The analytic subgroup theorem

Wintersemester 2020/21

Prof. Dr. Annette Huber-Klawitter

Fassung vom February 9, 2021

Dies ist ein Vorlesungsskript und kein Lehrbuch.
Mit Fehlern muss gerechnet werden!

Math. Institut
Ernst-Zermelo-Str. 1
79104 Freiburg

0761-203-5560
annette.huber@math.uni-freiburg.de

Contents

0 Introduction 1

1 Elementary theory of transcendence 5

2 Commutative algebraic groups I 11

3 Tangent spaces and the exponential map 19

4 Reduction to the semi-stable case 27

5 Analytic tools for the proof 31

6 Weil heights 39

7 Proof 49

8 Elliptic curves 59

9 Commutative algebraic groups II 73

10 1-motives 81

11 The period conjecture for 1-motives 87

Chapter 0

Introduction

The topic of this lecture is *transcendence theory.* Recall:

Definition 0.1. A complex number α is callecd *algebraic* if there is a non-zero polynomial P in $\mathbb{Q}[T]$ such that $P(\alpha) = 0$. It is called *transcendental* otherwise.

The algebraic numbers form an algebraically closed field, which we denote $\overline{\mathbb{Q}}$. Note that we have fixed an embedding $\overline{\mathbb{Q}} \subset \mathbb{C}$. This will remain the case for the rest of the semester.

The set $\overline{\mathbb{Q}}$ is countable because there are only countably many polynomials with coefficients in the countable set $\mathbb{Q}$ and they have finitely many zeroes each. On the other hand, $\mathbb{C}$ is uncountable. This means that most complex numbers are transcendental

Question 0.2. Given a complex number α, can we tell whether it is transcendental or not?

The most famous case is the number π. Lindemann (a professor at Freiburg at the time) solved this in 1882. This finally settled the question of whether the circle can be squared–no.

Shortly after, in his famous address at the ICM 1900, Hilbert asked in his 7th out of 23 problems whether α, β and $\gamma = \alpha^\beta$ can be algebraic numbers simultaneously. There are some obvious cases: $\alpha = 0$, $\alpha = 1$ or β rational. Is this the complete list? He considered this problem as more difficult to prove than the Riemann hypothesis. To much surprise Gelfond and Schneider succeeded in 1934 independently to answer Hilbert's problem. Theodor Schneider was a professor at Freiburg as well from 1959 to his retirement in 1976.

Exercise 0.1. *Show that the following two statements are equivalent:*

(i) $\alpha, \beta, \alpha^\beta \in \overline{\mathbb{Q}}$ *implies* $\alpha = 0, 1$ *or* $\beta \in \mathbb{Q}$.

(ii) If $\log(\alpha)$ *and* $\log(\gamma)$ *for* $\alpha, \gamma \in \overline{\mathbb{Q}}^*$ *are* $\overline{\mathbb{Q}}$*-linearly dependent, then they are* $\mathbb{Q}$*-linearly dependent.*

Note that α^β has to be defined as $\exp(\beta(\log(\alpha)))$*. The number depends on the choice of branch of* $\log$*. The above statements apply to all choices of branch.*

A generation later, Baker generalised from 2 to arbitrary many logarithms.

Theorem 0.3 (Baker 1967)**.** *Let $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{Q}}^*$. If* $\log(\alpha_1), \dots, \log(\alpha_n)$ *are $\overline{\mathbb{Q}}$-linearly dependent, then they are $\mathbb{Q}$-linearly dependent.*

Exercise 0.2. *Work out the relation between the rank of the multiplicative abelian group $\langle \alpha_1, \dots, \alpha_n \rangle \subset \overline{\mathbb{Q}}^*$ and the $\overline{\mathbb{Q}}$-vector space* $\langle \log(\alpha_1), \dots, \log(\alpha_n) \rangle$*.*

Similar considerations were also made in different geometric settings. In 1932 Siegel showed that the periods of an elliptic curve over $\overline{\mathbb{Q}}$ cannot both be algebraic. Shortly after, in 1935, Schneider showed that, actually, they are both transcendental. In fact, we now know that they are $\overline{\mathbb{Q}}$-linearly independent, unless the elliptic curve has complex multiplication, i.e., $\mathrm{End}(E)_\mathbb{Q} = \mathbb{Q}(\tau)$ for imaginary quadratic $\mathbb{Q}(\tau)/\mathbb{Q}$. We are going to come back to the geometry of this situation later.

The culmination of these developments was the *Analytic Subgroup Theorem* proved by Wüstholz in 1989. All the above mentioned results and much more can be deduced from it. Let us formulate it.

Theorem 0.4 (Wüstholz)**.** *Let G be a connected commutative algebraic group over $\overline{\mathbb{Q}}$. Let $\mathfrak{b} \subset \mathrm{Lie}(G)$ be a subvector space. Assume that the analytic subgroup $B = \exp(\mathfrak{b}_\mathbb{C})$ of G^{an} contains an algebraic point $0 \neq P \in G(\overline{\mathbb{Q}})$. Then there is an algebraic subgroup $H \subset G$ such that $\mathrm{Lie}(H) \subset \mathfrak{b}$ and $P \in H(\overline{\mathbb{Q}})$.*

This is not very digestible, in particular for readers not familiar with complex Lie groups. We will explain this later. Examples of connected commutative algebraic groups are elliptic curves, the additive and the multiplicative group.

Example 0.5. The *multiplicative group* $\mathbb{G}_m$ is the algebraic variety $V(XY - 1) \subset \mathbb{A}^2$. It is defined over $\mathbb{Z}$, but we consider it as a $\overline{\mathbb{Q}}$-variety. Hence

$$V(XY-1) = \{(x,y) \in \overline{\mathbb{Q}}^2 | xy = 1\}.$$

We can identify it with $\overline{\mathbb{Q}}^*$ via the projection to the first coordinate. Now note that $\overline{\mathbb{Q}}^*$ is an abelian group. The group multiplication is given by the formula

$$V(X_1Y_1 - 1) \times V(X_2Y_2 - 1) \to V(XY-1), \quad (x_1, y_1, x_2, y_2) \mapsto (x_1x_2, y_1y_2),$$

hence it is morphism of algebraic varieties. The same is true for the inversion map.

The Lie algebra of this group is simply $\overline{\mathbb{Q}}$. When replacing $\overline{\mathbb{Q}}$ by $\mathbb{C}$ as field of definition, we get a complex Lie group, namely $\mathbb{C}^*$ with Lie algebra $\mathbb{C}$. The exponential map of the abstract theory identifies with

$$\exp : \mathbb{C} \to \mathbb{C}^*.$$

The theorem says something about $\exp(\alpha)$ for $\alpha \in \overline{\mathbb{Q}}$ or conversely, about $\log(\beta)$ for $\beta \in \overline{\mathbb{Q}}^*$. It is not hard to deduce transcendence of $\log(\beta)$, but we leave this for later.

Exercise 0.3. *Determine the coordinate ring of $\mathbb{G}_m$ and the ring homomorphisms induced by the group multiplication map and the inversion.*

Plan

(i) As a warm-up, we are going to look into the elementary theory of transcendence and some classical results.

(ii) We then turn to the analytic subgroup theorem in the affine case. The group G is then equal to $\overline{\mathbb{Q}}^a \times (\overline{\mathbb{Q}}^*)^b$, so we do not need abstract theory. We will give the proof following Baker–Wüstholz and deduce the above mentioned results on π and values of log.

(iii) Depending on the background of participants, we are going to spend time on the fundamentals of commutative groups in the category of algebraic varieties and in the category of complex manifolds. We will then be able to revisit the statement of the Analytic Subgroup Theorem. Particular attention will be paid to the case of elliptic curves.

(iv) Finally, we aim for the proof of the full theorem following Wüstholz's original article.

Literature

(i) Alan Baker, Gisbert Wüstholz: Logarithmic Forms and Diophantine Geometry, Cambridge University Press, 2007.

(ii) Alan Baker: Transcendental number theory, Cambridge University Press, 1975.

(iii) Michel Waldschmidt, Diophantine Approximation on linear algebraic groups, Springer 2000.

(iv) Gisbert Wüstholz: Algebraische Punkte auf analytischen Untergruppen algebraischer Gruppen. Ann. of Math. (2) 129 (1989), no. 3, 501–517.

(v) Annette Huber, Gisbert Wüstholz, Transcendence and linear relations of 1-periods, Preprint on arXiv, new version in preparation.

Chapter 1

Elementary theory of transcendence

Theorem 1.1 (Liouville)**.** *If α is an algebraic number of degree $n > 1$, then, for all rationals p/q (here $p, q \in \mathbb{Z}$, $q > 0$) we have*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n}$$

for some constant $c > 0$ (depending only on α).

The degree of an algebraic number is the degree of its minimal polynomial.

Example 1.2. The number

$$\xi = \sum_{j=1}^{\infty} 10^{-j!} = 0{,}110001000000000000000001\ldots$$

is transcendental.

Proof. The number is not rational because its decimal expansion is neither finite nor periodic. Suppose it is algebraic of degree $n > 1$. Let c be the constant from the theorem.

Let $p_k = 10^{k!}\sum_{j=1}^{k} 10^{-j!}$, $q_k = 10^{k!}$. Then the p_k/q_k are the partial sums of ξ, and we have

$$\left|\xi - \frac{p_k}{q_k}\right| = \sum_{j=k+1}^{\infty} 10^{-j!} < 10^{-(k+1)!}\sum_{j=0}^{\infty} 10^{-j} = \frac{10}{9} q_k^{-(k+1)}$$

(check by induction that $(j)! > (k+1)! + j - k - 1$ for $j \geq k+1$). Hence

$$\frac{c}{q_k^n} < \frac{10}{9} q_k^{-(k+1)} \Rightarrow \frac{9c}{10} < q_k^{n-k-1}$$

for all k. This is a contradiction because the sequence on the right tends to 0. □

Proof of Liouville's Theorem. If $\alpha \notin \mathbb{R}$, then $|\alpha - p/q| \geq |\mathrm{Im}(\alpha)|$ and the theorem holds with $c = |\mathrm{Im}(\alpha)|$. Hence from now on $\alpha \in \mathbb{R}$. It suffices to find a bound for those p, q for which $|\alpha - p/q| < 1$ (in the other cases the bound 1 is enough).

Let P be the minimal polynomial of α over $\mathbb{Q}$. We choose it integrally such that the leading coefficient is positive and the gcd of the coefficients equals 1. By the mean value theorem, we have

$$P(\alpha) - P(p/q) = (\alpha - p/q)P'(\xi)$$

for some ξ between α and p/q. As p/q was assumed close to α, we have $\xi \in (\alpha - 1, \alpha + 1)$. The value $|P'(\xi)|$ is bounded on this interval, say by $1/c$. Since $P(\alpha) = 0$, we get

$$\left|\alpha - \frac{p}{q}\right| > c\left|P\left(\frac{p}{q}\right)\right|.$$

Since P is irreducible of degree $n > 1$, the rational number p/q cannot be a zero. Moreover, $|q^n P(p/q)|$ is an integer and hence at least of absolute value 1. This gives

$$|P(p/q)| > 1/q^n$$

and the estimate follows. □

Exercise 1.1. *Work out c for $\sqrt{2}$ and $\sqrt[3]{2}$.*

Exercise 1.2. *(Possible talk) The theory of continued fractions gives for every real number a sequence of fractions that converges very quickly. Explain the algorithm and compare to Liouville's theorem. The topic is typically covered in books on elementary number theory.*

Theorem 1.3. *The number* e *is transcendental.*

We follow Baker's book and start with a bit of preparation.

Lemma 1.4. *Let $f \in \mathbb{R}[x]$ be a polynomial of degree m, $t \in \mathbb{C}$. Then*

$$I(t) = \int_0^t \mathrm{e}^{t-u} f(u)du$$

satisfies

$$I(t) = \mathrm{e}^t \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(t).$$

Proof. Induction on m. If $m = 0$, then f is constant. We have

$$I(t) = \int_0^t \mathrm{e}^{t-u} f du = -f\mathrm{e}^{t-u}|_0^t = -\mathrm{e}^0 f + \mathrm{e}^t f$$

as claimed.

Let $m \geq 1$. By integration by parts we have

$$\begin{aligned} I(t) &= \int_0^t \mathrm{e}^{t-u} f(u)du \\ &= -\mathrm{e}^{t-u} f(u)|_0^t - \int_0^t -\mathrm{e}^{t-u} f'(u)du \\ &= \mathrm{e}^t f(0) - f(t) + \int_0^t \mathrm{e}^{t-u} f'(u)du. \end{aligned}$$

The polynomial f' has degree $m-1$, so we can use the inductive hypothesis and find the formula. □

Lemma 1.5. *Let $f \in \mathbb{R}[X]$ and $\overline{f}$ the polynomial obtained by replacing each coefficient by its absolute value. Then*

$$|I(t)| \leq |t|\mathrm{e}^{|t|}\overline{f}(|t|).$$

Proof.

$$|I(t)| \leq \int_0^t |\mathrm{e}^{t-u} f(u)|du.$$

We then use the triangle inequality and handle each summand seperately. In this case we use the estimate

$$\int_0^t |\mathrm{e}^{t-u} u^n|du \leq |t|\mathrm{e}^{|t|}|t|^n$$

of an integral versus the length of the path and an upper bound for the integrand. □

Proof of transcendence. Suppose that e is algebraic, so that

$$q_0 + q_1\mathrm{e} + \ldots q_n\mathrm{e}^n = 0$$

for $n > 0$, $q_0 \neq 0$, $q_0, \ldots, q_n \in \mathbb{Z}$. We shall compare estimates for

$$J = q_0 I(0) + q_1 I(1) + \cdots + q_n I(n)$$

where $I(t)$ is as in the lemma with

$$f(x) = x^{p-1}(x-1)^p \ldots (x-n)^p$$

where p is a large prime.

By the lemma, we have

$$\begin{aligned} J &= \sum_{k=0}^n q_k \left(\mathrm{e}^k \sum_{j=0}^m f^{(j)}(0) - \sum_{j=0}^m f^{(j)}(k) \right) \\ &= \sum_{j=0}^m \sum_{k=0}^n q_k \left(\mathrm{e}^k f^{(j)}(0) - f^{(j)}(k) \right) \ . \end{aligned}$$

The terms with $f^{(j)}(0)$ do not contribute by the defining equation for the q_i. Hence we are left with

$$J = -\sum_{j=0}^{m}\sum_{k=0}^{n} q_k f^{(j)}(k)$$

where $m = (n+1)p-1$. We claim that the integer J is divisble by $(p-1)!$, but not by $p!$. We investigate the summands one by one.

For $j < p, k > 0$ we have $f^{(j)}(k) = 0$. The same holds for $j < p-1$ and $k = 0$. For $j \geq p$, the number is divisble by $p!$. The only case left is $j = p-1$, $k = 0$. We have

$$f^{(p-1)}(0) = (p-1)!(-1)^{np}(n!)^p.$$

This is divisble by $(p-1)!$. If we choose $p > n$, then this summand is not divisble by $p!$, hence J is non-zero and thus

$$|J| \geq (p-1)!.$$

On the other hand we have the estimate from the second lemma

$$|J| \leq |q_1|\mathrm{e}\overline{f}(1) + |q_2|2\mathrm{e}^2\overline{f}(2) + \ldots |q_n|n\mathrm{e}^n\overline{f}(n)\ .$$

We also have $\overline{f}(k) \leq (2n)^m$ (expand the product for $f(x)$ and take every summand with a positive sign. Each is an m-fold product of numbers at most n. There are fewer than 2^m summands.) Together this gives

$$(p-1)! \leq (2n)^m < C^p$$

for some C independent of p. This is a contradiction for p large enough. □

Theorem 1.6. *The number π is transcendental.*

Proof. Let $\theta = i\pi$. Suppose it is algebraic of degree d. Let l be the leading coefficient of the minimal polynomial of θ (chosen with coprime integral coefficients, $l > 0$). This makes $l\theta$ an algebraic integer.

Let $\theta_1, \ldots, \theta_d$ be the conjugates of θ. Then

$$(\mathrm{e}^{\theta_1}+1)\ldots(\mathrm{e}^{\theta_d}+1) = 0$$

because θ is among the conjugates and $\mathrm{e}^{\theta} = -1$ by Euler's identity. We expand the left-hand side and obtain 2^d terms of the form e^{Θ} where

$$\Theta = \varepsilon_1\theta_1 + \cdots + \varepsilon_d\theta_d$$

with $\varepsilon_i = 0, 1$. We assume that precisely n of these numbers Θ are non-zero and denote them by $\alpha_1, \ldots, \alpha_n$. Note that the $l\alpha_k$ are also algebraic integers. We then have

$$q + \mathrm{e}^{\alpha_1} + \cdots + \mathrm{e}^{\alpha_n} = 0$$

where $q = 2^d - n$. We compare estimates for

$$J = I(\alpha_1) + \cdots + I(\alpha_n)$$

with $I(t)$ as in Lemma 1.4 with

$$f(x) = l^{np}x^{p-1}(x-\alpha_1)^p \dots (x-\alpha_n)^p = x^{p-1}(lx-l\alpha_1)^p \dots (lx-l\alpha_n)^p$$

for a large prime p. As in the proof of transcendence of e, we obtain

$$\begin{aligned} J &= \sum_{k=1}^{n} \mathrm{e}^{\alpha_k} \sum_{j=0}^{m} f^{(j)}(0) - \sum_{k=1}^{n}\sum_{j=0}^{m} f^{(j)}(\alpha_k) \\ &= -q\sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m}\sum_{k=1}^{n} f^{(j)}(\alpha_k) \end{aligned}$$

with $m = (n+1)p - 1$.

For $j < p$, the derivatives $f^{(j)}(\alpha_k)$ vanish. For $j \geq p$, we claim that the sum over k gives an integer divisible by $p!$. The expression over k is symmetric in the α_k, which are in turn symmetric in the θ_i. Hence the expression is invariant under the Galois group of $\overline{\mathbb{Q}}/\mathbb{Q}$ and gives a rational number. Actually, it is an algebraic integer divisible by $p!$. To see this note that the derivatives of $f(x)$ are computed using the product rule. When evaluating at α_k only the summands where $(x-\alpha_k)^p$ was derived at least p times contribute. This gives a factor of $p!$ in front of every summand. The summand has fewer that np factors (there are $(n+1)p-1$ factors in f, but the number went down by at least p), hence the l^{np} in front makes every factor integral.

For $j < p-1$, the derivatives $f^{(j)}(0)$ vanish. For $j \geq p$ the expression is again symmetric in the α_k, hence in $\mathbb{Q}$. Again it is even an integer divisble by $p!$.

This leaves the derivative $f^{(p-1)}(0)$. We have

$$f^{(p-1)}(0) = (p-1)!(-l)^{np}(\alpha_1 \dots \alpha_n)^p.$$

This is an integer divisble by $(p-1)!$ but not by $p!$ for p sufficiently large. Hence we get the estimate

$$(p-1)! \leq |J|.$$

From the second lemma we get as in the proof of transcendence of e

$$|J| \leq \sum_{k=1}^{n} |\alpha_k| \mathrm{e}^{|\alpha_k|} \overline{f}(|\alpha_k|) \leq C^p$$

for some C independent of p.

For large p this is a contradiction. □

Both are special cases of Lindemann's theorem.

Theorem 1.7 (Lindemann)**.** *Whenever $\alpha_0, \dots, \alpha_n$ are distinct algebraic numbers and $\beta_0, \dots, \beta_n \in \overline{\mathbb{Q}}^*$ we have*

$$\beta_0 \mathrm{e}^{\alpha_0} + \dots + \beta_n \mathrm{e}^{\alpha_n} \neq 0.$$

For the proof we refer to [Baker, Theorem 1.4].

Exercise 1.3. *Deduce the transcendence of* e*,* π *and* $\log(2)$ *from Lindemann's theorem.*

Chapter 2

Commutative algebraic groups I

We work over an algebraically closed field k of characteristic 0. (Actually any field or even $\mathbb{Z}$ would be ok, but let's fix the setting.)

Definition 2.1. An *algebraic group* over k is a connected k-variety G together with morphisms of varieties

$$\mu : G \times G \to G$$

and

$$\iota : G \to G$$

making the underlying set of (G, μ) into a group with $\iota(g) = g^{-1}$. It is called *linear* if G is affine. It is called commutative if (G, μ) is commutative.

We often write $G(k)$ for the underlying group.

Example 2.2. The *general linear group* Gl_n has as elements the invertible matrices in $M_n(k)$. It is an algebraic variety because it is defined by the polynomial inequality

$$\det(A) \neq 0.$$

It is affine because we can identify it with the subset of $\mathbb{A}^{n^2+1}$ defined by the equation

$$\det(A)T = 1$$

where T is the extra coordinate. The group multiplication is given by polynomials in the coefficients, so it is a morphism of algebraic varieties. The map $A \mapsto A^{-1}$ is given explicitly by Cramer's rule, so again by polynomials.

For $n = 1$ we recover the *multiplicative group* $\mathbb{G}_m$ from the introduction. For $n \geq 2$, the group is not commutative.

Example 2.3. The *additive group* $\mathbb{G}_a$ is the algebraic variety $\mathbb{A}^1$ with the group law $+$. It is a commutative linear algebraic group.

Exercise 2.1. *(i) Check that the* special linear group Sl_n*, the group of matrices with determinant* 1 *is a linear algebraic group.*

(ii) (harder) Check the same for the projective linear group PGl_n *with underlying group* $\mathrm{Gl}_n(k)/k^*$ *is a linear algebraic group.*

Algebraic groups form a category.

Definition 2.4. Let G, G' be algebraic groups over k. A morphism $f : G \to G'$ of algebraic groups is a morphism of algebraic varieties which is compatible with μ. It is an isomorphism if it has an inverse in the category of algebraic groups.

Exercise 2.2. *Consider the group* $U(n)$ *of upper triangular matrices with diagonal entries equal to* 1*. Show that:*

(i) it is an algebraic group isomorphic to $\mathbb{A}^m$ *as a variety. (Determine* m*)*

(ii) $U(2)$ *is isomorphic to* $\mathbb{G}_a$ *as an algebraic group.*

(iii) For $n \geq 3$*, the algebraic groups* $U(n)$ *and* $\mathbb{G}_a^m$ *are not isomorphic.*

Lemma 2.5. *Let* G *be a commutative algebraic group,* X *a variety. Then* $\mathrm{Mor}(X, G)$ *has a natural structure of commutative group. If* X *is an algebraic group, then the same is true for the subset of morphisms of algebraic groups.*

Proof. Given $f, g : X \to G$, we can define

$$f + g : X \xrightarrow{\Delta} X \times X \xrightarrow{(f,g)} G \times G \xrightarrow{\mu} G$$

where Δ is the diagonal morphism. This composition is again a morphism of algebraic varities. The group axioms follow from the properties of (G, μ).

If $f, g : G' \to G$ are compatible with the group structure, then the same is true for $f + g$. □

Remark 2.6. Identities for maps of varieties hold true, if they are satisfied on the underlying sets. Hence we are back in ordinary group theory. The non-formal part is the construction of $f + g$ as a morphism of varieties.

We write $\mathrm{Hom}(G', G)$ for the group of morphisms of algebraic groups.

In this chapter we restrict attention to linear commutative algebraic groups.

Definition 2.7. (i) An algebraic group $V \cong \mathbb{G}_a^n$ is called *vector group* of dimension n.

(ii) An algebraic group $T \cong \mathbb{G}_m^r$ is called *torus* of dimension r.

Theorem 2.8. *Under our assumptions on* k*, every linear commutative algebraic group is isomorphic to a product* $V \times T$ *for a vector group* V *and a torus* T*.*

Proof. Barsotti 1955, Chevalley 1960, Demazure-Gabriel Ch. IV §3 Théoréme 1.1, Serre 1988 Ch. III Proposition 12. □

For the next chapters, we are going to restrict to G of the form $V \times T$. By the theorem this is not really a restriction. The next step is to analyse morphisms for such G.

Proposition 2.9. *We have*

$$\mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_a) = \mathrm{Hom}(\mathbb{G}_a, \mathbb{G}_m) = 0$$

and

$$\mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m) = \mathbb{Z}, \quad \mathrm{Hom}(\mathbb{G}_a, \mathbb{G}_a) = k.$$

Proof. A morphism $f : \mathbb{G}_m \to \mathbb{G}_a$ is the same as an algebra homomorphism

$$\phi : k[X] \to k[Y, Y^{-1}].$$

It is uniquely determined by the Laurent-polynomial $\phi(X) = F \in k[Y, Y^{-1}]$. The commutative diagram

$$\begin{tikzcd}
\mathbb{G}_m \times \mathbb{G}_m \arrow[r] \arrow[d] & \mathbb{G}_m \arrow[d] \\
\mathbb{G}_a \times \mathbb{G}_a \arrow[r] & \mathbb{G}_a
\end{tikzcd}$$

translates into

$$\begin{tikzcd}
k[Y_1, Y_1^{-1}, Y_2, Y_2^{-1}] & k[Y, Y^{-1}] \arrow[l, "Y \mapsto Y_1 Y_2"'] \\
k[X_1, X_2] \arrow[u, "X_i \mapsto F(Y_i)"] & k[X]. \arrow[l, "X \mapsto X_1 + X_2"] \arrow[u, "X \mapsto F(Y)"']
\end{tikzcd}$$

so the condition is

$$F(Y_1 Y_2) = F(Y_1) + F(Y_2).$$

If F has degree n, then the left-hand side has total degree $2n$ and the right-hand side has degree n. This is only possible for $n = 0$, so $F = c$ is constant. Then the condition turns into $c = 2c \Rightarrow c = 0$.

For $\mathrm{Hom}(\mathbb{G}_a, \mathbb{G}_m)$ a morphism f corresponds to an algebra homomorphism

$$\phi : k[Y, Y^{-1}] \to k[X].$$

The image of Y is a unit of $k[X]$, so it is a constant $c \in k^*$. The compatibility with the group structure gives the condition $c = c^2$, so $c = 1$. This is the constant map to the neutral element of $\mathbb{G}_m$.

We turn to $\mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m)$. Elements correspond to ring homomorphisms

$$\phi : k[Y, Y^{-1}] \to k[Y, Y^{-1}],$$

which are uniquely determined by the image F of Y in $k[Y, Y^{-1}]^*$. We first determine these units. We have $F = Y^n F'$ for $n \in \mathbb{Z}$, $F' \in k[Y]$. We choose n, so that F' is not divisible by Y. We write it cG such that G has constant term 1. Then $F^{-1} = c^{-1}Y^{-n}G^{-1}$, so we concentrate on G. We have

$$G = c_0Y^m + c_1Y^{m-1} + \cdots + 1, G^{-1} = \sum_{i=-a}^{b} d_iY^i$$

and hence

$$1 = GG^{-1} = \sum_l \sum_{i+j=l} c_jd_iY^l.$$

We compare coefficients. The sum on the right starts with $l = -a$ and coefficient $1d_{-a}$. This vanishes for $a < 0$, so we have $a \geq 0$. This makes G a unit in $k[Y]$, so it is constant. We have shown

$$k[Y, Y]^* = k^*Y^{\mathbb{Z}}.$$

It remains to check compatibility with multiplication. The condition is

$$F(Y_1Y_2) = F(Y_1)F(Y_2) \Rightarrow cY_1^nY_2^n = c^2Y_1^nY_2^n.$$

This implies $c = 1$. All elements of $\mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m)$ are of the form $z \mapsto z^n$ for some $n \in \mathbb{Z}$.

Now $\mathrm{Hom}(\mathbb{G}_a, \mathbb{G}_a)$. The morphism is determined by $F \in k[X]$. The condition is

$$F(X_1 + X_2) = F(X_1) + F(X_2).$$

Let $F = c_nX^n + \dots$. In total degree n, the equality is

$$c_nX_1^n + c_nnX_1^{n-1}X_2 + \cdots + c_nX_2^n = c_nX_1^n + c_nX_2^n.$$

This is only possible for $n \leq 1$. (We are using characteristic 0 here!). So $F = aX + b$ and the equation is

$$a(X_1 + X_2) + b = aX_1 + b + aX_2 + b,$$

so simply $b = 0$. The map is identified with the image a of $1 \in \mathbb{G}_a$. □

Exercise 2.3. *Check that the identifications of* $\mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m)$ *and* $\mathrm{Hom}(\mathbb{G}_a, \mathbb{G}_a)$ *are compatible with the group laws on both sides.*

Exercise 2.4. *Check that there is an equivalence of categories between vector groups over k and finite dimensional k-vector spaces.*

Definition 2.10. Let $G \cong V \times T$ for a vector group V and torus T. We call

$$X(G) = \mathrm{Hom}(G, \mathbb{G}_m), X_*(G) = \mathrm{Hom}(\mathbb{G}_m, G)$$

the *character group* and *cocharacter group* of G.

Corollary 2.11. *We have*

$$X(G) \cong \mathbb{Z}^r, \quad X_*(G) \cong \mathbb{Z}^r.$$

for some $r \geq 0$.

Proof. We have $G \cong V \times T \cong \mathbb{G}_a^s \times \mathbb{G}_m^r$. Then

$$X(G) \cong X(\mathbb{G}_a^s \times \mathbb{G}_m^r) \cong X(\mathbb{G}_a)^s \times X(\mathbb{G}_m)^r = \mathbb{Z}^r$$

by the proposition. The same argument applies to $X_*(G)$. □

Lemma 2.12. *Let T be a torus with character group $X(T)$. Then its coordinate ring is the group ring*

$$k[T] = k[X(T)] = \bigoplus_{\chi \in X(T)} k\chi \ .$$

Proof. Every character is a map $T \to \mathbb{G}_m$, so it defines a function $\chi : T \to k$. This remark defines a map from right to left. It is natural in T. Hence it suffices to prove the claim for $T = \mathbb{G}_m^r$. The map is also compatible with product of tori:

$$k[T \times T'] = k[T] \otimes_k k[T'] \leftarrow k[X(T)] \otimes_k k[X(T')] = k[X(T) \times X(T')].$$

This reduces the claim to $T = \mathbb{G}_m$. In this case

$$k[\mathbb{G}_m] = k[X, X^{-1}] \cong k[\mathbb{Z}]$$

where $n \in \mathbb{Z}$ is identified with X^n. □

Proposition 2.13. *Let T be a torus and $H \subset T$ an algebraic subgroup. Then H is a torus itself and identifies with the intersection of the kernels of all $\chi \in X(T)$ vanishing on H. Every character of H lifts to a character of G.*

Proof. We have a commutative diagram

$$\begin{tikzcd} k[T] \arrow[r, two heads] & k[H] \\ k[X(T)] \arrow[u, "\cong"] \arrow[r] & k[X(H)] \arrow[u] \end{tikzcd}$$

This makes the map $k[X(H)] \to k[H]$ surjective. An element in the kernel is a k-linear combination of characters that vanishes when viewed as a map $H \to k$. However, it is a standard fact from algebra that characters are linearly independent in $\mathrm{Hom}_k(H, k)$, so the kernel is trivial.

This makes $X(T) \to X(H)$ surjective, so $X(H)$ is a finitely generated abelian group. It is torsion free because H is connected. Hence $k[X(H)] \cong k[\mathbb{G}_m^r]$ and H is a torus. □

Theorem 2.14. *Let $G \cong V \times T$ for a vector group V and a torus T. Let $G' \subset G$ be a subgroup. Then G' is of the form $V' \times T'$ for a subvector group $V' \subset V$ and a subtorus T' of T.*

Proof. Let V' be the kernel of the projection $G' \to G \to T$. It is an algebraic subgroup of V. Let T' be the kernel of the projection $G' \to G \to V$. It is an algebraic subgroup of T. Elements in the intersection are in the kernel of both projections, hence the intersection is trivial. We have found

$$V' \times T' \subset G' \subset V \times T.$$

We claim that $V' \times T' = G'$.

View G as subgroup of some Gl_n via the embedding $\mathbb{G}_a \subset \mathrm{Gl}_2$. The elements $g \in G$ are in Jordan normal form. By the Jordan decomposition, we have

$$g = g^u g^s$$

where g^u is unipotent ($E_n + N$ with N nilpotent) and g^s semi-simple (diagonalisable). The elements g^u and g^s are uniquely determined by these properties and the fact that they commute. (Of course we can read off g^u and g^s directly from the matrix of g.) Moreover—this is the crucial information for us—g^u and g^s are in G'. Obviously $g^u \in V'$ and $g^s \in T'$, so we have written any element of G' as an element of $V' \times T'$.

Now consider $V' \subset V \cong \mathbb{G}_a^s$. With every element v it also contains the infinite set $\{v, 2v, 3v, \dots\}$ (characteristic 0!). This set is Zariski-dense in $\mathbb{G}_a v$, hence V' contains $\mathbb{G}_a v$. This implies that $V' \subset V$ is a subvector space, itself a vector group.

Finally, $T' \subset T$ was considered already. □

Exercise 2.5. *(talk) report on the proof of the Jordan decomposition in the form claimed in the proof. References: Springer, Linear alg. groups or Borel, same title.*

We add a general property that we have used already.

Lemma 2.15. *Let G be an algebraic group and $H \subset G$ an algebraic subgroup (i.e., it is an algebraic group and the inclusion is a morphism of algebraic groups). Then H is a closed subvariety of G.*

Proof. Consider the closure $\overline{H}$ of H. The morphisms $\mu : H \times H \to H$ and $\iota : H \to H$ extend to $\overline{\mu} : \overline{H} \times \overline{H} \to \overline{H}$ and $\overline{\iota} : \overline{H} \to \overline{H}$. They satisfy the identities of a group because these identities are satisfied on the dense subset H. This makes $\overline{H}$ an algebraic group. We replace G by $\overline{H}$ for the rest or the argument, i.e., H is dense. We claim $H = G$.

The boundary $D = G \smallsetminus H$ has smaller dimension than $\dim H$. Its closure $\overline{D}$ keeps this dimension. Hence H contains an open subset $U \subset G$. We have

$$H = \bigcup_{h \in H} Uh,$$

hence $H \subset G$ is open. Let $S \subset G$ be a set of representatives for the cosets of H in G. Then

$$G = \bigcup_{s \in S} Hs.$$

Each coset is open. It is also the complement of the union of all the other cosets, hence closed. This makes it an open and closed subset of G. It particular, H itself is closed in G. This means $H = G$, as claimed. $\square$

Chapter 3

Tangent spaces and the exponential map

Our aim is to define the exponential map from the Lie algebra of G to G.

Definition 3.1. Let G be an algebraic group. The *Lie algebra* of G is the tangent space of G in e, or, equivalently, the k-vector space of G-left invariant vector fields. We denote it $\mathrm{Lie}(G)$ or $\mathfrak{g}$.

The vector space $\mathfrak{g}$ has an additional structure, the *Lie bracket.* We do not need it and will not discuss it. (It vanishes in the commutative case we are in.)

In order to make sense of the above definition, we need to define tangent spaces. We first discuss them informally. Let V be an algebraic variety, $P \in V$ a point. The *tangent space* T_PV of V in P is the space of all tangent directions in P. They form a vector space. It dual is the *cotangent space* T_P^*V. For varying P we get the *tangent bundle* and the *cotangent bundle*

$$TV = \coprod_{P\in V} T_PV, \quad T^*V = \coprod_{P\in V} T_P^*V.$$

They can be given structures of algebraic varieties, but again, we do not need this structure and do not discuss it. Sections of TV, i.e., maps

$$X : V \to TV \quad X(P) \in T_PV$$

are called *vector fields.* Sections of T^*V are called *differential forms.* Given a morphism $f : V \to W$ of algebraic varieties, we get induced linear maps

$$df_P : T_PV \to T_{f(P)}W, \quad f^* : T^*_{f(P)}W \to T_P^*V.$$

Vector fields are covariant, while differential forms are contravariant.

Example 3.2. Consider $V = V(XY - 1) \subset \mathbb{A}^2$. For every point in $\mathbb{A}^2$, we have a 2-dimensional space of tangent directions. Let $P = (x_0, y_0) \in V$. We identify V with the graph of $X \mapsto 1/X$. The tangent direction in P is given by the derivative $-1/X^2$, so the tangent space $T_P V \subset T_P \mathbb{A}^2 = k^2$ is spanned by $(1, -1/x_0^2)$. It is the line with the equation

$$Y = -\frac{1}{x_0^2} X \Leftrightarrow \frac{1}{x_0}^2 X + Y = 0.$$

This can be rewritten in the form

$$y_0 X + x_0 Y = 0.$$

More generally: if $V = V(F)$, then the tangent line in $P = (x_0, y_0)$ has the equation

$$\frac{\partial F}{\partial X}(P) X + \frac{\partial F}{\partial Y}(P) Y = 0.$$

In other word, these are the vectors dual to the differential

$$dF(P) = \frac{\partial F}{\partial X}(P) dX + \frac{\partial F}{\partial Y}(P) dY = 0.$$

Exercise 3.1. *Use the formulas of the example to give TV the structure of an algebraic variety in the case $V = V(F) \subset \mathbb{A}^2$.*

We want to write this in a way that is independent of an embedding. So what *is* a tangent vector? It is direction on V. We identify them with *directional derivatives.* Given a function near P (an element in the local ring $\mathcal{O}_P$), we may take its derivative in some direction. We turn this on its head.

Definition 3.3. Let V be an algebraic variety, $P \in V$. A *derivation* is a k-linear map

$$D : \mathcal{O}_P \to k$$

satisfying the *Leibniz rule*

$$D(fg) = f(P)D(g) + g(P)D(f).$$

Let $T_P V$ be the space of all derivations in P.

Example 3.4. Let $V = \mathbb{A}^n$, $P = (x_1, \ldots, x_n)$. Then

$$\partial_i : f \mapsto \frac{\partial f}{\partial X_i}(P)$$

(deriving polynomials and their fractions formally) is a derivation.

Lemma 3.5. *The set $T_P V$ is a vector space. It is dual to m_P/m_P^2.*

Proof. Obviously sums and multiples of derivations are derivations. For every f, we have

$$D(1f) = 1D(f) + f(P)D(1) \Rightarrow D(1) = 0.$$

By k-linearity this implies $D(a) = 0$ for all constant functions.

Every $f \in \mathcal{O}_P$ can be written as $f = f(P) + g$ with $g \in m_P$. We have

$$D(f) = 0 + D(g),$$

hence derivations are uniquely determined by their values on m_P.

Let $f, g \in m_P$. Then

$$D(fg) = f(P)D(g) + g(P)D(f) = 0 + 0 = 0.$$

In total, we have seen that a derivation induces a k-linear map $m_P/m_P^2 \to k$ and is uniquely determined by it.

We claim that the converse also holds. Let $\phi : m_P/m_P^2 \to k$ be k-linear. We put $D(f) = \phi(f - f(P))$ and need to check that it is a derivation. Clearly it is k-linear. We have

$$\begin{aligned} D(fg)-f(P)D(g)-g(P)D(f) &= \phi(fg-f(P)g(P))-\phi(f(P)(g-g(P)))-\phi(g(P)(f-f(P))) \\ &= \phi(fg - f(P)g(P) - f(P)g + f(P)g(P) - g(P)f + g(P)f(P)) \\ &= \phi((f - f(P))(g - g(P))) = 0 \end{aligned}$$

because ϕ vanishes on m_P^2. □

Example 3.6. For $U \subset \mathbb{A}^n$ open, the tangent space T_PU is generated by $\frac{\partial}{\partial X_i}$ for $i = 1, \dots, n$ where $X_1, \dots, X_n$ are the coordinates on $\mathbb{A}^n$. This applies in particular for $G = V \times T \subset \mathbb{A}^{s+r}$ for V a vector group of dimension s and T a torus of dimension r.

Exercise 3.2. *Use the description of $\mathbb{G}_m = V(XY - 1) \subset \mathbb{A}^2$. Compare the definition via derivations with the geometric interpretation as tangent lines. Make the comparison of the tangent spaces of $V(XY - 1)$ and the open subset of $\mathbb{A}^1$ explicit.*

Exercise 3.3. *Show that T_PV is always finite dimensional of dimension at least* $\dim V$.

Exercise 3.4. *Let $t \in k$ be fixed. Compute the tangent space of* 0 *on the curve with equation $Y^2 = X(X - t)(X - 1)$.*

We now have made sense of the definition of the Lie algebra of G as the tangent space in e. It is anti-climatic for our $G = V \times T$: just k^n for $n = \dim G$. Nevertheless, the definition tell us what the induced map is for morphisms of varieties.

Definition 3.7. Let $f : V \to W$ be a morphism of varieties, $P \in V$. We define

$$df_P : T_PV \to T_{f(P)}W$$

by mapping a derivation $D : \mathcal{O}_P \to k$ to the composition

$$f_*D : \mathcal{O}_{f(P)} \xrightarrow{g \mapsto g \circ f} \mathcal{O}_P \xrightarrow{D} k.$$

We are interested in this functoriality for the left multiplication by an element $g \in G$ on an algebraic group:

$$\tau_g : G \to G, \quad x \mapsto \mu(g,x).$$

Note that it is a morphism of algebraic varieties.

Definition 3.8. Let G be an algebraic group. A vector field $\phi : G \to TG$ is called *left-invariant* if

$$(d\tau_g)_x \phi_x = \phi_{gx}$$

for all $x \in G$ and $g \in G$.

Example 3.9. Let $G = \mathbb{G}_a$ with coordinate X. Then the vector field $\partial = \frac{\partial}{\partial X}$ is left-invariant. Indeed, for every $f \in \mathcal{O}_{g+x} \subset k(X)$ we have by the chain rule

$$((d\tau_g)_x\partial)f = \frac{\partial(f \circ \tau_g)}{\partial X}(x) = \frac{\partial f}{\partial X}(x+g)\frac{\partial \tau_g}{\partial X}(x) = \frac{\partial f}{\partial X}(x+g) = \partial f$$

because τ_g is the function $X \mapsto g + X$ with derivative 1.

Lemma 3.10. *Let G be an algebraic group. Then the space of left-invariant vector fields is naturally isomorphic to the tangent space in e. The isomorphism is induced by mapping $\phi : G \to TG$ to ϕ_e.*

Proof. For all $g \in G$, we have $g = \tau_g e$ and hence by the definition of a left-invariant vector field

$$\phi_g = (d\tau_g)_e \phi_e.$$

The vector field is uniquely determined by ϕ_e. Conversely every choice of ϕ_e extends to a vector field. □

Example 3.11. Consider $G = \mathbb{G}_m$. By restriction from $\mathbb{A}^1$, we have the vector field ∂. It is no longer invariant: For every $f \in \mathcal{O}_{gx}$ we have

$$((d\tau_g)_x\partial)f = \frac{\partial(f \circ \tau_g)}{\partial X}(x) = \frac{\partial f}{\partial X}(gx)\frac{\partial \tau_g}{\partial X}(x) = g\frac{\partial f}{\partial X}(gx) = g\partial f$$

because τ_g is the function $X \mapsto gX$ with derivative g. In fact, the invariant vector field is $X\partial$. By this we mean $x \mapsto x\partial \in T_x\mathbb{G}_m$. We check:

$$(d\tau_g)_x x\partial = x(d\tau_g)_x\partial = xg\partial.$$

Corollary 3.12. *Let $G = \mathbb{G}_a^s \times \mathbb{G}_m^r$ with coordinates $X_1, \dots, X_s, Y_1, \dots, Y_r$. Then*

$$\left(\frac{\partial}{\partial X_1}, \dots, \frac{\partial}{\partial X_s}, Y_1\frac{\partial}{\partial Y_1}, \dots, Y_r\frac{\partial}{\partial Y_r}\right)$$

is a basis for the space of invariant vector fields on G.

Proof. Evaluation at the neutral element gives the standard basis of k^{s+r}. □

Exercise 3.5. *Show that there is a natural isomorphism between $T_e^*G = m_e/m_e^2$ and the space $\Omega(G)^G$ of left-invariant differential forms. What is the invariant form on $\mathbb{G}_a$ and $\mathbb{G}_m$?*

The exponential map

So far, we have been working with algebraic varieties and algebraic groups. Everything is compatible with base change, e.g., from the ground field $\overline{\mathbb{Q}}$ to $\mathbb{C}$.

Over the complex numbers, an algebraic group G also gives rise to a complex manifold G^{an}. It is a *complex Lie group*, i.e., the group law and inversion are holomorphic (=complex differentiable).

Example 3.13. If $G = \mathbb{G}_a^s \times \mathbb{G}_m^r$, then $G^{\mathrm{an}} = \mathbb{C}^s \times (\mathbb{C}^*)^r$ viewed as a subspace of $\mathbb{C}^{s+r}$ with the metric topology.

The exponential function is a concept from differential geometry. Given a Riemann manifold M and point $P \in M$, there is map

$$\exp : U \to M$$

defined on an open neighbourhood U of $0 \in T_P M$ mapping an interval containing 0 to a geodesic through P. In the case of a Lie group, this map is even globally defined. We are only interested in the cases $M = \mathbb{C}$ and $M = \mathbb{C}^*$ and their products.

Definition 3.14. Let G^{an} be a commutative complex Lie group. The *exponential map* is the unique holomorphic group homomorphism

$$\exp_G : \mathrm{Lie}(G) \to G^{\mathrm{an}}$$

such that

$$(d \exp_G)_0 : \mathrm{Lie}(G) \to T_e G^{\mathrm{an}}$$

is the identity.

Lemma 3.15. *The map* $\exp_G$ *exists and is uniquely determined by these assumptions for* $G = V \times T$ *where* V *is a vector group and* T *a torus. It is given by the identity on* V *and coordinatewise by the complex exponential function on* T.

Proof. Let $v \in \mathrm{Lie}(G)$. We have to show that there is a unique holomorphic group homomorphism

$$\mathbb{C} \to G^{\mathrm{an}}$$

whose differential maps $\partial/\partial t$ to v. The statement is invariant under isomorphisms of Lie groups and compatible with products. Hence it suffices to consider the cases $G = \mathbb{G}_a$ and $G = \mathbb{G}_m$ separately.

We start with $\mathbb{G}_m$. We want a holomorphic map

$$E : \mathbb{C} \to \mathbb{C}^*,$$

so it is given by a converging power series $E(z) = \sum_{i=0}^{\infty} a_i z^i$. We have $a_0 = E(0) = 1$ because it is a group homomorphism and $a_1 = 1$ because $E'(0) = 1$. The property of being a group homomorphism translates into the identity

$$E(z_1)E(z_2) = E(z_1 + z_2) \Leftrightarrow \sum_{i,j} a_i a_j z_1^i z_2^j = \sum_n a_n (z_1 + z_2)^n.$$

Comparison of coefficients gives the system of equations

$$a_i a_j = \binom{i+j}{i} a_{i+j} \Rightarrow a_i = (i+1)a_{i+1} \Rightarrow a_i = \frac{1}{i!}.$$

Hence E is the ordinary exponential function.

In the case $\mathbb{G}_a$, the same argument gives $E(z) = z$. □

Exercise 3.6. *Let $G^{\mathrm{an}} = \mathbb{C}^s \times (\mathbb{C}^*)^r$. Show that $\mathrm{Lie}(G^{\mathrm{an}})$ is the universal covering space of G^{an} and deduce $\pi_1(G^{\mathrm{an}}) \cong \mathbb{Z}^r$. If you know about homology: Compute $H_1^{\mathrm{sing}}(G^{\mathrm{an}}, \mathbb{Z})$.*

The analytic subgroup theorem in our case

We are now ready to formulate:

Theorem 3.16 (Wüstholz)**.** *Let $G = V \times T$ be the product of a vector group and a torus over $\overline{\mathbb{Q}}$. Let $\mathfrak{b} \subset \mathrm{Lie}(G)$ be a subvector space. Assume that the analytic subgroup $B = \exp(\mathfrak{b}_{\mathbb{C}})$ of G^{an} contains an algebraic point $0 \neq P \in G(\overline{\mathbb{Q}})$. Then there is an algebraic subgroup $0 \neq H \subset G$ such that $\mathrm{Lie}(H) \subset \mathfrak{b}$ and $P \in H(\overline{\mathbb{Q}})$.*

Corollary 3.17. *The number π is transcendental.*

Proof. Assume $2\pi i$ is algebraic. We consider the algebraic group $G = \mathbb{G}_a \times \mathbb{G}_m$. Its Lie algebra is $\overline{\mathbb{Q}}^2$. By assumption $v = (1, 2\pi i)$ is an element. Let $\mathfrak{b} = \overline{\mathbb{Q}}v$. Its image $B \subset \mathbb{C} \times \mathbb{C}^*$ contains

$$P = \exp_G(v) = (1, \exp(2\pi i)) = (1, 1) \in G(\overline{\mathbb{Q}}).$$

By the analytic subgoup theorem there exists an algebraic subgroup $H \subset G$ such that $\mathrm{Lie}(H) \subset \mathfrak{b}$ and $P \in H(\overline{\mathbb{Q}})$. By the structure theory for groups of the form $V \times G$, the subgroup H has to be in the list

$$\{(0,1)\}, \mathbb{G}_a \times \{1\}, \{0\} \times \mathbb{G}_m, \mathbb{G}_a \times \mathbb{G}_m.$$

The only ones containing P are $\mathbb{G}_a \times \{1\}$ and $\mathbb{G}_a \times \mathbb{G}_m$. In the first case, the Lie algebra is $\overline{\mathbb{Q}} \times \{0\}$ and does not contain v. In the second case $\mathrm{Lie}(G)$ has dimension 2, so it cannot be contained in the 1-dimensional $\mathfrak{b}$. This is a contradiction. □

Exercise 3.7. *Let $\alpha \in \overline{\mathbb{Q}}^*$, not a root of unity. Let β, γ be different choices of $\log(\alpha)$. Show that they are $\overline{\mathbb{Q}}$-linearly independent.*

Corollary 3.18 (Extended Baker Theorem)**.** *Let $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{Q}}^*$ be multiplicatively independent. Then the system*

$$(1, 2\pi i, \log(\alpha_1), \dots, \log(\alpha_n))$$

is $\overline{\mathbb{Q}}$-linearly independent.

Proof. Suppose they are linearly dependent. This means that there are $a, b, c_1, \dots, c_n \in \overline{\mathbb{Q}}$ (not all of them 0) such that

$$a + b2\pi i + c_1 \log(\alpha_1) + \cdots + c_n \log(\alpha_n) = 0.$$

We consider $G = \mathbb{G}_a \times \mathbb{G}_m^{n+1}$. Its Lie algebra is $\overline{\mathbb{Q}}^{n+2}$. Let

$$\mathfrak{b} = (a, b, c_1, \dots, c_n)^{\perp} \subset \mathrm{Lie}(G)$$

(orthogonal complement with respect to the standard “scalar product”). The vector $v = (1, 2\pi i, \log(\alpha_1), \dots, \log(\alpha_n))$ is in $\mathfrak{b}_{\mathbb{C}}$. Its image

$$P = \exp_G(v) = (1, 1, \alpha_1, \dots, \alpha_n)$$

is in $G(\overline{\mathbb{Q}})$. We are in the situation of the analytic subgroup theorem. Hence there is an algebraic subgroup $H \subset G$ with $P \in G(\overline{\mathbb{Q}})$ and $\mathrm{Lie}(H) \subset \mathfrak{b}$.

By the structure theory for linear commutative algebraic groups, H is of the form $V \times T$ for a vector group $V \subset \mathbb{G}_a$ and a torus $T \subset \mathbb{G}_m^{n+1}$. From the shape of P, we see that $V = \mathbb{G}_a$. As $\mathfrak{b} \subsetneq \mathrm{Lie}(G)$, the torus T is a proper subtorus of $\mathbb{G}_m^{n+1}$. Hence there is a non-trivial character $\chi : \mathbb{G}_m^{n+1} \to \mathbb{G}_m$ which vanishes on T. It is of the shape $(z_0, \dots, z_n) \mapsto z_0^{m_0} \dots z_n^{m_n}$. This gives

$$\chi(1, \alpha_1, \dots, \alpha_n) = \alpha_1^{m_1} \dots \alpha_n^{m_n} = 1.$$

By assumption the α_i are multiplicatively independent, hence $m_1 = \cdots = m_n = 0$. This holds for all non-trivial characters and T is the intersection of the characters vanishing on it. Hence $\{1\} \times \mathbb{G}_m^n \subset T$. Together

$$V \times \{1\} \times \mathbb{G}_m^n \subset H.$$

We have even equality, because $H \neq G$. This means

$$\mathrm{Lie}(H) = \overline{\mathbb{Q}} \times \{0\} \times \overline{\mathbb{Q}}^n \subset \mathfrak{b}.$$

By definition of $\mathfrak{b}$ this implies $a = c_1 = \cdots = c_n = 0$. Our linear relation reduces to $b2\pi i = 0$, so also $b = 0$. We have reached a contradiction. □

Chapter 4

Reduction to the semi-stable case

We introduce an ad-hoc terminology:

Definition 4.1. Let $\pi : G \to G'$ be a surjective morphism of commutative algebraic groups. We say that it is *a proper quotient* if the kernel is connected and different from 0 and G.

Proposition 4.2. *Let $0 \neq H \subsetneq G$ be an inclusion of commutative algebraic groups. Then G/H is algebraic and $\pi : G \to G/H$ a proper quotient.*

Proof. We only treat the case $G = V \times T$. We put the general case on a todo list for later/refer to the literature.

In the linear case, we have $H = V' \times H'$, so we do the vector case and the torus case separately. For a subvectorspace $V' \subset V$, the quotient vector space V/V' is indentified with a power of $\mathbb{G}_a$ by choice of a basis. The k-linear map $V \to V/V'$ is a morphism of algebraic groups.

For a subtorus $T' \subset T$, we get a surjective map $X(T) \to X(T')$. Its kernel X'' is a free abelian group of finite rank. Hence the group ring $k[X'']$ defines a torus T'' with character group X''. This is T/T'. □

Definition 4.3. Let G be commutative algebraic group over $\overline{\mathbb{Q}}$, $V \subset \mathrm{Lie}(G)$ a sub vector space. We put

$$\tau(G, V) = \frac{\dim V}{\dim G}.$$

The vector space is called *semi-stable* if for all surjective morphisms ofcommutative algebraic groups $\pi : G \to G'$ with $\dim G' < \dim G$ and $G' \neq 0$, we have

$$\tau(G', \pi_* V) \geq \tau(G, V).$$

Remark 4.4. Let $W = \mathrm{Lie}(G)$. The choice of the subvector space can be interpreted as a filtration on W indexed by $0, 1, 2$:

$$F^2 W = 0 \subset F^1 W = V \subset F^0 W = W.$$

In the theory of filtered vector bundels (here: filtered vector spaces) there is the notion of the *slope* of a filtration:

$$\mu(F^*W)=\sum_i i\frac{\dim F^iW/F^{i+1}W}{\dim W}.$$

In our case this is $\tau(G,V)$. There is also the notion of *semi-stability* in the theory of filtered vector bundles. The exact relation is not clear to me.

Note that $\dim V\leq\dim G$, hence $\tau(G,V)\leq 1$ with equality for $V=\mathrm{Lie}(G)$.

Example 4.5. (i) $V=\mathrm{Lie}(G)$ is semi-stable because $\pi_*V=\mathrm{Lie}(G')$ and $1\geq 1$.

(ii) $V=0$ is semi-stable because $\pi_*V=0$ for all π and $0\geq 0$.

Semi-stability is about the interaction of V and the subvector space $\mathrm{Ker}(\pi_*)\subset\mathrm{Lie}(G)$. Let us consider the two extremes: Let $d=\dim V$, $d'=\dim\pi_*(V)$, $n=\dim G$, $n'=\dim G'$.

- If $\mathrm{Ker}(\pi_*)\cap V=0$, then $d=d'$ and hence
$$\tau(G,V)=\frac{d}{n}\leq\frac{d}{n'}=\tau(G',\pi_*(V))$$
because $n'\leq n$. This is allowed for semi-stable V.
- If $\mathrm{Ker}(\pi_*)\subset V$, then $d'=d-m$, $n'=n-m$ for $m=\dim\mathrm{Ker}(\pi_*)$, so
$$\tau(G,V)=\frac{d}{n}>\frac{d-m}{n-m}=\tau(G',\pi_*(V))$$
(unless $m=0$). This is not allowed for semi-stable V.

Exercise 4.1. *Determine all semi-stable subspaces V for $G=\mathbb{G}_m^2$, $G=\mathbb{G}_a^2$ and $G=\mathbb{G}_m\times\mathbb{G}_a$.*

Proposition 4.6. *Let G be a non-trivial commutative algebraic group over $\overline{\mathbb{Q}}$, $V\subset\mathrm{Lie}(G)$ a subvector space. Then there is a surjective morphism of commutative algebraic groups $\pi:G\to G^*$, either the identity or a proper quotient, such that $\tau(G^*,V^*)$ (here $V^*=\pi_*(V)$) is minimal. Moreover, $V^*\subset\mathrm{Lie}(G^*)$ is semi-stable.*

Proof. We show existence. If (G,V) is semi-stable, there is nothing to show. Otherwise, we consider all proper quotients $\pi:G\to G'$ with $\dim G'<\dim G$. There are only finitely many possibilities for $\dim G'$ and only finitely many possibilities for $\dim\pi_*(V)$. Hence the set of $\tau(G',\pi_*(V))$ is finite and the minimum is attained in some (G^*,V^*).

We check that (G^*,V^*) is semi-stable. Let $\pi:G^*\to G'$ be surjective and $\tau(G',\pi'(V^*))<\tau(G^*,V^*)$, then $G\to G^*\to G'$ is also surjective. Let H be the connected component of the kernel of $G\to G'$. Then the map factors via

$G \to G/H \to G'$ and $\dim G/H = \dim G'$. This implies that $G/H \to G'$ is an isomorphism on tangent spaces. Hence

$$\tau(G/H, V') = \tau(G', V') < \tau(G^*, V').$$

This contradicts the minimality of $\tau(G^*, V^*)$. □

Exercise 4.2. *(not obvious) [Baker-Wüstholz] p. 138 claim that (G^*, V^*) is unique if* $\dim G^*$ *is chosen minimal. Deduce this from the theory of the Harder-Narasimhan filtration, see for example [Faltings-Wüstholz] p. 117/118.*

Lemma 4.7. *Let $G, \mathfrak{b}, B, P$ be as in the analytic subgroup theorem. Assume that (G, B) is semi-stable. If there is an algebraic subgroup $H \subsetneq G$ with* $\mathrm{Lie}(H) \subset \mathfrak{b}$ *and $P \in H(\overline{\mathbb{Q}})$, then $P = 0$.*

In other words: in the semi-stable case the analytic subgroup theorem predicts vanishing of $G(\overline{\mathbb{Q}}) \cap B$ or $\mathfrak{b} = \mathrm{Lie}(G)$.

Proof. Consider $\pi : G \to G/H$. We have $\mathrm{Ker}(\pi_*) = \mathrm{Lie}(H) \subset \mathfrak{b}$. As we worked out in the example, this is excluded by semi-stability. Hence $\mathrm{Lie}(H) = 0$ and H is trivial. As $P \in H(\overline{\mathbb{Q}})$ this means also $P = 0$. □

Proposition 4.8. *Suppose the analytic subgroup theorem holds whenever, in addition, B is stemi-stable. Then it holds in general.*

Proof. We argue by induction on $\dim G$. If G is of dimension 1, then $\mathfrak{b} \subset \mathrm{Lie}(G)$ has dimension 0 or 1. In the first case, $B = 0$, in the second $B = G^{\mathrm{an}}$. In both cases it is algebraic.

Suppose now that the theorem holds for all groups of dimension less than n. Let G be an algebraic group of dimension n, $\mathfrak{b} \subset \mathrm{Lie}(G)$, $B = \exp_G(\mathfrak{b}_{\mathbb{C}})$, $P \in G(\overline{\mathbb{Q}}) \cap B$. If B is semi-stable, the subgroup theorem holds by assumption. Otherwise, let $\pi : G \to G^*$ be the projection such that (G^*, B^*) with $B^* = \pi_*(B)$ is semi-stable. As $(G, \mathfrak{b})$ was not semi-stable, we have

$$\tau(G^*, \mathfrak{b}^*) < \tau(G, \mathfrak{b}) \leq 1.$$

In consequece $\mathfrak{b}^* \subsetneq \mathrm{Lie}(G^*)$ is a proper subspace and $\dim B < \dim G^{\mathrm{an}}$. Consider $P^* = \pi(P) \in B^* \cap G^*(\overline{\mathbb{Q}})$. By the analytic subgroup theorem in the semi-stable case, we have $P^* = 0$ (this was the lemma).

In other words, $P \in \mathrm{Ker}(\pi) =: K$. The map $G \to G^*$ is a proper quotient, i.e., K is connected and $K \subsetneq G$. We apply the analytic subgroup theorem to K, $\mathfrak{b} \cap \mathrm{Lie}(K)$, P. This is possible by inductive hypothesis. We find an algebraic subgroup $H \subset K$ with $\mathrm{Lie}(H) \subset \mathfrak{b} \cap \mathrm{Lie}(H) \subset \mathfrak{b}$ and $P \in H(\overline{\mathbb{Q}})$. This is the analytic subgroup theorem for the original data. □

So the actual work is in proving:

Theorem 4.9 (Semi-stability theorem)**.** *Let G a commutative algebraic group over $\overline{\mathbb{Q}}$, $\mathfrak{b} \subset \mathrm{Lie}(G)$ a subvector space which is semi-stable. Then $G(\overline{\mathbb{Q}}) \cap B = 0$ (where as before $B = \exp_G(\mathfrak{b}_{\mathbb{C}})$).*

Exercise 4.3. *Show that it is enough to establish the theorem in the case where* $\dim \mathfrak{b} = \dim G - 1$.

Chapter 5

Analytic tools for the proof

Multiplicity estimates

Let again k be an algebraically closed field of characteristic 0. Throughout, G will be a quasi-projective algebraic group over k and we fix an embedding $G \subset \mathbb{P}^N$. We also fix a subvector space $V \subset \mathrm{Lie}(G)$ and a point $g \in G$.

Example 5.1. Let $G = V \times T$ be the product of a vector group and a torus. By a choice of isomorphism to $\mathbb{G}_a^s \times \mathbb{G}_m^r$ we get an embedding $G \subset \mathbb{A}^{s+r} \subset \mathbb{P}^{s+r}$.

In fact, all algebraic groups are quasi-projective, so the assumption is not a restriction.

Let $\overline{G}$ be the closure of G in $\mathbb{P}^N$ and $S[\overline{G}]$ its homogeneous coordinate ring. Recall that $S[\overline{G}]$ is a graded ring. The multiplication on G extend to an operation

$$G \times \overline{G} \to \overline{G}.$$

Exercise 5.1. *Write down $S[\overline{G}]$ for $G = \mathbb{G}_a^s \times \mathbb{G}_m^r$.*

We want to choose the coordinates on $\mathbb{P}^N$ such that no multiple of g lies on the hyperplane $X_0 = 0$. This is possible.

Lemma 5.2. *Let $\Gamma \subset G$ be a finitely generated subgroup. Then there is a hyperplane $H \subset \mathbb{P}^N$ that does not meet Γ.*

Proof. The definition of G and the finitely many generators of Γ only involves finitely many polynomials over k. Hence G and Γ can be defined over a field k_0 which is finitely generated over $\mathbb{Q}$. It suffices to show that there is a hyperplane in $\mathbb{P}_k^N$ which does not contain any point in $\mathbb{P}^N(k_0)$. Let K/k_0 be a field extension of degree $N+1$. (Such an extension exists because k_0 is finitely generated over $\mathbb{Q}$.) Let $\omega_0, \dots, \omega_N$ be a k_0-basis of K. We consider the hyperplane

$$\omega_0 X_0 + \omega_1 X_1 + \cdots + \omega_N X_N = 0.$$

Let $[a_0 : \cdots : a_N] \in \mathbb{P}^N(k_0)$. If it was on the hyperplane, then we would have

$$\sum_{i=0}^{N} a_i \omega_i = 0,$$

contradicting the linear independence of the basis vectors. $\square$

Let $U_0 = \overline{G} \smallsetminus V(X_0)$. Its coordinate ring is generated by $Y_i = X_i/X_0$ for $i = 1, \dots, N$.

Example 5.3. For $G = \mathbb{G}_a^3$ with coordinates Y_1, Y_2, Y_3, we can use $N = 3$ and $\overline{G} = \mathbb{P}^3$. The homogeneous coordinate ring is $k[X_0, \dots, X_3]$. In this case $U_0 = G$ and $k[U_0] = k[Y_1, Y_2, Y_3]$. A polynomial P of degree D in $S[\overline{G}]$ gives rise to a function P_0 on U_0, itself an inhomogeneous polynomial of degree at most D.

Recall that a polynomial P in one variable has a zero of order bigger than T in a point a if the first T derivatives vanish in a. Analogously we can say that a polynomial in several variables has a zero of order bigger than T in a point a if the mixed derivatives of total order up to T vanish.

Example 5.4. The polynomial $P = X^2Y^3$ has zero of order bigger than 4 in $(0, 0)$ because the derivatives

$$\frac{\partial^i}{\partial X^i} \frac{\partial^j}{\partial Y^j} X^2 Y^3$$

vanish in $(0, 0)$. Indeed, the first (only) non-vanishing derivative is for $i = 2$, $j = 3$.

Exercise 5.2 (Taylor expansion). *Let $P \in k[Y_1, \dots, Y_n]$, $a = (a_1, \dots, a_n)$. Show that P can be written uniquely in the form*

$$P = \sum_{t \in \mathbb{N}_0^n} \frac{1}{t!} \frac{\partial^t}{\partial Y^t} P(a)(Y_1 - a_1)^{t_1} \dots (Y_n - a_n)^{t_n}$$

with only finitely many terms non-zero. Here we use multi-index notation as in analysis. Determine the vanishing order from the expansion.

If the vanishing order is high compared to the degree, then P has to vanish. We want to generalise this in several directions:

- use more than 1 point where the vanishing order is prescribed;
- do not use partial derivatives in all coordinate directions but only a d-dimensional space of tangent vectors instead;
- replace $\mathbb{G}_a^n$ by some commutative algebraic group.

Lemma 5.5. *Let $\partial \in \mathrm{Lie}(G)$ viewed as an invariant vector field, $U \subset G$ affine. Then ∂ defines an operator*

$$L : k[U] \to k[U]$$

such that for all $x \in U$ and $f \in k[U]$ we have

$$(Lf)(x) = \partial_x f.$$

Proof. The formula defines $L(f)$ as a function $U \to k$. We claim that it is algebraic. This follows from the general theory of the algebraic tangent bundle. We only verify the case $G = V \times T$. It suffices to consider the cases $\mathbb{G}_a$ and $\mathbb{G}_m$. We have explicit formulas for the basis of $\mathrm{Lie}(G)$. They are of the form $\partial/\partial X$ and $X\partial/\partial X$ in the standard coordinates on G. In both cases the value is given by algebraic functions. □

By shrinking U, we get an operator

$$L : \mathcal{O}_P \to \mathcal{O}_P.$$

Exercise 5.3. *Let ∂_1 and ∂_2 be linearly independent. Show that the induced L_1 and L_2 commute.*

Exercise 5.4. *Consider $\exp_G : \mathrm{Lie}G^{\mathrm{an}} \to G^{\mathrm{an}}$. Let $\partial \in \mathrm{Lie}(G^{\mathrm{an}})$ and L_∂ the corresponding invariant vector field. We may also view ∂ as an element in $T_0\mathrm{Lie}G^{\mathrm{an}}$ and extend it to an invariant vector vield of $\mathrm{Lie}G^{\mathrm{an}}$. Consider*

$$d\exp_x : T_x\mathrm{Lie}G^{\mathrm{an}} \cong T_0\mathrm{Lie}G^{\mathrm{an}} \to T_{\exp(x)}G^{\mathrm{an}}$$

for $x \in \mathrm{Lie}(G^{\mathrm{an}})$.

(i) Make this explicit for $G = \mathbb{G}_a$ and $G = \mathbb{G}_m$.

(ii) Verify that $d\exp_x$ is the map $\partial \mapsto (L_\partial)_x$, for $G = \mathbb{G}_m$ and in general.

Exercise 5.5. *Let G^{an} be the complex Lie group attached to a commutative algebraic group. Fix $\partial \in \mathrm{Lie}(G^{\mathrm{an}})$. Let $\phi : \mathbb{C} \to G^{\mathrm{an}}$ be the holomorphic group homomorphism inducing $\partial/\partial z \mapsto \partial$. Show that the operator L on holomorphic functions near 0 is the derivative in direction ϕ.*

Definition 5.6. Let $V \subset \mathrm{Lie}(G)$ with basis $\partial_1, \dots, \partial_d$, $f \in \mathcal{O}_P$. Let $L_1, \dots, L_d$ be the associated differential operators. We say that f *vanishes of order bigger than T in direction V* if for all $t_1, \dots, t_d$ with $\sum t_i \leq T$ all

$$L_1^{t_1} \dots L_d^{t_d} f$$

vanish at P.

This is also written using the *translation operator*

$$T_P : \mathcal{O}_P \to \mathcal{O}_0, \quad f \mapsto f \circ \tau_P$$

where $\tau_P : G \to G$ is the morphism defined by adding P. The condition than becomes vanishing of the

$$T_P L_1^{t_1} \dots L_d^{t_d} f$$

in 0.

Theorem 5.7 (Multiplicity estimate)**.** *Let G be a commutative algebraic group, $V \subset \mathrm{Lie}(G)$ semi-stable. Let $L_1, \dots, L_d$ be a basis of the space of linear operators of V and $g \in G$. Then there is a constant c depending only on G and V such that:*

Given $S, T, D \in \mathbb{N}_0$ with $ST^d > cD^n$ and $0 \neq P \in S[\overline{G}]_D$ viewed as a function on U_0 such that P vanishes of order bigger than T in the points $0, g, 2g, \dots, Sg$, then there is $0 < s' < S$ such that $s'g = 0$.

We defer the proof, even in the special case and first want to see how it is used.

Holomorphic one parameter subgroups

We are still in the same situaton: G a commutative algebraic group, $g \in G$ a point, $\mathfrak{b} \subset \mathrm{Lie}(G)$ such that $g \in B = \exp_G(\mathfrak{b}_\mathbb{C})$. We are interested in the case when all this data is defined over $\overline{\mathbb{Q}}$, but now look at the complex points from the analytic point of view.

Lemma 5.8. *Let $g \neq 0$. There is a holomorphic group homomorphism*

$$\Phi : \mathbb{C} \to G^{\mathrm{an}}$$

such that $\Phi(1) = g$. It is uniquely determined by the image u in $\mathrm{Lie}(G^{\mathrm{an}})$ of d/dz The image of Φ is contained in B.

Proof. Let $u \in \mathrm{Lie}(G^{\mathrm{an}})$ be the preimage of g under the exponential map. It is different from 0. We get Φ as

$$\mathbb{C} \to \mathrm{Lie}(G^{\mathrm{an}}) \xrightarrow{\exp_G} G^{\mathrm{an}}$$

where the first map is $1 \mapsto u$. We have $u \in \mathfrak{b}_\mathbb{C}$, hence $\mathbb{C}u \subset \mathfrak{b}_\mathbb{C}$ and $\Phi(\mathbb{C}) \subset B$. □

The image $\Phi(\mathbb{C})$ is a 1-*parameter subgroup*. It is a Riemann surface with the additional structure of an abelian group. Its Lie algebra has dimension one and the tangent vector is contained in $\mathfrak{b}$.

Exercise 5.6. *Show that $\Phi(\mathbb{C})$ is isomorphic to one of: $\mathbb{C}$, $\mathbb{C}^*$, $\mathbb{C}/\mathbb{Z} + \tau\mathbb{Z}$ for $\tau \in \mathbb{C} \smallsetminus \mathbb{R}$.*

Proposition 5.9. *Let $P_0 \in k[U_0]$ be an algebraic function that vanishes to order at least T in the points $0, g, 2g, \dots, Sg$. Then $\Phi^*(P_0)$ is holomorphic in $0, 1, \dots, S$ and vanishes to order at least T in these points.*

Proof. By definition $\Phi^*(P_0) = P_0 \circ \Phi$ is holomorphic and defined on the preimage of U_0 under Φ. We always have $0, g, \dots, Sg \in U_0$ and hence $0, 1, \dots, S$ in the preimage.

We have to compute the derivatives of $\Phi^*(P_0)$. This is nothing but the directional derivative of P_0 in the direction given by the one-parameter group. Let $L_1, \dots, L_d$ be a basis of $\mathfrak{b}$. We have

$$\frac{\partial}{\partial z} = \sum_{i=1}^{d} a_i L_i, \quad a_i \in \mathbb{C}$$

and by the chain rule

$$\frac{\partial}{\partial z} P \circ \Phi = \sum_{i=1}^{d} a_i L_i P.$$

This is evaluated in $\Phi(s) = sg$ for $0 \leq s \leq S$. Hence the assumption on the vanishing of the $L_1^{t_1} \dots L_d^{t_d} P_0(sg)$ for $\sum t_i \leq T$ translates into the vanishing of the derivatives of the $\Phi^*(P_0)$. □

Exercise 5.7. *For $G = V \times T$ and $\overline{G} = \mathbb{P}^N$, show that $\Phi^*(P)$ is defined on all of $\mathbb{C}$.*

The proof of the analytic subgroup theorem is done via estimates for $\Phi^*(P)$ for suitable polynomials P.

Some complex analysis

Consider holomorphic functions on a disc $B_R(0)$. For $0 < r < R$ we define for all holomorphic functions on $B_R(0)$

$$\|f\|_r = \sup_{|z|=r} |f(z)|.$$

By the *maximum principle* we have $|f(z)| \leq \|f\|_r$ for all z with $|z| \leq r$. In particular

$$\|f\|_{r'} \leq \|f\|_r$$

for $0 < r' < r$.

Lemma 5.10. *Let $0 \leq s \leq r' \leq r$. Then for $|z| = r$*

$$\left| \frac{r^2 - sz}{r(z - s)} \right| = 1$$

and for $|z| = r'$

$$\frac{r^2 + r'^2}{2rr'} \leq \left| \frac{r^2 - sz}{r(z - s)} \right|$$

Proof. We want to check

$$\begin{aligned} |r^2 - sz| = |r(z-s)| &\Leftrightarrow (r^2 - sz)(r^2 - s\overline{z}) = r^2(z-s)(\overline{z}-s) \\ &\Leftrightarrow r^4 - r^2 s(z+\overline{z}) + s^2 z\overline{z} = r^2(z\overline{z} - s(z+\overline{z}) + s^2) \end{aligned}$$

The last equation holds with $z\overline{z} = r^2$.

We turn to the second claim. By squaring both sides, using $z\overline{z} = |z|^2 = r'^2$ and multiplying with the denominators we obtain the equivalent inequality

$$(r^2 + r'^2)^2 r^2 (z-s)(\overline{z}-s) \leq 4r^2 r'^2 (r^2 - sz)(r^2 - s\overline{z})$$

or, after dividing by r^2,

$$(r^4 + 2r^2 r'^2 + r'^4)(r'^2 - s(z+\overline{z}) + s^2) \leq 4r'^2(r^4 - r^2 s(z+\overline{z}) + s^2 r'^2).$$

Expand the products:

$$\begin{aligned} r^4 r'^2 - r^4 s(z+\overline{z}) + r^4 s^2 + 2r^2 r'^4 - 2r^2 r'^2 s(z+\overline{z}) + 2r^2 r'^2 s^2 \\ + r'^6 - r'^4 s(z+\overline{z}) + r'^4 s^2 \\ \leq\ 4r^4 r'^2 - 4r^2 r'^2 s(z+\overline{z}) + 4r'^4 s^2. \end{aligned}$$

For the multiples of $s(z+\overline{z})$, we obtain for the difference of right hand side and left hand side

$$r^4 + r'^4 - 2r^2 r'^2 = (r^2 - r'^2)^2 \geq 0$$

and for the same difference for the other terms

$$s^2(3r'^4 - r^4 - 2r^2 r'^2) + r'^2(3r^4 - r'^4 - 2r^2 r'^2).$$

If $3r'^4 - r^4 - 2r^2 r'^2 \leq 0$, we can calculate

$$\begin{aligned} & s^2(3r'^4 - r^4 - 2r^2 r'^2) + r'^2(3r^4 - r'^4 - 2r^2 r'^2) \\ \geq\ & r'^2(3r'^4 - r^4 - 2r^2 r'^2) + r'^2(3r^4 - r'^4 - 2r^2 r'^2) \\ =\ & r'^2(3r'^4 - r^4 - 2r^2 r'^2 + 3r^4 - r'^4 - 2r^2 r'^2) \\ =\ & 2r'^2(r^4 + r'^4 - 2r^2 r'^2) \\ \geq\ & 0. \end{aligned}$$

Otherwise, we already have $s^2(3r'^4 - r^4 - 2r^2 r'^2) \geq 0$ and because of $r \geq r'$ trivially $3r^4 - r'^4 - 2r^2 r'^2 \geq 0$.

□

Proposition 5.11 (Variant of the Schwarz Lemma)**.** *Let f be holomorphic function on a disc $B_R(0)$ for $R > 0$. Assume that f has zeroes of order at least T in the points $0, 1, \ldots, S$. Let $S \leq r' \leq r$. Then*

$$\log \|f\|_{r'} \leq \log \|f\|_r + (S+1)T \log\left(\frac{2rr'}{r^2 + r'^2}\right).$$

Proof. We use the auxiliary function

$$g(z) = \prod_{s=0}^{S} \left(\frac{r^2 - sz}{r(z-s)} \right)^T .$$

By the lemma $\|g\|_r = 1$.

The product fg is holomorphic on $B_R(0)$. As remarked before, we have

$$\|fg\|_{r'} \leq \|fg\|_r \leq \|f\|_r \|g\|_r = \|f\|_r .$$

By the lemma, we also get the estimate

$$\left(\frac{r^2 + r'^2}{2rr'} \right)^{(S+1)T} \|f\|_{r'} \leq \|fg\|_{r'} .$$

Together this gives

$$\|f\|_{r'} \leq \|f\|_r \left(\frac{2rr'}{r^2 + r'^2} \right)^{(S+1)T}$$

□

Exercise 5.8. *Formulate the Schwarz Lemma and go through the proof.*

Remark 5.12. We are going to apply the estimate the function $\Phi^*(P_0)$ for $P_0 \in k[U_0]$ and the one parameter group Φ studied before.

In the non-affine case, a suitable modification of the definition will be used in order to get a holomorphic function on all of $\mathbb{C}$, not only $\Phi^{-1}(U_0)$.

Chapter 6

Weil heights

Reference: Silverman, The classical theory of heights, in: Cornell-Silverman, Arithemtic geometry, Springer Verlag.

Our aim is find a good polynomial $P \in \overline{\mathbb{Q}}[X_0, \dots, X_N]$ feeding into our estimates. We will find it as the solution of the system of linear equations given by the vanishing conditions. We also want this polynomial to have "small" coefficients. This is measured via heights.

We start with the case of rational numbers.

Lemma 6.1 (Siegel's lemma)**.** *Let M, N be integers with $N > M > 0$. For $1 \leq j \leq N$ and $1 \leq i \leq M$ let a_{ij} be an integer of absolute value at most A_i. Then there are integers $x_1, \dots, x_N$, not all zero with absolute value at most*

$$X = \prod_{i=1}^{M} (NA_i)^{\frac{1}{N-M}},$$

and such that

$$\sum_{j=1}^{N} a_{ij} x_j = 0, \quad 1 \leq i \leq M.$$

Note that the system of linear equations has solutions in $\mathbb{Q}$ because there are more variables than equations. By multiplying by a suitable denominator we can make the solution integral. The point of the lemma is about limiting the size of the solutions.

We follow Baker-Wüstholz Chapter 1.4.

Proof. Let $-V_i, W_i$ be the sums (wrt j) of the negative and positive a_{ij}, respectively. Note that

$$V_i + W_i \leq NA_i.$$

Let $B = [X]$. There are $(B+1)^N$ tuples $(x_1, \dots, x_N)$ of integers with $0 \leq x_i \leq B$. Let

$$y_i(x) = \sum_{j=1}^{N} a_{ij} x_j.$$

Then

$$-V_iB \leq y_i(x) \leq W_iB.$$

Hence there are at most

$$\prod_{i=1}^{M}(NA_iB+1)$$

possible tuples $y(x)$. By definition of B, we have

$$(B+1)^{(N-M)} > \prod_{i=1}^{M}(NA_i)$$

and because $A_i \geq 1$ this implies

$$(B+1)^N > \prod_{i=1}^{M}(NA_i).$$

Hence there are two tuples x which give rise to the same $y(x)$. Their difference is the required solution. □

We want to generalise this to coefficients in algebraic integers. The absolute value is replaced by the *Weil height*. We recall some facts from algebraic number theory.

Let $\mathbb{K}/\mathbb{Q}$ be finite, $m = [\mathbb{K} : \mathbb{Q}]$. A *place* of $\mathbb{K}$ is the equivalence class of non-trivial absolute values on $\mathbb{K}$. Here two absolute values are equivalent if they induce the same topology on $\mathbb{K}$. This happens precisely if

$$|\cdot|_1 = |\cdot|_2^\lambda$$

for some $\lambda > 0$. Places are classified: there is one non-archimedian one for every prime ideal of the ring of integers $\mathcal{O}_\mathbb{K}$ (i.e., the integral closure of $\mathbb{Z}$ in $\mathbb{K}$) and one archimedian one for every conjugacy class of embeddings $\mathbb{K} \to \mathbb{C}$.

Exercise 6.1. *(talk) Report on the proof of Ostrowski's theorem classifying the places of* $\mathbb{Q}$*.*

For every place v, there is a completion $\mathbb{K}_v$. It is a finite extension of $\mathbb{Q}_v$. The possible values for $\mathbb{Q}_v$ are $\mathbb{Q}_p$ (for a prime number p) and $\mathbb{R}$. We write $v|p$ and $v|\infty$, respectively. We normalise the absolute values by the condition

$$\|p\|_v = p^{-[\mathbb{K}_v:\mathbb{Q}_p]} \quad v|p$$
$$\|x\|_v = |x|^{[\mathbb{K}_v:\mathbb{R}]} \quad v|\infty$$

With this normalisation, we have

$$\prod_v \|x\|_v = 1$$

for all $x \in \mathbb{K}^*$. Moreover:

Exercise 6.2. *Verify the product formula for $\mathbb{K} = \mathbb{Q}$.*

Comment: In the case $v = \infty, \mathbb{K}_v = \mathbb{C}$, the function $\|\cdot\|_v = |\cdot|^2$ is not actually an absolute value—the triangle inequality fails. This will be an issue when applying a polynomial with bounded height to a point of bounded height. It would be better to use its m-th root through-out and formulate all bounds for the absolute rather than the relative height. We stick with the notation used in the literature.

Exercise 6.3. *Consider $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ and $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$. Work out the infinite/finite places and the $\mathbb{K}_v$. For information: $\mathcal{O}_{\mathbb{Q}(\sqrt{3})} = \mathbb{Z}[\sqrt{3}]$ and $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.*

Definition 6.2. Let $\mathbb{K}/\mathbb{Q}$ be finite. For $x = [x_0 : \cdots : x_N] \in \mathbb{P}^N(\mathbb{K})$ we put

$$H_{\mathbb{K}}(x) = \prod_v \max_i \|x_i\|_v .$$

The function H is called *Weil height.* The function

$$h(x) = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \log H_{\mathbb{K}}(x)$$

is called *absolute logarithmic Weil height.*

Note that the height is well-defined by the product formula.

Remark 6.3. The above definition of $H_{\mathbb{K}}$ is not compatible with inclusions of number fields, but the absolute logarithmic height is.

Exercise 6.4. *Let $\mathbb{K} = \mathbb{Q}$. Show that the Weil height on $\mathbb{P}^1$ is given by the following formula: Let $x = [x_0 : x_1]$ with coprime integers x_0, x_1. Then*

$$H(x) = \max\{|x_0|, |x_1|\}.$$

In particular, heights are bounded below!

Lemma 6.4. *Let $x \in \mathbb{P}^1(\mathbb{K})$. Then*

$$H_{\mathbb{K}}(x) \geq 1, \quad h(x) \geq 0.$$

Proof. We write $x = [1 : \alpha]$ or $[\alpha : 1]$ with $\alpha \in \mathbb{K}$. Hence

$$H_{\mathbb{K}}(x) = \prod_w \max\{\|\alpha\|_w , 1\}$$

Each factor in this product is at least 1, hence so is the product. □

Lemma 6.5 (Liouville inequality)**.** *Let v_0 be a place of $\mathbb{K}$, $\alpha \neq 0$. Then*

$$\|\alpha\|_{v_0} \geq \frac{1}{H_{\mathbb{K}}([1 : \alpha])}, \quad \log(\|\alpha\|_{v_0}) \geq -[\mathbb{K} : \mathbb{Q}]\, h([1 : \alpha]).$$

Proof. If $\|\alpha\|_{v_0} \geq 1$, then the claim follows from the previous lemma. Assume $\|\alpha\|_{v_0} < 1$. Then

$$H_{\mathbb{K}}([1:\alpha]) = \prod_{v\neq v_0} \max\{\|\alpha\|_v, 1\} \geq \prod_{v\neq v_0} \|\alpha\|_v = \frac{1}{\|\alpha\|_{v_0}} \prod_v \|\alpha\|_v = \frac{1}{\|\alpha\|_{v_0}}$$

Again this is the claim. □

The Weil height can be restricted to any subvariety V of $\mathbb{P}^n$ defined over $\mathbb{K}$. It depends on the embedding.

The usual applications in arithmetic geometry use the following observation:

Proposition 6.6. *Let $\mathbb{K}$ be a number field. Then for every C the set*

$$S_C = \{x \in \mathbb{P}^n(\mathbb{K}) | H(x) < C\}$$

is finite.

We omit the proof because we will not need this fact.

Remark 6.7. We can then ask for asymptotics for the size of S_C for subvarieties. The proof of the famous Mordell conjecture (a curve of genus at least 2 over a number field has only finitely many points with coordinates in $\mathbb{K}$) starts by considering points of bounded height. This set is finite.

Exercise 6.5. *(talk) Report on the use of heights in the proof of the Theorem of Mordell-Weil ($A(\mathbb{K})$ is a finitely generated abelian group for all abelian varieties A), e.g., in the chapter by Silverman mentioned before. For the case of elliptic curves, see also Silverman: Arithmetic of elliptic curves.*

We are going to apply the Weil height to our $G \subset \mathbb{P}^N$ and the points $0, g, 2g, \ldots$.

Lemma 6.8 (Height estimate)**.** *Let G be a commutative algebraic group over $\mathbb{K}$. Then there are are constants C_1, C_2, C_3, κ such that for all $g \in G(\mathbb{K})$ and $s \in \mathbb{N}$ we*

$$h(sg) \leq C_1 s^2(h(g)+1) + C_2, \quad h(g) \leq C_3 s^\kappa (h(sg)+1)$$

In the case $G = V \times T$, we have

$$h(sg) \leq s(h(g)+1).$$

Proof. We only treat the case $G = V \times T$. We start with $\mathbb{G}_a$. The group law is addition on $\mathbb{G}_a \subset \mathbb{P}^1$, $g = [1:a]$ with $a \in \mathbb{K}$, $sg = [1:sa]$. By definition

$$H_{\mathbb{K}}(sg) = \prod_v \max\{1, \|sa\|_v\} = \prod_v \max\{1, \|s\|_v \|a\|_v\}$$

For non-archemedian v, we have $\|s\|_v \leq 1$. The factors $\|s\|_v$ for the archimedian places multiply to $|s|^m$ (where $m = [\mathbb{K} : \mathbb{Q}]$) and we get the estimate

$$H_{\mathbb{K}}(sg) \leq s^m H_{\mathbb{K}}(g).$$

For the logarithmic height this gives

$$h(sg) \leq \log(s) + h(g) \leq s(h(g) + 1).$$

We can use $C_1 = 1$ and $C_2 = 0$.

Now consider $G = \mathbb{G}_m$. The group law is multiplication, $g = [1 : a]$, $sg = [1 : a^s]$. By definition

$$H_{\mathbb{K}}(sg) = \prod_v \max\{1, \|a^s\|_v\} = \prod_v \max\{1, \|a\|_v^s\} = \prod_v \max\{1, \|a\|\}^s$$

and hence

$$h(sg) = sh(g) \leq s^2 h(g).$$

Again $C_1 = 1$ and $C_2 = 0$ do the job.

For a product of $\mathbb{G}_a$'s and $\mathbb{G}_m$'s, we do the same estimats component wise for $g = [1 : a_1, \ldots, a_{r+s}]$.

We leave the second estimate as an excercise. □

Comment: We are going to use the estimate in the form

$$h(sg) \leq Cs^2 + C', \quad \text{for all } s \in \mathbb{N}_0$$

below. This is Prop. 5 in Serre: Quelques Quelques propriétés des groupes algébriques commutatifs Astérisque, tome 69–70 (1979), p. 191–202 for general G. The second height estimate in the above form is Proposition 2.0 in Wüstholz: Algebraische Punkte auf analytischen Untergruppen algebraischer Gruppen, Source: Annals of Mathematics , May, 1989, Second Series, Vol. 129, No. 3 pp. 501–517

Exercise 6.6. *Show the estimate for $h(g)$ in terms of $h(sg)$ for $G = \mathbb{G}_m$ and $G = \mathbb{G}_a$, maybe $\mathbb{K} = \mathbb{Q}$. Determine κ.*

Solving equations

Definition 6.9. Given a linear form

$$L = a_1 X_1 + \cdots + a_n X_n$$

with coefficients in $\mathbb{K}$, we put

$$h(L) = h([a_1 : \cdots : a_n]).$$

Proposition 6.10 (Siegel's lemma)**.** *Let $\mathbb{K}$ be a number field with $m = [\mathbb{K} : \mathbb{Q}]$. Suppose $N > mM$ and let*

$$L_i = \sum_{j=1}^{N} a_{ij} X_j$$

for $i = 1, \dots, M$ be linear forms with coefficients in $\mathbb{K}$. There exist $x_1, \dots, x_N \in \mathbb{Z}$ not all zero such that

$$L_i(x) = 0, \quad i = 1, \dots M$$

and

$$h(x) \leq \frac{mM}{N - mM} \left(\log(N) + \max h(L_i)\right).$$

Proof. Similar to the case $\mathbb{K} = \mathbb{Q}$. See Hindry, Silverman: Diophantine Geometry, p. 319. They make a statement about the absolute value of the integers. If we choose the solution with coprime entries, then this is the height. □

Considerations on polynomials

Application to our case

Let G be a commutative algebraic group of dimension n over $\mathbb{K}$, $g \in G(\mathbb{K})$. Let $L_1, \dots, L_d$ be linearly independent invariant vector fields.

We want to find a non-trivial homogeneous polynomial $P \in \mathbb{K}[X_0, \dots, X_N]$ of degree D vanishing in a point $[b_0 : \dots : b_N] \in \mathbb{P}^N(\mathbb{K})$. We treat the coefficients of P as variables

$$P = \sum_{|I|=D} a_I X^I.$$

The vanishing $P(b) = 0$ gives the condition

$$\sum_{|I|=D} a_I b^I = 0.$$

The tuple $\{b^I\}_{|I|=D}$ can itself be understood as a well-defined point of a projective space and hence has a height.

Lemma 6.11.

$$h([b^I]) = Dh(b).$$

Proof. We do the simpler case $b \in \mathbb{P}^N(\mathbb{Q})$. We may choose the b_i integral and coprime and have

$$H(b) = \max_i \{|b_i| | i = 0, \dots, N\}.$$

By definition

$$H([b^I]) = \prod_v \max_I \{|b^I|_v\}.$$

Let $v = p$ be a prime. Then there is b_i with $|b_i|_p = 1$. The maximum is attained in b_i^D and is 1. The finite primes do not contribute to the height.

Let $v = \infty$. There is b_i such that $H(b) = |b_i|$, i.e., the index where the maximum is attained. We have

$$|b^I| \leq |b_i|^D = H(b)^D.$$

This is the claim in the special case.

For the general case, wlog of generality $b_0 = 1$. It suffices to show

$$\max\{\left\|b^I\right\|_v\} = \max\{\|b_i\|\}^D$$

for every place v. We have $\|b_0\|_v = 1$, hence the maximum on the right is at least 1 and attained in b_i. Then the maximum on the left is attained in b_i^D. □

We also want to impose vanishing to higher order, so we have to understand what happens when we apply differential operators.

Let $L \in \mathrm{Lie}(G)$. We interpret LP as the homogenisation of LP_0. It has the same degree as P.

Example 6.12. If $G = \mathbb{G}_m$ with $S[\overline{G}] = k[X_0, X_1]$ and $L = Y\partial/\partial Y$, then $LP = X_1\partial/\partial X_1$. If $G = \mathbb{G}_a$ and $L = \partial/\partial Y$, then $LP = X_0\partial/\partial X_1$.

Let ∂ be one of the standard basis vectors for the Lie algebra of $G = \mathbb{G}_a^s \times \mathbb{G}_m^r$ and L the corresponding differential operator, say for the coordinate α. We interpret

$$LP(b) = 0$$

as a linear equation for the coefficients. It reads either

$$\sum_I a_I i_\alpha b_0^{i_0+1} b_1^{i_1} \dots b_j^{i_j-1} \dots b_n b^{i_n} = 0$$

or

$$\sum_I a_I i_\alpha b^I = 0.$$

We abbreviate I' for the new exponent vector. Note that i_j is an integer less or equal than D. The same argument as in the lemma gives a bound of

$$\log(D) + Dh(b)$$

for the height of the linear equation.

The next step is to consider linear combinations

$$L = \sum_{j=1}^{n} c_j \partial_j$$

where ∂_j is the standard basis vector corresponding to the coordinate j and $c_j \in \mathbb{K}$. Then the equation defined by $LP(b) = 0$ takes the shape

$$\sum_I a_I \left(\sum_j c_j i_j b^{I(j)} \right) = 0$$

where $I(j)$ is is obtained from I as determined by the operator ∂_j. The height of the coefficient vector does not change when we scale the c_j, so we may assume without loss of generality $c_j \in \mathcal{O}_K$. Again $c_j i_j b^{I'}$ is integral and the same argument as in the proof of the lemma gives a bound of

$$C + \log(D) + Dh(b)$$

where we choose

$$C \geq \log(n \left\|c_j\right\|_v).$$

for all j and $v|\infty$.

The final step is to interate the procedure up to T times.

Lemma 6.13. *Let $L_1, \ldots, L_d$ be our basis of $V \subset \mathrm{Lie}(G)$. There is a constant C (depending on the L_i, G) such that the linear equation for the coefficients of P*

$$L_1^{t_1} \ldots L_d^{t_d} P(b) = 0$$

with $\sum_i t_i \leq T$ has height bounded by

$$TC + T\log(D) + Dh(b).$$

Remark 6.14. In Wüstholz's paper the bound in the general case is given in the form

$$c'(D+T)\log(D+T) + c''Dh(b).$$

It follows from ours.

Proof. We only handle the case $G = \mathbb{G}_a^s \times \mathbb{G}_m^r$.

Let $\partial_1, \ldots, \partial_n$ be the standard base of $\mathrm{Lie}(G)$. We write

$$L_i = \sum_{j=1}^n c_{ij} \partial_i$$

with fixed $c_{ij} \in \mathbb{K}$. Without loss of generality even $c_{ij} \in \mathcal{O}_{\mathbb{K}}$. Choose C such that

$$C \geq \log(n \left\|c_{ij}\right\|_v) \quad \text{for all } i, j \text{ and } v|\infty.$$

Writing out the equation we find factors coming from the derivatives. They are bounded by D and occur at most T times. We find products of c_{ij}, again at most T times. They are bounded by $\exp(C)^T$. The rest of the argument is as in proof of the lemma. □

Proposition 6.15. *Let $T, S \in \mathbb{N}$, D such that*

$$D^n \geq 2mn! T^d S'$$

where S' is the number of elements of $\{0, g, \dots, Sg\}$. For T big enough, there is a homogeneous polynomial $P \in \mathbb{Z}[X_0, \dots, X_N]$ of degree D which does not vanish on G and such that

(i)

$$L_1^{t_1} L_2^{t_2} \dots L_d^{t_d} P(sg) = 0$$

for $\sum t_i \leq T$ and $s = 0, \dots, S$

(ii) and the height of the coefficient vector of P is bounded by

$$c_1(D+T)\log(D+T) + c_2 D S^2$$

for constants depending on the data, but not on S, T, D.

Proof. We restrict to $G = \mathbb{G}_a^s \times \mathbb{G}_m^r$. Recall that $\overline{G} = \mathbb{P}^n$. We have $n = N$. The space of homogeneous polynomials of degree D has dimension N_D

$$2D^n \geq N_D = \binom{D+n}{n} \geq \frac{D^n}{n!}$$

(the first inequality for $D \geq 2$, okay for T big enough). We treat the coefficients of P as unknowns

$$P_0 = \sum_{|I|=D} a_I X^I.$$

Each of the vanishing conditions amounts to a linear equation with coefficients in $\mathbb{K}$. Let M be the number of conditions. There are $(S+1)$ choices for s and at most T choices for each of the d numbers t_i. Hence there are at most

$$M \leq S' T^d$$

many equations. For D satisfying the bound in the proposition, we have

$$N_D \geq 2mM$$

and the system has a non-trivial solution. We now want to apply Siegel's lemma to get a bound on the coefficients. For this we have to bound the heights of the linear equations.

We have fixed g and view $h(g)$ as a constant. By the height estimate, we already have

$$h(sg) \leq c_1 S^2 + c_2.$$

The height of the linear equations was determined in the last lemma. We get a bound of

$$TC + T\log(D) + Dc_1 S^2 + DC_2$$

for each of the heights of an equation. By Siegel's lemma we get a solution (i.e, the coefficients of our polynomial) with height bounded by

$$\frac{mM}{N_D - mM}\left(\log(N_D) + TC + T\log(D) + Dc_1S^2 + DC_2\right)$$

We have $N_D \geq 2mM$ and hence $N_D - mM \geq mM$. The fraction is less or equal than 1. Using the estimate for N_D from above, we get

$$(n+T)\log(D) + Dc_1S^2 + DC_2.$$

□

A simpler argument estimates the heights of the derivates of P.

Lemma 6.16. *Let $P \in S[\overline{G}]_D$. Let $\Delta = L_1^{t_1}\dots L_d^{t_d}$. Then*

$$h(\Delta P) \leq c(D+T)\log(D+T) + h(P)$$

for a constant c independent of P, D, Δ. More precisely: let $\Delta P = \sum q_I X^I$. For non-archimedean v, we have

$$\max\{|q_I|_v\} \leq \max\{|a_I|_v\}.$$

For archimedean v, we have

$$\max\{|q_I|_v\} \leq (nCD)^T \max\{|a_I|_v\}.$$

where C is the constant used in Lemma 6.13

Proof. Let $P = \sum_i a_I X^I$ as before. From taking the derivatives we get integral factors and c_{ij}'s as before. We have to estimate their norms for all v. As the factors are integral, they are bounded by $|a_I|_v$ for the finite places. At the infinite places we get as before T-th powers of D and a bound for the c_{ij}. After taking log this is less than the above. □

Chapter 7

Proof

We fix the same setting as before: G a commutative algebraic group over $\overline{\mathbb{Q}}$, $\mathfrak{b} \subset \mathrm{Lie}(G)$ a semi-simple subvector space, $B = \exp_G(\mathfrak{b}_{\mathbb{C}})$, $g \in B \cap G(\overline{\mathbb{Q}})$. We want to show that $g = 0$, so we work under the assumption $g \neq 0$. We have fixed a basis $L_1, \dots, L_d$ of $\mathfrak{b}$ and an embedding $G \to \mathbb{P}^N$ such that $\mathbb{Z}g \subset U_0$. Let $\mathbb{K}$ be a number field such that G, g and $\mathfrak{b}$ are defined over $\mathbb{K}$. Let $\ell \geq 1$ be a big natural number.

Overview

We first explain how the argument works. We then need to fill in details on appropriate choices of ℓ, S, T, D and check some more estimates.

Let $P \in S[\overline{G}]_D$ be the non-vanishing algebraic function constructed in Proposition 6.15. It vanishes to order at least T in the points $0, \dots, Sg$. Moreover, we have bound on the height of all ΔP where Δ runs through the monomial differential operators of degree at most T.

The one-parameter subgroup through g contains an element γ such that $\ell\gamma = g$ (take $\exp(\frac{1}{\ell}u)$ for $\exp(u) = g$). It is an element of $B \cap G(\overline{\mathbb{Q}})$. Let $\mathbb{L}$ be a finite extension of $\mathbb{K}$ such that $\gamma \in G(\mathbb{L})$.

Claim: P vanishes to order $T/2$ in the $\ell S + 1$ points $0, \gamma, \dots, \ell S\gamma = Sg$.

Admitting this claim, we apply Theorem 5.7. If

$$\ell S(T/2)^d > cD^n$$

(with the constant there), then γ is a torsion point of order less than $\ell S + 1$. The inequality can be arranged. If g was not a torsion point, this finishes the argument. If it is, we have to argue more carefully with the torsion order.

In order to prove the claim, we have to show that

$$\delta := \Delta P(s\gamma) = 0$$

for all monomial differential operators of degree at most $T/2$ and $s = 0, \dots, \ell S$. Assume that it is not. We will make estimates from above and below that lead to a contradiction.

The upper bound uses the variant of the Schwarz lemma, Proposition 5.11. The lower bound follows from height estimates.

Choices of parameters

Definition 7.1. Let $S \geq 1$, big. Let S' be the order of the set $\{0, g, \dots, Sg\}$, so $S' \leq S$. We have $S' \geq 1$.

$$\begin{aligned} D &:= 2mn!S'S^{4d} \\ T &:= 2mn!S'^{(n-1)/d}S^{4n} \end{aligned}$$

If g is torsion, we ask S bigger than the order of g.

Lemma 7.2. *(i) The assumption of Proposition 6.15 (construction of P) is satisfied:*

$$D^n \geq 2mn!T^dS'.$$

(ii) $DS^2 \leq T$, $D + T \leq 2T$.

(iii) Let c be the constant in the multiplicity estimate, Theorem 5.7. The assumption for the multiplicity estimate is satisfied for ℓ big enough:

$$B(T/2)^d > cD^n$$

where $B = \ell S'$ is the number of elements of $\{0, \gamma, \dots, \ell S\gamma\}$.

Proof. The left-hand side is

$$D^n = (2mn!)^n S'^n S^{4dn} \geq (2mn!)S'T^d = (2mn!)^{d+1}S'^n S^{4nd}.$$

The second claim holds because

$$DS^2 = 2mn!S'S^{4d+2} \leq T = 2mn!S'^{(n-1)/d}S^{4n}$$

as $(n-1)/d \geq 1$, $4d + 2 \leq 4(n-1) + 2 \leq 4n$. Moreover, $D \leq T$.

Up to constants, the third claim is

$$BT^d = BS'^{n-1}S^{4nd} \geq D^n = S'^n S^{4dn},$$

or equivalently,

$$B > c'S'.$$

If g is not torsion, we have $B = \ell S + 1$, $S' = S + 1$. If g is torsion, then S' is its torsion order and $B = \ell S'$. In both cases the equality holds for ℓ big enough. □

Corollary 7.3. *Let P be as in Proposition 6.15, Δ a monomial differential operator in direction $\mathfrak{b}$ of order at most T. Then the height of ΔP is bounded by*

$$cT\log(T)$$

for a new constant c.

Proof. The height estimate for $h(P)$

$$c_1(D+T)\log(D+T)+c_2DS^2$$

is combined with the estimate of Lemma 6.16 for the derivatives

$$c(D+T)\log(D+T)+h(P).$$

We then simplify using the estimate for DS^2 and $D+T$. □

At this point we have to be more careful with the choice P. By the proof of Proposition 6.15 it can be chosen with integral coefficients. We specify that we want to have it in primitive form, i.e., the coefficients are coprime. In particular

$$H(P)=\max_I |a_I|.$$

This turns the height bound of Proposition 6.15 into a bound on the coefficients.

Corollary 7.4. *The coefficients of ΔP are bounded by*

$$cT\log T$$

for a constant c.

Proof. Go through the proof of Lemma 6.16 to deduce the bound for the derivatives from the bound for the coefficients of P. □

Estimates from above

Recall the one-parameter curve $\Phi:\mathbb{C}\to G^{\mathrm{an}}$. The polynomical ΔP gives rise to a holomorphic function

$$\psi:\mathbb{C}\to G^{\mathrm{an}}\to\mathbb{C}.$$

We want to estimate

$$\|\psi\|_r=\sup_{|z|\leq r}|\psi(z)|=\sup_{|z|=r}|\psi(z)|.$$

Lemma 7.5. *Assume that Δ is a differential operator of order at most $T/2$. There is a constant C such that*

$$\log\|\psi\|_r\leq C(T\log(T)+Dr).$$

Proof. We identify $\mathrm{Lie}G^{\mathrm{an}} \cong \mathbb{C}^n$ via our preferred coordinates. The image of $B_r(0)$ under $\mathbb{C} \to \mathrm{Lie}G^{\mathrm{an}}$ is contained in the ball $B_{\|u\|r}(0)$ where u is our preimage of g. It remains to bound

$$\log \Delta P(1, \exp_1(z_1), \ldots, \exp_n(z_n))$$

where $\exp_i$ is the exponential function for the i-th factor. It is bounded by $\exp \|z\|$. The polynomical ΔP has degree D, so less than D^{n+1} monomials (this was established in the proof of Proposition 6.15). Each of them has absolute value at most $e^{D\|u\|r}$. The coefficients are bounded by $cT\log(T)$. Together this gives

$$|\Delta P(1, \exp_1(z_1), \ldots, \exp_n(z_1))| \leq D^{n+1} cT \log(T) e^{D\|u\|r}$$

and after taking logarithms and changing constants (and because $D+T$ is of the same order as T)

$$\log \|\psi\|_r \leq c' \log(D+T)(D+r).$$

As $D+T$ is of the same order as T, this is the claim. □

Remark 7.6. In the non-affine case, the bound is with r^2 instead of r.

Corollary 7.7. *There is a constant such that for big enough S*

$$\log \|\psi\|_S \leq -CST\log(S).$$

In particular,

$$\log |\psi(s\gamma)| \leq -CST\log(S)$$

for all $0 \leq s \leq \ell S$.

Proof. Our function ψ has a zero of order at least $T/2$ in the points $0, \ldots, S$. We apply the variant of the Schwarz lemma (Proposition 5.11) with $r' = S$ and $r = S^2$ and obtain

$$\begin{aligned}\log \|\psi\|_S &\leq \log \|\psi\|_{S^2} + \frac{(S+1)T}{2} \log\left(\frac{2S^3}{S^4+S^2}\right)\\ &\leq CT\log(T) + DS^2 + \frac{(S+1)T}{2}\log\left(\frac{2S}{S^2+1}\right).\end{aligned}$$

The summand DS^2 is eaten by the first summand. We then have a term of order

$$T\log(T) \leq T(c_1 + c_2 \log(S))$$

and a second of order

$$ST\log(S)$$

with a negative sign. For a big enough S the second summand dominates. □

Estimate from below

We need to bound $h(s\gamma)$. Note that γ is not necessarily defined over $\mathbb{K}$, but it is defined over a finite extension $\mathbb{L}$ with degree $[\mathbb{L} : \mathbb{K}] \leq \ell^{2n}$ (actually ℓ^n is enough in the linear case because at most we are extracting an ℓth root in each component).

Lemma 7.8. *For $0 \leq s \leq \ell S'$ we have*

$$h(s\gamma) \leq c(S^2 + \ell^{c'}).$$

Proof. We decompose

$$s\gamma = s'g + s''\gamma$$

with $0 \leq s' \leq S$ and $0 \leq s'' < \ell$. In the linear case, there is a n estimate of the form

$$h(s\gamma) \leq h(s'g) + h(s''\gamma) + [\mathbb{L} : \mathbb{Q}] \log(2).$$

By the second height estimates, we have

$$h(\gamma) \leq C_3 \ell^{\kappa}$$

(treating $h(g)$ as a constant). By the first height estimate we also have

$$\begin{aligned} h(s'g) &\leq C_1 S^2(h(g) + 1) + C_2 = C_1' S^2 + C_2, \\ h(s''\gamma) &\leq C_1 \ell^2 (C_3 \ell^{\kappa} + 1) + C_2. \end{aligned}$$

Together this gives

$$h(s\gamma) \leq C_1' S^2 + C_1 \ell^2 + C_1'' \ell^{\kappa+2} + \ell^{2n} C$$

Choosing $c' \geq 2 + \kappa, 2n$ and adjusting contants this gives the claim. □

Exercise 7.1. *Show the estimate for the group law for $G = \mathbb{G}_a$ and $G = \mathbb{G}_m$.*

Lemma 7.9. *For $x = [1 : x_1 : \cdots : x_n] \in \mathbb{P}^n(\mathbb{L})$ we have*

$$h([1 : \Delta P_0(x)]) \leq CT \log(T) + Dh(x)$$

Proof. Let

$$\Delta P = Q = \sum q_I X^I.$$

There are $\binom{D+n}{n} \leq (D+1)^n$ many monomials. We estimate each $|Q(x)|_v$.

For each monomial we have

$$\max_I |q_I x^I|_v \leq \max_I |q_I| \max_{i=0,\dots,N} |x_i|_v^D$$

(if all $|x_i|_v$ for $i = 1, \dots, N$ are less than 1, then the maximum of all $|x_I|$ is also at most 1. If one is bigger than 1, than the maximum is less than the maximal $|x_i|_v$ to the maximal power, D.)

For non-archimedean v, this implies

$$\max_I |q_I x^I|_v \leq \max |x_i|_v{}^D.$$

(use Lemma 6.16 and $a_I \in \mathbb{Z}$). By the ultra-metric inequality even

$$|Q(x)|_v \leq (\max |x_i|_v)^D.$$

Note that the right hand side is bigger or equal to 1 because $x_0 = 1$.

In the archimedean case, the triangle inequality with Lemma 6.16 gives

$$\begin{aligned}|Q(x)|_v &\leq \binom{D+n}{n} \max_I |q_I|_v \max |x_i|_v^D \\ &\leq (D+1)^n \left((nCD)^T \max\{|a_I|\}\right) \max |x_i|_v^D \\ &\leq (D+1)^n (nCD)^T H(P) \max |x_i|_v^D\end{aligned}$$

Note again that this is at least 1 if we assume $C \geq 1$, as we may.

We raise this to the power $[\mathbb{L}_v : \mathbb{Q}_v]/[\mathbb{L} : \mathbb{Q}]$ and multiply. As the sum of the local degrees for $v|\infty$ is $[\mathbb{L} : \mathbb{Q}]$, we obtain

$$H([1 : Q(x)]) = \prod_v \max\{1, |Q(x)|_v\} \leq (D+1)^n (nCD)^T H(P) H(x)^D.$$

After applying log and get

$$h([1 : Q(x)]) \leq C'D + C'T \log(D) + h(P) + Dh(x).$$

With our estimates for D and $h(P)$ this gives the claim. □

Proposition 7.10. *Either* $\psi(\ell^{-1}s) = 0$ *or*

$$\log |\psi(\ell^{-1}s)| \geq -C\ell^{2n}(T \log(T) + c\ell^{c'})$$

for $0 \leq s \leq \ell S'$.

Proof. Note that $s\gamma$ and hence $\psi(\ell^{-1}s) = \Delta P(s\gamma)$ are algebraic numbers. We use Liouville's inequality for the place v_0 attached to $\mathbb{L} \subset \mathbb{C}$

$$\log \left\|\psi(\ell^{-1}s)\right\|_{v_0} \geq -[\mathbb{L} : \mathbb{Q}]h([1 : \psi(s)]).$$

Recall that $\left\|\psi(\ell^{-1}s)\right\|_{v_0} = |\psi(s)|^{[\mathbb{L}_v:\mathbb{R}]}$ and $[\mathbb{L} : \mathbb{Q}] \leq \ell^{2n}[\mathbb{K} : \mathbb{Q}]$. In all

$$\log |\psi(\ell^{-1}s)| \geq -c_0 \ell^{2n} h([1 : \psi(s)]).$$

It remains to bound $h([1 : \Delta P(s\gamma)])$ from above. This is what we have done in the last lemmas

$$\begin{aligned}h([1 : \Delta P(s\gamma)] &\leq CT \log(T) + Dh(s\gamma) \\ &\leq CT \log(T) + cD(S^2 + \ell^{c'})\end{aligned}$$

and DS^2 is bounded by T. This gives the estimate as we claimed it. □

Corollary 7.11. *If S is a high enough power of ℓ, then $\psi(\ell^{-1}s) = 0$.*

Proof. If $\psi(\ell^{-1}s) \neq 0$, then the combination of the two estimates gives

$$-C'\ell^{2n}(T\log(T) + c\ell^{c'}) \leq -CST\log(S)$$

with positive constants C, C', c, c'. We have

$$\log(T) \leq c_0 \log(S)$$

by our choice of T. This means

$$c_1\ell^{2n}(T\log(S) + c_2\ell^{c'}) \geq CST\log(S)$$

The inequality is false for S big compared to ℓ. □

Conclusion

With our choice for D, S, T and ℓ and S a high power of ℓ, we have seen that ΔP vanishes to order $T/2$ in the points $0, \gamma, \dots, \ell S'\gamma = S'g$. For big enough ℓ, the assumption of the multiplicity estimate is satisfied with S replaced by the number B of elements of $\{0, \gamma, \dots, S\ell\gamma = Sg\}$ and T replaced by $T/2$. Applying Theorem 5.7, we get that γ is a torsion point of order less that $\ell S'$. This contradicts the definition of S' as the order of g.

Hence $g = 0$. This establishes the semi-stability theorem (Theorem 4.9). We have seen in there that it implies the full theorem.

Addendum

The analytic subgroup theorem can be strengthened without extra effort.

Theorem 7.12 (Alternative version)**.** *Let $\mathfrak{b} \subset \mathrm{Lie}(G)$ be a subvector space, $u \in \mathfrak{b}_{\mathbb{C}}$ such that $P = \exp_G(u) \in G(\overline{\mathbb{Q}})$. Then there is an algebraic subgroup $H \subset G$ such that $u \in \mathrm{Lie}(H)^{\mathrm{an}}$, $P \in H(\overline{\mathbb{Q}})$ and $\mathrm{Lie}(H) \subset \mathfrak{b}$.*

Proof. If $u = 0$, we can use $H = 0$. Assume $u \neq 0$ but $P = 0$. The kernel of $\exp_G$ is discrete in $\mathrm{Lie}(G)_{\mathbb{C}}$, hence there is $n \in \mathbb{N}$ such that $u' = \frac{1}{n}u$ is not in the kernel. Then $P' = \exp_G(u')$ is a torsion element of G. All torsion elements are in $G(\overline{\mathbb{Q}})$. We also have $P' \in B$ because $u' \in \mathfrak{b}$. Without loss of generality, $P \neq 0$.

By the analytic subgroup theorem we find H_1 such that $P \in H_1(\overline{\mathbb{Q}})$ and $\mathrm{Lie}(H_1) \subset \mathfrak{b}$.

If $u \in \mathrm{Lie}(H_1)_{\mathbb{C}}$, we are done. Otherwise we consider G/H and the image $\overline{u}$ of u in $\mathrm{Lie}(G/H_1)_{\mathbb{C}}$. By induction on the dimension, there is $H_2 \subset G/H_1$ such that such that $\mathrm{Lie}(H_2) \subset \mathfrak{b}/\mathrm{Lie}(H_1)$ and $\overline{u} \in \mathrm{Lie}(H_2)_{\mathbb{C}}$. We then choose H as the preimage of H_2 under $G \to G/H_2$. It has the required properties. □

Outlook

We have brought the first half of the lecture to a close: We have proved the analytic subgroup theorem in the case of groups of the form $\mathbb{G}_a^s \times \mathbb{G}_m^r$. We have seen that this implies transcendence of π, $\log(\alpha)$ for $\alpha \in \overline{\mathbb{Q}}^*$ (except for the branch $\log(1) = 0$) and Baker's theorem.

Plan for the second half

- The next topic we want to get into are general commutative algebraic groups. We will discuss the case of elliptic curves in some detail, then present the structure theory in general. In particular, we will need to construct embeddings $G \subset \mathbb{P}^N$. The emphasis will be on understanding the facts rather than providing detailed proofs.

- In the context of Hodge theory, Deligne introduced the category of 1-motives: objects are of the form $[L \to G]$ where L (lattice) is a free finitely generated abelian group and G a semi-abelian variety (extension of an abelian variety by a torus). We will define the notion of a period of a 1-motives, formulate and prove a version of the analytic subgroup theorem for 1-motives and use it to establish the period conjecture for 1-motives.

- For every pair of algebraic varieties $Y \subset X$ over $\overline{\mathbb{Q}}$, there is a 1-motive reflecting the properties of $H_1^{\mathrm{sing}}(X^{\mathrm{an}}, Y^{\mathrm{an}}, \mathbb{Q})$. We are going to explain how the results on periods of 1-motives translate to period of algebraic varities, i.e., integrals of the form

$$\int_\gamma \omega$$

  where γ is a path with algebraic endpoints and ω an algebraic differential form.

- If there is enough time and interest, we are going to look into the proof of the multiplicity estimate, at least in the linear case.

Chapter 8

Elliptic curves

Before reviewing the general theory of commutative algebraic groups, we want to go into the details of a particular important example.

The algebraic story

We are going to work over an algebraically closed field k of characteristic 0.

Definition 8.1. An *elliptic curve* is a smooth proper algebraic curve over k of genus 1 together with the choice of a point $P_0 \in E$.

Recall that the genus of an algebraic curve is equal to the dimension of the space algebraic differential forms, so 1 in our case. It appears in the theorem of Riemann-Roch. In the case of elliptic curves it takes the shape

$$l(D) - l(-D) = \deg D$$

for all divisors D on E. Here

$$l(D) = \dim L(D) = \dim\{f \in k(E)^* | \mathrm{div}(f) \geq -D\}.$$

It vanishes for $\deg D < 0$.

We consider $D_n = n[P_0]$. Note that $l(-D_n) = 0$ for $n \geq 1$, so $l(D_n) = n$. For $n = 1$, $L(D_1) = k$ are the constant functions. Let

$$x \in L(D_2) - L(D_1), y \in L(D_3) - L(D_2.$$

The function x has a double pole 2 and y has a pole of order 3. In L_6 we have the 7 elements

$$1, x, x^2, x^3, y, xy, y^2.$$

They are linearly dependent, so we get an equation

$$a + bx + cx^2 + dx^3 + ey + fxy + gy^2 = 0.$$

The only terms of pole order 6 are x^3 and y^2. The other monomials have pairwise distinct pole orders. We need $d, g \neq 0$ to cancel this pole. Without loss of generality $g = 1$ and we rewrite

$$y^2 = P(x) + yQ(x) \tag{8.1}$$

where P is a cubic polynomial in x and Q is a linear polynomial in x. By elementary arguments (see: Silverman, Arithmetic of elliptic curves) we can make a change of variable and simplify to an equation of the form

$$y^2 = 4x^3 - g_2x - g_3.$$

(Weierstraß normal form). The point $[x : y : 1] \in \mathbb{P}^2(k(E))$ defines a rational map

$$i : E \to \mathbb{P}^2_k.$$

It is a morphism because E is a proper curve. The image is the subvariety E' defined by the equation (8.1). The composition

$$[x : 1] : E \to E' \to \mathbb{P}^1$$

has degree 2 (because the only pole of x is P_0 and it is a double pole.) Hence $[k(E) : k(E')]$ divides 2. With y instead of x we get $[k(E) : k(E')]|3$, so the function fields of E and E' agree. If E' is singular, then elementary considerations with the explicit equation show that it has genus 0 (Silverman Prop. III 1.6). On the other hand it is birational to E, so it has genus 1. Hence E' is non-singular and $E \cong E'$.

Exercise 8.1. *Check out the proof of genus computation for singular curves in Weierstraß form.*

Corollary 8.2. *All elliptic curves are projective. They are smooth planar cubics.*

The point P_0 did not play a role in the arguments. Note that

$$i(P_0) = [y^{-1}x(P_0) : 1 : y^{-1}P_0)] = [0 : 1 : 0],$$

so it is the point at infinity in the Weierstraß equation. Let $\mathrm{Cl}(E)$ be the *divisor class group*, the group of divisors up to linear equivalence. We put

$$\Phi : E \to \mathrm{Cl}^0(E); \quad P \mapsto [P] - [P_0].$$

Proposition 8.3. *This is a bijection The identifcation turns E into a group.*

Proof. We are going to show:
Claim: Given $P, Q \in E$ there is a unique $R \in E$ such that

$$[P] - [P_0] + [Q] \sim [R].$$

Note that we can rewrite the claim

$$\Phi(P) + \Phi(Q) \sim \ \Phi(R).$$

Putting $Q = P_0$, the uniqueness part of the claim gives injectivity of Φ. For surjectivity, we write a divisor $D = \sum a_i[P_i]$ of degree 0 in the form

$$D = \sum a_i(\Phi(P_i)).$$

The claim can be used to reduce this to a divisor of form $\Phi(P)$.

We turn to the proof of the claim. It is about existence of $g \in k(E)^*$ with

$$\mathrm{div}(g) = [R] + [P_0] - [P] - [Q].$$

Such a g is an element of $L([P]+[Q]-[P_0])$ and by Riemann-Roch the space has dimension 1, making g and its zero R unique. Conversely, a non-trivial element of the linear system has a zero in P_0. There are no elements in $k(E)^*$ with only a single pole, so g has two poles. They have to be in P and Q. The pole order is 2, so g also has two zeroes. One is P_0, the other we call R and have found a solution. This finishes the proof of bijectivity. □

The group law also has an explicit description in the plane. Let L be the line through P and Q. It has a third intersection point R' with E. Let L' be the line through P_0 and R'. Its third intersection point with E is R.

Exercise 8.2. *Verify this claim. For this write down the rational function g in terms of the homogenuous polynomicals of degree 1 describing L and L'.*

Theorem 8.4. *The group law on E is algebraic.*

Proof. For $P \neq Q$ the geometric procedure can be written out explicitly and gives explicit polynomials in terms of the coordinates. This gives

$$E \times E - \Delta \to E$$

with the properties of an algebraic group. To extend to all of $E \times E$ either show that the secant construction turns into the tangent. This can be done in the formal completion, i.e., the powers series expansion of the formulas. Alternatively, there is a theorem of Weil expanding "biratonal group laws" into group laws, see Serre: Algebraic Groups and Class fields, V §5 for precise references. □

Finally, we also need to understand the Lie algebra. As $\dim E = 1$, its Lie algebra is also of dimension 1. Actually, it is easier to understand the cotangent space.

Lemma 8.5. *Let E be an elliptic curve in Weierstraß form. Then*

$$\omega = \frac{dx}{y}$$

is an invariant algebraic differential.

Proof. The form is obviously regular away from the poles of x (the point at infinity) and the zeroes of y. We have the relation

$$0 = d(y^2 - 4x^3 + g_2x + g_3) = 2ydy - (12x^2 - g_2)dx \Rightarrow \omega = \frac{2dy}{12x^2 - g_2}.$$

It is regular away from the poles of y (again the point at infinity) and the zeroes of $12x^2 - g_2$. A zero of y would mean vanishing of $4x^3 - g_2x - g_3$. All zeroes are simple (non-singularity!), hence the derivative does not vanish in these points.

It remains to check the point at infinity. The function x has a pole of order 2, hence dx has a pole of order 3. This cancels with y^{-1} (which has a zero of order 3).

In all we have found a regular form on all of E. The invariant differential is another such. They have to agree up to a factor because $\Omega^1(E) = g(E) = 1$. □

The holomorphic story

We review the Weierstraß theory of elliptic functions. Reference: Ahlfors, Complex analysis, Chapter 7.

We work in one complex variable. We fix a lattice $\Lambda \subset \mathbb{C}$ generated by ω_1, ω which are $\mathbb{R}$-linear independent. We put $\Lambda' = \Lambda - \{0\}$.

Definition 8.6. The *Weierstraß σ-function* for the lattice Λ is given as

$$\sigma(z) = z \prod_{\omega \in \Lambda'} \left(1 - \frac{z}{\omega}\right) e^{\frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2}$$

The *Weierstraß ζ-function* and the *Weierstraß $\wp$-function* are defined as

$$\zeta(z) = \frac{\sigma'}{\sigma}, \quad \wp(z) = -\zeta'(z).$$

There is a general method for producing entire functions with prescribed divisor. The exponential factors are added to ensure absolute convergence of the infinite product. In our case, we get simple zeroes precisely in the lattice points. By passing to the logarithmic derivative, we obtain a function with simple poles in the lattice points. Its derivative has double poles there.

Exercise 8.3. *Verify convergence.*

We compute the derivatives. The logarithmic derivate turns the sum into a product. Moreover,

$$\frac{d \log}{dz} \left(1 - \frac{z}{\omega}\right) e^{\frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2} = -\frac{1}{\omega} \frac{1}{1 - \frac{z}{\omega}} + \frac{1}{\omega} + \frac{z}{\omega^2} = \frac{1}{z - \omega} + \frac{1}{\omega} + \frac{z}{\omega^2}$$

and hence

$$\zeta(z) = \frac{1}{z} + \sum_{\omega \in \Lambda'} \left(\frac{1}{z - \omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right).$$

Convergence can be checked by hand or follows from the convergence of σ. Deriving again we get

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda'}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

$$\wp'(z) - 2\sum_{\omega\in\Lambda'}\frac{1}{(z-\omega)^3}$$

Lemma 8.7. *The functions $\wp$ and $\wp'$ are* elliptic *for the lattice Λ, i.e., ω-periodic for all $\omega \in \Lambda$.*

Proof. In the case of $\wp'$ this is obvious from the series. Hence $\wp(z+\omega) - \wp(z)$ is constant. We determine the constant for $\omega = \omega_1, \omega_2$ (the basis vectors) by evaluating in $z = -\omega_i/2$. We have

$$\wp(z+\omega_i) - \wp(z) = \wp(\omega_i/2) - \wp(-\omega_i/2) = 0$$

because the function is even (and does not have a pole in $\omega_i/2$). Periodicity for ω_1, ω_2 implies periodicity for all $\omega \in \Lambda'$. □

We view elliptic functions as meromorphic functions on the compact Riemann surface $\mathbb{C}/\Lambda$. It has genus 1. The Theorem of Riemann-Roch in the Riemann surfact version applies. Comparing to what we have done in the algebraic case we see that x can be chosen as $\wp$ and y as $\wp'$. The same arguments as in the algebraic case imply the existence of a differential equation involving $\wp'^2$, $\wp^3$ and other products.

Lemma 8.8. *We have*

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3$$

with

$$g_2 = 60G_2 = 60\sum_{\omega\in\Lambda'}\frac{1}{\omega^4}, g_3 = 140G_3 = 140\sum_{\omega\in\Lambda'}\frac{1}{\omega^6}.$$

Proof. We calculate the Laurent expansion of $\zeta(z)$ at the origin. We have

$$\frac{1}{z-\omega} = -\omega^{-1}\frac{1}{1-\frac{z}{\omega}} = -\sum_{i=0}^{\infty}\frac{z^i}{\omega^{i+1}}$$

$$\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2} = \sum_{i=2}^{\infty}\frac{z^i}{\omega^{i+1}}$$

$$\zeta(z) = \frac{1}{z} - \sum_{i=2}^{\infty} z^i \sum_{\omega\in\Lambda'}\frac{1}{\omega^{i+1}}$$

Note that the lattice sum vanishes for even i (odd $i+1$) because the summands for ω and $-\omega$ cancel. We put

$$G_k = \sum_{\omega\in\Lambda'}\frac{1}{\omega^{2k}}$$

and get

$$\zeta(z) = \frac{1}{z} - \sum_{k=2}^{\infty} G_k z^{2k-1}.$$

By differentiating twice, we get the Laurent expansion of $\wp$ and $\wp'$. By comparing coefficients we see that

$$\wp'^2 - 4\wp^3 + g_2\wp + g_3$$

is holomorphic with constants term 0. As a holomorphic function on a compact Riemann surface, it vanishes. □

Corollary 8.9. *The Riemann surface $\mathbb{C}/\Lambda$ is projective. By the map*

$$\Phi : [\wp : \wp' : 1] : \mathbb{C}/\Lambda \to \mathbb{P}^2_{\mathbb{C}}$$

it is identified with the algebraic variety with equation

$$y^2 = 4x^3 - g_2x - g_3.$$

Proof. We have seen that we get a well-defined map. We can use the same arguments as in the algebraic case to see that it is an isomorphism. Or we analyse the zeroes of $4x^3 - g_2x - g_3$ and see that they have multiplicity 1, making the image an elliptic curve. By the Hurwitz formula, the map is unramified. We determine its degree by considering the preimage of the point of infinity: only the point 0. □

It is now clear, why chose the normalisation in the algebraic case as we did.

In the context of the proof of the analytic subgroup theorem, we also need to know:

Corollary 8.10. *The map ϕ lifts to a holomorphic map*

$$\Phi : \mathbb{C} \to \mathbb{C}^3 - \{0\},$$

i.e., there is a commutative diagram

$$\begin{tikzcd}
\mathbb{C} \arrow[r, "\phi"] \arrow[d] & \mathbb{C}^3 - \{0\} \arrow[d] \\
\mathbb{C}/\Lambda \arrow[r, "\Phi"'] & \mathbb{P}^2_{\mathbb{C}}.
\end{tikzcd}$$

Proof. We choose

$$\phi = (\sigma^3\wp, \sigma^3\wp', \sigma^3).$$

Obviously the diagram commutes. The entire function σ^3 has triple zeroes in the lattice points, canceling the poles of $\wp$ and $\wp'$. □

The Riemann surface $\mathbb{C}/\Lambda$ inherits a group structure from $\mathbb{C}$, turning it into a complex Lie group. The exponential map is simply the projection. The invariant differential is dz. We now need to relate these notions to the the algebraic group structure on the image in $\mathbb{P}^2$. Unsurpsingly:

Proposition 8.11. *The map Φ is a group homomorphism and $\Phi^*\frac{dx}{y} = dz$.*

Proof. We begin with the differential on the affine chart. We have $x \circ \Phi = \wp$, $y \circ \Phi = \wp'$. Hence

$$\Phi^* dx = d(x \circ \Phi) = \wp' dz, \quad \Phi^* \frac{dx}{y} = dz.$$

For the group structure, we use the characterisation of the group law via $\mathrm{Cl}(E)$. Given $P, Q \in \mathbb{C}/\Lambda$, the same Riemann-Roch argument as in the algebraic case gives the existence of a unique $R \in \mathbb{C}/\Lambda$ and an elliptic function g with divisor

$$[P] + [Q] - [0] - [R].$$

It is a general fact about elliptic functions that we then have

$$P + Q - 0 - R = 0.$$

This gives $R = P + Q$ and the group laws are compatible. □

Exercise 8.4. *Let f be elliptic with lattice Λ. Let $a_1, \dots, a_n$ be the zeroes of f in a fundamental domain of f and $b_1, \dots, b_n$ the poles. (Multiple zeroes are listed multiple times.) Consider the integral*

$$\int_{\partial P} \frac{zf'}{f}$$

along the boundary of a fundamental parallelogram in order to deduce

$$\sum a_i - \sum b_i \in \Lambda.$$

Remark 8.12. As a byproduct, we have found a description of exponential function of the elliptic curve defined by $y^2 = 4x^3 - g_2x - g_3$: it is given by Φ, so in terms of $\wp$ and $\wp'$.

From algebraic to holomorphic

It remains to understand the exponential function for an elliptic curve E in the sense of algebraic geometry, but viewed as compact Riemann surface. We need to determine the period numbers ω_1 and ω_2 such that $\mathbb{C}/\Lambda \cong E$ with $0 \mapsto P_0$. As the group law is determined by the identifcation with the divisor class group in both cases, the map is automatically a group homomorphism. We do this by defining the inverse of $\mathbb{C} \to E$, the elliptic version of the logarithm. As the classical logarithm it is multivalued.

Recall the construction of $\log : \mathbb{C}^* \to \mathbb{C}$:

$$\log(t) = \int_1^t \frac{dz}{z}.$$

The value depends on the choice of path in $\mathbb{C}^*$. Two choices differ by a closed path, so they differ by the period integral

$$\int_\gamma \frac{dz}{z} = 2\pi i n_\gamma$$

where n_γ is the winding number. Note that dz/z is nothing but the invariant differential on $\mathbb{C}^*$.

The same construction works for E, but with the fundamental group $\pi_1(E, P_0) \cong \mathbb{Z}^2$ instead of $\pi_1(\mathbb{C}^*, 1) \cong \mathbb{Z}$. So roughly:

$$\log_E(t) = \int_0^t \omega$$

where ω is the invariant differential form. The value depends on the choice of path. Any two choices differ by

$$\int_\gamma \omega$$

for a closed path γ. Let γ_1, γ_2 be a basis of $\pi_1(E)$ and put

$$\omega_i = \int_{\gamma_i} \omega.$$

Then two values of $\log_E(t)$ differ by an element

$$\omega \in \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 =: \Lambda.$$

We get a well-defined map

$$\log_E : E^{\mathrm{an}} \to \mathbb{C}/\Lambda.$$

Lemma 8.13. *The map $d\log_E : \mathrm{Lie}(E)^{\mathrm{an}} \to \mathbb{C}$ maps the dual basis vector of ω to 1.*

Proof. Let u be a local coordinate near 0. We have $\omega = gdu$ for a non-vanishing holomorphic function g. We have

$$\frac{d}{du}\int_{P_0}^u g(t)dt = g(u).$$

We may replace the coordinate u by $v = \log(u)$. In this coordinate

$$dv = d(\log(u)) = gdu = \omega$$

and the dual basis vector of $\mathrm{Lie}E^{\mathrm{an}}$ is simply d/dv and $\log_E$ is the map $v \mapsto z$. □

Let $\exp_E : \mathbb{C} \to E$ be the inverse of $\log_E$. It factors via $\mathbb{C}/\Lambda$.

More precisely, let $\pi : \tilde{E}^{\mathrm{an}} \to E^{\mathrm{an}}$ be the universal cover in the sense of Riemann surfaces. The map $\log_E$ is a holomorphic map $\tilde{E}^{\mathrm{an}} \to \mathbb{C}$. It induces $E^{\mathrm{an}} \cong \tilde{E}^{\mathrm{an}}/\pi_1(E, 0) \to \mathbb{C}/\Lambda$. This is a map of Riemann surfaces of genus 1, so surjective and unramified. Actually, it is an isomorphism. This is not obvious at all.

Theorem 8.14 (Abel-Jacobi)**.** *Let C be a compact Riemann surface of genus $g > 0$. Fix $P_0 \in C$. Then the map*

$$C \to \Omega^1(C)^*/H_1(C, \mathbb{Z})$$

defined by

$$P \mapsto \left(\omega \mapsto \int_{P_0}^{P} \omega\right)$$

is well-defined, holomorphic and injective.

Proof. Two choices of path from P_0 to P differ by a closed path. The integral over a closed path γ only depends on the homotopy class of $\gamma \in \pi_1(C, P_0)$. Integration is commutative in paths, so the value only depends on the class in $\pi_(C, P_0)^{\mathrm{ab}} = H_1(C, \mathbb{Z})$.

It is easy to see that the map is holomorphic by varying P and the chosen paths in a small open disc.

Injectivity is hard, see Forster, Lectures on Riemann Surfaces, Thm 20.7. (Loc. cit. gives that $[P] - [P_0]$ is principal. That's impossible because the sum of the residues vanishes.) □

Exercise 8.5. *(Talk) Explain how Abel's theorem is deduced from the Hodge decomposition and other properties of (co)homology.*

The identification $E^{\mathrm{an}} \cong \mathbb{C}/\Lambda$ defines $\mathbb{C} \to E^{\mathrm{an}}$. Everything we did so far, depended on the choice of ω. Let $\partial \in \mathrm{Lie}(E)^{\mathrm{an}}$ be the dual basis of ω. We identify $\mathrm{Lie}(E)^{\mathrm{an}} \cong \mathbb{C}$ by mapping ∂ to 1.

Proposition 8.15. *The composition*

$$\mathrm{Lie}(E)^{\mathrm{an}} \to \mathbb{C} \to \mathbb{C}/\Lambda \cong E^{\mathrm{an}}$$

is the exponential map of E.

Proof. We first check that the map is additive. The only non-obvious ingredient is $\log_E$. Let γ_1, γ_2 be paths from P_0 to P_1 and P_2, respectively. Let $P_1 + \gamma_2$ be the shifted path. The from ω is invariant, hence

$$\int_{\gamma_2 + P_1} \omega = \int_{\gamma_2} \omega = \log_E(P_2).$$

The concatenation of γ_1 and $\gamma_2 + P_1$ is a path from P_0 to $P_1 + P_2$, hence

$$\log_E(P_1 + P_2) = \int_{P_0}^{P_1 + P_2} = \int_{\gamma_1} \omega + \int_{\gamma_2 + P_1} \omega = \log_E(P_1) + \log_E(P_2).$$

The sequence of maps applied to ∂ gives on tangent spaces

$$\partial \mapsto \frac{\partial}{\partial z} \mapsto \frac{\partial}{\partial z} \mapsto \partial.$$

□

Transcendence

We now apply the analytic subgroup theorem to elliptic curves or product of linear commutative algebraic groups and elliptic curves.

Theorem 8.16 (Siegel, Schneider (?)). *Let E be an elliptic curve over $\overline{\mathbb{Q}}$ with invariant differential form $\omega \neq 0$, γ be a closed path on E^{an} which is not null-homotopic. Then*

$$\int_\gamma \omega$$

is transcendental.

The argument is very similar to our proof of transcendence of $2\pi i$.

Proof. Assume that $\alpha = \int_\gamma \omega$ is algebraic. Without loss of generality, γ starts and end in $0 \in E$. It lifts to a canonical element $l(\gamma) \in \mathrm{Lie}(E^{\mathrm{an}})$ because we can identify $\mathrm{Lie}(E^{\mathrm{an}})$ with the universal cover. In fact, $l(\gamma) = \log_E(0)$ with choice of γ for the path. Note that $l(\gamma) \neq 0$ because γ is not null-homotopic.

We want to apply the analytic subgroup theorem to the commutative algebraic group $G = \mathbb{G}_a \times E$. Let $b = (-\alpha, l(\gamma)) \in \mathrm{Lie}(G)$. By assumption $\exp(b) = (-\alpha, 0) \in G(\overline{\mathbb{Q}})$. We have $\tilde{\omega} = (dz, \omega) \in \mathrm{Lie}(G)^\vee$. Let $\mathfrak{b} \subset \mathrm{Lie}(G)$ be its annihilator. Note that $b \in \mathfrak{b}_\mathbb{C}$ because

$$\tilde{\omega}(b) = \int_0^{-\alpha} dz + \int_\gamma \omega = 0.$$

Hence there is an algebraic subgroup $H \subset G$ such that $\mathrm{Lie}(H) \subset \mathfrak{b}$ and $\exp(b) \in H(\overline{\mathbb{Q}})$.

The dimension of H is at most 1 because its Lie algebra is contained in $\mathfrak{b}$, which is 1-dimensional as the annihilator of a single non-zero element. If it is of dimension 0, then $l(\gamma) = 0$, a contradiction to γ not null-homotopic. So we have $\dim H = 1$.

We first concentrate on $\pi : H \to E$. This is a morphism of smooth algebraic curves. It extends to $\overline{\pi} : \overline{H} \to E$ where $\overline{H}$ is a smooth compactification of H. The map $\overline{\pi}$ is either constant or finite. If it was constant, then $H = \mathbb{G}_a \times \{0\}$. This contradicts again $l(\gamma) \neq 0$. So it is constant of some degree. Generically, the map is unramified and the degree is simply the number of points in the fibre. As π is a group homomorphism, all its fibres have the same number of elements. So in fact all preimages are already accounted for by H and we have $H = \overline{H}$.

Now consider $p : H \to \mathbb{G}_a$. As H is proper and $\mathbb{G}_a$ is not, the map is constant, so $H = \{0\} \times E$. This contradicts $\omega \neq 0$. □

Our next aim is to determine the dimension of the $\overline{\mathbb{Q}}$-vector space of numbers of the form

$$\int_\gamma \omega$$

with γ closed. We need to talk about morphisms of elliptic curves first.

Exercise 8.6. *Let $n \in \mathbb{Z}$. Show that multiplication by n is a morphism of elliptic curves. It is denotes $[n]$.*

A morphism of elliptic curves is either constant (and the zero map) or surjective and unramified. The latter are called *isogenies.* The order of the kernel is equal to the degree of the morphism, so it is always finite. If an isogeny $E_1 \to E_2$ exist, we call them *isogenous*.

Exercise 8.7. *Show that this is an equivalence relation. Hint: consider multiplication by the degree of the isogeny. (The argument is easy in the category of Riemann surfaces but requires extra arguments in the algebraic setting.)*

Exercise 8.8. *Let E_1, E_2 be non-isogenuous elliptic curves, i.e., there is no non-constant morphism $E_1 \to E_2$. Let*

$$\alpha_i = \int_{\gamma_i} \omega_{E_i}$$

be periods for non-contractible paths on E_1 and E_2. Show that α_1 and α_2 are linearly independent over $\overline{\mathbb{Q}}$.

We also need to understand the endormorphisms of E. We start in the holomorphic setting and compute $\mathrm{End}(\mathbb{C}/\Lambda)$. For every $n \in \mathbb{Z}$, the multiplication map $[n]$ is a morphism of elliptic curves, so $\mathbb{Z} \subset \mathrm{End}(E)$. Are there any others? Without loss of generality, $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ with $\mathrm{Im}(\tau) > 0$. Let $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ be holomorphic with $f(0) = 0$. It is automatically a group homomorphism. The induced map F on $\mathbb{C} = \mathrm{Lie}(\mathbb{C}/\Lambda)$ is linear, so of the form $F(z) = \alpha z$ for some $a \in \mathbb{C}$. In addition, $F(1), F(\tau) \in \Lambda$. This means

$$F(1) = \alpha = a + b\tau, \quad F(\tau) = \alpha\tau = a\tau + b\tau^2 = c + d\tau$$

with $a, b, c, d \in \mathbb{Z}$. This is a quadratic equation for τ, making it an algebgraic number with $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$. The same equation implies that $b\tau$ is an algebraic integer, hence also α:

$$\mathrm{End}(\mathbb{C}/\Lambda) \subset \mathcal{O}_{\mathbb{Q}(\tau)}.$$

Exercise 8.9. *Let $\mathbb{Q}(\tau)/\mathbb{Q}$ be imaginary quadratic.*

(i) Show that $E = \mathrm{End}(\mathbb{C}/\mathbb{Z} + \tau\mathbb{Z})$ is an order *of $\mathbb{Q}(\tau)$, i.e., E is a finitely generated abelian group and $E \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\tau)$.*

(ii) Find an example where $E \neq \mathcal{O}_{\mathbb{Q}(\tau)}$.

If E is an elliptic curve over $\overline{\mathbb{Q}}$ or $\mathbb{C}$, then the endormorphism ring is contained in $\mathrm{End}(E^{\mathrm{an}})$ (actually equal). Note that $f \in \mathbb{Z}$ if and only $\alpha \in \mathbb{R}$.

Definition 8.17. Let E be an elliptic curve. We say that it has *complex multiplication* if $\mathrm{End}(E) \supsetneq \mathbb{Z}$. In this case $\mathrm{End}(E) \subset \mathbb{Z}[\tau]$ for a imaginary quadratic irrational number.

Theorem 8.18 (Schneider)**.** *Let E be an elliptic curve over $\overline{\mathbb{Q}}$ with period lattice Λ. Then the $\overline{\mathbb{Q}}$-subvector space of $\mathbb{C}$ spanned by Λ has dimension 1 if E has complex multiplication and 2 if not.*

Proof. We begin with the case of complex multiplication. We need to show that there is a $\overline{\mathbb{Q}}$-linear relation between the periods. Let $f : E \to E$ be a morphism not in $\mathbb{Z}$. It operates by multiplicaton with $\alpha \notin \mathbb{R}$ Let γ be a generator of $\pi_1(E^{\mathrm{an}}, 0)$. Then $f_*\gamma$ is linearly indepdent from γ in $\pi_1(E^{\mathrm{an}}, 0)$, so rationally the space of periods is spanned by

$$\int_\gamma \omega, \quad \int_{f_*\gamma} \omega = \int_\gamma f^*\omega.$$

The pull-back of ω is again an invariant differential form, so a $\overline{\mathbb{Q}}$-multiple of ω. (In fact, it is $\alpha\omega$.) This give the $\overline{\mathbb{Q}}$ relation between the two periods.

Now assume that E does not have complex multiplication. Let γ_1, γ_2 be a basis of $\pi_1(E^{\mathrm{an}}, 0)$. We have to show that

$$\omega_1 = \int_{\gamma_1} \omega, \quad \omega_2 = \int_{\gamma_2} \omega$$

are $\overline{\mathbb{Q}}$-linearly independent. Assume that they are not. Then there are non-zero algebraic numbers a_1, a_2 such that

$$0 = a_1\omega_1 + a_2\omega_2.$$

We apply the analytic subgroup theorem to $E \times E$ and the point

$$b = (l(\gamma_1), l(\gamma_2)) \in \mathrm{Lie}(E \times E)^{\mathrm{an}}.$$

Its image in $E \times E$ is $(0, 0) \in E^2(\overline{\mathbb{Q}})$. Let $\mathfrak{b} \subset \mathrm{Lie}(E^2)$ be the annihilator of $0 \neq \tilde{\omega} = (a_1\omega, a_2\omega)$. It contains the element $b \neq 0$, hence $\dim \mathfrak{b} = 1$. Hence there is an algebraic subgroup $H \subset E \times E$ with Lie algebra $\mathfrak{b}$. The restriction of $\tilde{\omega}$ to $\mathrm{Lie}(H)$ vanishes. On the other hand, $b \in \mathrm{Lie}(H)^{\mathrm{an}}$ with $\exp_H(b) = 0$ Moreover, H is itself of dimension 1 and a closed subgroup of $E \times E$, hence complete. The two projection maps are either constant or finite. They cannot be constant because both $l(\gamma_i) \neq 0$. The covering maps are unramified because all fibres have the same number of elements. This makes H itself an elliptic curve. The element $b \in \mathrm{Lie}(H)^{\mathrm{an}}$ satisfies $\exp_H(b) = 0$ because $H^{\mathrm{an}} \to (E \times E)^{\mathrm{an}}$ is injective. Hence it is of the form

$$b = l(\gamma)$$

for a closed loop in H^{an}.

Consider the first projection $p_1 : H \subset E \times E \to E$. Let n_1 be the order of the kernel of p_1. Then the multiplication map $[n_1] : H \to H$ annihilates the kernel, hence it factors via E.

$$[n_1] : H \xrightarrow{p_1} E \xrightarrow{q} H.$$

Note that the compositions $q \circ p_1$, $q \circ p_2$ are endomorphisms of E, hence multiplications by some integers $[m_1]$, $[m_2]$. The map $E \to H$ is surjective on rationalised fundamental groups, so $a\gamma = q_*\gamma'$ for some $\gamma' \in \pi_1(E^{\mathrm{an}}, 0)$ and $a \in \mathbb{Z}$, $a \neq 0$. We get

$$a(l(\gamma_1), l(\gamma_2)) = b = l(\gamma) = q_* l(\gamma') = (m_1 l(\gamma'), m_2 l(\gamma')).$$

This contradicts the linear independence of γ_1 and γ_2. □

Chapter 9

Commutative algebraic groups II

We continue to work over an algebraically closed field of characteristic 0. We have seen affine commutative groups so far: basically $\mathbb{G}_m$ and $\mathbb{G}_a$.

Lemma 9.1. *All algebraic groups are non-singular.*

Proof. In characteristic 0, every variety has an open dense subset U which is non-singular. (In scheme theoretic language: because it is reduced.) All of G can be covered by translates of U, hence all of G is non-singular. □

Exercise 9.1. *Let p be a prime. We define*

$$\mu_p = \mathrm{Ker}([p] : \mathbb{G}_m \to \mathbb{G}_m, \quad \alpha_p = \mathrm{Ker}([p] : \mathbb{G}_a \to \mathbb{G}_a.$$

Work out what they are as varieties and (if you know the language) as group schemes. What happens if k has characteristic p? Are they smooth over k?

Definition 9.2. An algebraic group is called *abelian variety* if it is proper or complete over k.

Example 9.3. Elliptic curves are examples of abelian varieties.

Theorem 9.4. *Let C be a smooth complete curve of genus g. Then the divisor class group of degree 0 divisors $\mathrm{Cl}^0(C)$ carries a natural structure of abelian variety of dimension g, the* Jacobian *denoted* $\mathrm{Jac}(C)$. *For every $P_0 \in C$, the map*

$$C \to \mathrm{Jac}(C); \quad P \mapsto [P] - [P_0]$$

is an injective morphism of algebraic varieties.

Proof. See Serre, Algebraic Groups and Class Fields, Chapter V. □

Remark 9.5. We have seen the holomorphic version of the statement:

$$\mathrm{Jac}(C)^{\mathrm{an}} = \Omega^1(C)^*/H_1(C^{\mathrm{an}}, \mathbb{Z})$$

is a compact complex Lie group because $H_1(C, \mathbb{Z})$ is a lattice in $\Omega^1(C)^*$ (see Forster, Riemann surfaces). The map is the one appearing in the Theorem of Abel-Jacobi, so it is holomorphic and injective. The so-called Riemann relations can be used to show that $\mathrm{Jac}(C)$ is projective. Note an interesting consequence: The fundamental group of $\mathrm{Jac}(C)$ is isomorphic to $H_1(C^{\mathrm{an}}, \mathbb{Z})$ because vector spaces are simply connected. This implies that

$$H_1(\mathrm{Jac}(C)^{\mathrm{an}}, \mathbb{Z}) = H_1(C^{\mathrm{an}}, \mathbb{Z}).$$

Jacobians are commutative. This is a general fact:

Proposition 9.6. *Let A, B be abelian varieties. Then the group law is commutative. Every morphism of varities $f : A \to B$ with $f(0) = 0$ is a group homomorphism.*

The traditional reference for abelian varieties is Mumford's book. We follow the book of Milne, which is available online.

Proof. It suffices to show that the inversion map $\iota : A \to A$ is a group homomorphism. Hence it suffices to show the second statement. We consider the diagram

$$\begin{tikzcd}
A \times A \arrow[r, "\mu"] \arrow[d, "{(f,f)}"'] & A \arrow[d, "f"] \\
B \times B \arrow[r, "\mu"] & B
\end{tikzcd}$$

Consider the difference between the two maps

$$\phi(a, a') = f(a + a') - (f(a) + f(a')).$$

It satisfies $\phi(a, 0) = 0$ and $\phi(0, a) = 0$. This implies that ϕ is constant by the fact below. □

Proposition 9.7 (Rigidity)**.** *Let $\phi : V \times W \to U$ be a morphism of varieties with V complete, $V \times W$ irreducible. Assume that there are points $v \in V, w \in W, u \in U$ such that $\phi(v, W) = \phi(V, w) = u$. Then ϕ is constant.*

Proof. Note that V is connected and the projection map $q : V \times W \to W$ is closed.

Let $U_0 \subset U$ be an affine neighbourhood of u. Let

$$Z = q(\phi^{-1}(U \smallsetminus U_0)) \subset W.$$

It is closed. By definition, a point $\in W$ is in Z if it is the second cooridinate of a point of $V \times W$ mappint to U_0. Conversely, it is in $W \smallsetminus Z$ if $\phi(V, x) \subset U_0$. As V is complete and U_0 is affine, the map $V \times \{x\} \to U_0$ has to be constant. Actually, the image is u because $\phi(v, x) = u$. Hence ϕ is constant on $V \times (W \smallsetminus Z)$.

By assumption, $w \notin Z$, making $W \smallsetminus Z$ non-empty. As $V \times W$ is irreducible, the open subset is dense, hence the map is constant on all of $V \times W$. □

The same argument applies to compact Lie groups in the holomorphic setting, but not for real Lie groups.

Exercise 9.2. *Give an example of a compact non-commutative real Lie group.*

Exercise 9.3. *Let A be an abelian variety over $\mathbb{C}$. Use the exponential map to show that $A^{\mathrm{an}} \cong \mathbb{C}^g/\Lambda$ for a lattice (subgroup of maximal rank) in $\mathbb{C}^g$.*

Our next aim is to show that all abelian varieties are projective. The full argument can be found in Milne. We want to explain how the map is constructed.

Definition 9.8. Let X be an irreducible non-singular variety.

(i) A *prime divisor* is an irreducible subvariety of codimension 1. We denote the set of prime divisors by X^1.

(ii) A *divisor* is a formal $\mathbb{Z}$-linear combination of prime divisors.

(iii) For $f \in k(X)^*$, we define

$$\operatorname{div}(f) = \sum_{Z \in X^1} v_Z(f)[Z]$$

where v_Z is discrete valuation on $k(X)$ defined by the discrete valuation ring

$$\mathcal{O}_{X,Z} = \lim_{U \cap Z \neq \emptyset} \mathcal{O}(U).$$

(iv) For every divisor D, we define the *linear system*

$$L(D) = \{f \in k(X) | \operatorname{div}(f) \geq -D\}.$$

In the case of curves, we get back the standard theory that we have used before.

Given a divisor D and a basis $f_0, \ldots, f_n$ of $L(D)$, we get a rational map

$$\phi_D : X \to \mathbb{P}^n, \quad x \mapsto [f_0(x), \ldots, f_n(x)].$$

If x is neither a pole of some f_i or a common zero of all f_i, then ϕ_D is regular near x. We have to find D such that the map is defined everywhere, injective and an isomorphism on tangent spaces.

We explain the choice of D for an abelian variety A.

Lemma 9.9. *Let $P \in A$. Then there is an open affine subset $U \subset A$ containing 0 and P and a prime divisor containing 0 but not P.*

Proof. Let U be an affine neighbourhood of 0. The intersection of U and $U + P$ is non-empty because A is irreducible. Let Q be in the intersection. The affine subvariety $U + P - Q$ contains 0 because $Q \in U + P$ and P because $Q \in U$.

We replace U be $U + P - Q$. We can view it as a closed subvariety in $\mathbb{A}^n$. There is a hyperplane passing through 0 but not through P in U. Let Z be its closure in A. It is a prime divisor. □

We now construct a sequence Z_i of prime divisors such that $\bigcap_i Z_i = \{0\}$. Pick a point $P_1 \in A$ and a prime divisor Z_1 containing 0 but not P_1. Pick $P_2 \in A \smallsetminus Z_1$ and Z_2 containing 0 but not P_2. The sequence

$$A \supset Z_1 \supset Z_1 \cap Z_2 \supset Z_1 \cap Z_2 \cap Z_3 \supset \dots$$

has to end after finitely many steps because A satisfies the descending chain condition, say at Z_n. The divisor

$$D = Z_1 + \dots Z_n$$

"separates 0 from P for all P". Enlarging the divisor with additional components, we achieve that its "separates all $0 \neq t \in T_0 A$ from 0", i.e., $\bigcap T_0 Z_i = \{0\}$. The divisor $3D$ does the job. The verification that $3D$ "separates points and tangent vectors" uses facts on abelian varieties like the theorem of the cube that we do not want to review.

Exercise 9.4. *Go through the construction in the case of an elliptic curve and compare it to what we did before.*

The structure theorem

Theorem 9.10 (Structure theory)**.** *Let G be a connected commutative algebraic group. Then there is a canonical short exact sequence*

$$0 \to L \to G \to A \to 0$$

with an abelian variety A and a linear connected commutative algebraic group L. Moreover, there is a canonical split short exact sequence

$$0 \to V \to L \to T \to 0$$

with a torus T and a vector group V.

Proof. The first sequence is the commutative case of a theorem of Barsotti, also known as Chevalley's theorem, [Ch60]. By Demazure–Gabriel Ch. IV §3 Théoréme 1.1 or Serre's book Ch. III Proposition 12 we have $L \cong V \times T$ with V unipotent and a torus T. By Serre Ch. VII §2.7, all unipotent groups are powers of $\mathbb{G}_a$ in characteristic 0, hence V is a vector group. □

Corollary 9.11. *A commutative algebraic group is simple if and only if it is isomorphic to $\mathbb{G}_a$, $\mathbb{G}_m$ or a simple abelian variety.*

Theorem 9.12. *All comutative algebraic groups are quasi-projective.*

Proof. (Sketch) We start with a short exact sequence

$$0 \to \mathbb{G}_a^s \times \mathbb{G}_m^r \to G \to A \to 0$$

given by the structure theorem. Let $D = \sum Z_i$ be a divisor on A defining an embedding of A into projective space. Let $\tilde{D}$ be its "preimage" on G. We compactify $L = \mathbb{G}_a^s \times \mathbb{G}_m^r$ by $\overline{L} = (\mathbb{P}^1)^{s+r}$. It is projective. Expicitly: let $E_i \subset \overline{L}$ be the subvariety where the i-th component is $\{\infty\}$. The embedding is defined by the divisor $E = \sum E_i$. It remains to patch the two divisors together.

We view G as fibre bundle over A. Zariski-locally it is of the form $L \times U$ for $U \subset A$ open. (There is something to prove here!) The bundle is uniquely determined by the transition maps in the bundle. They are compatible with the L-operation. (In differential topology such an object is called an L-principal bundle). The group L operates on $\overline{L}$. We can use the same gluing data on patches $\overline{L} \times U$ to define a fibre bundle $\overline{G} \to A$ with fibre $\overline{L}$. On $\overline{G}$, we have the divisor

$$\tilde{D} + E.$$

It is easy to see that it separates points and tangent vectors on $\overline{G}$ because D and E do so on A and $\overline{L}$. Hence the linear system $L(\tilde{D} + E)$ defines an embedding of $\overline{G}$ into some projective space. The complete variety $\overline{G}$ is projective and G is quasi-projective. □

Falting and Wuestholz [Einbettungen kommutativer algebraischer Gruppen] describe these compactifications (in the holomorphic setting) completely explicitly in terms of theta functions. As in the elliptic case we get a lift to

$$\mathrm{Lie}(G)^{\mathrm{an}} \to \mathbb{C}^N \smallsetminus \{0\}.$$

Definition 9.13. Let G be a connected commmutative algebraic group over $\overline{\mathbb{Q}}$. The *periods* of G are the numbers of the form

$$\int_\gamma \omega$$

where ω is an invariant algebraic differential form over $\overline{\mathbb{Q}}$ and γ a path in G^{an} from 0 to a point $\gamma(1) \in G(\overline{\mathbb{Q}})$.

All transcendence results that we have mentioned so far (except e) are about numbers of this form. Our aim is to generalise Baker's theorem to this setting and characterise all $\overline{\mathbb{Q}}$-linear relations between such periods. This needs the language of 1-motives and a bit of preparation.

Extensions of algebraic groups

The category of commutative algebraic groups is obviously not abelian—kernels are not connected in general. It does indeed become abelian if we drop the connectedness assumption. We use a different solution.

Definition 9.14. The category of *commutative algebraic groups up to isogeny* has as objects commutative algebraic groups and as morphisms the $\mathbb{Q}$-vector space generated by $\mathrm{Hom}(G, G')$.

Exercise 9.5. *Make the composition law explicit. Show that isogenous elliptic curves become isomorphic in the category of algebraic groups up to isogeny.*

Exercise 9.6. *Compute endormorphisms of $\mathbb{G}_a$ and $\mathbb{G}_m$ in the category of commutative algebraic groups up to isogeny.*

Theorem 9.15. *The category of commutative algebraic groups up to isogeny is abelian.*

Proof. We have to build on the case of non-connected algebraic groups. Let G be such a group and G^0 the connected component of 0. The image of $G^0 \times G^0$ under the group multiplication is connected, hence again contained in G^0. This makes G^0 a subgroup. The number of connected components is finite. Let n be its order. We claim that

$$[n] : G \to G$$

has image contained in G^0. Indeed, G/G^0 is a finite abelian group and multiplication by n agrees with the zero map on the quotient. The map $1/n[n]$ is the inverse of the inclusion $G^0 \to G$, making the two groups isomorphic in the isogeny category. □

Definition 9.16. A commutative algebraic group is called *semi-abelian variety* if its linear part is a torus.

This means that we have an extension

$$0 \to T \to G \to A.$$

Semi-abelian varieties with abelian part A are classified by the dual abelian variety. We omit this aspect.

Definition 9.17. Let G be a commutative algebraic group. We say that G' is a *vector extension* if there is a short exact sequence

$$0 \to V \to G' \to G \to$$

with a vector group V.

We need to understand vector extensions, in particular of semi-abelian varieties.

Definition 9.18. Let $\mathcal{A}$ be an abelian category, for example the category of connected commutative algebraic groups up to isogeny. For $X, Y \in \mathcal{A}$ we define the Yoneda-Ext group

$$\mathrm{Ext}^1_{\mathcal{A}}(X, Y)$$

as the set of isomorphism classes of short exact sequences

$$0 \to Y \to E \to X \to 0$$

where two sequences are equivalent if there is a homomorphism of exact sequences inducing the identity on X and Y. We define an addition by the *Baer-sum*

$$\begin{tikzcd}
 & & & X \arrow[d, "\Delta"'] & \\
0 \arrow[r] & Y \oplus Y \arrow[r] \arrow[d, "s"'] & E_1 \oplus E_2 \arrow[r] & X \oplus X \arrow[r] & 0 \\
 & Y & & &
\end{tikzcd}$$

as the pull-back via the diagonal and push-out via the summation map.

Exercise 9.7. *Compute* $\mathrm{Ext}^1(\mathbb{Z}, \mathbb{Z})$ *and* $\mathrm{Ext}^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$ *in the category of abelian groups. Also work out the addition.*

Proposition 9.19. *This definitions yields abelian groups. Given a short exact sequence*

$$0 \to A \to B \to C \to 0$$

and an object X, there are natural exact sequences

$$0 \to \mathrm{Hom}(X, A) \to \mathrm{Hom}(X, B) \to \mathrm{Hom}(X, C) \to \mathrm{Ext}^1(X, A) \to \mathrm{Ext}^1(X, B) \to \mathrm{Ext}^1(X, C)$$

and

$$0 \to \mathrm{Hom}(C, X) \to \mathrm{Hom}(B, X) \to \mathrm{Hom}(A, X) \to \mathrm{Ext}^1(C, X) \to \mathrm{Ext}^1(B, X) \to \mathrm{Ext}^1(A, X)$$

Proof. These are standard facts that are typically shown in books on homological algebra. Another reference is Serre's book on algebraic groups mentioned before. We only explain the connecting morphism for the first sequence: Let $f : X \to C$. By pull-back of the exact sequence, we get an exact sequence

$$0tøA \to B \times_C X \to X \to 0.$$

□

Exercise 9.8. *If you know about derived functors: show that Yoneda-Ext agrees with* Ext^1 *as defined via injective or projective resolutions.*

Given a commutative algebraic group G and a vector group V, there is a natural bilinear pairing

$$\mathrm{Hom}(V, \mathbb{G}_a) \times \mathrm{Ext}^1(G, V) \to \mathrm{Ext}^1(G, \mathbb{G}_a).$$

It induces the *classifying map*

$$\mathrm{Ext}^1(G, V) \to \mathrm{Hom}(V^\vee, \mathrm{Ext}^1(G, \mathbb{G}_a)).$$

It is an isomorphism (decompose $V \cong \mathbb{G}_a^s$ on both sides to reduce to the trivial case $V = \mathbb{G}_a$). This means that we can reconstruct a vector extension from the classifying map.

Proposition 9.20. *Let G be semi-abelian. Then $\mathrm{Ext}^1(G,\mathbb{G}_a)$ is of dimension g where g is the dimension of the abelian part of G.*

Proof. We consider the decomposition

$$0\to T\to G\to A\to 0$$

of G into its torus and abelian part. This induces a long exact Hom-Ext sequence

$$\begin{aligned}0\to \mathrm{Hom}(A,\mathbb{G}_a)\to \mathrm{Hom}(G,\mathbb{G}_a)\to \mathrm{Hom}(T,\mathbb{G}_a)&\\ \to \mathrm{Ext}^1(A,\mathbb{G}_a)\to \mathrm{Ext}^1(G,\mathbb{G}_a)\to \mathrm{Ext}^1(\mathbb{G}_m,\mathbb{G}_a).&\end{aligned}$$

In the chapter on affine commutative groups, we have seen that $\mathrm{Hom}(T,\mathbb{G}_a)=0$. Part of the structure theorem is the assertion that all affine commutative algebraic groups are direct producs of a torus and a vector group. There are no non-trivial extension. Hence

$$\mathrm{Ext}^1(G,\mathbb{G}_a)\cong \mathrm{Ext}^1(A,\mathbb{G}_a).$$

Any object in $\mathrm{Ext}^1(A,\mathbb{G}_a)$ defines a fibre bundle over A. It is Zariski-locally trivial and can be described by a Čech-cocycle. The same cocycle also defines a class in $H^1(A,\mathcal{O})$. From the Hodge decomposition for $H^1(A^{\mathrm{an}},\mathbb{C})$ we get

$$\dim H^1(A,\mathcal{O})=\frac{1}{2}\dim H^1(A^{\mathrm{an}},\mathbb{C})=g.$$

□

Definition 9.21. Let $G^\natural$ be the vector extension of G with $V=\mathrm{Ext}^1(G,\mathbb{G}_a)^\vee$ and classifying map id. It is called the *universal vector extension.*

Exercise 9.9. *Verify the universal property of $G^\natural$: Given a vector extension*

$$0\to W\to G'\to G\to 0$$

there is a unique morphism $G^\natural\to G'$ compatible with the projection to G.

Chapter 10

1-motives

Let again k be an algebraically closed field of characteristic 0.

Definition 10.1 (Deligne 1974)**.** A 1-*motive* is a complex of length 1

$$[L \xrightarrow{f} G]$$

where G is a semi-abelian varieties, L a free abelian group of finite rank and f a homomorphism of abstract groups. Morphisms of 1-motives are morphisms of complexes. The category of *iso*-1-*motives* is the isogeny category of the category of 1-motives. We denote it $1{-}\mathrm{Mot}_k$.

We think of L as a *lattice*, hence the notation.

Exercise 10.1. *Show that the category* $1{-}\mathrm{Mot}_k$ *is abelian.*

Exercise 10.2. *Show that every object* $M = [L \to G]$ *has a canonical filtration*

$$[0 \to T] \subset [0 \to G] \subset [L \to G]$$

where T *is the torus part of* G*. Compute the associate gradeds.*

Why? Motives are supposed to capture all information obtained in the cohomology of algebraic varieties, for example their periods. 1-motives do this for information in degree 1.

Example 10.2. Let C be a smooth projective curve. We have seen that $H_1(C^{\mathrm{an}}, \mathbb{Q})$ agrees with $H_1(J(C)^{\mathrm{an}}, \mathbb{Q})$. We have to consider the 1-motive

$$[0 \to J(C)].$$

Actually, this generalises to all curves. Smooth curves need semi-abelian varieties. Homology of singular curves can be expressed in terms of homology of the normalisation relative to some points. This relative homology need the lattice part. Even more generally, the first homology of *any* varietiy can be related to homology of a smooth curve relative to a finite number of points.

Deligne came up with the definition because of its relation to *Hodge theory.* He introduced the notion of a mixed Hodge structure and showed that the singular cohomology of an arbitrary algebraic variety over $\mathbb{C}$ carries a canonical Hodge structure.

Theorem 10.3. *[Deligne 1974, Hodge III Constr. 10.1.3] Let $k = \mathbb{C}$. There is an equivalence of categories between the category of* 1*-motives and the category of polarisable mixed Hodge structures with whose only non-zero Hodge numbers are* $(-1,-1), (-1,0), (0,-1), (0,0)$.

We are interested in what 1-motives can say about periods. We are going to define a $\mathbb{Q}$-vector space $V_{\mathrm{sing}}(M)$, a k-vector space $V_{\mathrm{dR}}(M)$ and a *period isomorphism*

$$\phi : V_{\mathrm{sing}}(M) \otimes_{\mathbb{Q}} \mathbb{C} \to V_{\mathrm{dR}}(M) \otimes_k \mathbb{C}.$$

It induces the *period pairing*

$$V_{\mathrm{dR}}^{\vee}(M) \times V_{\mathrm{sing}}(M) \to \mathbb{C}$$

where $V_{\mathrm{dR}}^{\vee}(M)$ is the dual k-vector space of $V_{\mathrm{dR}}(M)$.

Definition 10.4. Let M be a 1-motive. We define the *set $\mathcal{P}(M)$ of periods of M* as the image of the period pairing. We define the *space $\mathcal{P}\langle M\rangle$ of periods of M* as the abelian subgroup of $\mathbb{C}$ generated by $\mathcal{P}(M)$.

Our aim is to describe $\mathcal{P}\langle M\rangle$ in terms of generators and relations.

Exercise 10.3. *Given an example that shows that $\mathcal{P}(M)$ is not a group in general. Show that $\mathcal{P}\langle M\rangle$ is a k-vector space.*

Exercise 10.4. *Let $f : M \to M'$ be an isomorphism in* $1\text{−}\mathrm{Mot}_k$*. Show that $\mathcal{P}\langle M\rangle = \mathcal{P}\langle M'\rangle$.*

The notation is suggested of singular homology and de Rham cohomolgy.

The singular realisation

Let $M = [L \xrightarrow{u} G]$ be a 1-motive. The associated exponential sequence is

$$0 \to H_1^{\mathrm{sing}}(G^{\mathrm{an}}, \mathbb{Z}) \to \mathrm{Lie}(G^{\mathrm{an}}) \xrightarrow{\exp} G^{\mathrm{an}} \to 0.$$

Definition 10.5. Let $T_{\mathrm{sing}}(M)$ be fibre product of L and $\mathrm{Lie}(G^{\mathrm{an}})$ over G^{an} under the structure map $u : L \to G^{\mathrm{an}}$ and the exponential map exp. The vector space $V_{\mathrm{sing}}(M) = T_{\mathrm{sing}}(M) \otimes \mathbb{Q}$ is called the *singular realisation* of M.

By construction, there is a short exact sequence

$$0 \to H_1(G^{\mathrm{an}}, \mathbb{Q}) \to V_{\mathrm{sing}}(M) \to L \otimes \mathbb{Q} \to 0.$$

In particular this gives, $V_{\mathrm{sing}}(M) \cong H_1(G^{\mathrm{an}}, \mathbb{Q})$ if $L = 0$ and $V_{\mathrm{sing}}(M) = L_{\mathbb{Q}}$ if G is trivial.

Exercise 10.5. *Compute* $\dim_{\mathbb{Q}} V_{\mathrm{sing}}(M)$ *in terms of the constitutents of M, i.e., the lattice, the torus and the abelian variety.*

The de Rham realisation

Definition 10.6. Let M be a one-motive over k. We define the *de Rham realisation of* M as

$$V_{\mathrm{dR}}(M) := \mathrm{Lie}(M^\natural)$$

where $M^\natural$ is the vector extension of G corresponding to the classifying map

$$\mathrm{Ext}^1(M, \mathbb{G}_a) \to \mathrm{Ext}^1(G, \mathbb{G}_a)$$

.

In order to understand this definition, we have to look into $\mathrm{Ext}^1(M, \mathbb{G}_a)$. It is defined as Yoneda-Ext in the category $1{-}\mathrm{MOT}_k$ of objects of the form $[L' \to G']$ with a lattice L' and a connected commutative algebraic group G'. We identify $\mathbb{G}_a$ with the object $[0 \to \mathbb{G}_a]$. The short exact sequence

$$0 \to [0 \to G] \to M \to [L \to 0]$$

gives rise to a long exact sequence

$$\mathrm{Hom}(G, \mathbb{G}_a) \to \mathrm{Ext}^1([L \to 0], \mathbb{G}_a) \to \mathrm{Ext}^1(M, \mathbb{G}_a) \to \mathrm{Ext}^1(G, \mathbb{G}_a)$$

The first group vanishes because G is semi-abelian. Consider an object in the second group. It is an extension

$$0 \to [L \to 0] \to [L' \to G'] \to [0 \to \mathbb{G}_a] \to 0.$$

This means $L = L'$ and $G' = \mathbb{G}_a$. The group identfies with $\mathrm{Hom}(L, \mathbb{G}_a)$ (in the category of abelian groups). Finally, we claim that the last map is surjective. Given an extension

$$0 \to \mathbb{G}_a \to G' \to G \to 0$$

we want

$$0 \to [0 \to \mathbb{G}_a] \to [L' \to G'] \to [L \to G] \to 0$$

We use $L' = L$ and any lift of $L \to G$ to G'. This is possible because L is free. In summary:

Lemma 10.7. *The sequence*

$$0 \to \mathrm{Hom}_{ab}(L, \mathbb{G}_a) \to \mathrm{Ext}^1(M, \mathbb{G}_a) \to \mathrm{Ext}^1(G, \mathbb{G}_a) \to 0$$

is exact.

In particular, these are finite dimensional vector spaces, making $M^\natural$ well-defined.

Exercise 10.6. *Show that there is a natural exact sequence*

$$0 \to G^\natural \to M^\natural \to L \otimes_{\mathbb{Z}} k \to 0$$

where $G^\natural$ is the universal vector extension of G of the last chapter.

Note that we have constructed more than just the group $M^\natural$. The same method as in the last chapter gives us a univeral vector extension

$$[L \to M^\natural]$$

of M.

Exercise 10.7. *Make $L \to M^\natural$ explicit in terms of the sequence of the last excercise. Show that its structural map is injective.*

The period isomorphism

In addition, there is a comparison isomorphism $V_{\mathrm{sing}}(M)_{\mathbb{C}} \cong V_{\mathrm{dR}}(M)_{\mathbb{C}}$, the *period isomorphism*, which is constructed as follows:

$$\begin{tikzcd}
L \arrow[r] & M^{\natural,\mathrm{an}} \arrow[r] & G^{\mathrm{an}} \\
& \mathrm{Lie}(M^\natural)_{\mathbb{C}} \arrow[u, "\exp"] \arrow[r] & \mathrm{Lie}(G)_{\mathbb{C}} \arrow[u, "\exp"] \\
& H_1^{\mathrm{sing}}(M^{\natural,\mathrm{an}},\mathbb{Z}) \arrow[u] \arrow[r, "\cong"] & H_1^{\mathrm{sing}}(G^{\mathrm{an}},\mathbb{Z}) \arrow[u]
\end{tikzcd}$$

The map at the bottom is an isomorphism by homotopy invariance because $M^\natural$ is a vector bundle over G. Hence the pull-back $T_{\mathrm{sing}}(M)$ of $L \to G^{\mathrm{an}}$ to $\mathrm{Lie}(G)_{\mathbb{C}}$ agrees with the pull-back

$$T_{\mathrm{sing}}(M) = L \times_{G^{\mathrm{an}}} \mathrm{Lie}(G)_{\mathbb{C}} \cong L \times_{M^{\natural,\mathrm{an}}} \mathrm{Lie}(M^\natural)_{\mathbb{C}}$$

of $L \to M^{\natural,\mathrm{an}}$ to $\mathrm{Lie}(M^\natural)_{\mathbb{C}}$.

Let

$$\phi_M : V_{\mathrm{sing}}(M)_{\mathbb{C}} \to \mathrm{Lie}(M^\natural)_{\mathbb{C}}$$

be the map obtained by this identification of pull-backs.

Lemma 10.8 (Hodge III (10.1.8))**.** *The morphism ϕ_M is an isomorphism.*

Proof. Both the construction of $V_{\mathrm{sing}}()$ and V_{dR} are natural and exact. Hence it suffices to treat the three cases $M = [L \to 0]$ and $M = [0 \to \mathbb{G}_m]$ and $M = [0 \to A]$ (abelian variety, separately.

In the first case, $M^\natural = L_k^\vee$ and and the exponential map is the identity. The period map is the identity as well.

In the second case, $T_{\mathrm{sing}}(M) = 2\pi\mathbb{Z} \subset \mathbb{C}$ and $\mathrm{Lie}(\mathbb{G}_m) = \overline{\mathbb{Q}}$, so they become isomorphic after extension of scalars.

In the case of abelian varieties, $T := T_{\mathrm{sing}}(M)$ has rank $2g$. This agrees with the dimension of $V_{\mathrm{dR}}(M) = \mathrm{Lie}(A^\natural) = 2g$. However, we also have to be careful with the maps. From the complex analytic point of view, T is a discrete subgroup of $\mathrm{Lie}(A)^{\mathrm{an}}$. The map

$$T\otimes\mathbb{C}/T\to\mathrm{Lie}(A)^{\mathrm{an}}\to\mathrm{Lie}(A)^{\mathrm{an}}/T=A^{\mathrm{an}}$$

is a vector extension. Note that $(A^\natural)^{\mathrm{an}}$ is the universal vector extension in the holomorphic category because $H^1(A_\mathbb{C},\mathcal{O})=H^1(A^{\mathrm{an}},\mathcal{O})$. Hence it suffices to show that $T\otimes\mathbb{C}/T$ is the universal vector extension. Given a vector extension

$$H\to A^{\mathrm{an}}$$

the map $T\to\mathrm{Lie}(A)^{\mathrm{an}}$ lifts to $\mathrm{Lie}(H)$ with the same argument as for $A^\natural$. This induces $T\otimes\mathbb{C}\to\mathrm{Lie}(H)\to Lie(H)/T=H$ and hence $T\otimes\mathbb{C}/T\to H$. We have verified the universal property. □

Exercise 10.8. *Express the period pairing in terms of intgegration of invariant differential forms.*

The analytic subgroup theorem for 1-motives

We work over $k=\overline{\mathbb{Q}}$ now.

Theorem 10.9. *Let M be a 1-motive over $\overline{\mathbb{Q}}$, $\omega\in V_{\mathrm{dR}}^\vee(M)$ and $\sigma\in V_{\mathrm{sing}}(M)$ such that $\omega(\sigma)=0$ under the period pairing. Then there is a short exact sequence in $1\mathrm{-Mot}_{\overline{\mathbb{Q}}}$*

$$0\to M_1\xrightarrow{\iota}M\xrightarrow{p}M_2\to0$$

and $\sigma_1\in V_{\mathrm{sing}}(M_1)$, $\omega_2\in V_{\mathrm{dR}}^\vee(M_2)$ with

$$\sigma=\iota_*\sigma_1,\quad \omega=p^*\omega_2.$$

The motive M_2 can chosen such that $p^*V_{\mathrm{dR}}^\vee(M_2)=\mathrm{Ann}(\sigma)$.

Exercise 10.9. *Show the converse: If $\sigma=i_*\sigma_1$ and $\omega=p^*\omega_2$ for a short exact sequence of motives, then $\omega(\sigma)=0$.*

Proof. Let $M=[L\to G]$. Without loss of generality, $\sigma\in T_{\mathrm{sing}}(M)$. We apply the analytic subgroup theorem to the commutative algebraic group $M^\natural$. This yields a short exact sequence

$$0\to H_1\xrightarrow{i}M^\natural\xrightarrow{p}H_2\to0$$

such that $u\in i_*\mathrm{Lie}(H_1)_\mathbb{C}$ and $\omega\in p^*\mathrm{coLie}(H_2)$. We can even achieve

$$p^*\mathrm{coLie}(H_2)=\mathrm{Ann}(\sigma)=\{x\in\mathrm{coLie}(M^\natural)|x(\sigma)=0\}.$$

Note that this annihilator contains only elements defined over $\overline{\mathbb{Q}}$. By ssumption it is non-empty, but we do not know its dimension.

Our aim is to define M_1 and M_2 such that $M_i^\natural = H_i$. Let G_i and V_i be the semi-abelian and vector parts of H_i,

$$L_1 = H_1 \cap L \subset M^\natural$$

and L_2 the free part of L/L_1. This defines an exact sequence of 1-motives up to isogeny

$$0 \to [L_1 \to G_1] \to [L \to G] \to [L_2 \to G] \to 0$$

compatible with the exact sequence in $1{-}\mathrm{MOT}_k$

$$0 \to [L_1 \to H_1] \to [L \to M^\natural] \to [L_2 \to H_2] \to 0.$$

The universal property of the vector extension induces a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & M_1^\natural \arrow[r] \arrow[d] & M^\natural \arrow[r] \arrow[d] & M_2^\natural \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & H_1 \arrow[r] & M^\natural \arrow[r] & H_2 \arrow[r] & 0 \end{tikzcd}$$

The morphism on the left is injective. By definition, $T_{\mathrm{sing}}(M_1)$ is the pull-back of $L_1 \to G$ to $\mathrm{Lie}(M_1^\natural)^{\mathrm{an}}$. On the other hand,

$$\mathrm{Lie}(H_1)_{\mathbb{C}} \cap T_{\mathrm{sing}}(M) = \exp_{H_1}^{-1} L_1.$$

The sequence

$$0 \to \mathrm{Ker}(\exp_{H_1}) \to \exp_{H_1}^{-1}(L_1) \to L_1 \to 0$$

is exact. The first term is $H_1(G_1^{\mathrm{an}}, \mathbb{Z})$ because H_1 is a vector extension of G_1. For $M_1^\natural$, we have the usual sequence

$$0 \to H_1(G_1^{\mathrm{an}}, \mathbb{Z}) \to T_{\mathrm{sing}}(M_1) \to L_1 \to 0.$$

The two are compatible under $M_1^\natural \to H_1$, so we see that

$$T_{\mathrm{sing}}(M_1) = \mathrm{Lie}(H_1)_{\mathbb{C}} \cap T_{\mathrm{sing}}(M).$$

By the choice of H_1, the element σ is on the right hand side, hence in $T_{\mathrm{sing}}(M_1)$.

The morphism $M_2^\natural \to H_2^\natural$ is surjective, hence the induced map

$$\mathrm{coLie}(H_2) \to \mathrm{coLie}(M_2^\natural)$$

is injective. All elements of $p^*\mathrm{coLie}(M_2^\natural)$ annihilate σ, hence

$$p^*\mathrm{coLie}(M_2^\natural) \subset \mathrm{Ann}(\sigma) = p^*\mathrm{coLie}(H_2).$$

This is the converse inclusion, so we have equality. □

Exercise 10.10. *Show that $M \mapsto M^\natural$ is exact and faithful, i.e., injective in morphisms. Is it also full, i.e., surjective on morphisms?*

Chapter 11

The period conjecture for 1-motives

There is a famous and deep conjecture of Grothendieck about the transcendence degree of subfields of $\mathbb{C}$ generated by periods of smooth and projective varieties. It was also generalised to periods of all varieties. The book of André explains this very well.

Algebraic relations between periods can also be interpreted as $\overline{\mathbb{Q}}$-linear relations between periods of product varieties. This alternative point of view was taken by Kontsevich in his formulation of the conjecture. Details and in particular the comparison of the two version can be found in Huber–Müller-Stach. It is proved for periods of curves (or for classes in degree 1 of general varieties) in Huber–Wüstholz.We have mentioned before that such periods appear as periods of 1-motives, so the result can be stated in these terms.

Definition 11.1. Let $\mathcal{P}^1$ the union of the $\mathcal{P}(M)$ for all 1-motives M.

Exercise 11.1. *Verifiy $\mathcal{P}(M_1) + \mathcal{P}(M_2) \subset \mathcal{P}(M_1 \oplus M_2)$. Deduce that $\mathcal{P}^1$ is a $\overline{\mathbb{Q}}$-vector space.*

By definition, elements of $\mathcal{P}^1$ are of the form $\omega(\phi(\sigma)) \in V_{\mathrm{dR}}^\vee(M) \times V_{\mathrm{sing}}(M)$ for varying M. There are two types of obvious relations:

- (bilinearity)

$$(a\omega + b\eta)(\phi(\sigma)) = a\omega(\sigma) + b\eta(\sigma)$$
$$\omega(\phi(c\sigma + d\tau)) = c\omega(\sigma) + d\omega(\tau)$$

  for all $a, b \in \overline{\mathbb{Q}}$, $c, d \in \mathbb{Q}$.

- (functoriality) For $f : M_1 \to M_2$, $\omega_2 \in V_{\mathrm{dR}}^\vee(M_2)$, $\sigma_1 \in V_{\mathrm{sing}}(M_1)$

$$\omega_2(f_*\sigma_1) = (f^*\omega_2)(\sigma_1)$$

The period conjecture claims that all $\overline{\mathbb{Q}}$-linear relations are induced from these.

Theorem 11.2 (Period conjecture)**.** *Let $\tilde{\mathcal{P}}^1$ be the $\mathbb{Q}$-vector space generated by symbolds of the form $(\omega,\sigma)_M$ for $\omega\in V_{\mathrm{dR}}^\vee(M)$, $\sigma\in V_{\mathrm{sing}}(M)$ for varying M with relations spanned by bilinearity and functoriality as above.*

Then the natural map $\tilde{\mathcal{P}}^1\to\mathcal{P}^1$ is bijective.

Exercise 11.2. *Verify that*

$$\begin{aligned}\tilde{\mathcal{P}}^1 &= \bigoplus_M V_{\mathrm{dR}}^\vee(M)\otimes_{\mathbb{Q}} V_{\mathrm{sing}}(M)/\textit{functoriality relations}\\ &\bigoplus_M \mathrm{Hom}_{\mathbb{Q}}(V_{\mathrm{sing}}(M),V_{\mathrm{dR}}(M))^\vee/\textit{functoriality relations}\end{aligned}$$

Make the functoriality relations explicit in both descriptions.

Proof. Let $\sum_{i=1}^n a_i(\omega_i,\sigma_i)_{M_i}$ with $a_i\in\overline{\mathbb{Q}}$ be a linear combination whose image in $\mathbb{C}$ vanishes. We want to show that it vanishes also in $\tilde{\mathcal{P}}^1$. By replacing ω_i by $a_i\omega_i$ we may assume that all a_i are equal to 1. Let

$$M=\bigoplus_{i=1}^n M_i.$$

Let ι_i and π_j be the natural inclusions and projections. They satisfy an orthonormality relation. We put

$$\omega=(\omega_1,\dots,\omega_n),\quad \sigma=(\sigma_1,\dots,\sigma_n).$$

By the bilinearity and functoriality relations

$$(\omega,\sigma)_M=\sum_{i,j}(\pi_i^*\omega_i,\iota_{j*}\sigma_j)_M=\sum_{i,j}(\iota_i^*\pi_{j*}\omega_i,\sigma_j)_{M_j}$$

in $\tilde{\mathcal{P}}$. Moreover, only the summand with $i\neq j$ are non-zero. By assumption

$$\omega(\sigma)=\sum_{i=1}^n\omega_i(\sigma_i)=0.$$

We may apply the analytic subgroup theorem for motives to M and obtain a short exact sequence of motives

$$0\to M_1\xrightarrow{i}M\xrightarrow{p}M_2\to 0$$

such that $\sigma=i_*\sigma_1$, $\omega=p^*\omega_2$. By the functoriality relation

$$(\omega,\sigma)_M=(p^*\omega_2,i_*\sigma_1)_M=(\omega_2,p_*i_*\sigma_1)_{M_2}=\omega_2,0)_{M_2}=0.$$

□

Remark 11.3. Looking more carefully that the relations between the periods of M are induced by bilinearity and functoriality in the subcategory $\langle M\rangle$ generated by M. More precisely: the full abelian subcategory of $1-\mathrm{Mot}_{\overline{\mathbb{Q}}}$ closed under subobjects.

If a period is $\overline{\mathbb{Q}}$-linearly independent of 1, it is transcendental.

Theorem 11.4 (Transcendence)**.** *Let $M = [L \to G]$ be a 1-motive, $\sigma \in V_{\mathrm{sing}}(M)$, and $\omega \in V_{\mathrm{dR}}^{\vee}(M)$. Then the integral*

$$\int_\sigma \omega$$

is in $\overline{\mathbb{Q}}$ if and only if there are $\phi, \psi \in V_{\mathrm{dR}}^{\vee}(M)$ with

$$\omega = \phi + \psi$$

such that $\int_\sigma \psi = 0$ and the image of ϕ in $V_{\mathrm{dR}}^{\vee}(G)$ vanishes.

Idea of proof. See Huber-Wüstholz. Consider $M \oplus [\mathbb{Z} \to 0]$ and apply the analytic subgroup theorem for 1-motives. □

By using the connection between co/homology of curves and 1-motives, this can be translated to differential forms on curves.

Corollary 11.5. *Let C be a smooth projective curve, Let C be a smooth projective curve over $\overline{\mathbb{Q}}$ and ω a meromorphic differential form defined over $\overline{\mathbb{Q}}$. Let $\sigma = \sum_{i=1}^n a_i\gamma_i$ where $\gamma_i : [0,1] \to C$ for $i = 1, \ldots, n$ are differentiable paths avoiding the poles of ω and $a_i \in \mathbb{Z}$. We assume that $\partial\sigma$ has support in $C(\overline{\mathbb{Q}})$.*

In this situation the period

$$\alpha = \int_\sigma \omega.$$

is algebraic if and only if ω is the sum of an exact form with no extra poles and a form with vanishing period.

To conclude, we want to give an explicit new example of a transcendental period. We work on an elliptic curve E over $\overline{\mathbb{Q}}$. Recall the Weierstraß-functions attached to E.

Theorem 11.6. *Let $u \in \mathbb{C}$ be such that $\wp(u) \in \overline{\mathbb{Q}}$ and $\exp_E(u)$ is non-torsion in $E(\overline{\mathbb{Q}})$. Then*

$$u\zeta(u) - 2\log\sigma(u)$$

is transcendental.

Idea of proof. See Huber-Wüstholz. It is possible to write down an explicit differential form on E with simple poles in $P = \exp_E(u)$ and the point at infinity

$$\xi_P = \frac{y + y(P)}{x - x(P)}\frac{dx}{y}.$$

Its pull-back under $\exp_E$ is given very explicity in terms of $\wp$ and $\wp'$. We choose a path from $u/2$ to $-u/2$ and integrate. This does not give quite the number in the theorem, but there is an explicit relation with other periods. We then write down the 1-motive that gives rise to the same periods and use that we understand the relations in this period space. $\square$