors

This inequality is using the same idea as Proposition 2.0 in [Wüs89].

Proposition 2.4.1. *Let G an algebraic group as defined above in this section and $n \in \mathbb{Z}$. Then there are constants C_1 dependent on n and C_2 independent of n such that for any $m \in \mathbb{N}_0$ and $g \in G(\overline{\mathbb{Q}})$*

$$h_{D_{a,b}}([n^m]_G g) \leq n^{2m} C_1 (h_{D_{a,b}}(g) + 1) + C_2.$$

Proof. Identify $\overline{G}$ with $\overline{G} \hookrightarrow \mathbb{P}^N$ by using the embedding induced by $D_{a,b}$. Take the projective height h on $\mathbb{P}^N$ that is the same as $h_{D_{a,b}}$ for points in $\overline{G}$. For any $g \in G$ and $C_2 = \max\{0, h(0_G)\}$ as well as any constant C

$$h([0]_G g) = h(0_G) \leq C_2 = 0 \cdot C(h(g) + 1) + C_2.$$

Therefore in this case the inequality will hold for $n = 0$.
For the case $n = 1$ take $C_1 \geq 1$ and C_2 as above.
When considering the case $n \neq 0, 1$ let again $C_2 = \max\{0, h(0_G)\}$. Let

$$\varphi^{(n)} : \mathbb{P}^N \to \mathbb{P}^N$$

be the rational map of degree n^2 and regular on G defined in Lemma 2.1.19. By Proposition 1.4.17 there is a constant C_1' dependent on $\varphi^{(n)}$ such that for any $g \in G(\overline{\mathbb{Q}})$

$$h([n]_G g) = h(\varphi^{(n)}(g)) \leq n^2 h(g) + C_1'. \tag{2.5}$$

Choose $C_1 = \max\{C_1', 1\}$, then

$$h([n]_G g) \overset{(2.5)}{\leq} n^2 h(g) + C_1' \leq n^2 h(g) + C_1 + C_2 \leq n^2 C_1 (h(g) + 1) + C_2.$$

This proves the case $m = 1$ and also covers the case $m = 0$ for any nontrivial multiplication factor n.
If $n = 0, 1$ nothing additional has to be shown for the case of general m. Since $(-1)^m$ is 1 or -1, the case $n = -1$ is covered by $m = 1$ as well. One just takes the maximum of the constants obtained in the inequality for multiplication with -1 and 1.
If $n \neq 0, 1, -1$ a repeated application of the case $m = 1$ gives the general statement.

$$\begin{aligned}
h([n^m]_G g) &= h([n]_G([n^{m-1}]_G g)) \\
&\leq n^2(h([n^{m-1}]_G g) + C_1' \\
&= n^2(h([n]_G[n^{m-2}]_G g) + C_1' \\
&\leq \ldots \\
&\leq n^{2m} h(g) + \left(n^{2(m-1)} + n^{2(m-2)} + \ldots + 1\right) C_1' \\
&\leq n^{2m} C_1 (h(g) + 1) \\
&\leq n^{2m} C_1 (h(g) + 1) + C_2.
\end{aligned}$$

□

Remark 2.4.2. Analogously to the situation in Remark 2.3.6 one can see that if n is chosen to be not equal to 0 the constant C_2 can be omitted.

Corollary 2.4.3. *Let G be an algebraic group as defined in the beginning of this section, E a very ample divisor on $\overline{G}$ and $n \in \mathbb{Z}$. Then there are constants C_1 dependent on the prime factors of n and C_2 independent of n such that for any $g \in G(\overline{\mathbb{Q}})$*

$$h_E([n^m]_G g) \leq n^{2m} C_1 (h_E(g) + 1) + C_2.$$

Proof. The statement for $E = D_{a,b}$ follows from the previous proposition. The statement for any other very ample E follows from Lemma 2.2.1. □

2.4.2 The inequality as in Serre

This section is following §2 in [SC79].

By the additive property of the Weil height machine 1.4.19 we get that

$$h_{D_{a,b}} \sim ah_{G_\infty} + bh_{p^*D} \sim ah_{G_\infty} + bh_D \circ p.$$

So we can treat the heights h_{G_∞} and h_{p^*D} separately to obtain an inequality.

The height associated to G_∞

Lemma 2.4.4 ([SC79], Lemme 1)**.** *Let $g_0 \in G(\overline{\mathbb{Q}})$ be an arbitrary element. There is a constant $C > 0$ dependent on g_0 such that for all $g \in G(\overline{\mathbb{Q}})$*

$$|h_{G_\infty}(g + g_0) - h_{G_\infty}(g)| \leq C.$$

Proof. Let τ_{g_0} be the translation on G by g_0. This agrees with G acting on G by g_0 and can therefore be continued to some morphism from $\overline{G}$ to $\overline{G}$ by Proposition 2.1.11. The divisor G_∞ is invariant under the group action of G on $\overline{G}$ defined in Proposition 2.1.11 and therefore the divisors G_∞ and $\tau_{g_0}G_\infty$ are linearly equivalent. The functoriality of the Weil height machine 1.4.19 implies

$$h_{G_\infty} \sim h_{\tau_{g_0}^* G_\infty} \sim h_{G_\infty} \circ \tau_{g_0}.$$

This is equivalent to the statement in the lemma. □

Remark 2.4.5. The construction in the height machine is in theory explicit enough to calculate a bound C for $O(1)$ in Lemma 2.4.4. But this needs explicit formulas for the translation τ_{g_0} as well as an explicit description of the linear systems of two basepoint free divisors E_1, E_2 such that $G_\infty = E_1 - E_2$.

Remark 2.4.6. By symmetry one sees that the same constants $C(g_0) = C(-g_0)$ can be chosen for g_0 and $-g_0$ since for any $g \in G(\overline{\mathbb{Q}})$

$$|h_{G_\infty}(g - g_0) - h_{G_\infty}(g)| = |h_{G_\infty}(g - g_0) - h_{G_\infty}((g - g_0) + g_0)| \leq C(g_0).$$

The triangle inequality implies that $C([n]_G g_0)$ can be chosen smaller or equal to $nC(g_0)$, which yields

$$\begin{aligned}
|h_{G_\infty}(g + [n]_G g_0) - h_{G_\infty}(g)| &= \left|\sum_{i=1}^{n} h_{G_\infty}(g + [i]_G g_0) - h_{G_\infty}(g + [i-1]_G g_0)\right| \\
&\leq \sum_{i=1}^{n} |h_{G_\infty}(g + [i]_G g_0) - h_{G_\infty}(g + [i-1]_G g_0)| \\
&\leq \sum_{i=1}^{n} C(g_0) = nC(g_0).
\end{aligned}$$

This leads to the height inequality found in the paper [SC79].

Proposition 2.4.7 ([SC79], Lemme 2)**.** *Let $g_1, \dots, g_m \in G(\overline{\mathbb{Q}})$. Then there are $C_1, C_2 > 0$ such that for all $n_1, \dots, n_m \in \mathbb{Z}^m$*

$$\left| h_{G_\infty}\left(\sum_{i=1}^m n_i g_i\right)\right| \leq C_1 + C_2 \sum_{i=1}^m |n_i|.$$

The constant C_2 depends on the points, while C_1 only depends on G and the divisor D.

Proof. For all g_i take $\widetilde{C}_i$ as the constant $C(g_i)$ from the preceding lemma. Set

$$C_1 := \max\{0, h_{G_\infty}(0_G)\}, \qquad C_2 := \max_{i=1,\dots m} \widetilde{C}_i.$$

With these constants the inequality follows for the empty sum (equalling 0). The general case can be shown inductively. Assuming the inequality already holds for $g_1, \dots, g_k \in G(\overline{\mathbb{Q}})$ with $k \leq m$, $n_1, \dots, n_{k-1}, n_k, l_k \in \mathbb{Z}$, $|l_k| < |n_k|$ and $l_k \geq 0$ there is the inequality

$$\begin{aligned}
\left| h_{G_\infty}\left(\overbrace{\sum_{i=1}^{k-1} n_i g_i + l_k g_k}^{=:g} + g_k\right)\right| &= |h_{G_\infty}(g + g_k) - h_{G_\infty}(g) + h_{G_\infty}(g)| \\
&\leq |h_{G_\infty}(g + g_k) - h_{G_\infty}(g)| + |h_{G_\infty}(g)| \\
&\overset{\text{IH}}{\leq} C_1 + C_2\left(\sum_{i=1}^{k-1} |n_i| + |l_k|\right) + |h_{G_\infty}(g + g_k) - h_{G_\infty}(g)| \\
&\leq C_1 + C_2\left(\sum_{i=1}^{k-1} |n_i| + |l_k|\right) + \widetilde{C}_k \\
&= C_1 + C_2\left(\sum_{i=1}^{k-1} |n_i| + |l_k| + 1\right).
\end{aligned}$$

If $l_k < 0$ the argument works completely analogously. □

Since any fibre of p is by Proposition 2.1.8 isomorphic to $\overline{L}$ the dependence behaviour height h_{G_∞} on such fibres can be described more explicitly.

Proposition 2.4.8. *For any $g \in G(\overline{\mathbb{Q}})$ there exists a constant C dependent on g such that for any $l \in L(\overline{\mathbb{Q}})$*

$$|h_{G_\infty}(g + i(l)) - (h_{G_\infty}(i(l)) + h_{G_\infty}(g))| \leq C.$$

Proof. Let

$$i : \overline{L} \to \overline{G}$$

be the continuation of the map from L into G as defined in the beginning of the section and constructed in 2.1.10. This is a morphism between projective varieties. Use the notation that for any $g \in G$

$$i_g := i \circ \tau_g.$$

This is again a morphism between projective varieties. One has that for any $g \in G$

$$i_g^{-1}(G_\infty) = i^{-1}(G_\infty) = L_\infty.$$

This follows from $\overline{G}$ and G_∞ being locally defined as a product combined with the invariance of G_∞ under the G-action on $\overline{G}$. Hence by the functoriality of heights (Theorem 1.4.19 (2)) there is some constant $C(g)$ dependent on g such that

$$|h_{L_\infty} - h_{G_\infty} \circ i_g| = \left| h_{i_g^* G_\infty} - h_{G_\infty} \circ i_g \right| \leq C(g). \tag{2.6}$$

The divisor L_∞ is very ample. Thus Corollary 1.4.26 implies that the height associated to L_∞ is equivalent up to some scalar to the height used in Lemma 2.3.10. The following holds for any $l \in L$

$$h_{G_\infty}(g + i(l)) = h_{G_\infty}(i_g(0_L) + i(l)) = h_{G_\infty}(i_g(l)).$$

Combined with the above inequality for the choice of $l = 0_L$ this leads to

$$|h_{G_\infty}(g)| = |h_{G_\infty}(g + i(0_L))| \overset{(2.6)}{\leq} |h_{L_\infty}(0_L) + C(g)| = |C(g)| = C(g),$$

which implies

$$\begin{aligned} |h_{G_\infty}(g + i(l)) - (h_{G_\infty}(i(l)) + h_{G_\infty}(g))| \leq & |h_{G_\infty}(g + i(l)) - h_{L_\infty}(l)| \\ & + |h_{L_\infty}(l) - h_{G_\infty}(i(l))| + |h_{G_\infty}(g))| \\ \leq & C(g) + C(0_G) + C(g) \\ \leq & 3 \max\{C(g), C(0_G)\} =: C. \end{aligned}$$

Or equivalently

$$h_{G_\infty}(g + i(l)) = h_{G_\infty}(i(l)) + h_{G_\infty}(g) + O(1)$$

with the absolute value of $O(1)$ bounded by C. □

The height associated to p^*D

In this section let D be a symmetric divisor on A. The height h_{p^*D} is defined as the height associated to the pullback of the divisor D. This implies that

$$h_{p^*D} \sim h_D \circ p$$

or equivalently that there exists some constant $C(D, p)$ such that for any $g \in G(\overline{\mathbb{Q}})$

$$|h_{p^*D}(g) - h_D(p(g))| \leq C(D, p). \tag{2.7}$$

This can be used to show an inequality analogous to Proposition 2.4.7. To obtain the constants one uses the following lemma.

Lemma 2.4.9. *Let $q : G(\overline{\mathbb{Q}}) \to \mathbb{R}$ a function fulfilling the parallelogram law, that is for any $g, g' \in G(\overline{\mathbb{Q}})$*

$$q(g + g') = 2(q(g) + q(g').$$

Then the following inequality holds for any $m \in \mathbb{N}_{>0}$ and $g_1, \ldots, g_m \in G(\overline{\mathbb{Q}})$

$$q\left(\sum_{i=1}^{m} g_i\right) \leq \frac{1}{m}\left(2^m + 2^{m-1} - 2\right)\sum_{i=1}^{m} q(g_i) =: C_m \sum_{i=1}^{m} q(g_i).$$

Proof. The constant $CM = \frac{1}{m}\left(2^m + 2^{m-1} - 2\right)$ can be constructed inductively.
The case $m = 1$ is trivial.
For $m = 2$ the constant follows from the parallelogram law:

$$\begin{aligned} q(g_1 + g_2) &\leq q(g_1 + g_2) + h_q(g_1 + g_2) \\ &= 2(q(g_1) + q(g_2)) \\ &= C_2(q(g_1) + q(g_2)). \end{aligned}$$

For $m \geq 2$ induction implies that for any $1 \leq j \leq m + 1$

$$\begin{aligned} q\left(\sum_{\substack{i=1 \\ i \neq j}}^{m+1} g_i + g_j\right) &= 2\left(q\left(\sum_{\substack{i=1 \\ i \neq j}}^{m+1} g_i\right) + q(g_j)\right) \\ &\overset{IH}{\leq} 2\left(\frac{1}{m}(2^m + 2^{m-1} - 2)\sum_{\substack{i=1 \\ i \neq j}}^{m+1} q(g_i) + q(g_j)\right). \end{aligned}$$

This is symmetric in the index j so by adding the inequalities for all indices $j = 1, \ldots, \; m+1$ it follows that

$$
\begin{aligned}
(m+1)q\left(\sum_{i=1}^{m+1} g_i\right) &\leq \left(\frac{2}{m}(2^m + 2^{m-1} - 2)\cdot m + 2\right)\sum_{i=1}^{m+1} q(g_i) \\
&= \left(2^{m+1} + 2^m - 2^2 + 2\right)\sum_{i=1}^{m+1} q(g_i) \\
&= \left(2^{m+1} + 2^m - 2\right)\sum_{i=1}^{m+1} q(g_i) \\
\implies q\left(\sum_{i=1}^{m+1} g_i\right) &\leq \frac{1}{m+1}\left(2^{m+1} + 2^m - 2\right)\sum_{i=1}^{m+1} q(g_i) \\
&= C_{m+1}\sum_{i=1}^{m+1} q(g_i).
\end{aligned}
$$

□

Proposition 2.4.10 ([SC79], compare 2.2 (1))**.** *Let $g_1, \ldots, g_m \in G(\overline{\mathbb{Q}})$. Then there are $C_1, C_2 > 0$ such that for all $n_1, \ldots, n_m \in \mathbb{Z}^m$*

$$\left| h_{p^*D}\left(\sum_{i=1}^{m} n_i g_i\right)\right| \leq C_1 + C_2\left(\sum_{i=1}^{m} |n_i|\right)^2.$$

The constant C_2 depends on the points, while C_1 only depends on G and the divisor D.

Proof. For any divisor $D \in \mathrm{Div}(A)$ the associated height is up to some bounded function $O(1)$ dependent on D a quadratic form h_q. So for all $g_1, \ldots, g_m \in G(\overline{\mathbb{Q}})$ and $n_1, \ldots, n_m \in \mathbb{Z}$

$$
\begin{aligned}
h_{p^*D}\left(\sum_{i=1}^{m} n_i g_i\right) &= h_q\left(\sum_{i=1}^{m} n_i p(g_i)\right) + O(1) \\
&= h_q\left(\sum_{i=1}^{m} n_i p(g_i)\right) + O(1) \\
&\leq C_m \sum_{i=1}^{m} n_i^2 h_q\left(p(g_i)\right) + O(1) \\
&\leq C_m\left(\left(\sum_{i=1}^{m} |n_i|\right)^2 \max_{i=1,\ldots,m} h_q(p(g_i))\right) + O(1) \\
&= C(m, g_1, \ldots, g_m, p, D)\left(\sum_{i=1}^{m} |n_i|\right)^2 + O(1).
\end{aligned}
$$

The constant C_m is the constant constructed in the previous lemma. To conclude take $C_1 := C(m, g_1, \ldots, g_m, p, D)$ and C_2 such that it is an upper bound for the absolute value of $O(1)$. □

Using the inequalities already proven on A it is also possible to find an inequality for the height associated to p^*D for which the dependence on the height of the point is more explicit.

Proposition 2.4.11 ([SC79], compare 2.2 (1))**.** *There exists a constant C only dependent on D and p such that for any $n \in \mathbb{Z} \setminus \{0\}$ and $g \in G(\overline{\mathbb{Q}})$*

$$h_{p^*D}([n]_G g) \leq n^2 C(h_{p^*D}(g) + 1).$$

Proof. Let $C(D,p)$ be the constant as in equation 2.7 in the beginning of the subsection such that for any $g \in G(\overline{\mathbb{Q}})$

$$|h_{p^*D}(g) - h_D(p(g))| \leq C(D,p).$$

Using Lemma 2.3.5 there is a constant $C' \geq 1$ independent of $g \in G(\overline{\mathbb{Q}})$ such that for any $n \in \mathbb{Z} \setminus \{0\}$

$$\begin{aligned} h_{p^*D}([n]_G g) &\leq h_D(p([n]_G(g))) + C(D,p) \\ &= h_D([n]_A p(g)) + C(D,p) \\ &\overset{2.3.5}{\leq} n^2 C'(h_D(p(g)) + 1) + C(D,p) \\ &\leq n^2 C'(h_{p^*D}(g) + C(D,p) + 1) + C(D,p) \\ &\leq n^2 \hat{C}(h_{p^*D}(g) + 1). \end{aligned}$$

Here $\hat{C}$ can be chosen as $C'C(D,p) + C' + C(D,p)$. □

Remark 2.4.12. Analogously to the Remarks 2.3.6 and 2.4.2 the inequality also holds for $n = 0$ if another constant $C_2 := \max\{0, h_{p^*D}(0_G)\}$ is introduced.

The inequality as in Serre for the height associated to $D_{a,b}$

Combining the estimates for G_∞ and p^*D leads to the following theorem, which is Proposition 5 in [SC79].

Theorem 2.4.13 ([SC79], Proposition 5)**.** *Let G be a connected commutative algebraic group defined over $\overline{\mathbb{Q}}$ and let $\psi : G \to \mathbb{P}^l$ be a projective morphism. For $g_1, \ldots, g_m \in G(\overline{\mathbb{Q}})$ there are constants $C_1, C_2 > 0$ such that for all $n_1, \ldots, n_m \in \mathbb{Z}$*

$$h_\psi\left(\sum_{i=1}^m n_i g_i\right) \leq C_1 + C_2 \left(\sum_{i=1}^m |n_i|\right)^2.$$

Proof. Let $g_1, \dots, g_m \in G(\overline{\mathbb{Q}})$ and $n_1, \dots, n_m \in \mathbb{Z}$. For the height associated to $h_{D_{a,b}}$ one has with appropriate constants:

$$\begin{aligned}
h_{D_{a,b}}\left(\sum_{i=1}^m n_i g_i\right) &\le a h_{p^*D}\left(\sum_{i=1}^m n_i g_i\right) + b h_{G_\infty}\left(\sum_{i=1}^m n_i g_i\right) + C(D_{a,b}, a, b, p, D, G_\infty) \\
&\overset{\substack{2.4.10\\2.4.7}}{\le} a\left(C(m, g_1, \dots, g_m, p, D)\left(\sum_{i=1}^m |n_i|\right)^2 + C(p, D)\right) \\
&\quad + b\left(C(G_\infty) + C(g_1, \dots, g_m, G_\infty)\left(\sum_{i=1}^m |n_i|\right)^2\right) + C(D_{a,b}, a, b, p, D, G_\infty) \\
&= C'(a, b, D_{a,b}, p, D, G_\infty) + C'(m, a, g_1, \dots, g_m, G_\infty, p, D)\left(\sum_{i=1}^m |n_i|\right)^2 \\
&=: C_1 + C_2\left(\sum_{i=1}^m |n_i|\right)^2 .
\end{aligned}$$

For general morphisms ψ the statement of Lemma 1.4.25 implies that there are constants $\lambda, \mu \in \mathbb{R}$ such that

$$\begin{aligned}
h_\psi\left(\sum_{i=1}^m n_i g_i\right) &\le \lambda + \mu h_{D_{a,b}}\left(\sum_{i=1}^m n_i g_i\right) \\
&\le \lambda + C_1 + \mu\left(C_2\left(\sum_{i=1}^m |n_i|\right)^2\right) \\
&=: \widetilde{C}_1 + \widetilde{C}_2\left(\sum_{i=1}^m |n_i|\right)^2 .
\end{aligned}$$

□

Corollary 2.4.14. *Let $D \in \mathrm{Div}(\overline{G})$ be a basepoint free divisor. For $g_1, \dots, g_m \in G(\overline{\mathbb{Q}})$ there are constants $C_1, C_2 > 0$ such that for all $n_1, \dots, n_m \in \mathbb{Z}$*

$$h_D\left(\sum_{i=1}^m n_i g_i\right) \le C_1 + C_2\left(\sum_{i=1}^m |n_i|\right)^2 .$$

Proof. Applying Corollary 1.4.26 instead of Lemma 1.4.25 in the situation of the preceding theorem gives the result of this corollary. □

2.5 The second height estimate

This section covers the height estimate which can be found as Proposition 2.0 in the paper [Wüs89] by Wüstholz. The estimate is similar to Proposition 2.4.1 because both estimates have a dependency on the number n by which the element in the group is multiplied.

Since division by an integer n will in general not be a morphism an effective version of the Hilbert Nullstellensatz is used in the proof of the result.

The sources used in this section are [Wüs89], [Mas83] and [Bro87].

2.5.1 The effective Nullstellensatz

In proof of Proposition 2.0 in [Wüs89] the paper [MW81] is cited in the context of showing that a high enough power of a polynomial is contained in some given ideal. The paper covers multiplicity estimates and does not seem to contain the statements which according to the author should be applied in the proof of Proposition 2.0. Because of that it seems reasonable to me to assume that instead [Mas83] was meant to be cited. That paper has a section which contains an effective version of the Hilbert Nullstellensatz and statements which seem to correspond to the ones mentioned in the proof of the proposition.

Proposition 2.5.1 ([Mas83], compare Theorem IV)**.** *Let K be a number field and let the polynomials $Q, P_1, \ldots, P_m \in K[X_1, \ldots, X_n]$ be each of total degree smaller or equal to $d \in \mathbb{N}_{>0}$. If the polynomial Q vanishes in all common zeros of $P_1, \ldots, P_m$ in $\mathbb{C}^n$, there is some integer $e \leq (8d)^{2^{2^{n-1}}}$ and polynomials $A_1, \ldots, A_m \in K[X_1, \ldots, X_n]$ such that*

$$Q^e = \sum_{i=1}^{m} A_i P_i.$$

Since the paper by Masser and Wüstholz was published there have been improvements on the upper bound of e. The bound can be given as exponential instead of doubly exponential in the number of variables. Using such an improved effective Nullstellensatz allows to find slightly better constants in the following subsection.

Proposition 2.5.2 ([Bro87], Corollary p.578)**.** *In the situation of the previous proposition the bound on the constant e can be changed to*

$$(\min\{n, m\} + 1)(n + 2)(d + 1)^{\min\{n,m\}+1}$$

Remark 2.5.3. An even better estimate was found by János Kollár in [Kol88], which bounds e by $d^{\min\{m,n\}}$ for most degrees of polynomials, but there are some assumptions made such that only a limited number of the polynomials may have degree ≤ 2. The author mentions that this is a purely technical assumption and in this case a slightly weaker bound should hold.

The following statement is Lemma 4 of chapter 4 in [Mas83] transcribed to the case of projective heights instead of sizes (i.e. maximal non archimedian absolute value of any coefficient) of algebraic integers.

Lemma 2.5.4 ([Mas83], compare Lemma 4)**.** *Let K be an algebraic number field. Let $p, q \in \mathbb{N}_{>0}$, $a_{ij} \in K$. If the system of linear equations*

$$\begin{gathered} a_{11}X_1 + \ldots + a_{1p}X_p = 0 \\ \vdots \\ a_{q1}X_1 + \ldots + a_{qp}X_p = 0 \end{gathered}$$

has a solution $x_1, \ldots, x_p \in K$ such that $x_t \neq 0$, it has a solution $x'_1, \ldots, x'_p \in K$ such that $x'_t \neq 0$ and

$$h\left([x'_1 : \ldots : x'_p]\right) \leq (p-1)\left(\log(p-1) + h\left([a_{11} : \ldots : a_{qp}]\right)\right).$$

Proof. Lemma 4 in [Mas83] claims that each coordinate of the solution $x'_1, \ldots, x'_p \in K$ is 0 or some r-minor of the system of linear equations (for $1 \leq r \leq q$ the rank of the system). If only one coordinate is non-vanishing or all non-vanishing coordinates are the same up to a factor, the claim on the height is trivial. Let $\delta_1, \ldots, \delta_s$ and $2 \leq s \leq r$ be the different non-trivial r-minors, which equal some coordinate x'_i for an $i \in \{1, \ldots, p\}$, then

$$\begin{aligned} h\left([\delta_1 : \ldots : \delta_s]\right) = h &\left(\left[\sum_{\sigma \in S_r} \operatorname{sgn}(\sigma) a_{i_1^{(1)}\sigma\left(i_1^{(1)}\right)} \cdots a_{i_r^{(1)}\sigma\left(i_r^{(1)}\right)} : \ldots\right.\right. \\ &\qquad \left.\left. \ldots : \sum_{\sigma \in S_r} \operatorname{sgn}(\sigma) a_{i_1^{(s)}\sigma\left(i_1^{(s)}\right)} \cdots a_{i_r^{(s)}\sigma\left(i_r^{(s)}\right)}\right]\right) \\ &\overset{1.4.10}{\leq} \log r! + h\left(\left[a_{i_1^{(1)} i_1^{(1)}} \cdots a_{i_r^{(1)} i_r^{(1)}} : a_{i_1^{(1)} i_2^{(1)}} a_{i_2^{(1)} i_1^{(1)}} \cdots a_{i_r^{(1)} i_r^{(1)}} : \ldots\right.\right. \\ &\qquad \left.\left. \ldots : a_{i_1^{(s)} i_1^{(s)}} \cdots a_{i_r^{(s)} i_r^{(s)}}\right]\right) \\ &\leq \log r^r + h\left([a_{11} \cdots a_{rr} : a_{11} \cdots a_{r-1\,r-1} a_{r+1\,r+1} : \ldots]\right) \\ &\overset{1.4.10}{\leq} r \log r + r h\left([a_{11} : \ldots : a_{qp}]\right) \\ &\leq (p-1)\left(\log(p-1) + h\left([a_{11} : \ldots : a_{qp}]\right)\right). \end{aligned}$$

The claim follows since

$$h([x'_1 : \ldots : x'_p]) \leq h\left([\delta_1 : \ldots : \delta_s].\right).$$

□

2.5.2 The second height estimate dependent on prime factors

This subsection is looking at the proof of Proposition 2.0 in [Wüs89].

I want to thank Prof. Dr. Philip Habegger for answering my questions regarding this proposition. The following is the proof in Wüstholz with some steps altered with the help of Prof. Dr. Habegger.
In one part of the proof Wüstholz claims that some specific polynomial must be contained in an ideal and have coefficients of sufficiently bounded height. The proof I am presenting here instead shows that there exists a collection of polynomials in that ideal with sufficiently bounded heights which additionally have the property of only having nonzero coefficients for some prediscribed monomials. This is a weaker statement than in the original formulation of the proof, but seems to be sufficient to get the desired estimate. I did not manage to understand the step of the proof as it is done by Wüstholz.

Proposition 2.5.5 ([Wüs89], compare Proposition 2.0)**.** *Let G be a commutative connected algebraic group defined over $\overline{\mathbb{Q}}$ and E a very ample divisor on $\overline{G}$. For any $n \in \mathbb{Z} \setminus \{0\}$ there are constants $C_1, C_2 > 0$ such that for any $g \in G(\overline{\mathbb{Q}})$*

$$h_E(g) \leq C_1 |n|^{C_2} (h_E([n]_G g) + 1).$$

Proof. The Lemma 2.2.1 implies that if the inequality holds for one very ample divisor, it holds for all very ample divisors.
Choose $E = D_{a,b}$, the divisor constructed in Corollary 2.1.16. This divisor embeds $\overline{G}$ into some projective space $\mathbb{P}^N$. The coordinates associated to this embedding will be denoted as $x_0, \ldots, x_N$. Identify $\overline{G}$ with its image under the embedding and define $d := \dim G$. Assume without loss of generality that $d \geq 1$, since the claim is trivial otherwise.
Let now $n \in \mathbb{Z} \setminus \{0\}$ be fixed and choose a point $g \in G(\overline{\mathbb{Q}})$. Assume without loss of generality that $x_0(g) \neq 0$.
To show the inequality one shows that it holds for the projective height of each pair of coordinates $[x_0(g) : x_i(g)]$ for $1 \leq i \leq N$. Proposition 1.4.14 implies that

$$h_{D_{a,b}}(g) = h\left([x_0(g) : \ldots : x_N(g)]\right) \leq \sum_{i=1}^{N} h\left([x_0(g) : x_i(g)]\right)$$

and thus, after multiplying the constant C_1 by N, the inequality will hold for the height of g.
The problem is now to show the inequality for the projective heights of these pairs of coordinates. First one notices that if $x_i(g) = 0$ the height $h\left([x_0(g) : x_i(g)]\right) = 0$ and therefore

$$h_{D_{a,b}}(g) = h\left([x_0(g) : \ldots : x_N(g)]\right) \leq \sum_{\substack{i=1 \\ x_i(g) \neq 0}}^{N} h\left([x_0(g) : x_i(g)]\right) \tag{2.8}$$

Now take $1 \leq t \leq N$ such that $x_t(g) \neq 0$.
Any homogeneous polynomial in two variables defined over an algebraically closed field factors into linear polynomials. Thus that a non-trivial homogeneous polynomial B_t in x_0, x_t vanishes in $[x_0(g) : x_t(g)]$ is equivalent to $x_0(g)x_t - x_t(g)x_0$ dividing B_t, i.e. there exists some polynomial Q such that $Q \cdot (x_0(g)x_t - x_t(g)x_0) = B_t$. This allows one to apply Gelfand's inequality (Proposition 1.4.34) and thus

$$\begin{aligned} h\left([x_0(g) : x_t(g)]\right) &= h\left([x_0(g) : -x_t(g)]\right) \\ &= h\left(x_0(g)x_t - x_t(g)x_0\right) \\ &\leq h\left(x_0(g)x_t - x_t(g)x_0\right) + h(Q) \\ &\overset{1.4.34}{\leq} h(B_t) + 2\deg B_t. \end{aligned} \tag{2.9}$$

Hence to show the claim for the pair of coordinates $x_0(g), x_t(g)$ it suffices to find a non-trivial homogeneous polynomial B_t in x_0 and x_t whose height and degree are appropriately bounded by $|n|$ and $h_{D_{a,b}}([n]g)$ such that $B_t(g) = B(x_0(g), x_t(g)) = 0$.

To find such a B_t one starts by defining an auxiliary polynomial R_t in x_0 and x_t which is non-trivial, vanishes in g and has its degree bounded by some power of $|n|$. For this let $g = g^{(1)}, \dots, g^{(\delta)}$ be the points in $G(\overline{\mathbb{Q}})$ such that

$$[n]_G g = [n]_G g^{(i)},$$

in other words,

$$\{g^{(1)}, \dots, g^{(\delta)}\} = [n]_G^{-1}\left([n]_G g\right).$$

Define

$$R_t := x_0 x_t \prod_{\substack{i=1 \\ x_0(g^{(i)}), x_t(g^{(i)}) \neq 0}}^{\delta} \left(x_t(g^{(i)})x_0 - x_0(g^{(i)})x_t\right).$$

By definition, this polynomial is a homogeneous polynomial in two variables which vanishes in $g = g^{(1)}, \dots, g^{(\delta)}$. The condition $x_0(g^{(i)}), x_t(g^{(i)}) \neq 0$ makes sure that R_t is a non-trivial polynomial. But this construction does not give enough information about the height of R_t.

Instead one uses this polynomial to find a different one whose height is controlled. For this the following ideal is needed. Let $\eta_i := x_i\left([n]_G\, g\right)$ for $1 \leq i \leq N$ and let $\varphi_0^{(n)}, \dots, \varphi_N^{(n)}$ be the homogeneous polynomials representing the multiplication-by-n-morphism $[n]_G$ which are constructed in Lemma 2.1.19. They are polynomials in $x_0, \dots, x_N$. One defines

$$f_{ij} = \eta_i \varphi_j^{(n)} - \eta_j \varphi_i^{(n)}.$$

for $1 \leq i, j \leq N$. In G these polynomials only cut out the points $g = g^{(1)}, \ldots, g^{(\delta)}$. Let $P_1, \ldots, P_\chi$ be homogeneous polynomials in $x_0, \ldots, x_N$ which cut out $\overline{G}$. The ideal generated by the f_{ij} and the P_k will be called $\mathcal{I}_{[n]g}$. Using the relations

$$f_{ij} + f_{ji} = 0 \qquad \text{and} \qquad \eta_l f_{ij} + \eta_j f_{li} + \eta_i f_{jl} = 0$$

for any $0 \leq i, j, l \leq N$ the subset of $\{f_{ij}\}_{1 \leq i,j \leq N}$ of the above set of generators of $\mathcal{I}_{[n]g}$ can be replaced by $\{f_{i'j}\}_{j \neq i'}$ for some fixed i' such that $\eta_{i'}$ is not zero. Each of these polynomials is homogeneous of degree n^2. The ideal $\mathcal{I}_{[n]g}$ vanishes at $g = g^{(1)}, \ldots, g^{(\delta)}$ and possibly some at points in $\overline{G} \setminus G = G_\infty$.

Since $G_\infty = \overline{G} \setminus G$ is a closed set in the Zariski topology, we can find a homogeneous polynomial S in $x_0, \ldots, x_N$ which vanishes on all of $\overline{G} \setminus G$ but is nonzero at g. Without loss of generality this S can be chosen as one of a fixed set $S_1, \ldots, S_\xi$ of homogeneous polynomials which generate the ideal associated to $\overline{G} \setminus G$. The polynomial SR_t vanishes at $g = g^{(1)}, \ldots, g^{(\delta)}$ and all of $\overline{G} \setminus G$. Hence the Hilbert Nullstellensatz implies that

$$SR_t \in \sqrt{\mathcal{I}_{[n]g}}.$$

This means that there is some $e \in \mathbb{N}_{>0}$ such that

$$S^e R_t^e = (SR_t)^e \in \mathcal{I}_{[n]g}.$$

The problem of finding all polynomials of a given degree in a homogeneous ideal $\mathcal{J} \subset \overline{\mathbb{Q}}[x_0, \ldots, x_N] =: \mathfrak{R}$ can be viewed as one of linear algebra. Let V be a homogeneous polynomial of degree d. For any $M \in \mathbb{N}$ the homogeneous polynomials of degree M form a $\binom{M+N}{M}$-dimensional vector space $\overline{\mathbb{Q}}[x_0, \ldots, x_N]_M =: \mathfrak{R}_M$. One basis of this vector space are the monomials of degree M. Multiplication by V induces a linear map

$$\begin{aligned} (V\cdot) : \mathfrak{R}_M &\to \mathfrak{R}_{M+d} \\ U &\mapsto V \cdot U. \end{aligned}$$

Analogously, the map defined by the coefficientwise addition of l homogeneous polynomials of the same degree is a linear map

$$\begin{aligned} +_l : \overbrace{\mathfrak{R}_M \times \ldots \times \mathfrak{R}_M}^{l \text{ factors}} &\to \mathfrak{R}_M \\ (U_1, \ldots, U_l) &\mapsto U_1 + \ldots + U_l. \end{aligned}$$

Note that this does not induce a map of the projective spaces. Let $V_1, \ldots, V_l$ be a set of homogeneous generators of $\mathcal{J}$ of degrees $d_1, \ldots, d_l$. If $M \geq \max\{d_1, \ldots, d_l\}$, the following is a well defined linear map:

$$J_M : \mathfrak{R}_{M-d_1} \times \ldots \times \mathfrak{R}_{M-d_l} \xrightarrow{((V_1\cdot), \ldots, (V_l\cdot))} \mathfrak{R}_M \times \ldots \times \mathfrak{R}_M \xrightarrow{+_l} \mathfrak{R}_M.$$

By construction, the image of this map will be the degree-M-part $\mathcal{J}^{(M)} := \mathcal{J} \cap \mathfrak{R}_M$ of $\mathcal{J}$. This implies that the kernel of

$$\begin{aligned}(J_M - Id_M) : \mathfrak{R}_{M-d_1} \times \ldots \times \mathfrak{R}_{M-d_l} \times \mathfrak{R}_M &\to \mathfrak{R}_M \\ (U_1, \ldots, U_l, U) &\mapsto J_M((U_1, \ldots, U_l) - U\end{aligned}$$

contains every polynomial in $\mathcal{J}^{(M)}$ together with the information on how it can be generated by $V_1, \ldots, V_l$.
Analogously, for any homogeneous polynomial V such that $\deg V = d \leq M$ the kernel of the map

$$\begin{aligned}(J_M - (V\cdot)) : \mathfrak{R}_{M-d_1} \times \ldots \times \mathfrak{R}_{M-d_l} \times \mathfrak{R}_{M-d} &\to \mathfrak{R}_M \\ (U_1, \ldots, U_l, U) &\mapsto J_M((U_1, \ldots, U_l) - V \cdot U\end{aligned}$$

contains all the degree-M-multiples of V in $\mathcal{J}$, that is every polynomial in $\mathcal{J}^{(M)}$ which is a multiple of V together with all possibilities of generating each from $V_1, \ldots, V_l$. By looking at the kernel of

$$\begin{aligned}(J_M - (V\cdot)) : \mathfrak{R}_{M-d_1} \times \ldots \times \mathfrak{R}_{M-d_l} \times \overline{\mathbb{Q}}[x_0, x_t]_{M-d} &\to \mathfrak{R}_M \\ (U_1, \ldots, U_l, U) &\mapsto J_M((U_1, \ldots, U_l) - V \cdot U\end{aligned} \tag{2.10}$$

for some $1 \leq t \leq N$ one gets the polynomials homogeneous in x_0, x_t whose V-multiple is contained in $\mathcal{J}^{(M)}$. The last four maps obviously depend on the set of generators chosen for $\mathcal{J}$.

One applies this last linear map (2.10) to S^e, the ideal $\mathcal{I}_{[n]g}$ with the set of generators $\{f_{i'j}, P_k\}_{\substack{0\leq j\leq N,\ j\neq i' \\ 1\leq k\leq \chi}}$, degree $M = e(\deg S + \deg R_t)$ and the coordinate x_t chosen to be the same one as in the definition of R_t. This gives polynomials of the same degree as R_t^e homogeneous in x_0 and x_t such that their product with S^e is in $\mathcal{I}_{[n]g}$.

Choose for each vector space of homogeneous polynomials of a given degree the monomials of this degree as a basis. The linear map defined in the previous paragraph can then be expressed by a matrix M_S whose entries are coefficients of the $f_{i'j}$, the P_k and S^e.

All the polynomials used in the definition of M_S are homogeneous, hence can be rescaled without changing their vanishing locus. Therefore assume without loss of generality that S^e, the $f_{i'j}$ and $P_1, \ldots, P_\chi$ are scaled in such a way that one of the coefficients of each is equal to one. Also note that this scaling does not change the height of any of the polynomials.

Claim. *The height of $M_S = (m_{ij})_{\substack{1\leq i\leq q \\ 1\leq j\leq p}}$ can be bounded by a constant C_{M_S} in the following way*

$$h\left([m_{11} : \ldots : m_{pq}]\right) \leq N h_{D_{a,b}}(g) + eC_{M_S}. \tag{2.11}$$

The constant $C_{M_S} \geq 1$ depends C_{M_S} depends on $S_1, \ldots, S_\xi, P_1, \ldots, P_\chi$, $\varphi_0^{(n)}, \ldots, \varphi_N^{(n)}$ and N. Hence it is dependent on n, the divisor $D_{a,b}$ and the geometry of G.

Proof. Let $M_S = (m_{ij})_{\substack{1\le i\le q\\ 1\le j\le p}}$ for some $p, q \in \mathbb{N}_{>0}$. By the definition of M_S any its entries is 0 or a coefficient of one of the $f_{i'j}$ for $0 \le i, j \le N$, one of $P_1, \ldots, P_\chi$ or S^e. Since omitting zeros or doubled coordinates does not change the height of a projective point one has

$$h\left([m_{11} : \ldots : m_{pq}]\right) = h\left([S^e : P_1 : \ldots : P_\chi : f_{i'0} : \ldots : f_{i'N}]\right)$$

Since each of the polynomials has at least one coefficients equal to one, a repeated application of Proposition 1.4.15 gives

$$h\left([S^e : P_1 : \ldots : P_\chi : f_{i'0} : \ldots : f_{i'N}]\right) \le h\left(S^e\right) + \sum_{\substack{j=0\\ j\neq i'}}^{N} h\left(f_{i'j}\right) + \sum_{k=1}^{\chi} h\left(P_k\right) \tag{2.12}$$

Applying Proposition 1.4.35 to $h(S^e)$ one has that

$$h(S^e) \le e\left(h(S) + (\deg S + N + 1)\log 2\right). \tag{2.13}$$

The height of the $f_{i'j}$ can be bounded in the following way:

$$\begin{aligned} h(f_{i'j}) &= h(\eta_{i'}\varphi_j^{(n)} - \eta_j\varphi_{i'}^{(n)}) \\ &\overset{1.4.10}{\le} h([\eta_{i'}\varphi_j^{(n)} : \eta_j\varphi_{i'}^{(n)}]) + \log 2 \\ &\overset{1.4.10}{\le} h([\eta_{i'} : \eta_j]) + h([\varphi_j^{(n)} : \varphi_{i'}^{(n)}]) + \log 2 \\ &\le h([\eta_0 : \ldots : \eta_N]) + h([\varphi_0^{(n)} : \ldots : \varphi_N^{(n)}]) + \log 2 \\ &= h_{D_{a,b}}(g) + h([\varphi_0^{(n)} : \ldots : \varphi_N^{(n)}]) + \log 2. \end{aligned} \tag{2.14}$$

Combining these inequalities gives

$$\begin{aligned} h\left([m_{11} : \ldots : m_{pq}]\right) =& h\left([S^e : P_1 : \ldots : P_\chi : f_{i'0} : \ldots : f_{i'N}]\right) \\ &\overset{(2.12)}{\le} h\left(S^e\right) + \sum_{\substack{j=0\\ j\neq i'}}^{N} h\left(f_{i'j}\right) + \sum_{k=1}^{\chi} h\left(P_k\right) \\ &\overset{(2.13)}{\le} e\left(h(S) + (\deg S + N + 1)\log 2\right) + \sum_{\substack{j=0\\ j\neq i'}}^{N} h\left(f_{i'j}\right) + \sum_{k=1}^{\chi} h\left(P_k\right) \\ &\overset{(2.14)}{\le} e\left(h(S) + (\deg S + N + 1)\log 2\right) \\ &\quad + N\left(h_{D_{a,b}}(g) + h([\varphi_0^{(n)} : \ldots : \varphi_N^{(n)}]) + \log 2\right) + \sum_{k=1}^{\chi} h\left(P_k\right) \\ &\overset{e\ge 1}{\le}: N h_{D_{a,b}}(g) + eC(N, P_1, \ldots, P_\chi, S, \varphi_0^{(n)}, \ldots, \varphi_N^{(n)}) \end{aligned}$$

Since S was chosen to be one of the polynomials in the fixed set $S_1, \ldots, S_\xi$ which cuts out $\overline{G} \setminus G$ the constant $C(N, P_1, \ldots, P_\chi, S, \varphi_0^{(n)}, \ldots, \varphi_N^{(n)})$ can be replaced by one depending on $\varphi_0^{(n)}, \ldots, \varphi_N^{(n)}$, N, $S_1, \ldots, S_\xi$, and $P_1, \ldots, P_\chi$ (by substituting $h(S) + \log 2 \deg S$ with $\max_{1 \le c \le \xi} (h(S_c) + \log 2 \deg S_c))$. The constant is bigger than 1 since all summands in the constant are positive and already

$$e(N+1)\log 2 \ge (N+1)\log 2 \ge 2\log 2 = \log 4 \ge 1.$$

□

Claim. *The matrix M_S has at most*

$$e^N |n|^{2Nd} C_p + 1 \tag{2.15}$$

rows. Here $C_p \ge 1$ is a constant only depending on $N, S_1, \ldots, S_\xi$ and χ. Hence C_p only depends the geometry of G and $D_{a,b}$.

Proof. The number of rows of M_S is the sum of the dimensions of the vector spaces of homogeneous polynomials of degrees $e(\deg S + \deg R_t) - \deg f_{i'j}$ for $0 \le j \le N$ and $j \ne i'$ as well as $e(\deg S + \deg R_t) - \deg P_k$ for $1 \le k \le \chi$ in $N+1$ variables and the dimension of the vector space of homogeneous $e \deg R_t$ polynomials in 2 variables. The degree of R_t is bounded by $\delta + 2$. Using Corollary 1.3.43 we get $\delta \le |n|^{2d}$ and $\deg R_t \le |n|^{2d} + 2$. Since S was chosen to be one of $S_1, \ldots, S_\xi$ we have $\deg S \le \max_{1 \le c \le \xi} \deg S_c$. Therefore we have that

$$\begin{aligned}
\dim \mathfrak{R}_{e(\deg S + \deg R_t) - \deg f_{i'j}} &= \binom{e(\deg S + \deg R_t) - \deg f_{i'j} + N}{N} \\
&\le \binom{e\left(\max_{1 \le c \le \xi} \deg S_c + |n|^{2d} + 2\right) - \deg f_{i'j} + N}{N} \\
&\le \binom{e\left(\max_{1 \le c \le \xi} \deg S_c + |n|^{2d} + 2\right) + N}{N}.
\end{aligned}$$

Analogously

$$\begin{aligned}
\dim \mathfrak{R}_{e(\deg S + \deg R_t) - \deg P_k} &= \binom{e(\deg S + \deg R_t) - \deg P_k + N}{N} \\
&\le \binom{e\left(\max_{1 \le c \le \xi} \deg S_c + |n|^{2d} + 2\right) - \deg P_k + N}{N} \\
&\le \binom{e\left(\max_{1 \le c \le \xi} \deg S_c + |n|^{2d} + 2\right) + N}{N}
\end{aligned}$$

and

$$\dim \overline{\mathbb{Q}}[x_0, x_t]_{e \deg R_t} = \binom{e \deg R_t + 1}{1} \le \binom{e(|n|^{2d} + 2) + 1}{1} = e(|n|^{2d} + 2) + 1.$$

For any integers $u, v \geq 0$ one has

$$\binom{u+v}{v} = \frac{(u+v)(u+v-1)\cdots(u+1)}{v!} = \frac{u+v}{v}\cdots\frac{u+1}{1} \leq (u+1)^v. \tag{2.16}$$

Therefore

$$\begin{aligned}
p = &\sum_{\substack{j=0\\ j\neq i'}}^{N} \dim \mathfrak{R}_{e(\deg S+\deg R_t)-\deg f_{i'j}} + \sum_{k=1}^{\chi} \dim \mathfrak{R}_{e(\deg S+\deg R_t)-\deg P_k} + \dim \overline{\mathbb{Q}}[x_0, x_t]_{e \deg R_t} \\
\leq &N \cdot \binom{e\left(\max_{1\leq c\leq \xi} \deg S_c + |n|^{2d} + 2\right) + N}{N} \\
&+ \chi \cdot \binom{e\left(\max_{1\leq c\leq \xi} \deg S_c + |n|^{2d} + 2\right) + N}{N} + e(n^{2d}+2) + 1 \\
\overset{(2.16)}{\leq} &N \cdot \left(e\left(\max_{1\leq c\leq \xi} \deg S_c + |n|^{2d} + 2\right) + 1\right)^N \\
&+ \chi\left(e\left(\max_{1\leq c\leq \xi} \deg S_c + |n|^{2d} + 2\right) + 1\right)^N + e(|n|^{2d}+2) + 1 \\
\overset{e,N\geq 1}{\leq} &e^N\left((N+\chi)\cdot\left(\max_{1\leq c\leq \xi} \deg S_c + |n|^{2d} + 3\right)^N + |n|^{2d} + 2\right) + 1
\end{aligned}$$

To pull the powers of $|n|$ to the front one uses that for any integers $u, v, w \in \mathbb{N}_{>0}$ the inequality

$$(uv+w)^N = u^N\left(v + \frac{w}{u}\right)^N \leq \ u^N(v+w)^N \tag{2.17a}$$

holds.

$$\begin{aligned}
\overset{(2.17a)}{\leq} &e^N\left((N+\chi)\cdot|n|^{2dN}\cdot\left(\max_{1\leq c\leq \xi} \deg S_c + 4\right)^N + |n|^{2d} + 2\right) + 1 \\
\overset{N\geq 1}{\leq} &e^N\left(|n|^{2dN}\left((N+\chi)\cdot\left(\max_{1\leq c\leq \xi} \deg S_c + 4\right)^N + 1\right) + 2\right) + 1 \\
\overset{(2.17a)}{\leq} &e^N|n|^{2dN}\left((N+\chi)\cdot\left(\max_{1\leq c\leq \xi} \deg S_c + 4\right)^N + 3\right) + 1 \\
:= &e^N|n|^{2dN}C(S_1, \ldots, S_c, N, \chi) + 1.
\end{aligned}$$

□

Claim. *The exponent e in the Hilbert Nullstellensatz can be chosen smaller than*

$$|n|^{2d(N+2)}C_e \tag{2.18}$$

where C_e is a constant depending on $S_1, \ldots, S_\xi, P_1, \ldots, P_\chi$ and N. Hence C_e depends on $D_{a,b}$ and the geometry of G.

Proof. This is an application of the effective Nullstellensatz by Brownawell (Proposition 2.5.2). We have polynomials in $N+1$ variables and the set of generators for the ideal $\mathcal{I}_{[n]g}$ we have chosen earlier has $N+\chi$ elements. As a bound for the degrees of the polynomials we choose the maximum of their degrees. Therefore

$$\begin{aligned}
e &\overset{2.5.2}{\leq} (\min\{N+1, N+\chi\}+1)\,(N+3) \\
&\quad\cdot\left(\max_{\substack{0\leq j\leq N,\ j\neq i'\\ 1\leq k\leq\chi}}\{\deg f_{i'j}, \deg P_k, \deg S+\deg R_t\}+1\right)^{\min\{N+1,N+\chi\}+1} \\
&= (\min\{N+1, N+\chi\}+1)\,(N+3) \\
&\quad\cdot\left(\max_{1\leq k\leq\chi}\{|n|^2, \deg P_k, \deg S+\deg R_t\}+1\right)^{\min\{N+1,N+\chi\}+1} \\
&\leq (N+2)(N+3)\left(\max_{1\leq k\leq\chi}\{|n|^2, \deg P_k, \deg S+|n|^{2d}+2\}+1\right)^{N+2} \\
&\overset{\deg S\geq 0}{\leq} (N+2)(N+3)\left(\max_{1\leq k\leq\chi}\{\deg P_k, \deg S+|n|^{2d}+2\}+1\right)^{N+2} \\
&\leq (N+2)(N+3)\left(\max_{1\leq k\leq\chi}\{\deg P_k, \deg S\}+|n|^{2d}+3\right)^{N+2} \\
&\leq (N+2)(N+3)\left(\max_{\substack{1\leq c\leq\xi\\ 1\leq k\leq\chi}}\{\deg P_k, \deg S_c\}+|n|^{2d}+3\right)^{N+2} \\
&\overset{(2.17a)}{\leq} |n|^{2d(N+2)}(N+2)(N+3)\left(\max_{\substack{1\leq c\leq\xi\\ 1\leq k\leq\chi}}\{\deg P_k, \deg S_c\}+4\right)^{N+2} \\
&=: |n|^{2d(N+2)}C(P_1,\ldots,P_\chi,S_1,\ldots,S_\xi,N)
\end{aligned}$$

□

We know that a vector y made up of R_t^e viewed as a point in $\overline{\mathbb{Q}}[x_0,x_t]_{e\deg R_t}$ together with some polynomials which are used as coefficients to generate $S^eR_t^e$ from the $f_{i'j}$ and $P_1,\ldots,P_\chi$ is a non-trivial solution of the homogeneous linear system of equations $M_Sy=0$. With the bounds found in the claims above, we can now apply Lemma 2.5.4 to this linear system of equations and (since R_t^e was non-trivial) get some non-trivial Polynomial B in x_0,x_t (as well coefficients polynomials for some way to write S^eB as a combination of the

$f_{i'j}$ and $P_1, \ldots, P_\chi$, which we will not need) such that

$$
\begin{aligned}
h(B) &\overset{2.5.4}{\leq} (p-1)\left(\log(p-1) + h\left([m_{11} : \ldots : m_{pq}]\right)\right) \\
&\leq \max\{1, p-1\}^2 \left(1 + h\left([m_{11} : \ldots : m_{pq}]\right)\right) \\
&\overset{(2.15)}{\leq} \left(e^N |n|^{2dN} C_p\right)^2 \left(1 + h\left([m_{11} : \ldots : m_{pq}]\right)\right) \\
&\overset{C_p \geq 1}{=} e^{2N} |n|^{4dN} C_p^2 \left(1 + h\left([m_{11} : \ldots : m_{pq}]\right)\right) \\
&\overset{(2.11)}{\leq} e^{2N} |n|^{4dN} C_p^2 \left(1 + N h_{D_{a,b}}(g) + e C_{M_S}\right) \\
&\overset{e, N \geq 1}{\leq} e^{2N+1} |n|^{4dN} (N C_p^2) \left(h_{D_{a,b}}(g) + (1 + C_{M_S})\right) \\
&\overset{C_{M_s} > 0}{\leq} e^{2N+1} |n|^{4dN} (N C_p^2)(1 + C_{M_S}) \left(h_{D_{a,b}}(g) + 1\right) \\
&\overset{(2.18)}{\leq} \left(|n|^{2d(N+2)} C_e\right)^{2N+1} |n|^{4dN} (N C_p^2)(1 + C_{M_S}) \left(h_{D_{a,b}}(g) + 1\right) \\
&= |n|^{2d(N+2)(2N+1)+4dN} \left(C_e^{2N+1} (N C_p^2)(1 + C_{M_S})\right) \left(h_{D_{a,b}}(g) + 1\right) \\
&=: |n|^{2d((N+2)(2N+1)+2N)} C(N, P_1, \ldots, P_\chi, S_1, \ldots, S_\xi, \varphi_0^{(n)}, \ldots, \varphi_N^{(n)}) \left(h_{D_{a,b}}(g) + 1\right).
\end{aligned}
\tag{2.19}
$$

The polynomial B_t therefore fulfils a height inequality of the form we want and is a homogeneous polynomial in x_0 and x_t. Its degree is bounded by

$$
\begin{aligned}
\deg B_t &= \deg R_t^e \\
&= e \deg R_t \\
&\leq e(\delta + 2) \\
&\leq e(|n|^{2d} + 2) \\
&\overset{(2.18)}{\leq} |n|^{2d(N+2)} C_e (|n|^{2d} + 2) \\
&\overset{|n|^{2d} \geq 1}{\leq} |n|^{2d((N+2)+1)} 3 C_e
\end{aligned}
\tag{2.20}
$$

The last inequality holds since $\delta \leq |n|^{2d}$ (for d dimension of G) due to Corollary 1.3.43. Hence, for B_t to be a polynomial we can use to estimate the height of $[x_0(g) : x_t(g)]$ the only thing left to show is that $B_t(g) = 0$. But this the case since by construction $S^e B_t(g) = 0$ and $S^e(g) \neq 0$. Therefore

$$
\begin{aligned}
h\left([x_0(g) : x_t(g)]\right) &\overset{(2.9)}{\leq} h(B_t) + 2 \deg B_t \\
&\leq h(B_t) + 6 |n|^{2d((N+2)+1)} C_e \\
&\leq |n|^{2d((N+2)(2N+1)+2N)} \left(C_e^{2N+1} (N C_p^2)(1 + C_{M_S})\right) \left(h_{D_{a,b}}(g) + 1\right) \\
&\quad + 6 |n|^{2d((N+2)+1)} C_e \\
&\leq |n|^{2d((N+2)(2N+1)+2N)} \left(C_e^{2N+1} (N C_p^2)(1 + C_{M_S}) + 1\right) \left(h_{D_{a,b}}(g) + 1\right)
\end{aligned}
\tag{2.21}
$$

Using (2.8) we get

$$
\begin{aligned}
h(g) &\overset{(2.8)}{\leq} \sum_{\substack{i=1\\ x_i(g)\neq 0}}^{N} h\left([x_0(g) : x_i(g)]\right) \\
&\overset{(2.21)}{\leq} \sum_{\substack{i=1\\ x_i(g)\neq 0}}^{N} |n|^{2d((N+2)(2N+1)+2N)} \left(C_e^{2N+1}(NC_p^2)(1+C_{M_S})+1\right)\left(h_{D_{a,b}}(g)+1\right) \\
&\leq N\left(|n|^{2d((N+2)(2N+1)+2N)}\left(C_e^{2N+1}(NC_p^2)(1+C_{M_S})+1\right)\left(h_{D_{a,b}}(g)+1\right)\right) \\
&= |n|^{2d((N+2)(2N+1)+2N)}\left(NC_e^{2N+1}(NC_p^2)(1+C_{M_S})+1\right)\left(h_{D_{a,b}}(g)+1\right) \\
&=: |n|^{C(d,N)}C(N,S_1,\ldots,S_\xi,P_1,\ldots,P_\chi,\varphi_0^{(n)},\ldots,\varphi_N^{(n)})\left(h_{D_{a,b}}(g)+1\right)
\end{aligned}
$$

which is the desired inequality. □

Remark 2.5.6. The above proof differs from the one in [Wüs89] in the definition of R_t and the S. Wüstholz takes R_t to be the product of the coordinates of all $g^{(1)},\ldots,g^{(\delta)}$ and chooses $\mu := x_0\cdots x_N$ as S for any g.

The idea of applying the fact that there is a homogeneous polynomial in two variables can be used to bound the height of its zeros to a polynomial obtained like B_t was suggested by Professor Habegger.

Corollary 2.5.7 ([Wüs89], compare Proposition 2.0)**.** *Let G be a commutative connected algebraic group defined over $\overline{\mathbb{Q}}$ and E a very ample divisor on $\overline{G}$. For any $n\in\mathbb{Z}\setminus\{0\}$ there are constants $C_1, C_2 > 0$ such that for any $m\in\mathbb{N}_0$ and $g\in G(\overline{\mathbb{Q}})$*

$$h_E(g) \leq C_1|n|^{mC_2}(h_E([n^m]_G g)+1).$$

Proof. The case $n = 1$ is trivial. Hence assume $|n| \geq 2$. Let $\widetilde{C}_1,\ \widetilde{C}_2$ be the constants $C_1,\ C_2$ obtained from Proposition 2.5.5. Set

$$
\begin{aligned}
C_1 &:= \max(\widetilde{C}_1, 1)\\
C_2 &:= \widetilde{C}_2 + C' + 1
\end{aligned}
$$

Here $C' > 0$ is a constant chosen such that $|n|^{C'} \geq C_1$.
$\mathbf{m = 0}$: In this case $[n^0]_G g = [1]_G g = g$. The statement follows from

$$h(g) = h([n^0]_G g) < h([n^0]_G g) + 1 \leq C_1|n|^{0\cdot C_2}(h(g)+1)$$

$\mathbf{m = 1}$: This is the statement of Proposition 2.5.5

$$h(g) \leq \widetilde{C}_1|n|^{\widetilde{C}_2}\left(h([n]_G g)+1\right) \leq C_1 l^{1\cdot C_2}\left(h([n^1]_G g)+1\right)$$

$\mathbf{m \geq 2}$: Assume the statement holds for a given $m \geq 1$.

$$
\begin{aligned}
h(g) &\overset{IH}{\leq} C_1|n|^{mC_2}(h([n^m]_G g) + 1) \\
&\overset{2.5.5}{\leq} C_1|n|^{mC_2}(\widetilde{C}_1|n|^{\widetilde{C}_2}(h([n^{m+1}]_G g) + 1) + 1) \\
&= C_1\widetilde{C}_1|n|^{mC_2+\widetilde{C}_2}h([n^{m+1}]_G g) + C_1|n|^{mC_2}(\widetilde{C}_1|n|^{\widetilde{C}_2} + 1) \\
&\overset{\widetilde{C}_1 \leq |n|^{C'}}{\leq} C_1|n|^{C'}|n|^{\widetilde{C}_2+mC_2}h([n^{m+1}]_G g) + C_1|n|^{mC_2}(|n|^{C'}|n|^{\widetilde{C}_1} + 1) \\
&= C_1|n|^{C'+\widetilde{C}_2+mC_2}h([n^{m+1}]_G g) + C_1|n|^{mC_2}\left(|n|^{C'+\widetilde{C}_1} + 1\right) \\
&\overset{|n|>1}{\leq} C_1|n|^{C'+\widetilde{C}_2+mC_2}h([n^{m+1}]_G g) + C_1|n|^{mC_2}|n|^{C'+\widetilde{C}_1+1} \\
&\leq C_1|n|^{C_2+mC_2}h([n^{m+1}]_G g) + C_1|n|^{mC_2+C_2} \\
&= C_1|n|^{(m+1)C_2}(h([n^{m+1}]_G g) + 1)
\end{aligned}
$$

□

Corollary 2.5.8. *Let G be a commutative connected algebraic group defined over $\overline{\mathbb{Q}}$ and E a very ample divisor on $\overline{G}$. For any $n \in \mathbb{Z} \setminus \{0\}$ there are constants $C_1, C_2 > 0$ only dependent on the prime factors of n such that for any $g \in G(\overline{\mathbb{Q}})$*

$$h_E(g) \leq C_1|n|^{C_2}(h_E([n]_G g) + 1).$$

Proof. This follows immediately from the previous corollary. □

Bibliography

[Bor91] Armand Borel. *Linear Algebraic Groups*. Springer New York, 1991.

[Bro87] W. Dale Brownawell. “Bounds for the Degrees in the Nullstellensatz”. In: *Annals of mathematics* 126.3 (1987), pp. 577–591.

[BSU13] Michel Brion, Preena Samuel, and V. Uma. *Lectures on the structure of algebraic groups and geometric applications*. Vol. 1. CMI Lecture Series in Mathematics. Hindustan Book Agency (India), 2013. ISBN: 978-93-86279-58-3.

[BW08] A. Baker and G. Wüstholz. *Logarithmic Forms and Diophantine Geometry*. Cambridge University Press, 2008. ISBN: 9780511542862.

[FH85] Knop F. and Lange H. “Some remarks on the compactification of commutative algebraic groups”. In: *Commentarii mathematici helvetici* 60 (1985), pp. 497–507.

[FL84] Knop F. and H. Lange. “Commutative algebraic groups and intersections of quadrics”. In: *Mathematische Annalen* 267.4 (Dec. 1984), pp. 555–571.

[GW10] Ulrich Görtz and Torsten Wedhorn. *Algebraic Geometry I - Schemes, With Examples and Exercises*. Ed. by Ulrike Schmickler-Hirzebruch. 1st ed. Vieweg + Teubner, 2010. ISBN: 978-3-8348-0676-5.

[Har77] Robin Hartshorne. *Algebraic Geometry*. 1st ed. Springer New York, 1977. ISBN: 978-1-4757-3849-0.

[HS00] Marc Hindry and Joseph H. Silverman. *Diophantine Geometry*. 1st ed. Springer New York, 2000. ISBN: 978-0-387-98981-5.

[Hub21] Annette Huber-Klawitter. *The analytic subgroup theorem*. lecture notes. Feb. 2021.

[Kol88] János Kollár. “Sharp effective Nullstellensatz”. In: *Journal of the American Mathematical Society* 1.4 (Oct. 1988), pp. 963–975.

[Lan94] Serge Lang. *Algebraic Number Theory*. 2nd ed. Springer New York, 1994. ISBN: 978-1-4612-0853-2.

[Mas83] D.W. ; Wüsteholz G. Masser. “Fields of Large Transcendence Degree generated by Values Of Elliptic Functions”. In: *Inventiones Mathematicae* 72 (Oct. 1983), pp. 407–464.

[Mat70] Hideyuki Matsumara. *Commutative Algebra.* W. A. Benjamin, Inc., 1970.

[MFK94] David Mumford, John Fogarty, and Frances Kirwan. *Geometric invariant theory.* 3rd ed. Springer-Verlag Berlin Heidelberg, 1994. ISBN: 978-0-387-56963-4.

[Mil13] James S. Milne. *A Proof of the Barsotti-Chevalley Theorem on Algebraic Groups.* 2013.

[Mil15] James S. Milne. *Algebraic Groups -The theory of group schemes of finite type over a field.* Version 2.0, preliminary. Dec. 2015.

[Mum70] David Mumford. *Abelian Varieties.* 1970.

[Mum76] David Mumford. *Algebraic Geometry I. Complex Projective Varieties.* Springer-Verlag, 1976.

[MW81] D. W. Maser and G. Wüstholz. “Zero estimates on group varieties I”. In: *Inventiones mathematicae* 64 (1981), pp. 489–516.

[Ros56] Maxwell Rosenlicht. “Some Basic Theorems on Algebraic Groups”. In: *American Journal of Mathematics* 78.2 (Apr. 1956), pp. 401–443.

[SC79] Jean-Pierre Serre and Collectif. “Appendice II : Quelques propriétés des groupes algébriques commutatifs”. fr. In: *Nombres transcendants et groupes algébriques.* Astérisque 69-70. Société mathématique de France, 1979.

[Ser97] Jean-Pierre Serre. *Algebraic Groups and Class Fields.* 2nd ed. Graduate Texts in Mathematics 117. Springer Science + Business Media New York, 1997. ISBN: 978-1-4612-1035-1.

[Sha13a] Igor R. Shafarevich. *Basic Algebraic Geometry 1.* Springer Berlin Heidelberg, 2013. ISBN: 978-3-642-37956-7.

[Sha13b] Igor R. Shafarevich. *Basic Algebraic Geometry 2.* Springer Berlin Heidelberg, 2013.

[Spr98] T. A. Springer. *Linear Algebraic Groups.* Birkhäuser Boston, 1998. ISBN: 978-0-8176-4840-4.

[Staa] Stacks. https://stacks.math.columbia.edu/tag/01VG. Last accessed: 16.02.2023.

[Stab] Stacks. https://stacks.math.columbia.edu/tag/01PR. Last accessed: 16.02.2023.

[Wüs84] Gerd Faltings; Gisbert Wüstholz. “Einbettungen kommutativer algebraischer Gruppen und einige ihrer Eigenschaften”. In: *Journal für reine und angewandte Mathematik* 1984.354 (1984), pp. 175–205.

[Wüs89] Gisbert Wüstholz. “Algebraische Punkte auf Analytischen Untergruppen algebraischer Gruppen”. In: *Annals of Mathematics* 129.3 (May 1989), pp. 501–517.