new mathematical monographs: 4

Heights in Diophantine Geometry

Enrico Bombieri and
Walter Gubler

CAMBRIDGE

CAMBRIDGE www.cambridge.org/9780521846158

This page intentionally left blank

Heights in Diophantine Geometry

The first half of the book is devoted to the general theory of heights and its applications, including a complete, detailed proof of the celebrated subspace theorem of W. M. Schmidt. The second part deals with abelian varieties, the Mordell–Weil theorem and Faltings's proof of the Mordell conjecture, ending wih a self-contained exposition of Nevanlinna theory and the related famous conjectures of Vojta. The book concludes with a comprehensive list of references. It is destined to be a definitive reference book on modern diophantine geometry, bringing a new standard of rigor and elegance to the field.

Professor ENRICO BOMBIERI is a professor of Mathematics at the Institute of Advanced Study, Princeton.

Dr WALTER GUBLER is a lecturer in Mathematics at the University of Dortmund.

New Mathematical Monographs

Editorial Board

For information about Cambridge University Press mathematics publications visit http://publishing.cambridge.org/stm/mathematics/

HEIGHTS IN DIOPHANTINE GEOMETRY

Enrico Bombieri
Institute of Advanced Study, Princeton

Walter Gubler
University of Dortmund

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 2RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521846158

First published in print format 2006

ISBN-13 978-0-511-13809-6 eBook (Adobe Reader)
ISBN-10 0-511-13809-1 eBook (Adobe Reader)

ISBN-13 978-0-521-84615-8 hardback
ISBN-10 0-521-84615-3 hardback

Contents

Preface

Diophantine geometry, the study of equations in integer and rational numbers, is one of the oldest subjects of mathematics and possibly the most popular part of number theory, for the professional mathematician and the amateur alike. Certainly, one of its main attractions is that, far from being a disconnected assembly of isolated results, it provides glimpses of a view which hints at a well-organized underlying structure.

Diophantine equations are of course determined by the underlying algebraic equations and therefore their associated algebraic geometry, obtained by dropping the condition that the solutions must be integers or rational numbers, plays a big role in their study. However, algebraic geometry is already not an easy subject. A pioneer and one of the founding fathers of algebraic geometry, the German mathematician Max Noether, after seeing the theory of algebraic curves with its elegance, simplicity, and also depth of results, and comparing it with the collection of the existing examples of algebraic surfaces at the time, for which nothing comparable could be found, used to say that algebraic curves were created by God and algebraic surfaces by the Devil. Only later, with the development of new tools, in particular the introduction of cohomological and topological methods, the theory of surfaces and higher-dimensional varieties over a field found a satisfactory status.

Of special importance for arithmetic was the development of algebraic geometry over fields of positive characteristic and p-adic fields, since the study of polynomial congruences leads very naturally to such problems. The next big step, the study of varieties over general rings (in contrast to fields), was done by Grothendieck in his monumental construction of the theory of schemes. This provided the basic setting for the study of diophantine equations from a geometric point of view. Bits and pieces of a theory were provided at an early stage (Weil's proof of the Mordell–Weil theorem is possibly the first example) and Weil's theory of heights, with its good arithmetic and geometric properties, was for a long time the main tool. However, the development of a consistent theory was hindered by two major obstacles.

An algebraic curve X over, for example, the ring $\mathbb{Z}$ of rational integers is, from the point of view of schemes, a two-dimensional object, an arithmetic surface, endowed with a morphism $f : X \to \mathrm{Spec}(\mathbb{Z})$. Ideally, we would like to find an

analogue of the classical theory of algebraic surfaces which applies in this arithmetic setting.

This can be done only to some extent. First of all, global results require working with complete varieties, and a first problem was to compactify $\mathrm{Spec}(\mathbb{Z})$ and develop a good intersection theory for divisors. This step was brilliantly solved by Arakelov, using adeles and introducing metrics on the "fibre at infinity." Arakelov's work can be regarded as the start of a beautiful new theory, aptly named "arithmetic geometry." As an example, in arithmetic geometry the theory of heights is a special chapter of the much more precise arithmetic intersection theory.

Arakelov's theory did not solve all problems and major questions remain. In the "horizontal direction" given by the base $\mathrm{Spec}(\mathbb{Z})$, infinitesimal methods are no longer at our disposal and genuine new difficulties, with no counterpart in the classical theory, do appear. This is one of the major stumbling blocks for further progress. Thus at the present stage we may take a view half-way towards Max Noether's view: Arithmetic surfaces were also created by God, but their study encounters devilish difficulties.

Today, there are already good books devoted to the subject, and we can mention here Lang's [**169**], Serre's [**277**], the more expository but very comprehensive account of Lang's [**171**] and Hindry and Silverman's [**153**]. So, why a new book on diophantine geometry?

As is often the case, this book grew from introductory lectures at the graduate level, given over a decade ago at the Scuola Normale Superiore di Pisa and the Mathematisches Forschungsinstitut of the Eidgenössische Technische Hochschule in Zürich. An advanced knowledge of algebra or algebraic geometry was not a prerequisite of the courses. Thus the subject was developed mainly through classical lines, namely the theory of varieties over fields of characteristic 0 insofar as algebraic geometry was concerned, and the theory of heights for the number theoretic aspects.

Already with the initial rough notes, embracing the view that in order to learn tools it is best to use them in practice, it was decided to keep mathematical rigor as a strict requirement, supplying references whenever needed and making a clear distinction between a proof and a plausible argument. Examples, including unusual ones, and advanced sections in which deeper aspects of the theory were either developed or described, were included whenever possible. Rather than including this type of material as "exercises" at various levels of difficulty, often disguising good research papers as exercises, it was decided to include proofs and extended comments also for them. However, in the time needed to put the original material together, the subject matter continued to advance at a fast pace, whence the need for inclusion of additional interesting material, as well as substantial revisions of what had been done before.

In the final product, this book is basically divided into three parts. Chapters 1 to 7 develop the elementary theory of heights and its applications to the diophantine geometry of subvarieties of the split torus $\mathbb{G}_m^n$, including applications to diophantine approximation with proofs of Roth's theorem and Schmidt's subspace theorem and some unusual applications.

Chapters 8 to 11 deal with abelian varieties and the diophantine geometry of their subvarieties, ending with a detailed proof of Faltings's celebrated theorem establishing Mordell's conjecture for curves, following Vojta's proof as simplified in [**29**]. However, we felt that a proper treatment of Faltings's big theorem, namely his proof of Lang's conjectures about rational points on subvarieties of abelian varieties, was best done in the context of arithmetic geometry and with regrets we limited ourselves on this matter only to a few comments about the theorem itself and to some of its applications.

Chapters 12 to 14 are more speculative and at times straddle the borderline between diophantine geometry and arithmetic geometry. Chapter 12 deals with the so-called abc-conjecture over number fields, including a complete proof of Belyĭ's theorem and its application to Elkies's theorem, various examples, concluding with a finiteness result for the generalized Fermat equation, due to Darmon and Granville. Chapter 13, which is largely self contained, is an exposition of the classical Nevanlinna theory, with proofs of the first and second main theorems of Nevanlinna, and also Cartan's extension of them to the theory of meromorphic curves. Its purpose is to motivate the final Chapter 14 dealing with the well-known Vojta conjectures, which have spurred a great deal of work in the field.

Proofs are usually given in full detail, but of course it was not feasible to develop all algebra and algebraic geometry from scratch and they tend to be fairly condensed at times. To alleviate this, Appendix A summarizes all concepts of algebraic geometry needed in this book and Appendix B gathers the necessary facts about ramification in number theory and algebraic geometry. Both are provided with complete references to standard books and should help the reader in understanding which notions and notations we use. Finally Appendix C contains an account of Minkowski's geometry of numbers, with proofs, at least to the extent we need in this book.

Some sections in this book appear in small print. Their meaning is simply that they can be omitted in a first reading, either because they require more advanced knowledge of algebra and geometry, or because they deal with side topics not appearing elsewhere in the book. At the end of every chapter, the reader will find some bibliographical notes, containing both historical comments and references to additional literature. However, in no way do these references pretend to be complete and they only represent our personal choices for additional reading.

This book does not represent an introduction to diophantine geometry, nor a complete treatment of the theory of heights. Neither do we strive for maximum generality, and most of the book is concerned only with a number field as ground field, dealing only marginally with the function field case and even less with ground fields of positive characteristic. Also, we do not extend the theory to semiabelian varieties or non-split commutative linear groups, which are also quite important and lead to delicate questions.

The whole theory of effective diophantine approximation, and Baker's theory of logarithmic forms, are missing entirely from this book and relegated to a few comments at the end of Chapter 5. This is not due to a perception of lack of importance of the subject. Rather, an adequate treatment of the topic would have required a second large volume for this already large book.

The same can be said for arithmetic geometry, which no doubt deserves an advanced monograph by itself, also for the arithmetic theory of elliptic curves and abelian varieties, and for the arithmetic theory of modular functions and its applications to diophantine problems.

Our goal in writing this book was to provide, in addition to the existing literature, a wide selection of topics in the subject, containing foundational material with complete proofs, numerous examples, and additional material viewed as a bridge between the classical theory and arithmetic geometry proper. A fair portion of this book is meant to be accessible to a reader with only a basic course in algebra and algebraic geometry, but even the specialist in the field should be able to find interesting material in it. We made no serious attempt to reach completeness about the history of the subject, also referenced material (we never quote from secondary sources) is for this very reason mostly from literature in the English and French languages. Finally, although we attempted to put together a comprehensive bibliography, in no way do we pretend it to be complete. We apologize in advance for the inevitable omissions in our bibliography, regarding priorities and precursor works.

At the end of the book the reader will find an index of mathematical names in lexicographic order and an index of notations ordered by page number. The vanity index (index of authors mentioned in the text) has been omitted.

Terminology

We try to use standard terminology, but for convenience of the reader we gather here some of the most frequently used notation and conventions.

In set theory, $A \subset B$ means that A is a subset of B. In particular, A may be *equal* to B. If this case is excluded, then we write $A \subsetneq B$. The complement of A in B is denoted by $B \setminus A$ as we reserve $-$ for algebraic purposes. We denote the number of elements of A by $|A|$ (possibly ∞). The identity map is id.

A quasi-compact topological space is characterized by the Heine–Borel property for open coverings. In this book, a compact space is quasi-compact *and* Hausdorff.

We denote by $\mathbb{N}$ the set of natural numbers *with* 0 *included* and $\mathbb{Z}$ is the ring of rational integers. Then $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are the fields of rational, real, and complex numbers. A positive number means $x > 0$, but we use $\mathbb{R}_+$ for the non-negative real numbers. The Kronecker symbol δ_{ij} is 0 for $i \neq j$ and 1 for $i = j$.

The real (resp. imaginary) part of a complex number z is denoted by $\Re z$ (resp. $\Im z$) and $\overline{z}$ is complex conjugation.

The floor function $\lfloor x \rfloor$, defined for $x \in \mathbb{R}$, is the largest rational integer $\leq x$. The ceiling function $\lceil x \rceil$ denotes the smallest rational integer $\geq x$.

The real functions on X are denoted by $\mathbb{R}^X$. For $f, g \in \mathbb{R}^X$, the Landau symbol $f = O(g)$ means $|f(x)| \leq Cg(x)$ for some unspecified positive constant C. If we want to emphasize the dependence of C on parameters $\varepsilon, L, \ldots$ we write $f = O_{\varepsilon,L,\ldots}(g)$. As a special case, $f = O(1)$ means that f is a bounded function on X. We also use, with the same meaning, the equivalent Vinogradov's symbol $f \ll g$ and $f \ll_{\varepsilon,L,\ldots} g$. The symbol $g \gg f$ is interpreted as $f \ll g$.

If X is a topological space and f, g are defined on a subset Y with an accumulation point x, then $f = O(g)$ for $y \to x$ means that $|f(y)| \leq Cg(y)$ holds for all $y \in Y$ contained in a neighbourhood of x. If this is true for all $C > 0$ (with neighbourhoods depending on C), then we use the Landau symbol $f = o(g)$ for $y \to x$. The asymptotic relation $f \sim g$ for $y \to x$ means that $f - g = o(|g|)$.

The Landau symbols and the Vinogradov symbol must be used with caution in presence of parameters, not just because the constant involved may depend on parameters, but especially because the neighbourhood in which the inequality holds will also depend on the parameters, an easily overlooked fact.

In number theory, we use $\mathrm{GCD}(a, b)$ for the greatest common multiple of a and b. As usual, $a|b$ means that a divides b. The number of primes up to x is $\pi(x)$.

The group of multiplicative units of a commutative ring with identity is denoted by $R^\times$. We use the symbol V^* to denote the dual of a vector space V. Rings and algebras are always assumed to be associative, fields are always commutative. If the rings have an identity, then we assume that ring homomorphisms send 1 to 1. The ideal generated by $g_1, \ldots, g_m$ is denoted by $[g_1, \ldots, g_m]$. The characteristic of a field K is $\mathrm{char}(K)$ and we write $\mathbb{F}_q$ for the finite field with q elements.

The ring of polynomials in the variable x with coefficients in K is denoted by $K[x]$. A monic polynomial has highest coefficient 1. The minimal polynomial of an algebraic number α over a field is assumed to be monic and its degree is the degree of α, denoted by $\deg(\alpha)$. If we consider the minimal polynomial over $\mathbb{Z}$ (or any factorial ring), then we replace monic by the assumption that the coefficients are coprime. We use $\mathbf{x}$ to denote a vector with entries x_i, thus $K[\mathbf{x}]$ is the ring of polynomials in the variables x_i. By $\overline{K}$ we denote a choice of an algebraic closure of the field K.

For the terminology used in algebraic geometry, the reader is referred to Appendix A.

The numbering in this book is by chapter (appendices in capitals), section, and statement, in progressive order. Equations are numbered separately by chapter (appendices in capitals) and statement in progressive order, with the label enclosed in parentheses. References to equations not occurring on the same page or the preceding page also give the page numbers; the first example is: (A.13) on page 558, occurring on page 15.

1 HEIGHTS

1.1. Introduction

This chapter contains preliminary material on absolute values and the elementary theory of heights on projective varieties. Most of this material is quite standard, although we have included some of the finer results on classical heights which are not usually treated in other texts.

In Section 1.2 we start with absolute values, and places are introduced as equivalence classes of absolute values. The definitions of residue degree and ramification index are given, as well as their basic properties and behaviour with respect to finite degree extensions. In Sections 1.3 and 1.4 we introduce normalized absolute values and the all-important product formula in number fields and function fields. Section 1.5 contains the definition of the absolute Weil height in projective spaces, the characterization of points with height 0, and a general form of Liouville's inequality in diophantine approximation. Section 1.6 studies the height of polynomials and Mahler's measure and proves Gauss's lemma and its counterpart at infinity, Gelfond's lemma. Section 1.7, which can be omitted in a first reading, elaborates further on various comparison results about heights and norms of polynomials, including an interesting result of Per Enflo on ℓ_1-norms.

The presentation of the material in this chapter is self contained with the exception of Section 1.2, where the basic facts about absolute values are quoted from standard reference books (N. Bourbaki [**47**], Ch.VI, S. Lang [**173**], Ch.XII, and N. Jacobson [**157**], Ch.IX).

1.2. Absolute values

Definition 1.2.1. *An **absolute value** on a field K is a real valued function $|\ |$ on K such that:*

(a) $|x| \geq 0$ *and* $|x| = 0$ *if and only if* $x = 0$.

(b) $|xy| = |x|\ |y|$.

(c) $|x + y| \leq |x| + |y|$ *(triangle inequality).*

1.2.2. The **trivial absolute value** is equal to 1 except at 0. If an absolute value satisfies instead of the triangle inequality (c) the stronger condition

(c′) $|x+y| \leq \max\{|x|, |y|\}$,

then it is called **non-archimedean**. If (c′) fails to hold for some $x, y \in K$, then the absolute value is called **archimedean**. The distance of $x, y \in K$ is $|x-y|$. This metric induces a topology on K. In the non-archimedean case, we have an ultrametric distance and (c′) is called the **ultrametric triangle inequality** . If two absolute values define the same topology, they are called **equivalent** .

Proposition 1.2.3. *Two absolute values* $|\ |_1$, $|\ |_2$ *are equivalent if and only if there is a positive real number* s *such that*

$$|x|_1 = |x|_2^s$$

for $x \in K$.

Proof: See [**157**], Th.9.1 or [**173**], Prop.XII.1.1. □

1.2.4. A **place** v is an equivalence class of non-trivial absolute values. By $|\ |_v$ we denote an absolute value in the equivalence class determined by the place v. If the field L is an extension of K and v is a place of K, we write $w|v$ for a place w of L if and only if the restriction to K of any representative of w is a representative of v, and say that w extends v and, equivalently, that w lies over v. We also employ the notation $w|v$ (that is, w divides v), motivated by the fact that non-archimedean places in number fields correspond to prime ideals.

The **completion** of K with respect to the place v is an extension field K_v with a place w such that:

(a) $w|v$.

(b) The topology of K_v induced by w is complete.

(c) K is a dense subset of K_v in the above topology.

The completion exists and is unique up to isometric isomorphisms ([**157**], Th.9.7 or [**173**], Prop.XII.2.1). By abuse of notation, we shall denote the unique place w also by v.

Example 1.2.5. If the field is $\mathbb{Q}$, then there is only one archimedean place ∞ on $\mathbb{Q}$, given by the ordinary absolute value $|\ |$. We also write $|\ |_\infty$ for this absolute value (cf. [**157**], Th.9.4).

For a prime p we have the ***p*-adic absolute value** $|\ |_p$ determined as follows. Let $m/n \in \mathbb{Q}$ be a rational number and write it in the form

$$\frac{m}{n} = p^a \frac{m'}{n'},$$

where m', n' are integers coprime with p. Then we set

$$\left|\frac{m}{n}\right|_p = p^{-a}.$$

In fact, it suffices to define $|\ |_p$ by the conditions

$$|q|_p = \begin{cases} 1 & \text{for primes } q \neq p \\ \frac{1}{p} & \text{if } q = p. \end{cases}$$

The p-adic absolute values so defined give us a set of inequivalent representatives for all non-archimedean places on $\mathbb{Q}$ ([**157**], Th.9.5). The field $\mathbb{Q}_p$ of p-adic numbers is the completion of $\mathbb{Q}$ with respect to the place p. The compact subset $\mathbb{Z}_p$ of p-adic integers is the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$ (for compactness, see [**47**], Ch.VI, §5, no.1, Prop.2). On the other hand, the completion of $\mathbb{Q}$ with respect to the archimedean place ∞ is $\mathbb{R}$. In full generality, we have the following well-known **Theorem of Ostrowski**:

Theorem 1.2.6. *The only complete archimedean fields are $\mathbb{R}$ and $\mathbb{C}$.*

Proof: [**157**], §9.5 or [**47**], Ch.VI, §6, no.4, Th.2. □

Proposition 1.2.7. *Let K be a field which is complete relative to an absolute value $|\ |_v$ and let L be a finite-dimensional extension field of K. Then there is a unique extension of $|\ |_v$ to an absolute value $|\ |_w$ of L. For any $x \in L$ the equation*

$$|x|_w = |N_{L/K}(x)|_v^{1/[L:K]}$$

holds, where $N_{L/K}$ is the norm from L to K. Moreover, the field L is complete with respect to $|\ |_w$.

Proof: [**157**], Th.s 9.8, 9.9, 9.12 or [**47**], Ch.VI, §8, no.7, Prop.10. □

Remark 1.2.8. Clearly, the preceding proposition implies that there is a unique extension to an absolute value on the algebraic closure of K. Note however that the last clause of this proposition need not hold for infinite-dimensional extensions; a well-known example is an algebraic closure of the p-adic field $\mathbb{Q}_p$ (cf. S. Bosch, U. Güntzer, and R. Remmert [**43**], 3.4.3).

1.2.9. Let K be a field with a non-archimedean place v and let L be a finite-dimensional field extension of K. Assume that w is a place of L with $w|v$. The ring

$$R_v := \{x \in K \mid |x|_v \leq 1\}$$

is called the **valuation ring** of v. The definition is obviously independent of the representative $|\ |_v$ of v. R_v is a local ring with unique maximal ideal $\mathfrak{m}_v := \{x \in K \mid |x|_v < 1\}$.

The **residue field** $k(v)$ is defined by $R_v/\mathfrak{m}_v$. The quotient map $R_v \to k(v), x \mapsto \overline{x}$ is called the **reduction**. Applying it to coefficients, it extends to polynomials and to power series.

The **residue degree** $f_{w/v}$ of L/K in w is the dimension of $k(w)$ over $k(v)$. Let $|\ |_w$ be an absolute value representing w and $|\ |_v$ the restriction of $|\ |_w$ to K. The **value group** $|K^\times|_v$ is a multiplicative subgroup of $|L^\times|_w$ and its index is called the **ramification index** $e_{w/v}$ of w in v.

The place v is called **discrete** if the value group $|K^\times|_v$ is cyclic. Then $\mathfrak{m}_v$ is a principal ideal and any principal generator is called a **local parameter**.

The following result is the very useful **Hensel's lemma**.

Lemma 1.2.10. *Let K be complete with respect to a non-archimedean place v. Let $f(t) \in K[t]$ be a monic polynomial with reduction $\overline{f}(t) = \overline{g}(t)\overline{h}(t)$ for some monic coprime polynomials $\overline{g}(t), \overline{h}(t) \in k(v)[t]$. Then there exist monic polynomials $G(t), H(t) \in R_v[t]$ with $F(t) = G(t)H(t)$ and $\overline{G}(t) = \overline{g}(t)$, $\overline{H}(t) = \overline{h}(t)$.*

Proof: For discrete valuations, we refer to [**157**], §9.11. The general case is proved in [**43**], 3.3.4. □

Proposition 1.2.11. *Let L/K and $w|v$ be as in 1.2.9.*

(a) *The residue degree and the ramification index do not change if we pass to completions.*

(b) *The product of the residue degree and the ramification index is at most $[L : K]$, with equality if v is discrete and K is complete relative to v.*

Proof: [**157**], §9.10 or [**173**], Prop.s XII.4.2, XII.6.1, and §XII.5. □

1.2.12. A **number field** is a finite-dimensional field extension of $\mathbb{Q}$. The ring of algebraic integers of K is denoted by O_K. Now let L be a locally compact field containing a number field K as a dense subset and assume that the topology is not discrete. Then it follows that L is complete because it is locally compact. The classification of non-discrete locally compact fields is well known and tells us that there is a place v of K such that L is the completion of K with respect to v. Moreover, if L is connected, then L is isomorphic to $\mathbb{R}$ or $\mathbb{C}$ or to a finite extension of $\mathbb{Q}_p$. The closure of O_K in L coincides with the valuation ring R_v of L.

On the other hand, every completion of a number field with respect to a non-archimedean place is a finite extension of $\mathbb{Q}_p$, hence locally compact. For details, we refer to [**47**], Ch.VI, §9, no.3, Th.1. The following result of Artin and Whaples is called the **approximation theorem**:

Theorem 1.2.13. *Let $|\ |_1, \ldots, |\ |_n$ be inequivalent non-trivial absolute values on a field K. Then for $x_1, \ldots, x_n \in K$ and $\varepsilon > 0$ there is $x \in K$ such that*

$$|x - x_k|_k < \varepsilon \quad (k = 1, \ldots, n).$$

Proof: [**157**], §9.2 or [**173**], Th.XII.1.2. □

1.3. Finite-dimensional extensions

Let K be a field with a fixed non-trivial absolute value $|\ |_v$.

Proposition 1.3.1. *Let L be a finite-dimensional field extension of K generated by a single element ξ. If $f(t)$ is the monic minimal polynomial of ξ over K and*

$$f(t) = f_1^{k_1}(t) \cdots f_r^{k_r}(t)$$

is its decomposition into different irreducible monic factors $f_j(t) \in K_v[t]$, then for each j there is an injective homomorphism

$$\iota : L \longrightarrow K_j := K_v[t]/(f_j(t))$$

of field extensions over K, given by $\xi \mapsto t$. There is a unique extension $|\ |_j$ of the absolute value of K_v to K_j. The absolute values $|\ |_j$ are pairwise inequivalent. Moreover, K_j is the completion of L with respect to $|\ |_j$ and the embedding ι. For any absolute value $|\ |_w$ extending $|\ |_v$ to L, there is a unique $j \in \{1, \ldots, r\}$ such that the restriction of $|\ |_j$ to L is equal to $|\ |_w$.

Proof: Proposition 1.2.7 leads to the unique extension $|\ |_j$ of the absolute value of K_v. The map ι is a well-defined homomorphism of field extensions over K and the image of ι is dense in K_j. Hence K_j is the completion of L with respect to $|\ |_j$. If the restrictions of $|\ |_j$ and $|\ |_k$ are equivalent, then we have an isometric isomorphism of K_j onto K_k, leaving K_v fixed. Therefore, the images of ξ have to be roots of the same irreducible factor of $f(t)$ in $K_v[t]$, yielding $j = k$. Let $|\ |_w$ be an absolute value on L extending $|\ |_v$. The closure of K in L_w can be identified with K_v. Now ξ generates a finite-dimensional subfield of L_w over K_v which is complete by Proposition 1.2.7, therefore this subfield is L_w itself. Also ξ must be a root of some f_j, hence L_w is isomorphic to K_j over K_v. Moreover, we can assume that L is fixed under this isomorphism. Then it is clear from Proposition 1.2.7 that $|\ |_w$ is equal to the restriction of $|\ |_j$ to L. □

Corollary 1.3.2. *If L is a finite-dimensional separable field extension of K, then*

$$\sum_{w|v} [L_w : K_v] = [L : K],$$

where the sum ranges over all places w of L with $w|v$.

Proof: By the primitive element theorem (see N. Jacobson [**156**], §4.14), there is an element ξ of L which generates L over K. Proposition 1.3.1 implies the formula. □

Remark 1.3.3. If the extension is not separable, we still have $\sum_{w|v}[L_w : K_v] \leq [L : K]$. If L is generated by a single element over K, this is clear from Proposition 1.3.1. For the general case, we use induction on the degree.

Definition 1.3.4. *The number $[L_w : K_v]$ is called the **local degree** of L/K in w.*

Corollary 1.3.5. *Let L/K be a finite-dimensional Galois extension with Galois group $G = \mathrm{Gal}(L/K)$ and let $|\ |_{w_0}$, $|\ |_w$ be absolute values on L extending $|\ |_v$. Then there is an element $\sigma \in G$ with*

$$|x|_w = |\sigma(x)|_{w_0} \quad \text{for} \quad x \in L.$$

The completions L_w and L_{w_0} are isomorphic over K_v. However, they need not to be isomorphic over L.

Proof: As in the proof of Corollary 1.3.2, there is an element ξ of L with $L = K(\xi)$. If $f(t)$ is the minimal polynomial of ξ over K, then L_w is obtained by adjoining a root of $f_j(t)$ to K_v in a fixed splitting field of f over K_v, where $f_j(t)$ is an irreducible factor of $f(t)$ in $K_v[t]$. Since L is a Galois extension, all roots of f are contained in L_w, therefore $L_w = L_{w_0}$ as a field. Then the absolute values $|\ |_{w_0}$ and $|\ |_w$ correspond to embeddings ι_0 and ι of L into L_{w_0} over K. There is a unique $\rho \in \mathrm{Gal}(L_{w_0}/K_v)$ with $\iota = \rho \circ \iota_0$, given by $\iota_0(\xi) \mapsto \iota(\xi)$. If $|\ |$ is the unique absolute value of L_{w_0} extending the one of K_v and if σ is the unique element of G with $\rho \circ \iota_0 = \iota_0 \circ \sigma$, then

$$|x|_w = |\iota(x)| = |\rho \circ \iota_0(x)| = |\iota_0 \circ \sigma(x)| = |\sigma(x)|_{w_0} \quad \text{for } x \in L. \qquad \square$$

1.3.6. Let K be a field with a fixed non-trivial absolute value $|\ |_v$. We consider a finite-dimensional separable extension field L of K and a place w of L with $w|v$. For any $x \in L$, we define

$$\|x\|_w := |N_{L_w/K_v}(x)|_v$$

and

$$|x|_w := |N_{L_w/K_v}(x)|_v^{1/[L:K]}.$$

We know from Proposition 1.2.7 that the restriction of $|N_{L_w/K_v}|_v^{1/[L_w:K_v]}$ to L is a representative of w extending $|\ |_v$. The obvious inequality $[L_w : K_v] \leq [L : K]$ implies that $|\ |_w$ is an absolute value representing w. If v is not archimedean or $[L_w : K_v] = 1$, we have that $\|\ \|_w$ is also an absolute value representing w. On the other hand, if v is archimedean and $[L_w : K_v] = 2$, we have $L_w = \mathbb{C}$ and $K_v = \mathbb{R}$. Assume that the restriction of $|\ |_v$ to $\mathbb{Q}$ is the ordinary absolute value; then $\|\ \|_w$ is not an absolute value because the triangle inequality is not satisfied.

Lemma 1.3.7. *Let $x \in K \setminus \{0\}$ and $y \in L \setminus \{0\}$. With the notation above*

$$\sum_{w|v} \log |x|_w = \log |x|_v \,,$$

$$\sum_{w|v} \log \|y\|_w = \log |N_{L/K}(y)|_v.$$

Proof: Corollary 1.3.2 implies the first statement. There is an element ξ of L with $L = K(\xi)$. With the notation of Proposition 1.3.1, we have $k_1 = \cdots = k_r = 1$ and an isomorphism

$$L \otimes_K K_v \xrightarrow{\sim} \prod_{j=1}^{r} K_v[t]/(f_j(t))$$

of K_v-algebras, given by $\xi \longrightarrow (t)_{j=1,\ldots,r}$ (this is a form of the Chinese remainder theorem). By Proposition 1.3.1 we get

$$N_{L/K}(y) = \prod_{w|v} N_{L_w/K_v}(y),$$

proving the second claim. □

1.3.8. If K is a number field, the archimedean absolute values of K are determined by the embeddings $\sigma : K \longrightarrow \mathbb{C}$ of K into the complex numbers. There are exactly $[K : \mathbb{Q}]$ such embeddings. An embedding σ is said to be real if $\sigma(K)$ is in the real subfield $\mathbb{R}$ of $\mathbb{C}$, and complex otherwise. If σ is a complex embedding, composition with complex conjugation yields a conjugate embedding $\overline{\sigma}$, and it is clear that σ and $\overline{\sigma}$ determine the same archimedean absolute value. Conversely, if σ and σ' are two embeddings of K in $\mathbb{C}$ determining the same absolute value, we have $\sigma' = \sigma$ or $\sigma' = \overline{\sigma}$. All this is immediate from Proposition 1.3.1, because K has a primitive element over $\mathbb{Q}$.

The completion of K at an archimedean place is isometric to either $\mathbb{R}$ or $\mathbb{C}$. Accordingly, the set of archimedean places is subdivided into **real places** and **complex places**.

Example 1.3.9. Let p be an odd prime and $K = \mathbb{Q}(\zeta)$ with ζ a primitive pth root of unity. Our goal in this example is to determine all extensions of an absolute value of $\mathbb{Q}$ to K.

The minimal polynomial of ζ over $\mathbb{Q}$ is given by

$$f(t) = t^{p-1} + t^{p-2} + \cdots + 1,$$

which is proved by applying Eisenstein's criterion to $f(t+1)$.

To begin with, we determine the extensions of the ordinary absolute value $|\ |_\infty$ of $\mathbb{Q}$ to K. The irreducible factors of $f(t)$ in $\mathbb{R}[t]$ have degree 2. By Proposition 1.3.1, there are exactly $\frac{p-1}{2}$ extensions of $|\ |_\infty$; all archimedean absolute values of K are associated to the $(p-1)/2$ pairs of complex conjugate embeddings of K and the local degree is equal to 2.

Next, we consider the extensions of the non-archimedean absolute value associated to a prime number q. Suppose first that $q \neq p$. We need to decompose $f(t)$ into irreducible factors over $\mathbb{Q}_q$. There is a smallest number $r \geq 1$ with $p | q^r - 1$, determined by the property that $\mathbb{F}_{q^r}$ is the smallest field of characteristic q containing a non-trivial pth root of unity (note also that, by Fermat's little theorem, $r | p-1$). In that case, the field $\mathbb{F}_{q^r}$

contains all pth roots of unity. Hence $f(t)$ is a product of $\frac{p-1}{r}$ distinct irreducible factors in $\mathbb{F}_q[t]$, each degree r. The same is true in $\mathbb{Q}_q[t]$ by Hensel's lemma (see Lemma 1.2.10). We conclude again by Proposition 1.3.1 that there are exactly $\frac{p-1}{r}$ extensions of $|\ |_q$ to K and the local degrees are equal to r. It is obvious that ζ remains a unit in any completion of K with respect to such an absolute value and its representative in the residue field is also a non-trivial primitive pth root of unity. By Proposition 1.2.11, the residue degree is equal to r and the ramification index is 1.

It remains to consider the place p. As before, Eisenstein's criterion shows that the polynomial $f(t)$ is irreducible in $\mathbb{Q}_p[t]$. Then there is only one extension $|\ |_v$ of $|\ |_p$ to K and the local degree is $p-1$. The minimal polynomial of $\zeta - 1$ over $\mathbb{Q}_p$ is $f(t+1)$ and so $N_{K_v/\mathbb{Q}_p}(\zeta - 1) = p$. Proposition 1.2.7 implies

$$|\zeta - 1|_v = p^{-1/(p-1)}.$$

By Proposition 1.2.11, the ramification index is equal to $p-1$ and the residue degree is equal to 1.

1.3.10. In the final part of this section, we handle finite-dimensional field extensions without separability assumptions. It turns out that it suffices to adjust the exponents in the normalization 1.3.6. Since we focus almost exclusively on number fields, the reader may skip the rest of this section in a first reading.

Let K be a field with absolute values $|\ |_v$ and let L/K be a finite-dimensional field extension. Our goal is to generalize Proposition 1.3.1 describing the extensions of $|\ |_v$ to the field L.

Since $L \otimes_K K_v$ is a finite-dimensional K_v-algebra, the structure theorem of commutative artinian rings ([**157**], Th.7.13) gives uniquely determined ideals R_j, which are local K_v-algebras with maximal ideals $\mathfrak{m}_j$ and such that

$$L \otimes_K K_v = \prod_{j=1}^{r} R_j. \tag{1.1}$$

We have natural embeddings of L and K_v into the residue field $K_j = R_j/\mathfrak{m}_j$ of R_j. By Proposition 1.2.7, there is a unique extension $|\ |_j$ of $|\ |_v$ to K_j. Clearly, L is dense in K_j, whence K_j is the completion of L with respect to this absolute value.

Proposition 1.3.11. *The restrictions of $|\ |_j$, $j = 1, \ldots, r$, to L are all extensions of $|\ |_v$ to absolute values on L and they are pairwise inequivalent.*

Proof: Suppose the restrictions to L of $|\ |_j$ and $|\ |_k$ are equivalent. Then there is an isomorphism $\varphi : K_j \xrightarrow{\sim} K_k$ which is the identity on L and K_v. Let φ_j be the canonical isomorphism of $L \otimes_K K_v$ onto K_j. Then $\varphi = \varphi_k \circ \varphi_j^{-1}$ (check on L and K_v), which is possible only if $j = k$. This proves the last clause of our claim.

Let $|\ |_w$ be an extension of $|\ |_v$ to L. The closure of K in L_w will be identified with K_v. Since L is finite dimensional over K, it follows that LK_v is a closed subfield of L_w, from which we conclude that $LK_v = L_w$. By the universal property of the tensor product, there is a homomorphism of $L \otimes_K K_v$ onto L_w. The kernel of this homomorphism is a maximal ideal, hence equal to $\mathfrak{m}_j \times \prod_{k \neq j} R_k$ for some j. Therefore, K_j is isomorphic to

L_w as a K_v-algebra, and by Proposition 1.2.7 we infer that it is in fact an isometry. This shows that the restriction of $|\ |_j$ to L is $|\ |_w$, as we wanted. □

1.3.12. Now we are ready to define the correct normalizations of the absolute values as above. We have seen that the places w of L with $w|v$ are in one-to-one correspondence with the local K_v-algebras in (1.1), thus we may write

$$L \otimes_K K_v = \prod_{w|v} T_w \tag{1.2}$$

and identify the residue field of T_w with the completion L_w. For $y \in L$, we set

$$\|y\|_w := |N_{L_w/K_v}(y)|_v^{[T_w:L_w]}$$

and

$$|y|_w := \|y\|_w^{1/[L:K]}.$$

With these modifications the analogue of Lemma 1.3.7 still holds, namely:

Lemma 1.3.13. *If $x \in K \setminus \{0\}$ and $y \in L \setminus \{0\}$, then*

$$\sum_{w|v} \log |x|_w = \log |x|_v\,, \tag{1.3}$$

$$\sum_{w|v} \log \|y\|_w = \log |N_{L/K}(y)|_v\,. \tag{1.4}$$

Proof: Formula (1.4) is a trivial consequence of Proposition 1.2.7 and (1.2). If we set $y = x$ in (1.4), then (1.3) follows immediately from (1.2). □

1.4. The product formula

The product formula over $\mathbb{Q}$ may be stated and proved as a consequence of the factorization of a non-zero rational number into a product of primes and a unit. In spite of its simplicity and essentially trivial nature, it plays a fundamental role and its importance cannot be overstated. The fact that it involves all places, including the places at ∞, means that, from the geometrical point of view, we are dealing with a complete variety. In the case considered here, the general fibre of the variety is a point and everything is quite simple. However, the best interpretation of the product formula and its generalizations is found in the framework of Arakelov theory.

1.4.1. Let K be a field and M_K be a set of non-trivial inequivalent absolute values on K such that the set

$$\{\,|\ |_v \in M_K \mid |x|_v \neq 1\}$$

is finite for any $x \in K\backslash\{0\}$. We identify the elements of M_K with the corresponding places and say that M_K satisfies the **product formula** if

$$\prod_{v \in M_K} |x|_v = 1$$

for any $x \in K\backslash\{0\}$.

We shall also refer to

$$\sum_{v \in M_K} \log |x|_v = 0$$

as the product formula for $x \neq 0$.

If L/K is a finite-dimensional extension and M_K is a set of places with associated normalized absolute values satisfying the product formula, we obtain a set of places M_L consisting of representatives $|\ |_w$ of $w|v$ for $v \in M_K$, normalized as in 1.3.6 and 1.3.12.

Proposition 1.4.2. *The set of places M_L so normalized again satisfies the product formula.*

Proof: Let $x \in L^\times$. We need to check that $|x|_w \neq 1$ only for finitely many $w \in M_L$. Since x is algebraic over K, we have

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \tag{1.5}$$

for suitable $a_i \in K$. By assumption, we have $|a_i|_v \in \{0, 1\}$ up to finitely many $v \in M_K$. Since there are only finitely many $w \in M_L$ lying over a given v (Corollary 1.3.2), we have $|a_i|_w \leq 1$, up to finitely many $w \in M_L$. Clearly, there are only finitely many archimedean places in M_K and hence in M_L. Thus it is enough to consider non-archimedean $w \in M_L$ and then the ultrametric inequality applied to (1.5) shows that $|x|_w \leq 1$ whenever all coefficients $|a_i|_w \leq 1$. The same argument applied to $1/x$ completes the proof that $|x|_w = 1$ up to finitely many $w \in M_L$.

Once this is done, it is immediate from Lemmas 1.3.7 and 1.3.13 that the normalized set of absolute values on L satisfies the product formula. □

1.4.3. By Example 1.2.5, we get

$$M_{\mathbb{Q}} := \{|\ |_p \mid p \text{ prime number or } p = \infty\},$$

normalized as follows. If $p = \infty$, then $|\ |_p$ is the ordinary absolute value on $\mathbb{Q}$, and, if p is prime, then the absolute value is the p-adic absolute value on $\mathbb{Q}$, with $|p|_p = 1/p$.

Let K be a number field and let M_K be the associated set of places and normalized absolute values, obtained from the above construction applied to the extension $K/\mathbb{Q}$.

Proposition 1.4.4. *If K is a number field, M_K satisfies the product formula.*

Proof: By the above discussion, we can assume that K is equal to $\mathbb{Q}$ and it is obviously enough to show the product formula for a prime number x

$$\prod_{p \in M_{\mathbb{Q}}} |x|_p = |x|_x\ |x|_\infty = \frac{1}{x}\, x = 1. \qquad \square$$

In this book, whenever we talk about M_K of a number field it will always be the set so constructed from $M_{\mathbb{Q}}$. This is important for our normalizations, which we repeat: If $p = \infty$, then $|\ |_p$ is the ordinary absolute value on $\mathbb{Q}$, and, if p is prime, then the absolute value is the p-adic absolute value on $\mathbb{Q}$, with $|p|_p = 1/p$. In either case, we have

$$|x|_v := |N_{K_v/\mathbb{Q}_p}(x)|_p^{1/[K:\mathbb{Q}]} \tag{1.6}$$

for $x \in K$ and $v|p$.

As an application of our previous considerations in this chapter, we prove the following refinement of Theorem 1.2.13 for a number field K, called the **strong approximation theorem**:

Theorem 1.4.5. *Let $(|\ |_v)_{v\in S}$ be representatives for a finite set S of non-archimedean places of the number field K, let $x_v \in K_v$ for every $v \in S$, and let $\varepsilon > 0$. Then there is $x \in K$ with $|x - x_v|_v < \varepsilon$ for all $v \in S$ and $|x|_v \le 1$ for all non-archimedean $v \notin S$.*

Proof: There is no loss of generality in assuming that $x_v \in K$, because, by definition of completion, K is dense in K_v. By Proposition 1.2.3, we may also assume that the absolute values extend the p-adic absolute values $|\ |_p$ from Example 1.2.5. By Corollary 1.3.2, there are only finitely many places lying over a natural prime number, hence we may enlarge S to the set of all places lying over a finite set S_0 of prime numbers, taking $x_v = 0$ at every new place v introduced by doing so. For any $x \in K^\times$, Proposition 1.4.2 shows that $|x|_v \neq 1$ only for finitely many places v. Now take x to be the approximation to x_v $(v \in S)$ obtained from Theorem 1.2.13 with $\varepsilon = 1$. Then there is a finite set S_1 of prime numbers, disjoint from S_0, such that $|x|_v = 1$ for all places v of K, which do not lie over $S_0 \cup S_1$. By the Chinese remainder theorem, there is $m \in \mathbb{Z}$ with $|m - 1|_p < \delta$ for $p \in S_0$ and $|m|_p < \delta$ for $p \in S_1$. If we choose $\delta > 0$ sufficiently small, then the approximation mx satisfies the conclusion of Theorem 1.4.5. □

1.4.6. Function fields (see A.4.11) are also important examples in diophantine geometry, where the product formula holds and we devote the rest of this section to its discussion. In order to understand the background from algebraic geometry, the reader may consult the material on divisors in Sections A.8 and A.9. Since the focus of this book is mostly on number fields, we may skip the proofs in a first reading.

Let X be a projective irreducible variety over a field K and let us fix an ample line bundle L (see A.6.10). We denote by $\deg(Z)$ the degree of a cycle Z with respect to L. Since the function field does not change by passing to the normalization (see A.12.6), we may and shall assume that X is regular in codimension 1 (see A.8.10). For any prime divisor Z of X, the local ring $\mathcal{O}_{X,Z}$ is a discrete valuation ring and the valuation of $f \in K(X)^\times$ is the order of f at Z. The latter is denoted by $\mathrm{ord}_Z(f)$. Since the degree of a principal divisor is 0, we have

$$\sum_Z \mathrm{ord}_Z(f)\deg(Z) = 0. \tag{1.7}$$

We normalize the absolute value corresponding to ord_Z by

$$|f|_Z := c^{\mathrm{ord}_Z(f)\deg(Z)},$$

where c is some fixed number, $0 < c < 1$.

Proposition 1.4.7. *The absolute values $|\ |_Z$, Z prime divisor of X, are not trivial, inequivalent, and satisfy the product formula.*

Proof: Since $\mathcal{O}_{X,Z}$ is a discrete valuation ring, the absolute value $|\ |_Z$ is not trivial. Let Y, Z be different prime divisors. We may think of X as embedded in projective space. There is a hyperplane not containing Y, Z. Let H be the corresponding very ample divisor on X and let $n \in \mathbb{N}$ be so large that $nH + Y$ is very ample (see A.6.10). By the same argument as above, there is an effective divisor H' not containing Y and Z such that

$$H' = nH + Y + \mathrm{div}(f)$$

for some $f \in K(X)^\times$. We have $|f|_Z = 1$ and $|f|_Y = c^{-\deg(Y)}$. We conclude that $|\ |_Y$ and $|\ |_Z$ are inequivalent. The product formula is a consequence of (1.7). □

Example 1.4.8. Let C be an irreducible projective curve over K. The curve is regular if and only if it is normal (see A.8.10). So let C be regular (note however that this does not mean that C is smooth, see A.13.3). Then C is a regular model for the function field $K(C)$. The prime divisors of C are in one-to-one correspondence with orbits of points under $\mathrm{Gal}(\overline{K}/K)$ (see A.2.7). The order at a prime divisor is the order at any point in the associated orbit.

This example fits with the preceding considerations if $L = O([P_0])$ for some point $P_0 \in C(K)$ (and L is of course automatically ample). The product formula follows from the fact that any rational function $f \in K(C)^\times$ has the same number of zeros and poles.

1.4.9. On the function field $K(X)$, we shall always use the set of absolute values considered above. We denote it by M_X to emphasize the role of the model X. Obviously, the choice of the constant c is irrelevant. Usually, we shall choose $c = 1/e$.

Lemma 1.4.10. *The following statements hold:*

(a) *Any finitely generated field over K is a function field of an irreducible projective normal variety over K.*

(b) *Two irreducible varieties are birationally equivalent over K if and only if they have isomorphic function fields over K.*

(c) *If L is a finite-dimensional extension of the function field $K(X)$ of an irreducible projective variety X over K, then there are an irreducible projective normal variety Y over K, and a finite surjective morphism $\varphi : Y \longrightarrow X$, such that $L \cong K(Y)$ and the inclusion $K(X) \subset L$ corresponds to $\varphi^\sharp : K(X) \longrightarrow K(Y)$.*

(d) *In* (c)*, there is a distinguished choice for Y called the* ***normalization of X in L****, uniquely characterized up to isomorphisms by the following property: Given a dominant morphism $\varphi' : Y' \to X$ of an irreducible normal K-variety Y' to X and a homomorphism $\rho : K(Y) \hookrightarrow K(Y')$ over $K(X)$, then there is a unique dominant morphism $\psi : Y' \to Y$ with $\psi^\sharp = \rho$.*

Proof: Let L be a finitely generated field over K with generators $x_1, \ldots, x_n$. Let $\mathfrak{I}$ be the kernel of the homomorphism

$$K[t_1, \ldots, t_n] \longrightarrow L$$

given by $t_i \mapsto x_i$. Denote the corresponding closed subvariety of $\mathbb{A}^n$ by X. Since $\mathfrak{I}$ is prime, X is an irreducible variety. Obviously, $K(X)$ is isomorphic to L. The closure $\overline{X}$ of X in $\mathbb{P}^n_K$ is a projective variety. The normalization of $\overline{X}$ is a projective normal variety (see A.12.7) with function field L (see A.12.6, A.12.7). This proves (a).

For (b), see A.11.4.

To prove (c) and (d), a generalization of the construction in A.12.6 leads to the normalization of X in L. If X were affine, then we would take the integral closure of $K[X]$ in L. For any variety X, we glue the normalizations of the affine open charts to get the normalization of X (see A. Grothendieck [**135**], 6.3.9). The morphism from the normalization to X is finite ([**135**], 6.3.10) and hence projectivity of X implies projectivity of the normalization (see A.12.7). □

Remark 1.4.11. Note that a curve regular in codimension 1 is regular and hence determined up to isomorphism by its function field. For a higher-dimensional function field $K(X)$, there is no canonical choice for the model X. Even if X is smooth, we may blow up a point to get another smooth model X' for $K(X)$ and it is clear that $M_X \subsetneq M_{X'}$. Hence we always fix a model when dealing with higher-dimensional function fields.

If $L/K(X)$ is a finite extension, then Lemma 1.4.10 (d) shows that the normalization $\varphi : Y \to X$ of X in L is a canonical model for the function field L. Let $\varphi' : Y' \to X$ be any finite surjective morphism of an irreducible projective variety Y' onto X with $K(Y') = L$ and with $K(X) \hookrightarrow L$ equal to $(\varphi')^\sharp$. We claim that $M_Y = M_{Y'}$.

We first show that we may replace Y' by its normalization Y'' (in L) without changing the set of places. Indeed, the normalization morphism $\pi : Y'' \to Y'$ is finite and birational. Since Y' and Y'' are projective, the valuative criterion of properness (see A.11.10) shows that π induces an isomorphism outside of subsets of codimension ≥ 2 in Y'' and Y', hence $M_{Y'} = M_{Y''}$. So we may assume Y' normal and then Lemma 1.4.10 (d) yields a unique dominant morphism $\psi : Y' \to Y$ factoring through φ'. The morphism ψ is proper (see A.6.15) and has finite fibres, hence ψ is finite (see A.12.4). Since $K(Y') = K(Y) = L$, the morphism ψ is also birational (Lemma 1.4.10 (b)) and the same argument as above shows that ψ is an isomorphism in codimension 1, hence $M_Y = M_{Y'}$.

We see that the set of places of L is well determined by X and in the following examples we will show that M_Y is the set of places of L extending the places of M_X.

Example 1.4.12. Let us consider a finite-dimensional field extension of the function field $K(C)$ of an irreducible projective regular curve C over the ground field K. By Lemma 1.4.10, there is an irreducible projective regular curve C' over K and a morphism $\varphi : C' \to C$ such that the extension corresponds to the extension $K(C')/K(C)$ induced by φ. We know from the above that the order at a closed irreducible subset Z of dimension 0 induces an absolute value $|\ |_v \in M_C$. Since C is regular, Cartier divisors can be identified

with Weil divisors (cf. A.8.21) and $\varphi^*(Z)$ is well defined. We have

$$\varphi^*(Z) = \sum_{Z'} m_{Z'} Z',$$

where Z' ranges over all irreducible closed subsets of C' lying over Z and where $m_{Z'}$ denotes the multiplicity in Z'. Note that for $f \in K(C)^\times$ we have $\mathrm{ord}_{Z'}(f) = m_{Z'} \mathrm{ord}_Z(f)$. Thus Z' induces a place v' on C' with $v'|v$. Its ramification index and residue degree are

$$e_{v'/v} = m_{Z'}, \qquad f_{v'/v} = [K(Z') : K(Z)] .$$

The projection formula for proper intersection products (see W. Fulton [**125**], Prop.2.5(c)) gives

$$Z.\varphi_*(C') = \varphi_*(\varphi^*(Z)),$$

hence

$$[K(C') : K(C)] = \sum_{Z'} m_{Z'} [K(Z') : K(Z)] = \sum_{v'} e_{v'/v} f_{v'/v}.$$

By Remark 1.3.3 and Proposition 1.2.11, we see that all places v' dividing v are induced by the "fibre points" Z' and the local degree satisfies

$$[K(C')_{v'} : K(C)_v] = m_{Z'} [K(Z') : K(Z)] .$$

Example 1.4.13. In order to extend the above example to higher dimensions, we use the language of schemes. Let us consider a finite-dimensional extension of a function field $K(X)$. By Lemma 1.4.10, we may identify this extension with an extension $K(X')/K(X)$ induced by a finite surjective morphism $\varphi : X' \to X$ of irreducible projective varieties over K and regular in codimension 1.

Let Z be a prime divisor on X with corresponding place v. To study the places v' of X' with $v'|v$, we may assume that X, and hence X', are affine. The fibre over the generic point ζ of Z is the affine scheme

$$\varphi^{-1}(\zeta) = \mathrm{Spec}\left(K[X'] \otimes_{K[X]} K(\zeta)\right),$$

where $K(\zeta)$ is the residue field of $\mathcal{O}_{X,\zeta}$. By the structure theorem of finite-dimensional algebras ([**157**], Th.7.13), we have

$$K[X'] \otimes_{K[X]} K(\zeta) \cong \prod_{\xi \in \varphi^{-1}(\zeta)} \mathcal{O}_{\varphi^{-1}(\zeta),\xi}.$$

Note that $K[X'] \otimes_{K[X]} \mathcal{O}_{X,\zeta}$ is a finitely generated module over the discrete valuation ring $\mathcal{O}_{X,\zeta}$. Since it is also torsion free (as a subring of $K(X')$), it is free of rank $[K(X') : K(X)]$. We conclude that

$$[K(X') : K(X)] = \sum_{\xi \in \varphi^{-1}(\zeta)} [\mathcal{O}_{\varphi^{-1}(\zeta),\xi} : K(\zeta)].$$

Clearly, the order at any point $\xi \in \varphi^{-1}(\zeta)$ yields a place v' of $K(X')$ with $v'|v$. Indeed, denoting by t_ζ a local parameter in $\mathcal{O}_{X,\zeta}$, we have

$$\mathrm{ord}_\xi(f) = \mathrm{ord}_\xi(t_\zeta) \mathrm{ord}_\zeta(f),$$

for any $f \in K(X)^\times$. Moreover, we verify that

$$e_{v'/v} = \mathrm{ord}_\xi(t_\zeta), \qquad f_{v'/v} = [K(\xi) : K(\zeta)] .$$

Now, using $\mathcal{O}_{\varphi^{-1}(\zeta),\xi} = \mathcal{O}_{X',\xi}/\langle t_\zeta \rangle$, we see that

$$[\mathcal{O}_{\varphi^{-1}(\zeta),\xi} : K(\zeta)] = e_{v'/v} f_{v'/v}.$$

Therefore, as in the preceding example, we conclude that all places of $K(X')$ dividing v are induced by points of $\varphi^{-1}(\zeta)$.

Moreover, let L be an ample line bundle on X. Then the absolute values are normalized by

$$|f|_v := c^{\operatorname{ord}_v(f)\deg_L(v)} \quad (v \in M_{K(X)}, f \in K(X))$$

to satisfy the product formula for some constant c. If we use the normalizations from 1.3.6 on $K(X')$ and the equation

$$\deg_{\varphi^* L}(w) = [K(w) : K(v)] \deg_L(v)$$

obtained from the projection formula (A.13) on page 558, then the above implies

$$|g|_w = c_1^{\operatorname{ord}_w(g)\deg_{\varphi^* L}(w)} \quad (w \in M_{K(X')}, g \in K(X'))$$

for $c_1 := c^{1/[K(X'):K(X)]}$. Note that $\varphi^* L$ is ample (cf. A.12.7) and hence the normalizations on $K(X')$ fit with 1.4.6 for the new constant c_1.

1.5. Heights in projective and affine space

1.5.1. We denote by $\overline{\mathbb{Q}}$ a choice of an algebraic closure of $\mathbb{Q}$. Let us consider the projective space $\mathbb{P}^n_{\overline{\mathbb{Q}}}$ with standard global homogeneous coordinates $\mathbf{x} = (x_0 : x_1 : \cdots : x_n)$. Let $P \in \mathbb{P}^n_{\overline{\mathbb{Q}}}$. We now define a function, called **height**, on algebraic points of $\mathbb{P}^n_{\overline{\mathbb{Q}}}$, which may be considered as a measure of the "algebraic complication" needed to describe P. This is a fundamental notion at the basis of diophantine geometry.

Let P be a point of $\mathbb{P}^n_{\overline{\mathbb{Q}}}$ represented by a homogeneous non-zero vector $\mathbf{x}$ with coordinates in a number field K. Then we set

$$h(\mathbf{x}) := \sum_{v \in M_K} \max_j \log |x_j|_v.$$

Lemma 1.5.2. *$h(\mathbf{x})$ is independent of the choice of K.*

Proof: Let L be another number field containing the coordinates $x_0, \ldots, x_n$ of $\mathbf{x}$. We can assume that $K \subset L$. Then

$$\sum_{w \in M_L} \max_j \log |x_j|_w = \sum_{v \in M_K} \sum_{w|v} \max_j \log |x_j|_w.$$

Our claim now follows from the first formula of Lemma 1.3.7. □

Lemma 1.5.3. *$h(\mathbf{x})$ is independent of the choice of coordinates.*

Proof: Let $\mathbf{y}$ be another coordinate vector. By the preceding lemma, we may assume that $x_0, \dots, x_n$, $y_0, \dots, y_n \in K$. There is $\lambda \in K$, $\lambda \neq 0$, with $\mathbf{y} = \lambda \mathbf{x}$, hence

$$h(\mathbf{y}) = \sum_{v \in M_K} \max_j \log |y_j|_v = \sum_{v \in M_K} \log |\lambda|_v + \sum_{v \in M_K} \max_j \log |x_j|_v.$$

Thus we get $h(\mathbf{y}) = h(\mathbf{x})$ by the product formula. □

These two lemmas show that the height so defined depends only on the point P and not on the choice of coordinates of a homogeneous vector representing P.

Definition 1.5.4. *We call* $h(\mathbf{x})$ ***the absolute logarithmic height*** *(briefly,* ***height****) of* P *and we denote it by* $h(P)$. *We also use the* ***multiplicative height*** $H(P) = e^{h(P)}$.

Example 1.5.5. If the coordinates $x_0, \dots, x_n$ of $P \in \mathbb{P}^n_{\mathbb{Q}}$ can be chosen in $\mathbb{Q}$, we can assume that they are integers and that $x_0, \dots, x_n$ have no common factors. If we take such a representative for the coordinates of P, then the non-archimedean places give no contribution to the height, and we obtain

$$h(P) = \max_j \log |x_j|_\infty.$$

1.5.6. A similar notion holds for affine space. Let $\mathbb{A}^n_{\overline{\mathbb{Q}}}$ be the affine space of dimension n over $\overline{\mathbb{Q}}$, together with the usual embedding in $\mathbb{P}^n_{\overline{\mathbb{Q}}}$ given by

$$P = (x_1, \dots, x_n) \mapsto (1 : x_1 : \cdots : x_n);$$

then we define $h(P)$ as the height of the image of P.

1.5.7. It should always be clear from the context whether we are dealing with points in affine or projective space, and there should be no problem in using the same notation h for heights in affine or projective space.

In performing local calculations, it proves to be convenient to introduce the function

$$\log^+ t = \max(0, \log t)$$

on the positive real numbers, extended by $\log^+ 0 = 0$. Then it is immediate that the height on affine space is given by

$$h(x_1, \dots, x_n) = \sum_{v \in M_K} \max_j \log^+ |x_j|_v.$$

As a special case, the **height of an algebraic number** α is

$$h(\alpha) = \sum_{v \in M_K} \log^+ |\alpha|_v$$

with K any number field with $\alpha \in K$.

1.5.8. Since any point in projective space admits a homogeneous representative with one coordinate equal to 1, it is clear that the height so defined is never negative. The next result, **Kronecker's theorem**, characterizes the case of equality.

Theorem 1.5.9. *The height of $\zeta \in \overline{\mathbb{Q}}^\times$ is 0 if and only ζ is a root of unity.*

Proof: Let K be a number field and let $\zeta \in K^\times$. If ζ is a root of unity, then its absolute values are all equal to 1, and hence its height is 0.

Conversely, assume $h(\zeta) = 0$. Then $|\zeta|_v \leq 1$ for every $v \in M_K$; in particular, ζ is an algebraic integer (for a formal argument, see the successive Remark 1.5.11). Let d be the degree of ζ and let $\boldsymbol{\zeta} = (\zeta_1, \ldots, \zeta_d)$ be a full set of conjugates of ζ. Now consider, for every positive integer m, the elementary symmetric functions $s_i(\boldsymbol{\zeta}^m)$, $i = 0, \ldots, d$, of $\zeta_1^m, \ldots, \zeta_d^m$. Since ζ is an algebraic integer, we have $s_i(\boldsymbol{\zeta}^m) \in \mathbb{Z}$ for every m.

Since $|\zeta_j|_v = 1$ for every j and v, and since $s_i(\boldsymbol{\zeta}^m)$ is the sum of $\binom{d}{i}$ terms each of which is a product of factors not exceeding 1 in absolute value, it is now clear that

$$\sum_{i=0}^{d} |s_i(\boldsymbol{\zeta}^m)| \leq \sum_{i=0}^{d} \binom{d}{i} = 2^d.$$

There are only finitely many possibilities for the vector of such symmetric functions, and by Dirichlet's pigeon-hole principle there are two integers m, n with $m > n$ and with the same vector of symmetric functions.

Obviously, this is the same as saying that $\boldsymbol{\zeta}^m = \pi(\boldsymbol{\zeta}^n)$ for some permutation π of $\{1, \ldots, d\}$ and by iterating this relation we find that $\zeta_i^{m^k} = \zeta_{\pi^k(i)}^{n^k}$. If we take k such that π^k is the identity, we conclude that $\zeta^{m^k - n^k} = 1$ with $m^k - n^k > 0$. □

1.5.10. We recall here some basic facts about S-integers and S-units in a number field K. Let $S \subset M_K$ be a finite set of places, which includes the set S_∞ of all archimedean places of K. An element $x \in K$ is an ***S*-integer** if $|x|_v \leq 1$ for $v \notin S$. The S-integers of K form a subring $O_{S,K}$ of K. The units in $O_{S,K}$ are called the ***S*-units** of K and form a group $U_{S,K}$. An element $x \in O_{S,K}$ is an S-unit if and only if $|x|_v = 1$ for all $v \notin S$.

Remark 1.5.11. An easy application of the non-archimedean triangle inequality and Gauss's lemma (see Lemma 1.6.3) shows that an S_∞-integer is the same as an algebraic integer in K. If $S = S_\infty$, we simply talk about the integers and the units of the number field K. The units of K are the algebraic integers $x \in K$ with norm $N_{K/\mathbb{Q}}(x) = \pm 1$, as we see from writing the norm as a product of conjugates of x.

1.5.12. We consider the following homomorphism

$$\phi : U_{S,K} \to \mathbb{R}^{|S|}, \qquad x \mapsto (\log |x|_v)_{v \in S}$$

of groups. By taking the logarithm of the product formula, we see that the image of ϕ is contained in the hyperplane $\sum_{v\in S} y_v = 0$, $\mathbf{y} \in \mathbb{R}^{|S|}$. By Kronecker's theorem, the kernel of ϕ is the group μ_K of roots of unity in K. This is part of **Dirichlet's unit theorem**:

Theorem 1.5.13. *Let S be as in 1.5.10. The image of ϕ is a lattice of maximal rank $|S|-1$ in the hyperplane $\sum_{v\in S} y_v = 0$. Hence $U_{S,K} \cong \mu_K \times \mathbb{Z}^{|S|-1}$.*

We will not prove this result here, and refer instead to W. Narkiewicz [**215**], Th.3.6, or S. Lang [**172**], p.104.

1.5.14. The **Segre embedding**

$$\mathbb{P}^n_{\overline{\mathbb{Q}}} \times \mathbb{P}^m_{\overline{\mathbb{Q}}} \longrightarrow \mathbb{P}^{(n+1)(m+1)-1}_{\overline{\mathbb{Q}}}$$

is given by

$$(\mathbf{x}, \mathbf{y}) \longmapsto \mathbf{x} \otimes \mathbf{y} := (x_i y_j)\,,$$

where the pairs ij are, for example, ordered lexicographically (see A.6.4). An easy calculation shows that

$$h(\mathbf{x} \otimes \mathbf{y}) = h(\mathbf{x}) + h(\mathbf{y}),$$

using $\max_{ij} |x_i y_j|_v = \max_i |x_i|_v \cdot \max_j |y_j|_v$ for every v.

This notion extends in an obvious fashion to finite products of projective spaces with an arbitrary number of factors.

Proposition 1.5.15. *If $P_1, \dots, P_r$ are points of $\mathbb{A}^n_{\overline{\mathbb{Q}}}$, then*

$$h(P_1 + \cdots + P_r) \le h(P_1) + \cdots + h(P_r) + \log r.$$

Proof: Let $\mathbf{x}^{(k)}$ be coordinate vectors of P_k, $k = 1, \dots, r$, which we assume to be in a suitable number field K. Then

$$h(P_1 + \cdots + P_r) = \sum_{v\in M_K} \max_j \log^+ |x_j^{(1)} + \cdots + x_j^{(r)}|_v.$$

If v is not archimedean, then

$$|x_j^{(1)} + \cdots + x_j^{(r)}|_v \le \max_k |x_j^{(k)}|_v.$$

If instead v is archimedean, we use the triangle inequality for the ordinary absolute value getting

$$|x_j^{(1)} + \cdots + x_j^{(r)}|_v \le |r|_v \max_k |x_j^{(k)}|_v.$$

Then Lemma 1.3.7 implies

$$\sum_{v|\infty} \log |r|_v = \log r$$

leading to

$$h(P_1 + \cdots + P_r) \leq \log r + \sum_{v \in M_K} \max_{j,k} \log^+ |x_j^{(k)}|_v.$$

The obvious fact

$$\max_{j,k} \log^+ |x_j^{(k)}|_v \leq \sum_k \max_j \log^+ |x_j^{(k)}|_v$$

concludes the proof. □

1.5.16. The following considerations show that the inequality in Proposition 1.5.15 cannot be improved upon in general.

Let $\alpha_1, \ldots, \alpha_r$ be algebraic numbers. By the preceding Proposition 1.5.15, we have

$$h(\alpha_1 + \cdots + \alpha_r) \leq h(\alpha_1) + \cdots + h(\alpha_r) + \log r.$$

Now suppose that equality occurs for some $r \geq 2$. Looking at the proof above, we must have

$$\log^+ |\alpha_1 + \cdots + \alpha_r|_v = \log^+(|r|_v \max_k |\alpha_k|_v) = \log |r|_v + \log^+ \max_k |\alpha_k|_v$$

for any archimedean prime v. This is equivalent to the two conditions

$$\max_k |\alpha_k|_v \geq 1$$

and

$$|r|_v \max_k |\alpha_k|_v = |\alpha_1 + \cdots + \alpha_r|_v.$$

Hence $\alpha_1 = \cdots = \alpha_r$ and we conclude directly

$$h(\alpha_1 + \cdots + \alpha_r) = h(r\alpha_1) \leq \log r + \sum_{v \in M_K} \log^+ |\alpha_1|_v = \log r + h(\alpha_1).$$

On the other hand, the equality assumption implies $h(r\alpha_1) = \log r + r h(\alpha_1)$, hence $h(\alpha_1) = 0$ because $r \geq 2$. Thus by Kronecker's theorem in 1.5.9, α_1 is a root of unity and we get $h(r\alpha_1) = h(r) = \log r$.

Another example yielding almost equality in Proposition 1.5.15 is obtained taking $\alpha_i = l/(l + a_i)$ with $1 \leq a_i \leq N$ and distinct a_i and with $l = N!t + 1$, t any positive integer. Then the numbers $l, l + a_1, \ldots, l + a_r$ are coprime in pairs and an easy calculation shows that $h(\alpha_i) = \log(l + \alpha_i)$ and $h(\sum \alpha_i) = \sum \log(l + a_i) + \log(\sum \alpha_i)$. Hence $h(\alpha_1 + \cdots + \alpha_r) > h(\alpha_1) + \cdots + h(\alpha_r) + \log r - \varepsilon$ for sufficiently large t.

The following result, quite useful in practice, expresses the fact that the height is invariant by Galois conjugation.

Proposition 1.5.17. *Let P be a point of affine or projective space with coordinates (x_j) in $\overline{\mathbb{Q}}$. If $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and if the point $\sigma(P)$ is given by the coordinates $(\sigma(x_j))$, then $h(P) = h(\sigma(P))$.*

Proof: We choose a finite-dimensional Galois extension K of $\mathbb{Q}$ containing all coordinates. Let $|\ |_p$ be an element of $M_{\mathbb{Q}}$ and $|\ |$ be an extension to an absolute value of K. The composition of $|\ |$ and σ is again an extension. Thus we have an action of $\mathrm{Gal}(K/\mathbb{Q})$ on the absolute values of K extending $|\ |_p$. Therefore, σ permutes the extensions and we have

$$\sum_{v|p} \max_j \log |x_j|_v = \sum_{v|p} \max_j \log |\sigma(x_j)|_v. \qquad \square$$

Lemma 1.5.18. *If $\alpha \in K \setminus \{0\}$, and $\lambda \in \mathbb{Q}$, then $h(\alpha^\lambda) = |\lambda| \cdot h(\alpha)$. In particular, $h(1/\alpha) = h(\alpha)$.*

Proof: If $\lambda \geq 0$, the result is clear by definition of height. Thus we need only consider $\lambda = -1$. For any absolute value $|\ |_v$ of K, we have

$$\log |\alpha|_v = \log^+ |\alpha|_v - \log^+ |1/\alpha|_v.$$

If we sum over v, the left-hand side is 0 by the product formula and the right-hand side equals $h(\alpha) - h(1/\alpha)$. $\square$

1.5.19. Let $S \subset M_K$ be a finite set of places. For $\alpha \in K \setminus \{0\}$, we have

$$\sum_{v \in S} \log |\alpha|_v \leq h(\alpha).$$

If we use $1/\alpha$ instead of α, then the preceding lemma shows that

$$\sum_{v \in S} \log |\alpha|_v \geq -h(\alpha).$$

This proves the so-called **fundamental inequality**

$$-h(\alpha) \leq \sum_{v \in S} \log |\alpha|_v \leq h(\alpha). \tag{1.8}$$

1.5.20. Now let L be a finite-dimensional field extension of K and consider a finite set S of places $w \in M_L$. A classical problem of diophantine approximation is that of approximating an element $\alpha \in L$ by elements $\beta \in K$, at all places $w \in S$. Classically, this is done with absolute values normalized relative to the field K rather than L, i.e. with $\|\ \|_w$ as in 1.3.6. In order to emphasize that this normalization depends on $v \in M_K$, we shall use the notation $\|\ \|_{w,K}$, hence for $x \in L$ we have

$$\|x\|_{w,K} = |N_{L_w/K_v}(x)|_v.$$

With this normalization relative to K, the fundamental inequality applied to $\alpha - \beta$ gives

$$-h(\alpha - \beta) \leq \sum_{w \in S} \log \big\|\alpha - \beta\big\|_{w,K}^{1/[L:K]} \leq h(\alpha - \beta)$$

under the assumption $\alpha \neq \beta$. Now applying Proposition 1.5.15 we find **Liouville's inequality**:

Theorem 1.5.21. *If $\alpha \in L$ and $\beta \in K$ with $\alpha \neq \beta$, then*

$$(2H(\alpha)H(\beta))^{-[L:K]} \leq \prod_{w \in S} \|\alpha - \beta\|_{w,K} \leq (2H(\alpha)H(\beta))^{[L:K]}.$$

The left-hand side inequality is a general formulation of the familiar Liouville inequality in diophantine approximation.

1.5.22. Heights can be introduced in any field with a product formula. We indicate the necessary changes. Let F be a field with a set M_F of non-trivial inequivalent absolute values, satisfying the product formula. This field F will play the role of $\mathbb{Q}$ in our previous considerations.

Let K/F be a finite-dimensional field extension and consider all places w with $w|v$ for some $v \in M_F$, together with corresponding absolute values $|\ |_w$ normalized as in 1.3.12. Then the set M_K of such absolute values satisfies the product formula, because of (1.4) on page 9. As before, this yields a non-negative height on $\mathbb{P}^n_F$, independent of the choice of coordinates. On the other hand, Kronecker's theorem does not hold in general, as the following example shows.

Example 1.5.23. Let K be a field and let $F = K(X)$ be the function field of an irreducible projective variety X over K, which is regular in codimension 1 (see 1.4.9). Let $P \in \mathbb{P}^n(F)$, hence $P = (f_0 : \cdots : f_n)$ for certain rational functions f_i on X. Then

$$h(P) = -\sum_Z \deg(Z) \min_j \operatorname{ord}_Z(f_j),$$

where Z ranges over all prime divisors and the degree is with respect to a fixed ample class. In particular, the height of a rational function $f \in K(X)^\times$ is

$$h(f) = h((1 : f)) = -\sum_Z \deg(Z) \min(0, \operatorname{ord}_Z(f)).$$

Thus $h(f) = 0$ if and only if f has no poles. By $h(f) = h(f^{-1})$, this is equivalent to $\operatorname{div}(f) = 0$.

If X is normal, a function without poles is regular (R. Hartshorne [**148**], Proposition I.6.3A), hence constant on the irreducible components of $X_{\overline{K}}$. We conclude that in this case $h(f) = 0$ if and only if f is locally constant on X (use A.6.15).

1.6. Heights of polynomials

Definition 1.6.1. *The **height of a polynomial***

$$f(t_1, \ldots, t_n) = \sum_{j_1, \ldots, j_n} a_{j_1 \ldots j_n} t_1^{j_1} \cdots t_n^{j_n} = \sum_{\mathbf{j}} a_{\mathbf{j}}\, \mathbf{t}^{\mathbf{j}}$$

with coefficients in a number field K is the quantity

$$h(f) = \sum_{v \in M_K} \log |f|_v,$$

where

$$|f|_v := \max_{\mathbf{j}} |a_{\mathbf{j}}|_v \tag{1.9}$$

is the ***Gauss norm*** *for any place* v.

Proposition 1.6.2. *Let* $f(t_1, \dots, t_n)$ *and* $g(s_1, \dots, s_m)$ *be polynomials in different sets of variables. Then*

$$h(fg) = h(f) + h(g).$$

Proof: Note that the height of a polynomial is equal to the height of the vector of coefficients in appropriate projective space. Then the claim follows from 1.5.14. □

We will need estimates for $h(fg)$ in terms of $h(f)$ and $h(g)$, without assuming different sets of variables for f and g. For finite places we have **Gauss's lemma**.

Lemma 1.6.3. *If* v *is not archimedean, then* $|fg|_v = |f|_v|g|_v$.

Proof: The inequality $|fg|_v \le |f|_v|g|_v$ is immediate because v is not archimedean. Let us assume first that $f(t)$ and $g(t)$ are polynomials in one variable t. We denote by c_j the coefficient

$$\sum_{j=k+l} a_k b_l$$

of $f(t)g(t)$. Without loss of generality, we can assume that $|f|_v = 1$, $|g|_v = 1$. Suppose $|fg|_v < 1$. Let j be the smallest index with $|a_j|_v = 1$. Since $|c_j|_v < 1$ and $|a_k|_v < 1$ for $k < j$, we get $|b_0|_v < 1$. Now we apply the above formula for the coefficient c_{j+l} and conclude $|b_l|_v < 1$ by induction. This contradiction proves the lemma in the one-variable case. For several variables, let d be an integer larger than the degree of fg. The Kronecker substitution

$$x_j = t^{d^{j-1}} \qquad (j = 1, \dots, n)$$

reduces the problem to the one-variable case. □

1.6.4. Gauss's lemma applies to every non-archimedean absolute value of a field. The archimedean case is more complicated and will be handled below.

If $f(t_1, \dots, t_n)$ is a polynomial with complex coefficients, we define $|f|_\infty$ as in (1.9), namely the maximum of the euclidean absolute value $|\ |$ of the coefficients of f.

Another very useful quantity in studying polynomials is the **Mahler measure**

$$M(f) := \exp\left(\int_{\mathbb{T}^n} \log|f(e^{i\theta_1}, \dots, e^{i\theta_n})|\, \mathrm{d}\mu_1 \cdots \mathrm{d}\mu_n\right),$$

where we have abbreviated $\mathbb{T}$ for the unit circle $\{e^{i\theta} \mid 0 \le \theta < 2\pi\}$ equipped with the standard measure $\mathrm{d}\mu = (1/2\pi)\mathrm{d}\theta$. Its main advantage is the multiplicativity

property

$$M(fg) = M(f)M(g).$$

Let $f(t) = a_d t^d + \cdots + a_0$ be a polynomial with complex coefficients and factorization

$$f(t) = a_d\,(t-\alpha_1)\cdots(t-\alpha_d).$$

Now we note that the mean value of $\log|t-\alpha|$ on the unit circle is $\log^+|\alpha|$. In fact, for $|\alpha|>1$ the function $\log|t-\alpha|$ is harmonic in the unit disk, therefore its mean value on the unit circle is its value at the centre, namely $\log|\alpha| = \log^+|\alpha|$. If instead $|\alpha|<1$, the function $\log|1-\alpha\bar{t}|$ is harmonic in the unit disk and coincides with $\log|t-\alpha|$ on the unit circle, while its value at the centre is 0, that is $\log^+|\alpha|$. Finally the case $|\alpha|=1$ is deduced by continuity.

We have shown that $M(t-\alpha) = \log^+|\alpha|$. If we combine this with the multiplicativity property of the Mahler measure, we obtain **Jensen's formula**:

Proposition 1.6.5.

$$\log M(f) = \log\,|a_d| + \sum_{j=1}^{d} \log^+|\alpha_j|.$$

The following result shows the connexion between the Mahler measure and the height and gives a bound for the absolute norm of an algebraic number.

Proposition 1.6.6. *Let $\alpha \in \overline{\mathbb{Q}}$ and let f be the minimal polynomial of α over $\mathbb{Z}$. Then*

$$\log M(f) = \deg(\alpha)h(\alpha).$$

In particular

$$\log|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)| \le \deg(\alpha)h(\alpha).$$

Proof: Let $d=\deg(\alpha)$ and write

$$f(t) = a_d t^d + \cdots + a_0.$$

We choose a number field K which contains α and is a Galois extension over $\mathbb{Q}$, with Galois group G. Then the list $(\sigma\alpha)_{\sigma\in G}$ contains every conjugate of α exactly $[K:\mathbb{Q}]/d$ times. Gauss's lemma gives

$$|a_d|_v \prod_{\sigma\in G} \max\left(1, |\sigma\alpha|_v\right)^{d/[K:\mathbb{Q}]} = 1 \tag{1.10}$$

for any non-archimedean $v \in M_K$.

We have

$$\begin{aligned}[K:\mathbb{Q}]\, h(\alpha) &= \sum_{v\in M_K}\sum_{\sigma\in G}\log^+|\sigma\alpha|_v && \text{(by Proposition 1.5.17)}\\ &= \sum_{v|\infty}\sum_{\sigma\in G}\log^+|\sigma\alpha|_v - \frac{[K:\mathbb{Q}]}{d}\sum_{v\not|\infty}\log|a_d|_v && \text{(by (1.10))}\\ &= \frac{[K:\mathbb{Q}]}{d}\sum_{v|\infty}\left(\log|a_d|_v + \sum_{j=1}^{d}\log^+|\alpha_j|_v\right),\end{aligned}$$

where in the last step we have used the product formula and collected the elements $\sigma\alpha$ into the conjugates α_j, $j=1,\dots,d$, of α. By Jensen's formula, this proves the first claim.

By the second formula of Lemma 1.3.7, we also have

$$\log|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)| \sum_{v|\infty}\sum_{j=1}^{d}\log^+|\alpha_j|_v$$

and the second claim follows from the preceding computation. □

The following lemma is useful in estimates. Let $f(t)=a_dt^d+\cdots+a_d$ be a polynomial of degree d with complex coefficients, and for $1\le p<\infty$ denote by $\ell_p(f)$ the norm

$$\ell_p(f) := \left(\sum_{j=0}^{d}|a_j|^p\right)^{1/p}.$$

For $p=\infty$, we set $\ell_\infty(f)=\max|a_j|=|f|_\infty$.

Lemma 1.6.7. *If $f(t)$ is as above, then $M(f)\le\ell_1(f)$. Moreover*

$$\binom{d}{\lfloor d/2\rfloor}^{-1}\ell_\infty(f)\le M(f)\le\ell_2(f)\le(d+1)^{1/2}\ell_\infty(f).$$

Proof: The first inequality is obvious from the definition of $M(f)$ and the pointwise bound $|f(e^{i\theta})|\le\ell_1(f)$ on $\mathbb{T}$.

Next, by convexity, we get

$$M(f)\le\left(\int_{\mathbb{T}}|f(e^{i\theta})|^2\,\mathrm{d}\mu\right)^{1/2}.$$

By Parseval's formula, the right-hand side equals

$$\ell_2(f)=\left(\sum_{j=0}^{d}|a_j|^2\right)^{1/2}\le(d+1)^{1/2}\ell_\infty(f).$$

Finally, we remark that

$$\Big|\frac{a_{d-r}}{a_d}\Big| = \Big|\sum_{j_1<\cdots<j_r} \alpha_{j_1}\cdots\alpha_{j_r}\Big|,$$

hence

$$|a_{d-r}| \le \binom{d}{r} |a_d| \prod_{j=1}^{d} \max(1, |\alpha_j|).$$

By Jensen's formula, we conclude that

$$|a_{d-r}| \le \binom{d}{r} M(f). \qquad \square$$

The following consequence, **Northcott's theorem**, is very important.

Theorem 1.6.8. *There are only finitely many algebraic numbers of bounded degree and bounded height.*

Proof: Let α be algebraic of degree d and height $h(\alpha) \le \log H$. Let $f(t) = a_d t^d + \cdots + a_0$ be the minimal polynomial of α over $\mathbb{Z}$. By Proposition 1.6.6, we have $M(f) \le H^d$. Also, Lemma 1.6.7 shows that $\max|a_i| \le 2^d M(f)$. Therefore, the coefficients of f are bounded by $(2H)^d$. Since there are $d+1$ integer coefficients for each f, they give rise to not more than $(2\lfloor(2H)^d\rfloor+1)^{d+1}$ distinct polynomials f. Since each f has d roots, the number of algebraic integers of degree d and height at most H is at most $d(2\lfloor(2H)^d\rfloor+1)^{d+1} \le (5H)^{d^2+d}$. $\square$

For later use, we prove here a result of K. Mahler [**188**], which gives a bound for the discriminant in terms of the Mahler measure.

Proposition 1.6.9. *Let $f(x) = a_d x^d + \cdots + a_0$ be a polynomial with real or complex coefficients, with roots $\alpha_1, \ldots, \alpha_d$. Let*

$$D = a_d^{2d-2} \prod_{i>j} (\alpha_i - \alpha_j)^2$$

be its discriminant. Then

$$|D| \le d^d\, M(f)^{2d-2}.$$

In particular, if $f(x)$ is the minimal polynomial over $\mathbb{Z}$ of an algebraic number ξ of degree d, it holds

$$\frac{1}{d}\log|D| \le \log d + (2d-2)h(\xi).$$

Proof: We write D as the product of a_d^{2d-2} and the square of a Vandermonde determinant (see B.1.10 and Remark B.1.5) and estimate the determinant using

Hadamard's inequality,* obtaining

$$|D| = |a_d|^{2d-2} \left| \det \begin{pmatrix} 1 & \alpha_1 & \dots & \alpha_1^{d-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{d-1} \\ \vdots & \vdots & \dots & \vdots \\ 1 & \alpha_d & \dots & \alpha_d^{d-1} \end{pmatrix} \right|^2 \le |a_d|^{2d-2} \prod_{i=1}^{d} \left(\sum_{j=0}^{d-1} |\alpha_i^j|^2 \right).$$

The right-hand side of this inequality does not exceed

$$|a_d|^{2d-2} d^d \prod_{1=1}^{d} \max(1, |\alpha_i|)^{2d-2}$$

and the first statement follows from Jensen's formula, Proposition 1.6.5.

The second statement is also clear from Proposition 1.6.6. □

Lemma 1.6.10. *Let $f(t_1, \dots, t_n)$ be a polynomial with complex coefficients and partial degrees $d_1, \dots, d_n$. Then*

$$\prod_{j=1}^{n} (d_j + 1)^{-1/2} M(f) \le \ell_\infty(f) \le \prod_{j=1}^{n} \binom{d_j}{\lfloor d_j/2 \rfloor} M(f).$$

Proof: The same proof as in Lemma 1.6.7 holds for the inequality on the left. We prove the other assertion by induction on n. We can write uniquely

$$f(t_1, \dots, t_n) = \sum_{j=0}^{d_n} f_j(t_1, \dots, t_{n-1})\, t_n^j$$

for certain polynomials $f_j(t_1, \dots, t_{n-1})$. By definition, it holds

$$\log M(f) = \int_{\mathbb{T}^{n-1}} \log M\big(f(e^{i\theta_1}, \dots, e^{i\theta_{n-1}}, t)\big)\, \mathrm{d}\mu_1 \cdots \mathrm{d}\mu_{n-1}$$

and this is not smaller than

$$\int_{\mathbb{T}^{n-1}} \log \max_j |f_j(e^{i\theta_1}, \dots, e^{i\theta_{n-1}})|\, \mathrm{d}\mu_1 \cdots \mathrm{d}\mu_{n-1} - \log \binom{d_n}{\lfloor d_n/2 \rfloor}$$

by Lemma 1.6.7, and which in turn is not smaller than

$$\max_j \int_{\mathbb{T}^{n-1}} \log |f_j(e^{i\theta_1}, \dots, e^{i\theta_{n-1}})|\, \mathrm{d}\mu_1 \cdots \mathrm{d}\mu_{n-1} - \log \binom{d_n}{\lfloor d_n/2 \rfloor}.$$

---

*The inequality states that a determinant of a real matrix is majorized by the product of the euclidean lengths of its rows. Geometrically, it says that the volume of a parallelepiped generated by real vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ of given length is maximal when the vectors $\mathbf{v}_i$ are pairwise orthogonal, which is quite easy to prove. The result also holds for complex matrices. Hadamard's proof of 1893 can be found, among an interesting analysis of extremal cases with entries ± 1 (the so-called Hadamard's matrices), in [**143**]. The result was known much earlier to Lord Kelvin and was proved by T. Muir in 1885, see [**209**], p.32.

We conclude that

$$\binom{d_n}{\lfloor d_n/2 \rfloor} M(f) \geq \max_j M(f_j)$$

and the induction hypothesis implies the claim. □

As remarked above, Lemma 1.6.7 leads to **Gelfond's lemma**:

Lemma 1.6.11. *Let $f_1, \ldots, f_m$ be complex polynomials in n variables and set $f := f_1 \cdots f_m$. Then*

$$2^{-d} \prod_{j=1}^{m} \ell_\infty(f_j) \leq \ell_\infty(f) \leq 2^d \prod_{j=1}^{m} \ell_\infty(f_j),$$

where d is the sum of the partial degrees of f.

Proof: Let $\left(d_1^{(j)}, \ldots, d_n^{(j)}\right)$ be the partial degrees of f_j. By carrying out the multiplication, we see that

$$\ell_\infty(f) \leq C \prod_{j=1}^{m} \ell_\infty(f_j)$$

with

$$C = \prod_{j=1}^{m-1} \prod_{k=1}^{n} \left(1 + d_k^{(j)}\right) \leq 2^d.$$

In the other direction, Lemma 1.6.10 implies

$$\prod_{j=1}^{m} \ell_\infty(f_j) \leq \left(\prod_{j=1}^{m} \prod_{k=1}^{n} \binom{d_k^{(j)}}{\lfloor d_k^{(j)}/2 \rfloor} \right) \left(\prod_{k=1}^{n} \left(1 + \sum_{j=1}^{m} d_k^{(j)} \right)^{1/2} \right) \ell_\infty(f).$$

The next lemma completes the proof.

Lemma 1.6.12. *Let $a \leq A, b \leq B$ and d be natural numbers. Then $\binom{A}{a}\binom{B}{b} \leq \binom{A+B}{a+b}$ and $\binom{d}{\lfloor d/2 \rfloor}(d+1)^{1/2} \leq 2^d$.*

Proof: The first statement is a trivial consequence of the identity

$$(1+t)^A (1+t)^B = (1+t)^{A+B}.$$

For the second claim (which also follows from a straightforward application of Stirling's formula), we proceed by induction. The inequality is obviously satisfied for $d = 0$ and $d = 1$. Set $C_d := \binom{d}{\lfloor d/2 \rfloor}(d+1)^{1/2}$ and let $m \in \mathbb{N}$; then

$$C_{2m+1}/C_{2m} = 2\left(1 - \frac{1}{2m+2}\right)^{1/2} < 2$$

and

$$C_{2m+2}/C_{2m} = 4\left(1 - \frac{1}{(2m+2)^2}\right)^{1/2} < 4.$$

The induction hypothesis implies the second statement. □

Gelfond's and Gauss's lemma together with Lemma 1.3.7 give us

Theorem 1.6.13. *Let $f_1, \dots, f_m$ be polynomials in n variables with coefficients in $\overline{\mathbb{Q}}$ and let d be the sum of the partial degrees of $f := f_1 \cdots f_m$. Then*

$$-d \log 2 + \sum_{j=1}^{m} h(f_j) \leq h(f) \leq d \log 2 + \sum_{j=1}^{m} h(f_j).$$

Remark 1.6.14. For the upper bound, only the sum d' of the partial degrees of $f_1 \cdots f_{m-1}$ does matter. In fact, the proof of Gelfond's lemma shows

$$|f|_v \leq \left(\prod_{j=1}^{m-1} \prod_{k=1}^{n} |1 + d_k^{(j)}|_v \right) \prod_{j=1}^{m} |f_j|_v \leq |2|_v^{d'} \prod_{j=1}^{m} |f_j|_v$$

for any archimedean place v of a number field containing all the coefficients. Then

$$h(f) \leq \sum_{j=1}^{m} h(f_j) + \sum_{j=1}^{m-1} \sum_{k=1}^{n} \log(1 + d_k^{(j)}) \leq \sum_{j=1}^{m} h(f_j) + d' \log 2,$$

which is often important for applications.

1.6.15. We conclude this section by mentioning an interesting question raised by D.H. Lehmer ([**180**], p.476), known today as the **Lehmer conjecture** (in Lehmer's paper, this was addressed as a problem rather than a conjecture). If $\alpha \neq 0$ is algebraic with minimal polynomial f, the Mahler measure of α is $M(\alpha) := M(f)$. By Proposition 1.6.6, we have $M(\alpha) = H(\alpha)^{\deg(\alpha)}$. Now the question raised by Lehmer is whether there is an absolute constant c such that $M(\alpha) \geq c > 1$ for $\alpha \in \overline{\mathbb{Q}}^{\times}$ not a root of unity. Alternatively, $h(\alpha) \geq c/d$ for some absolute constant c.

The last inequality in the proof of Lemma 1.6.7 with $r = 0$ or d shows that $h(\alpha) \geq (\log 2)/d$ unless α is a unit. The same argument also shows that

$$h(\alpha) \geq -\log 2 + \frac{1}{d} \log \ell_\infty(f)$$

for all α. In particular, $h(\alpha) \geq (\log 2)/d$ if $\ell_\infty(f) \geq 2^{d+1}$. Since there are only finitely polynomials f of degree d with integer coefficients and with $\ell_\infty(f) < 2^{d+1}$, by Kronecker's theorem 1.5.9 we deduce that there is $c(d) > 0$ such that any α of degree d, not a root of unity, satisfies $h(\alpha) \geq c(d)$. Thus in studying Lehmer's problem we may assume that d is arbitrarily large.

The algebraic number α with minimal polynomial $x^{10}+x^9-x^7-x^6-x^5-x^4-x^3+x+1$ has $M(\alpha) = 1.17628081825991\dots$ and is conjectured to yield the infimum of the Mahler measure of an algebraic number.[†]

[†] This polynomial already appears in Lehmer's paper *loc. cit.*, with a slightly different numerical value which we have corrected here.

If f is not reciprocal (a reciprocal polynomial $f(z)$ satisfies $f(z) = \pm z^{\deg(f)} f(1/z)$), a nice theorem by C.J. Smyth [**287**] states that the minimum of $M(\alpha)$ occurs for the cubic number with minimal equation $x^3 - x - 1$. This non-reciprocal number α is about $\alpha = 1.32471795724474\ldots$. In the general case, for large d we have E. Dobrowolski's theorem [**90**]

$$M(\alpha) \geq 1 + c\left(\frac{\log\log d}{\log d}\right)^3,$$

following from Theorem 4.4.1.

1.7. Lower bounds for norms of products of polynomials

We elaborate here further on the question of lower bounds for norms of products of polynomials. The interesting question is to obtain lower bounds which are proportional to the product of the norms, as in Gelfond's lemma of the preceding section. It turns out that for certain natural norms the constants involved in such lower bounds depend only on the degrees of the polynomials, not on the number of variables. This section will not be needed at other places of the book.

1.7.1. Let us denote by $\ell_p(f)$ the ℓ_p-norm of the coefficients of a complex polynomial f. We shall prove that for $p = 1$ and $p = 2$ the ℓ_p-norm has the properties mentioned above. This result extends to all p, $1 \leq p < \infty$, but we will not prove this extension here. The more difficult case $p = 1$ is due to Enflo, who used it in his work on invariant subspaces of bounded operators in Banach spaces.

Theorem 1.7.2. *Let $d, e \in \mathbb{N}$. Then there is a constant $C(d,e) > 0$ such that*

$$\ell_1(fg) \geq C(d,e)\ell_1(f)\ell_1(g)$$

for complex polynomials f, g of degree d, e in several variables.

Proof: (H.L. Montgomery) For $k \in \mathbb{N}$, we define

$$C(d,e,k) := \inf \frac{\ell_1(P^k Q)}{\ell_1(P)^k \ell_1(Q)},$$

where the infimum ranges over all homogeneous polynomials P, Q of degree d, e.

We shall use in the sequel Euler's formula

$$\sum_j t_j \frac{\partial f}{\partial t_j} = df$$

for a homogeneous polynomial $f \in \mathbb{C}[t_1, \ldots, t_n]$ of degree d, and the formula

$$\sum_j \ell_1\left(\frac{\partial f}{\partial t_j}\right) = \sum_j \ell_1\left(t_j \frac{\partial f}{\partial t_j}\right) = d\ell_1(f).$$

Both are proved directly by looking at each monomial in f.

Lemma 1.7.3. *The following two estimates hold:*

$$C(d,0,k+1) \geq C(d-1, dk, 1)\, C(d,0,k) \qquad \text{if } d \geq 1,$$

$$C(d,e,k) \geq \frac{e}{2kd+e}\, C(d,e-1,k+1) \quad \text{if } e \geq 1.$$

Proof: Let f be homogeneous of degree d. We compute

$$\begin{aligned}\ell_1\Big(\frac{\partial}{\partial t_j} f^{k+1}\Big) &= (k+1)\,\ell_1\Big(f^k \frac{\partial f}{\partial t_j}\Big)\\ &\geq (k+1)\,C(d-1,dk,1)\,\ell_1\Big(\frac{\partial f}{\partial t_j}\Big)\,\ell_1\Big(f^k\Big)\\ &\geq (k+1)C(d-1,dk,1)\,C(d,0,k)\,\ell_1\Big(\frac{\partial f}{\partial t_j}\Big)\,\ell_1(f)^k\,.\end{aligned}$$

Summing over j, we find

$$(k+1)\,d\,\ell_1\Big(f^{k+1}\Big) \geq (k+1)\,C(d-1,dk,1)\,C(d,0,k)\,d\,\ell_1(f)^{k+1}$$

proving the first statement.

In a similar fashion, for f and g homogeneous of degrees d and e, we also have

$$\begin{aligned}C(d,e-1,k+1)\,\ell_1(f)^{k+1}\,\ell_1\Big(\frac{\partial g}{\partial t_j}\Big) &\leq \ell_1\Big(f^{k+1}\frac{\partial g}{\partial t_j}\Big)\\ &= \ell_1\Big(f\frac{\partial}{\partial t_j}(f^k g) - k f^k g \frac{\partial f}{\partial t_j}\Big)\\ &\leq \ell_1(f)\,\ell_1\Big(\frac{\partial}{\partial t_j}(f^k g)\Big) + k\,\ell_1\Big(f^k g\Big)\,\ell_1\Big(\frac{\partial f}{\partial t_j}\Big)\,.\end{aligned}$$

Summing over j, we obtain

$$\begin{aligned}C(d,e-1,k+1)\,e\,\ell_1(f)^{k+1}\,\ell_1(g) &\leq (dk+e)\,\ell_1(f)\,\ell_1\Big(f^k g\Big) + kd\,\ell_1\Big(f^k g\Big)\,\ell_1(f)\\ &= (2kd+e)\,\ell_1(f)\,\ell_1\Big(f^k g\Big)\,.\end{aligned}$$

After cancelling a factor $\ell_1(f)$, we get the claim. □

The proof of Enflo's theorem is now easy. There is no loss of generality in assuming that f and g are homogeneous polynomials. We order the triples (d,e,k) lexicographically. Proceeding by induction, we prove that $C(d,e,k) > 0$. If $d = 0$ or $k = 0$, then $C(d,e,k) = 1$. So let us assume that $d > 0, k > 0$. By Lemma 1.7.3, it is enough to show the claim for a smaller triple, and we are done. This gives Theorem 1.7.2, with $C(d,e) := C(d,e,1) > 0$. □

1.7.4. The double induction in the proof of the theorem is very expensive for the final estimates. Let us compute some of the constants so obtained. We define recursively $\Gamma(d,e,k)$ as follows

$$\Gamma(d,e,k) = \begin{cases} 1 & \text{if } d = 0 \text{ or } k = 0\\ \Gamma(d-1,d(k-1),1)\,\Gamma(d,0,k-1) & \text{if } e = 0 \text{ and } dk \neq 0\\ \frac{e}{2kd+e}\,\Gamma(d,e-1,k+1) & \text{if } dek \neq 0\end{cases}$$

and hence $\Gamma(d,e,k) \le C(d,e,k)$. For example

$$\Gamma(d,0,1) = 1 \qquad C(d,0,1) = 1$$
$$\Gamma(1,1,1) = 1/3 \qquad C(1,1,1) = \frac{1}{2}$$
$$\Gamma(2,2,1) = 1/34020$$
$$\Gamma(3,3,1) = 1/(3.840584... \times 10^{95})$$
$$\Gamma(4,4,1) = 1/(2.089942... \times 10^{13529})$$
$$\Gamma(5,5,1) = 1/(6.562189... \times 10^{19906418})$$

and the computer took too much time for $\Gamma(6,6,1)$.

1.7.5. The solution for the case $p = 2$ uses the concept of **hypercube representation** of a polynomial. The usual way of writing a homogeneous polynomial of degree d in n variables is to represent it in the form

$$f(t_1,\dots,t_n) = \sum_{i_1+\cdots+i_n=d} \cdots \sum a_{i_1\dots i_n} t_1^{i_1} \cdots t_n^{i_n}.$$

The sum here runs over the lattice points in the hyperplane $i_1 + \cdots + i_n = d$ of the n-dimensional cube $0 \le i_\nu \le d$, $\nu = 1,\dots,n$. Note that the number of lattice points in this cube is $(d+1)^n$, growing exponentially in n for fixed d.

There is another way of writing the same polynomial, namely

$$f(t_1,\dots,t_n) = \frac{1}{d!} \sum_{i_1=1}^{n} \cdots \sum_{i_d=1}^{n} \frac{\partial^d f}{\partial t_{i_1} \cdots \partial t_{i_d}}\, t_{i_1} \cdots t_{i_d}\,;$$

we define this as the hypercube representation of f, since now the sum is indexed by the lattice points of the d-dimensional cube $1 \le i_\delta \le n$, $\delta = 1,\dots,d$. The number of lattice points in this cube is n^d, which grows polynomially in n for fixed d.

The hypercube representation of a polynomial is very convenient if we want to study polynomials of low degree in a large number of variables.

1.7.6. Define for $p \ge 1$

$$[f]_p := \frac{1}{d!} \left(\sum_{i_1=1}^{n} \cdots \sum_{i_d=1}^{n} \left| \frac{\partial^d f}{\partial t_{i_1} \cdots \partial t_{i_d}} \right|^p \right)^{1/p}.$$

If we compare this norm with the ℓ_p-norm of the coefficients, simple combinatorics lead to

$$\left(\frac{1}{d!}\right)^{1-\frac{1}{p}} \ell_p(f) \le [f]_p \le \ell_p(f). \tag{1.11}$$

1.7.7. Let $d, e \in \mathbb{N}$. A **shuffle of type** (d,e) is a pair (K,L), where K and L are disjoint subsets of $\{1,\dots,d+e\}$ of cardinality d and e. The set of shuffles of type (d,e) will be denoted by $\mathrm{sh}(d,e)$. Its cardinality is equal to $\binom{d+e}{d}$. For $\mathbf{x} = (x_1,\dots,x_{d+e}) \in [0,1]^{d+e}$, we define $\mathbf{x}_K := (x_{k_1},\dots,x_{k_d})$, where $\{k_1,\dots,k_d\} = K$ and $k_1 < \cdots < k_d$.

Let $k_p(d,e)$ be the largest constant such that

$$[fg]_p \geq k_p(d,e)\,[f]_p[g]_p$$

holds for all homogeneous polynomials f, g of degree d, e. Moreover, we define $c_p(d,e)$ as the largest constant for which

$$\left\| \sum_{(K,L)\in \mathrm{sh}(d,e)} F(\mathbf{x}_K)G(\mathbf{x}_L) \right\|_p \geq c_p(d,e)\,\|F\|_p\,\|G\|_p$$

holds for all symmetrical functions $F \in L^p([0,1]^d)$, $G \in L^p([0,1]^e)$, with $\|\ \|_p$ denoting the L^p-norm.

Lemma 1.7.8. *The constants $c_p(d,e)$ and $k_p(d,e)$ are related by*

$$c_p(d,e) = \binom{d+e}{d} k_p(d,e).$$

Proof: Let $f(t_1,\dots,t_n)$ be a homogeneous polynomial of degree d and let F be the symmetrical step function on $[0,1)^d$ given by

$$F(x_1,\dots,x_d) = n^{d/p}\,\frac{1}{d!}\,\frac{\partial^d f}{\partial t_{i_1}\cdots\partial t_{i_d}}$$

for $\frac{i_1-1}{n} \leq x_1 < \frac{i_1}{n}, \dots, \frac{i_d-1}{n} \leq x_d < \frac{i_d}{n}$. Also, let $g(t_1,\dots,t_n)$ be a homogeneous polynomial of degree e and define G in the same way as F.

Then we verify that

$$[f]_p = \|F\|_p, \qquad [g]_p = \|G\|_p, \qquad [fg]_p = \frac{d!e!}{(d+e)!}\left\| \sum_{(K,L)\in \mathrm{sh}(d,e)} F(\mathbf{x}_K)G(\mathbf{x}_L) \right\|_p.$$

The rest of the proof is an approximation argument. Consider the discretization i/n, $i = 1,\dots,n$ of $[0,1]$; given continuous F, G on $[0,1]^d$ and $[0,1]^e$, we approximate F, G by step functions as above and construct corresponding polynomials f, g. As $n \to \infty$, these functions are dense in $L^p([0,1]^d)$ and $L^p([0,1]^e)$. □

Proposition 1.7.9. *The constant $c_2(d,e)$ is*

$$c_2(d,e) = \binom{d+e}{d}^{1/2}.$$

Proof: Let F, G be symmetrical L^2-functions as in 1.7.7. Then

$$\left\| \sum_{(K,L)\in \mathrm{sh}(d,e)} F(\mathbf{x}_K)G(\mathbf{x}_L) \right\|_2^2 = \sum_{\substack{(K,L)\in \mathrm{sh}(d,e)\\ (K',L')\in \mathrm{sh}(d,e)}} \int_{[0,1]^{d+e}} F(\mathbf{x}_K)G(\mathbf{x}_L)\,\overline{F(\mathbf{x}_{K'})G(\mathbf{x}_{L'})}\,\mathrm{d}\mathbf{x}$$

and this is equal to

$$\binom{d+e}{d}\|F\|_2^2\,\|G\|_2^2 + \sum_{(K,L)\neq(K',L')} \int_{[0,1]^{d+e}} F(\mathbf{x}_K)\overline{G(\mathbf{x}_{L'})}\ \overline{F(\mathbf{x}_{K'})}G(\mathbf{x}_L)\,\mathrm{d}\mathbf{x}.$$

The integral is not negative, as we verify as follows. We have

$$\int_{[0,1]^{d+e}} F(\mathbf{x}_K)\overline{G(\mathbf{x}_{L'})}\ \overline{F(\mathbf{x}_{K'})}\,G(\mathbf{x}_L)\,\mathrm{d}\mathbf{x} =$$
$$\int_{[0,1]^{d+e}} F(\mathbf{x}_{K\cap K'},\mathbf{x}_{K\cap L'})\overline{G(\mathbf{x}_{K\cap L'},\mathbf{x}_{L\cap L'})}\times$$
$$\overline{F(\mathbf{x}_{K\cap K'},\mathbf{x}_{L\cap K'})}G(\mathbf{x}_{L\cap K'},\mathbf{x}_{L\cap L'})\,\mathrm{d}\mathbf{x}_{K\cap K'}\,\mathrm{d}\mathbf{x}_{K\cap L'}\,\mathrm{d}\mathbf{x}_{L\cap K'}\,\mathrm{d}\mathbf{x}_{L\cap L'}.$$

Now we integrate first with respect to $\mathrm{d}\mathbf{x}_{K\cap L'}\,\mathrm{d}\mathbf{x}_{L\cap K'}$. By Fubini's theorem, we obtain

$$\left|\int F(\mathbf{x}_{K\cap K'},\mathbf{z})\overline{G(\mathbf{z},\mathbf{x}_{L\cap L'})}\,\mathrm{d}\mathbf{z}\right|^2.$$

This proves non-negativity and $c_2(d,e) \geq \binom{d+e}{e}^{1/2}$.

The choices

$$F(x_1,\dots,x_d) = \cos(2\pi x_1)\cdots\cos(2\pi x_d), \quad G(x_1,\dots,x_e) = \sin(2\pi x_1)\cdots\sin(2\pi x_e),$$

also show, by orthogonality, that the constant $\binom{d+e}{e}^{1/2}$ is sharp. □

Corollary 1.7.10. *Let f, g be complex polynomials of degree d, e. Then:*

(a) $k_2(d,e) = \binom{d+e}{e}^{-1/2}$.

(b) $\ell_2(fg) \geq \frac{1}{\sqrt{(d+e)!}}\,\ell_2(f)\,\ell_2(g)$.

Proof: We may suppose that f, g are homogeneous. The first claim follows from Lemma 1.7.8 and Proposition 1.7.9. The second follows from (a) and (1.11) on page 31. □

1.8. Bibliographical notes

The material in the first five sections of this chapter is quite standard and was mainly taken from S. Lang [**169**] and J.-P. Serre [**277**]. However, the reader must be warned that our normalization for absolute values does not always agree with the normalization used by other authors. The rationale for our normalization is that the degree $[K:\mathbb{Q}]$ does not appear in the first formula in Lemma 1.3.7, and therefore it is absent in the definition of the absolute logarithmic height. This leads to formulas invariant by field extensions.

The proof of Gelfond's lemma in Section 1.6 follows K. Mahler [**187**], where the important Mahler's height is introduced. The inequality $M(f) \leq \|f\|_{L^2(\mathbb{T})}$ appearing in the proof of Lemma 1.6.7 can be found in E. Landau [**164**], Satz 443, with a somewhat different proof.

Section 1.7 is mostly from B. Beauzamy, E. Bombieri, P. Enflo, and H.L. Montgomery [**18**].

2 WEIL HEIGHTS

2.1. Introduction

In this chapter we study heights from a geometric point of view.

We begin with the important Section 2.2 introducing local Weil heights associated to Cartier divisors on a projective variety X, and studying their properties. These considerations are given here only for projective varieties, where the treatment is simpler.

Section 2.3 studies global Weil heights and their equivalence classes up to bounded functions.

In Section 2.4, we study the height on a projective variety induced by the height in the ambient projective space and in particular we prove the important Northcott's theorem on the finiteness of the number of points of bounded degree and bounded height in a fixed projective space.

These three sections are very important for the handling of heights in diophantine geometry and are required from Chapter 9 onwards.

In Section 2.5, which contains new material, the notion of presentation of a projective variety is introduced and explicit comparison theorems for the heights of a variety X in two different projective embeddings are given, in terms of presentations of these embeddings. This section may be skipped in a first reading. It will be used only partially in Section 11.7 and implicitly in questions dealing with effectivity.

Sections 2.6 and 2.7 extend the results obtained on local and global Weil heights to the associated heights of locally bounded metrized line bundles on a complete variety. They will be also used in the second half of the book.

Section 2.8 studies heights on Grassmann varieties and their properties. We need it only for Section 2.9, where we state the important Siegel's lemma in a strong form, as a consequence of Minkowski's geometry of numbers. For a quick tour, the reader may take from the last two sections only the elementary version of Siegel's

lemma over $\mathbb{Z}$ given in 2.9.1 and its Corollary 2.9.2 over number fields, where the constants are not made explicit, but which is quite often enough for applications.

2.2. Local heights

The reader should be familiar with the concept of Cartier divisors and its connexion to meromorphic sections of line bundles, as in A.8.

In this section we introduce local heights associated to Cartier divisors on a projective variety X. However, in order to define them properly we need additional data beyond the divisor D itself, namely a realization $O(D) = O(D_+) \otimes O(-D_-)$ with base-point-free line bundles $O(D_\pm)$ coming with given sets of generating global sections. The set of Cartier divisors equipped with these additional data forms a monoid, and the local heights so defined behave functorially with respect to this monoid. This removes the need of working modulo bounded functions when studying Weil heights, a point of crucial importance for applications because it allows precise estimates.

2.2.1. Let K be a field and let us fix an absolute value $|\ |$ on $\overline{K}$. Let X be a projective variety over K, which for simplicity we assume here to be irreducible.

Let D be a Cartier divisor on X with associated line bundle $O(D)$ and meromorphic section s_D. For construction of $O(D)$ and s_D, see A.8.18. Note that the associated Cartier divisor $D(s_D)$ of s_D is equal to D.

There are base-point-free line bundles L, M on X such that $O(D) \cong L \otimes M^{-1}$ (cf. A.6.10 (a)). Now choose generating global sections $s_0, \dots, s_n$ of L and $t_0, \dots, t_m$ of M, and call the data

$$\mathcal{D} = (s_D;\ L, \mathbf{s};\ M, \mathbf{t})$$

a **presentation** of the Cartier divisor D.

2.2.2. For $P \notin \operatorname{supp}(D)$, we define

$$\lambda_{\mathcal{D}}(P) := \max_k \min_l \log \left| \frac{s_k}{t_l s_D}(P) \right|.$$

We use the notation $t_l s_D$ for $t_l \otimes s_D$ and s_k/s' for $s_k \otimes (s')^{-1}$. Hence $s_k/(t_l s_D)$ is a rational function on X.

We call $\lambda_{\mathcal{D}}(P)$ the **local height** of P relative to the presentation $\mathcal{D}$ and, by abuse of language, relative to D. In fact, it depends on the choice of s_D as well as on L, M and their generating sections. The local height is a real-valued function defined outside of the support of the divisor D.

Example 2.2.3. Let f be a non-zero rational function on X with Cartier divisor $D := D(f)$. Then $O(D) = O_X$ and f is a meromorphic section of

$O(D)$. Thus there is a local height λ_f relative to D, given by the presentation $(f;\, O_X, 1;\, O_X, 1)$. For $P \notin \operatorname{supp}(D)$, we have

$$\lambda_f(P) = -\log |f(P)|.$$

If g is another non-zero rational function on X, then $\lambda_{fg} = \lambda_f + \lambda_g$ and $\lambda_{f^{-1}} = -\lambda_f$.

2.2.4. Let D_1 and D_2 be Cartier divisors with presentations

$$\mathcal{D}_i = (s_{D_i};\, L_i, \mathbf{s}_i;\, M_i, \mathbf{t}_i)$$

and local heights $\lambda_{\mathcal{D}_i}$. Then $\mathbf{s}_1\mathbf{s}_2 = (s_{1k}s_{2k'})$, $\mathbf{t}_1\mathbf{t}_2 = (t_{1l}t_{2l'})$ are generating global sections of $L_1 \otimes L_2$, $M_1 \otimes M_2$, and we define $\lambda_{\mathcal{D}_1+\mathcal{D}_2}$ as the local height relative to the presentation

$$\mathcal{D}_1 + \mathcal{D}_2 = (s_{D_1}s_{D_2};\, L_1 \otimes L_2, \mathbf{s}_1\mathbf{s}_2;\, M_1 \otimes M_2, \mathbf{t}_1\mathbf{t}_2)$$

of the divisor $D_1 + D_2$. It is obvious that with this presentation we have

$$\lambda_{\mathcal{D}_1+\mathcal{D}_2}(P) = \lambda_{\mathcal{D}_1}(P) + \lambda_{\mathcal{D}_2}(P)$$

for $P \in X$, $P \notin \operatorname{supp}(D_1) \cup \operatorname{supp}(D_2)$.

2.2.5. If $\lambda_{\mathcal{D}}$ is a local height with presentation $(s_D;\, L, \mathbf{s};\, M, \mathbf{t})$, then $\lambda_{-\mathcal{D}}$ is defined by the presentation $(s_D^{-1};\, M, \mathbf{t};\, L, \mathbf{s})$ and we have

$$\lambda_{-\mathcal{D}}(P) = -\lambda_{\mathcal{D}}(P)$$

for $P \in X \setminus \operatorname{supp}(D)$. With these operations, the space of local heights is an abelian group.

2.2.6. Another important operation on presentations is the pull-back. If

$$\mathcal{D} = (s_D;\, L, \mathbf{s};\, M, \mathbf{t})$$

is a presentation of D on X and $\pi : Y \longrightarrow X$ is a dominant morphism of irreducible projective varieties over K, then

$$\pi^*\mathcal{D} = (\pi^*s_D;\, \pi^*L, \pi^*s;\, \pi^*M, \pi^*\mathbf{t})$$

is a presentation of π^*D. We have $\lambda_{\pi^*\mathcal{D}}(P) = \lambda_{\mathcal{D}}(\pi(P))$ for every $P \in Y$ such that $\pi(P) \notin \operatorname{supp}(D)$. More generally, this works for a morphism $\pi : Y \to X$ of irreducible projective varieties such that $\pi(Y)$ is not contained in $\operatorname{supp}(D)$.

We consider an affine variety U over K.

Lemma 2.2.7. *Let $h_j \in K[U]$, $j = 1, \ldots, N$, be without common zero in U. Then the ideal generated by the functions h_j is equal to $K[U]$.*

Proof: Choose a closed embedding $U \longrightarrow \mathbb{A}^n_K$ and let $I(U)$ be the ideal of U in $K[t_1, \ldots, t_n]$. The K-algebra $K[U]$ can be identified with $K[t_1, \ldots, t_n]/I(U)$. Let $\mathfrak{I}$ be the inverse image of the ideal generated by $h_1, \ldots, h_m$ under the projection

$$K[t_1, \ldots, t_n] \longrightarrow K[t_1, \ldots, t_n]/I(U).$$

We claim that $\mathfrak{I}$ is equal to $K[t_1, \ldots, t_n]$. In fact, the polynomials in $\mathfrak{I}$ have no common zero, and our claim follows from Hilbert's Nullstellensatz in A.2.2. □

Definition 2.2.8. *The set $E \subset U(\overline{K})$ is **bounded** in U if for any $f \in K[U]$ the function $|f|$ is bounded on E.*

Lemma 2.2.9. *Let $\{f_1, \ldots, f_N\}$ be generators of $K[U]$ as a K-algebra. If*

$$\sup_{P \in E} \max_{j=1,\ldots,N} |f_j(P)| < \infty$$

holds, then E is bounded.

Proof: Let $f \in K[U]$. Then we can write $f = p(f_1, \ldots, f_N)$ with p a polynomial with coefficients in K. Let C be the number of monomials in p and let d be the degree of p. We define

$$\delta := \begin{cases} 1 & \text{if the absolute value is archimedean} \\ 0 & \text{otherwise.} \end{cases}$$

Then, with $|p|$ the Gauss norm of p from 1.6.3, we find

$$\sup_{P \in E} |f(P)| \leq C^{\delta} |p| \max\left(1, \sup_{P \in E} \max_{j=1,\ldots,N} |f_j(P)|\right)^d < \infty, \tag{2.1}$$

concluding the proof. □

Lemma 2.2.10. *If $\{U_l\}$ is a finite affine open covering of the affine K-variety U and if E is bounded in U, then there are bounded subsets E_l of U_l such that $E = \bigcup_l E_l$.*

Proof: It is enough to prove the claim for a refinement of $\{U_l\}$. Hence we can assume that there are regular functions h_l on U such that $U_l = \{x \in U \mid h_l \neq 0\}$, see A.2.10. By Lemma 2.2.7 there are regular functions g_l on U such that $\sum_l g_l h_l = 1$. If C is the cardinality of the covering and δ is as before, then

$$\inf_{P \in E} \max_l |h_l(P)| \geq C^{-\delta} \left(\sup_{P \in E} \max_l |g_l(P)|\right)^{-1} > 0. \tag{2.2}$$

We define

$$E_l := \{P \in E \mid |h_l(P)| = \max_k |h_k(P)|\}.$$

Obviously, $E_l \subset U_l(\overline{K})$ and $E = \bigcup_l E_l$. Let $f_1, \ldots, f_N$ be a set of generators of $K[U]$. Then $f_1, \ldots, f_N, 1/h_l$ are generators of $K[U_l]$. By Lemma 2.2.9, it is enough to show that $|1/h_l|$ is bounded on E_l. In fact, the bound

$$\sup_{P \in E_l} |1/h_l(P)| \leq C^{\delta} \sup_{P \in E} \max_k |g_k(P)| < \infty. \tag{2.3}$$

follows from (2.2). □

Theorem 2.2.11. *Let X be a projective variety over K and let $\mathcal{D}$, $\mathcal{D}'$ be two presentations of the Cartier divisor D. Then*

$$|\lambda_{\mathcal{D}} - \lambda_{\mathcal{D}'}| \leq \gamma$$

for some constant $\gamma < \infty$.

Proof: By 2.2.4, we see that $\lambda_{\mathcal{D}} - \lambda_{\mathcal{D}'}$ is a local height relative to the presentation $\mathcal{D} - \mathcal{D}'$ of the zero divisor. Therefore, the left-hand side of the inequality extends to a well-defined real function on X. Moreover, it is enough to show the claim for $D = 0$ and $\mathcal{D}' = (1;\, L, 1;\, M, 1)$. Then $\mathcal{D}$ has the form $(1;\, L, \mathbf{s};\, L, \mathbf{t})$. We need to find γ as above such that

$$-\gamma \leq \max_k \min_l \log \left| \frac{s_k}{t_l}(P) \right| \leq \gamma.$$

To this end, it suffices to obtain only the right-hand of this inequality, because we can interchange the role of $\mathbf{s}$ and $\mathbf{t}$.

Now choose a closed embedding of X into $\mathbb{P}^N_K$ with standard coordinates $(x_0 : \cdots : x_N)$, let U_i be the affine open subset $\{x \in X \mid x_i \neq 0\}$ of X, and let U_{il} be the affine open subset $\{x \in U_i \mid t_l(x) \neq 0\}$. The restrictions of $g_{kl} := s_k/t_l$ to U_{il} are regular functions. The functions $f_{ij} := x_j/x_i$, $j = 0, \ldots, N$, generate $K[U_i]$ as a K-algebra (see A.2.10). Then define sets E_i by

$$E_i := \{P \in X(\overline{K}) \mid |x_i(P)| = \max_j |x_j(P)|\}.$$

It is clear that, if $P \in E_i$, we have

$$\max_j |f_{ij}(P)| = 1, \tag{2.4}$$

hence E_i is bounded in U_i (Lemma 2.2.9). Thus we can apply Lemma 2.2.10 to U_i, E_i and the covering $\{U_{il}\}$, obtaining bounded subsets E_{il} of U_{il} such that $E_i = \bigcup_l E_{il}$ and

$$\sup_{P \in E_{il}} \max_k |g_{kl}(P)| < \infty.$$

Since the sets E_{il} cover $X(\overline{K})$, we get the claim. □

2.2.12. Since Hilbert's Nullstellensatz is effective, the constant γ in Theorem 2.2.11 is effectively computable in terms of presentations of $\mathcal{D}$ and $\mathcal{D}'$. An effective version of the Nullstellensatz can be found in D. Masser and G. Wüstholz [**195**], Th.IV.

Remark 2.2.13. For the purpose of giving a precise meaning to the words "effectively computable," we need a closer look at the bounds in the results above.

In Lemma 2.2.9, there are finitely many elements $p_a \in K$ and $d \in \mathbb{N}$ such that

$$\sup_{P \in E} |f(P)| \leq \max_a |p_a| \max \left(1, \sup_{P \in E} \max_j |f_j(P)|\right)^d.$$

The elements p_a may be chosen to be the coefficients of the polynomial p in (2.1) on page 37 if the absolute value is not archimedean, while in the archimedean case it suffices to add to this list C times the coefficients of the list, where C is the number of coefficients. Note also that the list of elements p_a so obtained and the degree d depend only on the geometric data $(U, f, f_1, \ldots, f_N)$, but not on E, nor on the absolute value.

In the situation of Lemma 2.2.10, the bound of $f \in K[U_l]$ is again of the same type, namely

$$\sup_{P \in E_l} |f(P)| \leq \max_m |p_m| \max\left(1, \sup_{P \in E} \max_j |f_j(P)|\right)^d,$$

where again $f_1, \ldots, f_N$ are generators of $K[U]$, the finitely many elements $p_m \in K$, and d, depend only on geometric data (f, the covering, generators) but not on E, the absolute value $|\ |$, or the decomposition $\{E_l\}$. This is clear by applying the above result to $f \in K[U_l]$ with generators $f_1, \ldots, f_N, 1/h$ and then again to every $g_l \in K[U]$ in (2.3) on page 37.

If we apply these remarks to the proof of Theorem 2.2.11 and use (2.4), then we may choose

$$\gamma = \max_m \log^+ |p_m|$$

for a certain finite set of elements $p_m \in K$, independent of the absolute value $|\ |$ and determined exclusively in terms of geometric data.

2.3. Global heights

In this section, starting from the local heights previously defined, we consider the case in which K is a number field and define global heights.

2.3.1. Let X be an irreducible projective variety defined over K.

We consider a Cartier divisor D on X with presentation

$$\mathcal{D} = (s_D;\ L, \mathbf{s};\ M, \mathbf{t}).$$

Let F be a number field with $K \subset F \subset \overline{K}$ and let $P \in X(F) \setminus \operatorname{supp}(D)$. For $v \in M_F$, we define the **local height**

$$\lambda_{\mathcal{D}}(P, v) := \max_k \min_l \log \left| \frac{s_k}{t_l s_D}(P) \right|_v$$

using our normalizations from 1.3.6. Let $p \in M_{\mathbb{Q}}$ be the restriction of v to $\mathbb{Q}$ and let $|\ |_u$ be an absolute value on $\overline{K}$ such that the restriction to K is equivalent to $|\ |_v$ and such that the restriction to $\mathbb{Q}$ is equal to $|\ |_p$. The existence of $|\ |_u$ follows from Proposition 1.3.1. Then

$$\lambda_{\mathcal{D}}(P, v) = \frac{[F_v : \mathbb{Q}_p]}{[F : \mathbb{Q}]} \lambda_{\mathcal{D}}(P, u),$$

where $\lambda_{\mathcal{D}}(P, u)$ is the local height relative to the absolute value $|\ |_u$ from 2.2.2. This allows us to apply the results from Section 2.2 to $\lambda_{\mathcal{D}}(P, v)$.

Example 2.3.2. The hyperplane $\{x_0 = 0\}$ in $\mathbb{P}^n_K$ has the presentation

$$\mathcal{D} = (x_0;\, O_{\mathbb{P}^n}(1), x_0, \ldots, x_n;\, O_{\mathbb{P}^n}, 1).$$

For $P \in \mathbb{P}^n(F)$ with $x_0(P) \neq 0$ and $v \in M_F$ the corresponding local height is

$$\lambda_{\mathcal{D}}(P, v) = \max_k \log \left|\frac{x_k}{x_0}(P)\right|_v$$

and the product formula becomes

$$h(P) = \sum_{v \in M_F} \lambda_{\mathcal{D}}(P, v).$$

This explains the name local height. This notion will be extended later to arbitrary divisors.

2.3.3. We go back to the general case in 2.3.1. Let $\lambda_{\mathcal{D}}$ be a local height relative to the presentation $\mathcal{D} = (s_D;\, L, \mathbf{s};\, M, \mathbf{t})$ of a Cartier divisor D on X. For $P \in X$ there are s_j and t_l such that $s_j(P) \neq 0$, $t_l(P) \neq 0$. Therefore, we can find a non-zero meromorphic section s of $O(D)$ such that P is not contained in the support of the Cartier divisor $D(s)$. Then $\mathcal{D}(s) = (s;\, L, \mathbf{s};\, M, \mathbf{t})$ is a presentation of $D(s)$ and we have

$$\lambda_{\mathcal{D}(s)} = \lambda_{\mathcal{D}} + \lambda_f,$$

where f is the rational function s/s_D. If F is a finite extension $K \subset F \subset \overline{K}$ such that $P \in X(F)$, the local height $\lambda_{\mathcal{D}(s)}(P, v)$ is finite for any $v \in M_L$, because P is not in the support of $D(s)$. Then we define the **global height** of P relative to $\lambda := \lambda_{\mathcal{D}}$ by

$$h_\lambda(P) := \sum_{v \in M_F} \lambda_{\mathcal{D}(s)}(P, v).$$

The next result justifies the definition and the name global height.

Proposition 2.3.4. *The global height h_λ is independent of the choices of F and of the section s.*

Proof: By Lemma 1.3.7, the global height is independent of F. Its independence from the choice of s can be verified as follows. Let t be another non-zero meromorphic section of $O(D)$ with $P \notin \operatorname{supp}(D(t))$. Then 2.2.4 and 2.2.5 show that

$$\lambda_{\mathcal{D}(s)}(P, v) - \lambda_{\mathcal{D}(t)}(P, v) = \lambda_{s/t}(P, v)$$

for any $v \in M_F$. On the other hand, the product formula shows that the global height of P relative to $\lambda_{s/t}$ is 0, proving the claim. □

Remark 2.3.5. As an immediate consequence the global height relative to the natural local height of a non-zero rational function is identically 0. It is also clear that the map $\lambda \mapsto h_\lambda$ is a group homomorphism.

Theorem 2.3.6. *Let λ, λ' be local heights relative to Cartier divisors D, D' with $D - D'$ a principal divisor. Then $h_\lambda - h_{\lambda'}$ is a bounded function.*

Proof: By Remark 2.3.5, we can assume $D = D' = 0$ and $\lambda' = 0$, hence we need only to show that h_λ is a bounded function for any local height relative to the zero divisor. Theorem 2.2.11 and Remark 2.2.13 give us a family $\{\gamma_v\}_{v\in M_K}$ of non-negative real numbers, almost all 0, such that

$$|\lambda(P,u)|_u \leq \gamma_v$$

for any $P \in X$ and any place u on $\overline{K}$ with $u|v$. As before, let F be a finite extension $K \subset F \subset \overline{K}$ such that $P \in X(F)$. By 2.3.1, we obtain

$$|\lambda(P,w)| \leq \tfrac{[F_w:\mathbb{Q}_p]}{[F:\mathbb{Q}]}\,\gamma_v$$

for any $w \in M_F$, which divides $v \in M_K$ and $p \in M_\mathbb{Q}$. By Corollary 1.3.2, we have

$$\sum_{w|v} [F_w : K_v] = [F : K]$$

and we get

$$|h_\lambda(P)| \leq \sum_{w\in M_F} |\lambda(P,w)| \leq \sum_{v\in M_K} \tfrac{[K_v:\mathbb{Q}_p]}{[K:\mathbb{Q}]}\,\gamma_v < \infty. \qquad \square$$

2.3.7. There is an isomorphism of the group of Cartier divisors modulo principal Cartier divisors onto $\mathrm{Pic}(X)$, given by $\mathrm{cl}(D) \mapsto \mathrm{cl}(O(D))$. Let us denote the real functions on X by $\mathbb{R}^X$ and the subspace of bounded functions by $O(1)$. Let $\mathbf{c} \in \mathrm{Pic}(X)$ and choose a Cartier divisor D with $\mathbf{c} = \mathrm{cl}(O(D))$ and a local height λ relative to D. By Theorem 2.3.6, the image $\mathbf{h_c}$ of h_λ under the projection

$$\mathbb{R}^X \longrightarrow \mathbb{R}^X/O(1)$$

is independent of the choice of D and λ. A representative of $\mathbf{h_c}$ is called a **height function** associated to $\mathbf{c}$.

In other words, an isomorphism class of line bundles determines a real-valued height function up to bounded functions. We note however that considering only equivalence classes of heights modulo bounded functions, as propounded by Weil, although it has attractive functorial properties, it also has the great disadvantage of throwing away the finer properties of heights needed to prove the deeper theorems of diophantine geometry. A better point of view is offered in the next sections.

Theorem 2.3.8. *The map*

$$\mathbf{h} : \mathrm{Pic}(X) \longrightarrow \mathbb{R}^X/O(1),$$

given by $\mathbf{c} \mapsto \mathbf{h_c}$*, is a homomorphism. If* $\varphi : Y \to X$ *is a morphism of irreducible projective varieties over* K*, then*

$$\mathbf{h}_{\varphi^*\mathbf{c}} = \mathbf{h_c} \circ \varphi$$

for any $\mathbf{c} \in \mathrm{Pic}(X)$.

Proof: The first claim follows from Remark 2.3.5 and Theorem 2.3.6. The second one is an immediate consequence of 2.2.6. □

It is quite trivial, but important, to remark that a base-point-free line bundle has always a non-negative height function. A more general result is the following

Proposition 2.3.9. *Let D be an effective Cartier divisor on X. Then there is a local height λ relative to D such that, for any $P \notin \mathrm{supp}(D)$ and for any place u of $\overline{K}$, it holds $\lambda(P,u) \geq 0$.*

Proof: There are base-point-free line bundles L, M on X such that $O(D) \cong L \otimes M^{-1}$. Choose generating global sections $t_0, \ldots, t_l$ of M. We can complete $s_D t_0, \ldots, s_D t_l$ to a family $s_0, \ldots, s_k$ of generating global sections of L. The local height given by the presentation

$$\mathcal{D} = (s_D;\, L, \mathbf{s};\, M, \mathbf{t})$$

is non-negative outside of the support of D. □

2.3.10. The results of Sections 2.2 and 2.3 extend immediately to varieties which are not necessarily irreducible. Here we must be careful to require that all meromorphic sections considered are invertible, i.e. not identically 0 on any irreducible component of X. For the functorial property of 2.2.6, we must assume that no irreducible component of Y is mapped into the support of D, in order to guarantee a well-defined pull-back of the Cartier divisor.

2.3.11. We may introduce global heights for any field with product formula as long as we work with properly normalized absolute values (see 1.3.6 for a perfect field and 1.3.12 in general). Then all results of this section continue to hold.

2.3.12. We may also replace the ground field K by $\overline{K}$. Then all geometric data as varieties, morphisms, line bundles, and sections are defined over a sufficiently large number field K and there is no problem about considerations with global heights relative to the ground field K. Since the global height does not depend on the ground field, it also makes sense to consider it as a global height over the algebraically closed field $\overline{K}$.

2.4. Weil heights

In this section we consider global heights given by a morphism of a projective variety to a projective space. In fact, we will see that any global height is the difference of two such Weil heights. We will formulate Theorem 2.3.8 and Northcott's theorem in terms of Weil heights. The results are based on the previous sections.

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

Definition 2.4.1. *Let $\varphi : X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}$ be a morphism over $\overline{\mathbb{Q}}$. The **Weil height** of $P \in X(\overline{\mathbb{Q}})$ relative to φ is defined by $h_\varphi(P) := h \circ \varphi(P)$, with h the usual height on $\mathbb{P}^n_{\overline{\mathbb{Q}}}$.*

2.4.2. If $\psi : X \to \mathbb{P}^m_{\overline{\mathbb{Q}}}$ is another morphism over $\overline{\mathbb{Q}}$, the **join** $\varphi\#\psi$ is the morphism

$$X \to \mathbb{P}^{(n+1)(m+1)-1}_{\overline{\mathbb{Q}}}, \qquad x \mapsto (\varphi_j(x)\psi_k(x)),$$

with the lexicographic ordering on pairs (i,j).

It may be viewed as the composition of the graph morphism $G(\psi) : X \to X \times \mathbb{P}^m_{\overline{\mathbb{Q}}}$, the product map $\varphi \times \mathrm{id} : X \times \mathbb{P}^m_{\overline{\mathbb{Q}}} \to \mathbb{P}^n_{\overline{\mathbb{Q}}} \times \mathbb{P}^m_{\overline{\mathbb{Q}}}$, and the Segre embedding $\mathbb{P}^n_{\overline{\mathbb{Q}}} \times \mathbb{P}^m_{\overline{\mathbb{Q}}} \to \mathbb{P}^{(n+1)(m+1)-1}_{\overline{\mathbb{Q}}}$ (cf. A.6.4).

Remark 2.4.3. If φ is a closed embedding, then $\varphi\#\psi$ is a closed embedding. In order to prove this claim, note that $G(\psi)$ is always a closed embedding (see A. Grothendieck [**134**], Cor.5.4.3). If φ is a closed embedding, then $\varphi \times \mathrm{id}$ is a closed embedding ([**134**], Prop.4.3.1). The Segre embedding is also a closed embedding (cf. A.6.4). Since the composition of closed embeddings remains a closed embedding ([**134**], Prop.4.2.5), we conclude that $\varphi\#\psi$ is a closed embedding.

The following proposition formalizes a remark already made in 1.5.14 about the height in Segre embeddings.

Proposition 2.4.4. *If $\varphi : X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}$ and $\psi : X \to \mathbb{P}^m_{\overline{\mathbb{Q}}}$ are morphisms over $\overline{\mathbb{Q}}$, then*

$$h_{\varphi\#\psi} = h_\varphi + h_\psi.$$

2.4.5. We claim that every Weil height may be viewed as a global height in the sense of Section 2.3. There is a linear form $\ell = \ell_0 x_0 + \cdots + \ell_n x_n$, which does not vanish identically on any irreducible component of X. Then it follows from Example 2.3.2 and 2.2.6 that h_φ is the global height relative to the presentation $\varphi^*(\ell; O_{\mathbb{P}^n_{\overline{\mathbb{Q}}}}(1), x_0, \ldots, x_n; O_{\mathbb{P}^n_{\overline{\mathbb{Q}}}}, 1)$.

2.4.6. Conversely, we can write every global height as a difference of two Weil heights. Let h_λ be the global height relative to the presentation

$$\mathcal{D} = (s; L, s_0, \ldots, s_n; M, t_0, \ldots, t_m).$$

We consider the morphisms

$$\varphi : X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}, \qquad x \mapsto (s_0(x) : \cdots : s_n(x))$$

and

$$\psi : X \to \mathbb{P}^m_{\overline{\mathbb{Q}}}, \qquad x \mapsto (t_0(x) : \cdots : t_m(x))$$

as in A.6.8. Then it follows from the independence of h_λ from s and 2.4.5 that

$$h_\lambda = h_\varphi - h_\psi.$$

2.4.7. Note that in 2.4.6 we may even assume that φ and ψ are closed embeddings into projective spaces. This follows from Remark 2.3.5 and Proposition 2.4.4, choosing any closed embedding θ of X into some projective space over $\overline{\mathbb{Q}}$ and replacing φ, ψ by $\varphi\#\theta$, $\psi\#\theta$.

Theorem 2.4.8. *If $\varphi : X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}$ and $\psi : X \to \mathbb{P}^m_{\overline{\mathbb{Q}}}$ are morphisms over $\overline{\mathbb{Q}}$ with $\varphi^* O_{\mathbb{P}^n}(1) \cong \psi^* O_{\mathbb{P}^m}(1)$, then $h_\varphi - h_\psi$ is a bounded function.*

Proof: Using 2.4.5, this is a reformulation of Theorem 2.3.6. □

Our next result is the general version of **Northcott's theorem**, which is both simple and fundamental.

Theorem 2.4.9. *Let X be a projective variety defined over the number field K and let $h_{\mathbf{c}}$ be a height function associated to an ample class $\mathbf{c} \in \mathrm{Pic}(X)$. Then the set*

$$\{P \in X(\overline{K}) \mid h_{\mathbf{c}}(P) \le C,\ [K(P) : K] \le d\}$$

is finite for any constants $C, d \in \mathbb{R}$.

Proof: There is $m \in \mathbb{N}$ such that $m\mathbf{c}$ is very ample. By Theorem 2.3.8, $mh_{\mathbf{c}}$ is a height function associated to $m\mathbf{c}$. Therefore, we can assume without loss of generality that $\mathbf{c}$ is very ample. By Theorem 2.4.8, it is enough to prove the statement for $X = \mathbb{P}^n_{\overline{\mathbb{Q}}}$ and $\mathbf{c} = \mathrm{cl}(O_{\mathbb{P}^n}(1))$, i.e. for the standard height on $\mathbb{P}^n_{\overline{\mathbb{Q}}}$.

Let $U := \{x_j \neq 0\}$ be a standard affine subset of $\mathbb{P}^n_{\overline{\mathbb{Q}}}$. We have to show that there are only finitely many points P in $U(\overline{\mathbb{Q}})$ with $h(P) \le C$ and $[K(P) : K] \le d$. The height of $P \in U$ is an upper bound for the heights of the coordinates. Therefore, the case $n = 1$ implies the general statement. This is Theorem 1.6.8, ending the proof. □

Remark 2.4.10. Clearly, we may also introduce Weil heights for any field with product formula and all results above remain true with the exception of Northcott's theorem. We may use Example 1.5.23 as a counterexample if the field is infinite.

Example 2.4.11. The following example shows that Weil heights in the geometric case may be interpreted in terms of intersection theory, as a degree function. This is conceptually very important, because it allows us to use the intuition and methods of algebraic geometry in dealing with heights.

The corresponding result in the arithmetic case lies much deeper and requires intersection theory in the setting of arithmetic algebraic geometry (see Example 2.7.20).

Let X be an irreducible regular projective variety over an arbitrary field K, and let $\deg$ be the degree of cycles corresponding to a fixed embedding of X into a projective space $\mathbb{P}^n_K$. By Proposition 1.4.7, we have a canonical set of absolute values on $K(X)$ satisfying the product formula. A point $P \in \mathbb{P}^n_K(K(X))$ is given by coordinates $f_0, \dots, f_n \in K(X)$. Let φ be the rational map

$$X \dashrightarrow \mathbb{P}^n_K, \qquad x \mapsto \varphi(x) = (f_0(x) : \cdots : f_n(x)).$$

Let $x_0, \ldots, x_n$ be the coordinates of $\mathbb{P}^n_K$, viewed as global sections of $O_{\mathbb{P}^n}(1)$. Choose $j \in \{0, \ldots, n\}$ such that $x_j|_{\varphi(X)} \neq 0$. Then the vector $(f_0, \ldots, f_n)$ is proportional to

$$(\varphi^* x_0/\varphi^* x_j, \ldots, \varphi^* x_n/\varphi^* x_j) \in K(X)^{n+1}$$

and we may assume that they are equal. By Example 1.5.23, we have

$$\begin{aligned} h(P) &= -\sum_Z \min_{i=0,\ldots,n} \operatorname{ord}_Z(f_i) \deg Z \\ &= \sum_Z \left(\operatorname{ord}_Z(\varphi^* x_j) - \min_{i=0,\ldots,n} \operatorname{ord}_Z(\varphi^* x_i) \right) \deg Z, \end{aligned}$$

where the sums range over all prime divisors Z of X. By the valuative criterion of properness (cf. A.11.10), the domain U of φ has a complement of codimension at least 2. The local ring associated to a prime divisor was introduced in A.8.7. By choosing a trivialization of $(\varphi|_U)^* O_{\mathbb{P}^n}(1)$ at a generic point of Z, we may view $\varphi^*(x_i)$ as regular functions in Z. Therefore, we have

$$\min_{i=0,\ldots,n} \operatorname{ord}_Z(\varphi^* x_i) = 0$$

and thus

$$h(P) = \sum_Z \operatorname{ord}_Z(\varphi^* x_j) \deg Z.$$

Since $X \backslash U$ is of codimension at least 2, the restriction map induces an isomorphism

$$\operatorname{Pic}(X) \xrightarrow{\sim} \operatorname{Pic}(U)$$

(because on a regular variety Cartier divisors and Weil divisors can be identified, cf. A.8.21). So it makes sense to view $(\varphi|_U)^* O_{\mathbb{P}^n}(1)$ as an element of $\operatorname{Pic}(X)$, which we simply denote by $\varphi^* O_{\mathbb{P}^n}(1)$. It follows that

$$h(P) = \deg\, \varphi^* O_{\mathbb{P}^n}(1),$$

where the right-hand side denotes the degree of any divisor of a non-zero meromorphic section of $\varphi^* O_{\mathbb{P}^n_K}(1)$ (see A.9.26). If Y is a projective variety over $K(X)$ and $\iota : Y \to \mathbb{P}^n_{K(X)}$ is a closed embedding over $K(X)$ into projective space, then $P \in Y(K(X))$ induces a rational map

$$\varphi : X \dashrightarrow Y$$

as above, and we have

$$h_\iota(P) = \deg\, \varphi^* O_Y(1),$$

where $O_Y(1)$ is the pull-back of $O_{\mathbb{P}^n}(1)$ to Y.

2.5. Explicit bounds for Weil heights

This is a somewhat technical section, the reading of which can be omitted at first. Its ultimate purpose is to give a meaning to the phrase "effectively computable," which otherwise would be only a hollow claim, devoid of true mathematical significance.

The main tool in this section is the concept of presentation of a closed embedding of a projective variety in projective space. The basic idea can be described as follows. Let $X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}$ be a projective algebraic variety over the algebraically closed field $\overline{\mathbb{Q}}$, embedded in projective space $\mathbb{P}^n_{\overline{\mathbb{Q}}}$. It is well known that every rational function on X is then induced

by restriction of a rational function in the ambient space $\mathbb{P}^n_{\overline{\mathbb{Q}}}$. On the other hand, we often need to compare situations relative to different embeddings. The point of view taken in this section is therefore the following. Since we are dealing with the function field $\overline{\mathbb{Q}}(X)$ of X, we are allowed to choose a hypersurface in $\mathbb{P}^{r+1}_{\overline{\mathbb{Q}}}$ as a birational model. The homogeneous coordinate ring S is the quotient of a polynomial ring by a principal ideal. This allows us to introduce a height in S. Thus fixing this choice gives us a reference description of elements in S.

This being done, we consider an arbitrary closed embedding $X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}$. Then a presentation of the embedding $X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}$, relative to the reference ring S, consists in expressing the rational functions $(x_i/x_j)|_X$ as elements of S. Now the problem of comparing heights relative to different embeddings can be solved by comparing corresponding presentations. This leads to very explicit comparison estimates for heights. The details are as follows.

2.5.1. Let X be an irreducible projective variety over $\overline{\mathbb{Q}}$ of dimension r. There is a $\overline{\mathbb{Q}}$-morphism

$$\pi : X \longrightarrow \mathbb{P}^{r+1}_{\overline{\mathbb{Q}}}$$

such that X is mapped birationally onto a hypersurface (cf. A.11.5 and A.11.6). We denote by $z_0, \dots, z_{r+1}$ the standard coordinates of $\mathbb{P}^{r+1}_{\overline{\mathbb{Q}}}$. Then we may assume that the hypersurface is given by an irreducible homogeneous polynomial f of degree d of the form

$$f(z_0, \dots, z_{r+1}) = f_0 + f_1 z_{r+1} + \cdots + f_{d-1} z_{r+1}^{d-1} + z_{r+1}^d,$$

where $f_i \in \overline{\mathbb{Q}}[z_0, \dots, z_r]$ is homogeneous of degree $d - i$, $f(0, \dots, 0, 1) \neq 0$ and d is the degree of X with respect to $\pi^* O_{\mathbb{P}^{r+1}}(1)$ (cf. A.11.7). This situation is fixed for the whole section.

2.5.2. Let S be the homogeneous coordinate ring of $\pi(X)$. We have

$$S = \overline{\mathbb{Q}}[z_0, \dots, z_{r+1}]/\mathfrak{I},$$

where $\mathfrak{I}$ is the homogeneous ideal generated by f. Let $\overline{z}_i$ be the image of z_i in S $(0 \leq i \leq r+1)$ and note that $\overline{z}_{r+1}$ is integral over $\overline{\mathbb{Q}}[\overline{z}_0, \dots, \overline{z}_r]$. The variables $\overline{z}_0, \dots, \overline{z}_r$ are algebraically independent, because the transcendence degree of $\overline{\mathbb{Q}}(\pi(X)) = \overline{\mathbb{Q}}(X)$ is r (cf. A.4.11). By abuse of notation, we denote them again by $z_0, \dots, z_r$. The minimal polynomial of $\overline{z}_{r+1}$ over the polynomial ring $\overline{\mathbb{Q}}[z_0, \dots, z_r]$ is equal to $f(z_0, \dots, z_r, \cdot)$, since

$$0 = f_0 + f_1 \overline{z}_{r+1} + \cdots + f_{d-1} \overline{z}_{r+1}^{d-1} + \overline{z}_{r+1}^d. \tag{2.5}$$

The elements $1, \overline{z}_{r+1}, \dots, \overline{z}_{r+1}^{d-1}$ form a basis of S over $\overline{\mathbb{Q}}[z_0, \dots, z_r]$ and so we have an isomorphism of $\overline{\mathbb{Q}}$-vector spaces

$$S \xrightarrow{\sim} \{p \in \overline{\mathbb{Q}}[z_0, \dots, z_{r+1}] \mid \deg_{z_{r+1}}(p) < d\}.$$

By means of this map, we define the height of an element of S as the height of the corresponding polynomial.

2.5.3. For $l \in \mathbb{N}$, there are uniquely determined $q_{lj} \in \overline{\mathbb{Q}}[z_0, \dots, z_r]$ $(j = 0, \dots, d-1)$ such that

$$\overline{z}_{r+1}^l = \sum_{j=0}^{d-1} q_{lj} \overline{z}_{r+1}^j. \tag{2.6}$$

The polynomials q_{lj} are homogeneous of degree $l-j$ (elements of negative degree are 0), and $q_{lj} = \delta_{lj}$ for $0 \le l \le d-1$, where δ_{lj} is Kronecker's symbol. We may now assume that $l \ge d$. Equation (2.5) shows

$$\overline{z}_{r+1}^{l} = -\sum_{k=0}^{d-1} f_k \overline{z}_{r+1}^{k+l-d} = -\sum_{j=0}^{d-1}\sum_{k=0}^{d-1} f_k\, q_{k+l-d,j}\, \overline{z}_{r+1}^{j},$$

leading to the recursive formula

$$q_{lj} = -\sum_{k=0}^{d-1} f_k\, q_{k+l-d,j}, \tag{2.7}$$

where $j = 0, \dots, d-1$. Let F be a number field containing the coefficients of $f_0, \dots, f_{d-1}$ and for $v \in M_F$ define δ_v to be 1 if v is archimedean and 0 otherwise. The recursion (2.7) yields a bound

$$|q_{lj}|_v \le \left|\binom{d+r+1}{r+1}\right|_v^{\delta_v} |f|_v \max_{l'=l-d,\dots,l-1} |q_{l'j}|_v$$

for the Gauss norms. Here we have used that f_k has $\binom{d-k+r}{r}$ summands and

$$\sum_{k=0}^{d} \binom{d-k+r}{r} = \binom{d+r+1}{r+1}. \tag{2.8}$$

By induction we obtain

$$|q_{lj}|_v \le \left|\binom{d+r+1}{r+1}\right|_v^{(l-d)\delta_v} |f|_v^{l-d+1} \tag{2.9}$$

and thus Lemma 1.3.7 leads to

$$h(q_{lj}) \le (l-d+1)h(f) + (l-d)\log\binom{d+r+1}{r+1}.$$

Let $\varphi : X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}$ be a closed embedding over $\overline{\mathbb{Q}}$ and let $x_0, \dots, x_n$ be the standard coordinates of $\mathbb{P}^n_{\overline{\mathbb{Q}}}$. Let $\mathbf{p}$ be a vector with entries $p_i \in S$, $i = 0, \dots, n$, homogeneous of degree $d(\mathbf{p})$.

Definition 2.5.4. *The vector $\mathbf{p}$ is said to be a **presentation** of φ if the following conditions are satisfied:*

(a) *If $l \in \{0, \dots, n\}$ and $x_l|_X \ne 0$, then we have $p_l \ne 0$.*

(b) *If l as in (a) and $i \in \{0, \dots, n\}$, then*

$$\frac{p_i}{p_l} = \left.\frac{x_i}{x_l}\right|_X$$

in $\overline{\mathbb{Q}}(X)$.

2.5.5. The number $d(\mathbf{p})$ is called the **degree** of $\mathbf{p}$. Consider the vector whose entries are given by all the coefficients of $p_0, \dots, p_n$. The height of the corresponding point in appropriate projective space is called the **height** of the presentation, denoted by $h(\mathbf{p})$. The existence of a presentation of φ is an obvious consequence of $\overline{\mathbb{Q}}(X) = \overline{\mathbb{Q}}(\pi(X))$.

Lemma 2.5.6. *Let $\varphi_j : X \to \mathbb{P}^{n_j}_{\overline{\mathbb{Q}}}$, $j = 1, \dots, k$, be closed embeddings over $\overline{\mathbb{Q}}$ with presentations $\mathbf{p}^{(j)}$ and let $n := (n_1 + 1) \cdots (n_k + 1) - 1$. Then the join $\varphi_1 \# \cdots \# \varphi_k$ gives a closed embedding*

$$\varphi : X \longrightarrow \mathbb{P}^n_{\overline{\mathbb{Q}}}, \qquad P \longmapsto \left(\varphi_{1 i_1}(P) \cdots \varphi_{k i_k}(P)\right)_{i_j \in \{0, \dots, n_j\}}.$$

It has a presentation $\mathbf{p}$ defined by

$$p_{\mathbf{i}} := p^{(1)}_{i_1} \cdots p^{(k)}_{i_k} \qquad (i_j \in \{0, \dots, n_j\})$$

of degree $d(\mathbf{p}) = d(\mathbf{p}^{(1)}) + \cdots + d(\mathbf{p}^{(k)})$ and height

$$h(\mathbf{p}) \le \sum_{j=1}^{k} h(\mathbf{p}^{(j)}) + r \sum_{j=1}^{k-1} \log\left(6 + 6\, d(\mathbf{p}^{(j)})/r\right) + C \cdot (k-1)$$

with

$$C = (d-1)h(f) + d(d + r + 1).$$

Proof: By Remark 2.4.3, φ is a closed embedding. Also, $\mathbf{p}$ is a presentation of φ of degree

$$d(\mathbf{p}) = d(\mathbf{p}^{(1)}) + \cdots + d(\mathbf{p}^{(k)}).$$

To prove the estimate for the height, by induction we may assume $k = 2$. We have the decomposition

$$p^{(j)}_{i_j} = \sum_{m=0}^{d-1} p^{(j)}_{i_j m}\, \overline{z}^m_{r+1} \qquad (j = 1, 2),$$

whence

$$p_{\mathbf{i}} = \left(\sum_{m_1=0}^{d-1} p^{(1)}_{i_1 m_1}\, \overline{z}^{m_1}_{r+1}\right)\left(\sum_{m_2=0}^{d-1} p^{(2)}_{i_2 m_2}\, \overline{z}^{m_2}_{r+1}\right).$$

Equation (2.6) on page 46 leads to the decomposition

$$p_{\mathbf{i}} = \sum_{m=0}^{d-1} p_{\mathbf{i}m}\, \overline{z}^m_{r+1}$$

with

$$p_{\mathbf{i}m} := \sum_{m_1 + m_2 = m} p^{(1)}_{i_1 m_1} p^{(2)}_{i_2 m_2} + \sum_{l=d}^{2d-2} \sum_{\substack{m_1 + m_2 = l \\ m_1, m_2 \le d-1}} p^{(1)}_{i_1 m_1}\, p^{(2)}_{i_2 m_2}\, q_{lm}.$$

Let F be a number field extension of $\mathbb{Q}$ containing the coefficients of $f_0, \dots, f_{d-1}$ and of all $p^{(j)}_{i_j m_j}$, $j = 1, 2$, and for $v \in M_F$ define δ_v as in 2.5.3. Then we verify

$$|p_{\mathbf{i}m}|_v \le |B|_v^{\delta_v}\, |p^{(1)}_{i_1}|_v\, |p^{(2)}_{i_2}|_v \max_{l=d,\dots,2d-2} (1, |q_{lm}|_v), \tag{2.10}$$

where B is an upper bound for

$$\sum_{m_1=0}^{m} \binom{r + d(\mathbf{p}^{(1)}) - m_1}{r} + \sum_{l=d}^{2d-2} \sum_{m_1 = l-d+1}^{d-1} \binom{r + d(\mathbf{p}^{(1)}) - m_1}{r} \binom{r + l - m}{r}.$$

Thereby we have used the fact that number of monomials of degree D in $r+1$ variables is equal to $\binom{r+D}{D}$. We use the estimates

$$\binom{r+d(\mathbf{p}^{(1)})-m_1}{r} \leq \frac{1}{r!}\left(r+d(\mathbf{p}^{(1)})\right)^r < \left(3+3\,d(\mathbf{p}^{(1)})/r\right)^r$$

and

$$\binom{r+l-m}{r} \leq 2^{r+l-m}$$

to conclude that

$$B := d\,2^{r+2d}\,\left(3+3\,d(\mathbf{p}^{(1)})/r\right)^r$$

is such an upper bound. From (2.9) on page 47 and (2.10), we get

$$h(\mathbf{p}) \leq h(\mathbf{p}^{(1)}) + h(\mathbf{p}^{(2)}) + \log B + (d-1)h(f) + (d-2)\log\binom{r+d+1}{d+1}.$$

With the above value for B, we have

$$h(\mathbf{p}) \leq h(\mathbf{p}^{(1)}) + h(\mathbf{p}^{(2)}) + r\log(6+6\,d(\mathbf{p}^{(1)})/r)) + C$$

with

$$C := (d-1)h(f) + d(d+r+1). \qquad \square$$

Remark 2.5.7. If we work over a fixed number field K and with an irreducible reduced projective variety, then the constructions in 2.5.1 to 2.5.3 can be done over K and every K-morphism to projective space has a presentation defined over K. Moreover, Lemma 2.5.6 remains valid.

2.5.8. We use the following notation. For a multi-index $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_N) \in \mathbb{N}^{N+1}$, we set

$$|\boldsymbol{\alpha}| := \alpha_0 + \cdots + \alpha_N$$

and for $\mathbf{x} = (x_0, \ldots, x_N) \in \overline{\mathbb{Q}}^{N+1}$ we define

$$\mathbf{x}^{\boldsymbol{\alpha}} := x_0^{\alpha_0} \cdots x_N^{\alpha_N}.$$

If Y is a closed subvariety of $\mathbb{P}^N_{\overline{\mathbb{Q}}}$, we denote by $\mathcal{J}_Y$ the ideal sheaf of Y.

Proposition 2.5.9. *Let $\varphi : X \to \mathbb{P}^n_{\overline{\mathbb{Q}}}$, $\psi : X \to \mathbb{P}^m_{\overline{\mathbb{Q}}}$ be closed embeddings over $\overline{\mathbb{Q}}$, with corresponding presentations $\mathbf{p}$, $\mathbf{q}$. We assume*

$$\varphi^* O_{\mathbb{P}^n}(1) \cong \psi^* O_{\mathbb{P}^m}(1).$$

There is a positive integer k_ψ such that if $k \geq k_\psi$, then

$$H^1\left(\mathbb{P}^m_{\overline{\mathbb{Q}}}, \mathcal{J}_{\psi X} \otimes O_{\mathbb{P}^m}(k)\right) = 0.$$