Università di Pisa

Finiteness of Multiplicatively Dependent n-tuples of Singular Moduli

Master Thesis
in Mathematics

Candidate
Lorenzo Furio

Advisor
Yuri Bilu
Université de Bordeaux

Co-advisor
Davide Lombardo
Università di Pisa

Academic Year 2020 - 2021

Contents

CHAPTER 1

Introduction

In recent years, Umberto Zannier and Jonathan Pila [PZ08] gave a new proof of the Manin-Mumford conjecture using the theory of o-minimal structures, in particular the theorem of Pila-Wilkie [PW$^+$06]. This has been a breakthrough in the field of unlikely intersections and since its publication, o-minimality continues to be applied to a large number of related problems.

In this thesis we will show how the Pila-Wilkie theorem can be use to prove the finiteness of multiplicatively dependent n-tuples of singular moduli, a result proved by Jonathan Pila and Jacob Tsimerman in 2014 and then published in 2017 [PT17].

We recall that, given the complex upper half-plane $\mathcal{H} := \{z \in \mathbb{C} | \operatorname{Im}(z) > 0\}$, we have the modular function $j : \mathcal{H} \to \mathbb{C}$ which allows us to parametrize the complex elliptic curves up to isomorphism. In particular, given $\tau \in \mathcal{H}$ we can take the lattice $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ and then take the quotient $E = \mathbb{C}/\Lambda$, which is a complex torus. Such a torus is isomorphic to an elliptic curve $y^2 = x^3 + ax + b$ with a point at infinity through the Weierstrass function $\wp$, where $0 \mapsto \infty$ and $z \mapsto (\wp(z), \wp'(z))$. The j-invariant of the curve is defined as $j(E) = 1728\frac{4a^3}{4a^3+27b^2}$ and it can be shown that two elliptic curves have the same j-invariant if and only if they are isomorphic as complex tori. The endomorphism ring $\operatorname{End}(E)$ of an elliptic curve E is either isomorphic to $\mathbb{Z}$ or to an order in a complex quadratic field, so it is a free $\mathbb{Z}$-module of rank 2. In the latter case, we say that the elliptic curve E has complex multiplication and will call it a CM curve. It is not difficult to prove that the elliptic curve E given by the lattice $\mathbb{Z}[\tau]$ has complex multiplication if and only if $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$.

Definition 1.0.1. We define a *singular modulus* as the j-invariant of a CM curve, or equivalently as $j(\tau)$ with $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$.

Definition 1.0.2. We define a *singular-dependent n-tuple* as a n-tuple of distinct singular moduli $(\sigma_1, ..., \sigma_n)$ which are multiplicatively dependent, i.e. there exist $k_1, ..., k_n \in \mathbb{Z}$ not all 0 such that $\prod_{i=1}^{n} \sigma_i^{k_i} = 1$, but no proper subset is multiplicatively dependent.

Remark 1.0.3. The independence of the proper subsets is needed to avoid trivial relations. For example, if there exist $k_1, k_2 \neq 0$ such that $\sigma_1^{k_1}\sigma_2^{k_2} = 1$, then we get $\prod_{i=1}^{n} \sigma_i^{k_i} = 1$ by taking $k_3 = ... = k_n = 0$.

Theorem 1.0.4. *For every $n \in \mathbb{Z}$ there are finitely many singular-dependent n-tuples.*

Theorem 1.0.4 is the main result of the article of Pila and Tsimerman and it is the one that we will prove in this thesis.

At first, in chapter 2, we will introduce some basics that will be needed to deal with the proof of the problem, such as modular curves or the height function.

In chapter 3, we present special varieties and some transcendental results above the exponential function and the j function. In particular, there will be some Ax-Schanuel variants and their corollaries, such as weak complex Ax.

In chapter 4, we define o-minimal structures and we talk about the theorem linking model theory to number theory: the Pila-Wilkie theorem. This will be our main ingredient in the proof of theorem 1.0.4.

In chapter 5, we eventually give the proof of theorem 1.0.4. To prove the finiteness, we will show that if there were infinitely many n-tuples satisfying the condition, then some contradicting inequalities would hold, involving the number of these n-tuples with bounded height. The lower bound can be found studying Galois orbits of the points, while the upper bound is given by the theorem of Pila-Wilkie. Finally, to explicit this contradiction, we will need to apply the Ax-Schanuel results and a technical lemma, which will be proven by considering the graphs of p-adic lattices and their properties.

CHAPTER 2

Preliminaries

2.1 The ring class group

It is known that in number fields the nonzero fractional ideals form an abelian group and that if we quotient it by the principal ideals then we obtain a finite group called the ideal class group. This construction can be generalized for the ideals of the orders whenever the number field considered is a complex quadratic field.

Most of the propositions and properties stated in this section, as well as in most of the sections of this chapter, are given without proof. A proof of these statements can be found in the book of Cox [Cox11].

Definition 2.1.1. Let A be a finite dimensional algebra over $\mathbb{Q}$. An *order* $\mathcal{O}$ in A is a subring which is a free abelian group generated by a $\mathbb{Q}$-basis of A.

In our particular case, this definition works out to the following:

Definition 2.1.2. Let K be a complex quadratic field. An *order* $\mathcal{O}$ in K is a subring which is a finitely generated $\mathbb{Z}$-module of rank 2.

Remark 2.1.3. The ring of integers $\mathcal{O}_K$ is an order in K; moreover, every other order $\mathcal{O}$ in K is a subring of $\mathcal{O}_K$.

As we do for the ring of integers $\mathcal{O}_K$, we can define the fractional ideals of an order $\mathcal{O}$ as the $\mathcal{O}$-submodules of K finitely generated over $\mathcal{O}$. Though fractional ideals in the ring of integers are always invertible, this doesn't happen for orders. Nevertheless, we can restrict to a subset of ideals that are invertible.

Definition 2.1.4. A fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is said to be *invertible* if there exists another fractional ideal $\mathfrak{b}$ of $\mathcal{O}$ such that $\mathfrak{ab} = \mathcal{O}$.

Definition 2.1.5. A fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is said to be *proper* if

$$\{\beta \in K | \beta\mathfrak{a} \subseteq \mathfrak{a}\} = \mathcal{O}$$

Remark 2.1.6. In general, $\mathcal{O} \subsetneq \{\beta \in K | \beta\mathfrak{a} \subseteq \mathfrak{a}\}$, but if $\mathcal{O} = \mathcal{O}_K$ is the ring of integers of K, then equality holds for every fractional ideal.

Proposition 2.1.7. *A fractional ideal $\mathfrak{a}$ is proper if and only if it is invertible.*

This proposition clarifies why all fractional ideals in rings of integers are invertible. Also, it shows that the proper fractional ideals of an order form a group, since there is always an inverse and the product of two of them is still proper: if $\mathfrak{a}, \mathfrak{b}$ are proper, then they are invertible and $\mathfrak{b}^{-1}\mathfrak{a}^{-1}$ is the inverse of $\mathfrak{ab}$, that is therefore invertible and hence proper.

Definition 2.1.8. We will call $\mathcal{F}(\mathcal{O})$ the group of the proper fractional ideals of the order $\mathcal{O}$.

Definition 2.1.9. We will call $\mathcal{P}(\mathcal{O})$ the subgroup of the principal ideals in $\mathcal{F}(\mathcal{O})$.

Remark 2.1.10. $\mathcal{F}(\mathcal{O})$ is an abelian group, so $\mathcal{P}(\mathcal{O})$ is a normal subgroup.

Definition 2.1.11. We define the *ideal class group* as the quotient $Cl(\mathcal{O}) := \frac{\mathcal{F}(\mathcal{O})}{\mathcal{P}(\mathcal{O})}$.

It can be shown that $Cl(\mathcal{O})$ is a finite group. This is widely known when $\mathcal{O} = \mathcal{O}_K$ is the ring of integers of K, but it is still true when $\mathcal{O}$ is a generic order.

Definition 2.1.12. We will call $h_{\mathcal{O}} = |Cl(\mathcal{O})|$ the *class number* of the order $\mathcal{O}$.

If K is a complex quadratic field and $\mathcal{O} \subset K$, we know that $\mathcal{O} \subset \mathcal{O}_K$, moreover, they have the same rank over $\mathbb{Z}$, so we can give the following definition:

Definition 2.1.13. Let K be a complex quadratic field, $\mathcal{O} \subset K$ an order. The integer $f = [\mathcal{O}_K : \mathcal{O}]$ is called the *conductor* of $\mathcal{O}$.

If d_K is the discriminant of K and $w_K = \frac{d_K + \sqrt{d_K}}{2}$, it is known that $\mathcal{O}_K = \mathbb{Z} \oplus w_K\mathbb{Z} = \langle 1, w_K \rangle$.

Proposition 2.1.14. *The only order of conductor f in a quadratic number field K is*

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = \langle 1, fw_K \rangle$$

Proof. By the definition of conductor we have that $f\mathcal{O}_K \subseteq \mathcal{O}$, so $\mathbb{Z} + f\mathcal{O}_K \subseteq \mathcal{O}$. On the other hand, $\mathbb{Z} + f\mathcal{O}_K = \langle 1, fw_K \rangle$ has index f in $\langle 1, w_K \rangle = \mathcal{O}_K$, hence $\mathcal{O} = \langle 1, fw_K \rangle$. □

Definition 2.1.15. Let $\mathcal{O}$ be an order of conductor f, we say that the ideal $\mathfrak{a} \subseteq \mathcal{O}$ is *prime to* f if $\mathfrak{a} + f = \mathcal{O}$.

Lemma 2.1.16. *Let $\mathcal{O}$ be an order of conductor f, then:*

- *$\mathfrak{a} \subseteq \mathcal{O}$ is prime to f if and only if $(f, N(\mathfrak{a})) = 1$.*
- *Every $\mathfrak{a} \subseteq \mathcal{O}$ prime to f is proper.*

Proof. The quotient $\frac{\mathcal{O}}{\mathfrak{a}}$ is a finite abelian group. If we consider the multiplication by f, $m_f : \frac{\mathcal{O}}{\mathfrak{a}} \to \frac{\mathcal{O}}{\mathfrak{a}}$, we have that

$$\mathfrak{a} + f\mathcal{O} = \mathcal{O} \iff m_f \text{ is surjective } \iff m_f \text{ is an isomorphism}$$

But m_f is an isomorphism if and only if f is prime to $\left|\frac{\mathcal{O}}{\mathfrak{a}}\right| = N(\mathfrak{a})$, hence the first point is proved.
To show the second point, let $\beta \in K$ satisfy $\beta\mathfrak{a} \subseteq \mathfrak{a}$: then $\beta \in \mathcal{O}_K$ and

$$\beta\mathcal{O} = \beta(\mathfrak{a} + f\mathcal{O}) \subseteq \mathfrak{a} + f\mathcal{O}_K = \mathcal{O}$$

so $\beta \in \mathcal{O}$, i.e. $\mathfrak{a}$ is proper. □

Corollary 2.1.17. *Let $\mathcal{O}$ be an order of conductor f. The fractional ideals prime to f are invertible and closed by multiplication, hence they form a group $\mathcal{F}(\mathcal{O}, f)$ and the principal ideals prime to f form a subgroup $\mathcal{P}(\mathcal{O}, f)$.*

Proposition 2.1.18. *The inclusion morphism $\mathcal{F}(\mathcal{O}, f) \subseteq \mathcal{F}$ induces an isomorphism*

$$\mathcal{F}(\mathcal{O}, f)\big/\mathcal{P}(\mathcal{O}, f) \cong \mathcal{F}(\mathcal{O})\big/\mathcal{P}(\mathcal{O}) = Cl(\mathcal{O})$$

In addition, it can be shown that the contraction of ideals from $\mathcal{O}_K$ to $\mathcal{O}$ gives an isomorphism $\mathcal{F}_K(f) := \mathcal{F}(\mathcal{O}_K, f) \cong \mathcal{F}(\mathcal{O}, f)$, and through this map $\mathcal{P}(\mathcal{O}, f)$ becomes

$$\mathcal{P}_{K,\mathbb{Z}}(f) := \langle \{\alpha\mathcal{O}_K | \alpha \in \mathcal{O}_K, \exists a \in \mathbb{Z} \text{ such that } \alpha \equiv a \pmod{f\mathcal{O}_K}, (a, f) = 1\} \rangle$$

This implies:

Proposition 2.1.19.

$$Cl(\mathcal{O}) = \mathcal{F}(\mathcal{O})\big/\mathcal{P}(\mathcal{O}) \cong \mathcal{F}(\mathcal{O}, f)\big/\mathcal{P}(\mathcal{O}, f) \cong \mathcal{F}_K(f)\big/\mathcal{P}_{K,\mathbb{Z}}(f)$$

2.2 The height function

The first part of the proof of theorem 1.0.4 will need an upper and lower bound on the number of certain singular moduli; to find these bounds, we will use some arithmetic estimates that involve the height of algebraic numbers. In this section section we are going to define the height function and study some of its properties.

Definition 2.2.1. Let $\alpha = \frac{a}{b} \in \mathbb{Q}$ be a rational number reduced to lowest terms. We define the *height* of α as $\mathrm{H}(\alpha) := \max\{|a|, |b|\}$.

The definition above cannot be generalized to number fields, however one can notice that, if $M_{\mathbb{Q}}$ is the set of the places of $\mathbb{Q}$, it is equivalent to

$$\mathrm{H}(\alpha) = \prod_{\nu \in M_{\mathbb{Q}}} \max\{1, |\alpha|_\nu\}$$

We can then generalize it as follows:

Definition 2.2.2. Let $\alpha \in K$, where $[K : \mathbb{Q}] = n$, let M_K be the set of places of K, let $n_\nu := [K_\nu : \mathbb{Q}_{\bar{\nu}}]$ be the local degree of ν, where $\bar{\nu}$ is the place of $\mathbb{Q}$ lying under ν. We define the *height* of α as

$$\mathrm{H}(\alpha) := \left(\prod_{\nu \in M_K} \max\{1, |\alpha|_\nu\}^{n_\nu} \right)^{\frac{1}{n}}$$

Definition 2.2.3. Let $\alpha \in K$, where $[K : \mathbb{Q}] = n$, let M_K be the set of places of K, let $n_\nu := [K_\nu : \mathbb{Q}_{\bar{\nu}}]$ be the local degree of ν, where $\bar{\nu}$ is the place of $\mathbb{Q}$ lying under ν. We define the *logarithmic height* of α as

$$\mathrm{h}(\alpha) := \log(\mathrm{H}(\alpha)) = \frac{1}{n} \sum_{\nu \in M_K} n_\nu \log(\max\{1, |\alpha|_\nu\})$$

Proposition 2.2.4. *The definition of height and logarithmic height doesn't depend on the choice of the number field containing α. Indeed, if K, L are number fields and $\alpha \in K \cap L$, then*

$$\frac{\sum_{\nu \in M_K} n_\nu \log(\max\{1, |\alpha|_\nu\})}{[K : \mathbb{Q}]} = \frac{\sum_{\mu \in M_L} n_\mu \log(\max\{1, |\alpha|_\mu\})}{[L : \mathbb{Q}]}$$

Proof. We just need to prove that both of the heights are equal to the height computed over $K \cap L$, so we can assume that $K \subseteq L$. Since for every extension L/K we have the equality $\prod_{\mu|\nu} |\alpha|_\mu^{[L_\mu : K_\nu]} = |N_{L/K}(\alpha)|_\nu$, for $\alpha \in K$ we have $\prod_{\mu|\nu} |\alpha|_\mu^{[L_\mu : K_\nu]} = |\alpha|_\nu^{[L:K]}$. It follows that $\prod_{\mu|\nu} \max\{1, |\alpha|_\mu\}^{[L_\mu : K_\nu]} =$

$\max\{1, |\alpha|_\nu\}^{[L:K]}$, because $|\alpha|_\nu > 1$ if and only if $|\alpha|_\mu > 1$ for every $\mu|\nu$. Hence we have

$$\sum_{\mu|\nu} [L_\mu : K_\nu] \log(\max\{1, |\alpha|_\mu\}) = [L : K] \log(\max\{1, |\alpha|_\nu\})$$

So we can compute

$$\begin{aligned} &\frac{\sum_{\nu \in M_K} n_\nu \log(\max\{1, |\alpha|_\nu\})}{[K : \mathbb{Q}]} = \\ =&\frac{\sum_{\nu \in M_K} n_\nu \sum_{\mu|\nu} [L_\mu : K_\nu] \log(\max\{1, |\alpha|_\mu\})}{[K : \mathbb{Q}][L : K]} = \\ =&\frac{\sum_{\mu \in M_L} n_\mu \log(\max\{1, |\alpha|_\mu\})}{[L : \mathbb{Q}]} \end{aligned}$$

which concludes the proof. □

Remark 2.2.5. It is not difficult to notice that $\mathrm{h}(\alpha) \geq 0$ for every $\alpha \in \bar{\mathbb{Q}}$, since it is a sum of positive numbers.

The following proposition lists all the basic properties of the height function.

Proposition 2.2.6. *1. If α and β are conjugate over $\mathbb{Q}$ then $\mathrm{h}(\alpha) = \mathrm{h}(\beta)$.*

2. Let K be a number field, $\alpha, \beta \in K$. If $\beta \neq 0$, then

$$\mathrm{h}\left(\frac{\alpha}{\beta}\right) = \frac{1}{[K : \mathbb{Q}]} \sum_{\nu \in M_K} n_\nu \log(\max\{|\alpha|_\nu, |\beta|_\nu\})$$

3. For every $\alpha_1, ..., \alpha_n \in \bar{\mathbb{Q}}$ we have

$$\mathrm{h}(\alpha_1 \cdot ... \cdot \alpha_n) \leq \mathrm{h}(\alpha_1) + ... + \mathrm{h}(\alpha_n), \quad \mathrm{h}(\alpha_1 + ... + \alpha_n) \leq \mathrm{h}(\alpha_1) + ... + \mathrm{h}(\alpha_n) + \log n$$

4. For every $\alpha \in \bar{\mathbb{Q}}$ and $n \in \mathbb{Z}$ (with $\alpha \neq 0$ if $n < 0$) we have $\mathrm{h}(\alpha^n) = |n| \, \mathrm{h}(\alpha)$.

*5. **Northcott's finiteness theorem:** For any real number $T > 0$ there exists only finitely many $\alpha \in \bar{\mathbb{Q}}$ such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq T$ and $\mathrm{h}(\alpha) \leq T$.*

*6. **Kronecker's first theorem:** $\mathrm{h}(\alpha) = 0$ if and only if $\alpha = 0$ or α is a root of unity.*

*7. **Kronecker's second theorem:** For every integer $d > 0$ there exists $\epsilon(d) > 0$ such that for every $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d$, either $\mathrm{h}(\alpha) = 0$ or $\mathrm{h}(\alpha) \geq \epsilon(d)$.*

Proof. 1. It is known that an isomorphism τ from $\mathbb{Q}(\alpha)$ to $\mathbb{Q}(\beta)$ such that $\tau(\alpha) = \beta$ induces a bijection $\tau_* : M_{\mathbb{Q}(\alpha)} \to M_{\mathbb{Q}(\beta)}$ by $\nu \mapsto \nu \circ \tau^{-1}$, in addition it preserves the local degree $n_\nu = n_{\tau_*\nu}$. Hence, if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}] = n$, we have

$$\begin{aligned}\mathrm{h}(\beta) &= \frac{1}{n} \sum_{\mu \in M_{\mathbb{Q}(\beta)}} n_\mu \log(\max\{1, |\beta|_\mu\}) = \\ &= \frac{1}{n} \sum_{\nu \in M_{\mathbb{Q}(\alpha)}} n_{\tau_*\nu} \log(\max\{1, |\tau^{-1}(\beta)|_{\tau_*\nu}\}) = \\ &= \frac{1}{n} \sum_{\nu \in M_{\mathbb{Q}(\alpha)}} n_\nu \log(\max\{1, |\alpha|_\nu\}) = \mathrm{h}(\alpha)\end{aligned}$$

2. We can notice that $\max\left\{1, \left|\frac{\alpha}{\beta}\right|_\nu\right\} = \frac{1}{|\beta|_\nu} \max\{|\alpha|_\nu, |\beta|_\nu\}$, so

$$\begin{aligned}\mathrm{h}\left(\frac{\alpha}{\beta}\right) &= \frac{1}{[K : \mathbb{Q}]} \sum_{\nu \in M_K} n_\nu \log\left(\max\left\{1, \left|\frac{\alpha}{\beta}\right|_\nu\right\}\right) = \\ &= \frac{1}{[K : \mathbb{Q}]} \sum_{\nu \in M_K} n_\nu \left(\log(\max\{|\alpha|_\nu, |\beta|_\nu\}) - \log(|\beta|_\nu)\right) = \\ &= \frac{1}{[K : \mathbb{Q}]} \sum_{\nu \in M_K} n_\nu \log(\max\{|\alpha|_\nu, |\beta|_\nu\})\end{aligned}$$

where the third equality is due to the fact that for every number field K and $\beta \in K^*$ we have $\prod_{\nu \in M_K} |\beta|_\nu^{n_\nu} = 1$.

3. Let $K = \mathbb{Q}(\alpha_1, ..., \alpha_n)$. For every $\nu \in M_K$ we know that $|\alpha_1 \cdot ... \cdot \alpha_n|_\nu = |\alpha_1|_\nu \cdot ... \cdot |\alpha_n|_\nu$, hence in particular

$$\max\{1, |\alpha_1 \cdot ... \cdot \alpha_n|_\nu\} \leq \max\{1, |\alpha_1|_\nu\} \cdot ... \cdot \max\{1, |\alpha_n|_\nu\}$$

so by taking the logarithms and their weighted sum we get $\mathrm{h}(\alpha_1 \cdot ... \cdot \alpha_n) \leq \mathrm{h}(\alpha_1) + ... + \mathrm{h}(\alpha_n)$.
We know that for non-archimedean absolute values $\nu \in M_K$ we have $|\alpha_1 + ... + \alpha_n|_\nu \leq \max\{|\alpha_1|_\nu, ..., |\alpha_n|_\nu\}$, while archimedean absolute values satisfy the triangular inequality, so

$$|\alpha_1 + ... + \alpha_n|_\nu \leq |\alpha_1|_\nu + ... + |\alpha_n|_\nu \leq n \max\{|\alpha_1|_\nu, ..., |\alpha_n|_\nu\}$$

hence in both cases we can write $|\alpha_1 + ... + \alpha_n|_\nu \leq |n|_\nu \max\{|\alpha_1|_\nu, ..., |\alpha_n|_\nu\}$, and therefore

$$\begin{aligned}\max\{1, |\alpha_1 + ... + \alpha_n|_\nu\} &\leq |n|_\nu \max\{1, |\alpha_1|_\nu, ..., |\alpha_n|_\nu\} \leq \\ &\leq |n|_\nu \max\{1, |\alpha_1|\} \cdot ... \cdot \max\{1, |\alpha_n|\}\end{aligned}$$

By taking the logarithms and their weighted sum we obtain the desired inequality

$$\mathrm{h}(\alpha_1 + ... + \alpha_n) \leq \mathrm{h}(\alpha_1) + ... + \mathrm{h}(\alpha_n) + \mathrm{h}(n) = \mathrm{h}(\alpha_1) + ... + \mathrm{h}(\alpha_n) + \log n$$

4. For $n \geq 0$, since $\max\{1, |\alpha^n|_\nu\} = \max\{1, |\alpha|_\nu\}^n$ for every absolute value $\nu \in M_{\mathbb{Q}(\alpha)}$, taking the logarithms and their weighted sum we easily get $\mathrm{h}(\alpha^n) = n\,\mathrm{h}(\alpha)$. For $n < 0$ we just need to notice that by point 2 we have $\mathrm{h}\left(\frac{1}{\alpha}\right) = \mathrm{h}(\alpha)$ so we can change n to $-n$.

5. Let $\alpha \in \bar{\mathbb{Q}}$ satisfying the hypothesis and let $x^n + a_{n-1}x^{n-1} + ... + a_0$ be its minimal polynomial, with $n \leq T$. The coefficients a_k are given by

$$a_k = \sum_{\substack{\sigma_1,...,\sigma_k \in \mathrm{Gal}\left(\mathbb{Q}(\alpha)/\mathbb{Q}\right) \\ \sigma_i \neq \sigma_j \forall i \neq j}} \sigma_1(\alpha) \cdot ... \cdot \sigma_k(\alpha)$$

so by point 3 we get

$$\mathrm{h}(a_k) \leq \log \binom{n}{k} + \sum_{\substack{\sigma_1,...,\sigma_k \in \mathrm{Gal}\left(\mathbb{Q}(\alpha)/\mathbb{Q}\right) \\ \sigma_i \neq \sigma_j \forall i \neq j}} \mathrm{h}(\sigma_1(\alpha) \cdot ... \cdot \sigma_k(\alpha))$$

For every $\sigma_1, ...\sigma_k$ we have

$$\mathrm{h}(\sigma_1(\alpha) \cdot ... \cdot \sigma_k(\alpha)) \leq \mathrm{h}(\sigma_1(\alpha)) + ... + \mathrm{h}(\sigma_k(\alpha)) = k\,\mathrm{h}(\alpha)$$

hence

$$\mathrm{h}(a_k) \leq \log \binom{n}{k} + \binom{n}{k} k\,\mathrm{h}(\alpha) \leq n \log n + n^n kT \leq T \log T + T^{T+2}$$

In particular, the coefficients have bounded height, hence we can assume only finitely many values, so there are only finitely many polynomials of which α can be a root, and therefore only finitely many possible α.

6. It is easy to see that 0 and the roots of unity have height equal to 0, so we just need to prove the converse statement. Given $\alpha \in \bar{\mathbb{Q}}$ such that $\mathrm{h}(\alpha) = 0$, by point 4 we know that all the powers of α have height equal to 0. Moreover, their degree is bounded by $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. By Northcott's theorem, we know that only finitely many powers of α can be distinct, hence there exist integers $n > m$ such that $\alpha^n = \alpha^m$, which is what we wanted to prove.

7. Let us consider all the algebraic numbers with degree bounded by d and height bounded by 1. By Northcott's theorem, there are only finitely many of them, so there exists one among them with the minimum height, hence we just need to take its height as $\epsilon(d)$.

□

We now give some inequalities involving the height of singular moduli. If σ is a singular modulus, we will call $\mathcal{O}_\sigma$ the associated quadratic order[1] and Δ_σ its discriminant.

Proposition 2.2.7. *Let $\epsilon > 0$, there is a constant $c(\epsilon)$ such that for every singular modulus σ we have*

$$\mathrm{h}(\sigma) \leq c(\epsilon)|\Delta_\sigma|^\epsilon$$

A proof of this proposition can be found in [HP12, lemma 4.3]
There is also a similar explicit bound on the multiplicative height of the preimage of a singular modulus.

Proposition 2.2.8. *Let τ be a quadratic number in the fundamental domain of the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$ and let $\sigma = j(\tau)$ be the corrispondent singular modulus. The inequality*

$$\mathrm{H}(\tau) \leq 2|\Delta_\sigma|$$

holds.

This proposition is a special case of [Pil11, proposition 5.7], where the reader may find a proof.

For later use, we also want to give some bounds for the degree over $\mathbb{Q}$ of the singular moduli. The next proposition will be helpful for this aim.

Proposition 2.2.9. *Let $[\mathbb{Q}(\sigma) : \mathbb{Q}] = |Cl(\mathcal{O}_\sigma)|$ for a singular modulus σ and let $\epsilon > 0$. There exist two constants $c(\epsilon), C(\epsilon) > 0$ such that for every σ*

$$c(\epsilon)|\Delta_\sigma|^{\frac{1}{2}-\epsilon} \leq |Cl(\mathcal{O}_\sigma)| \leq C(\epsilon)|\Delta_\sigma|^{\frac{1}{2}+\epsilon}$$

The first inequality is known as Landau-Siegel; the second inequality can be found in [Pau14, proposition 2.2].

Finally, we give an estimate on the exponents of a multiplicative dependence relation in terms of the bases.

Proposition 2.2.10. *Let $n \geq 1$, let K be a number field of degree $d \geq 2$, let $\alpha_1, ..., \alpha_n \in K$ and $b_1, ..., b_n \in \mathbb{Z}$ not all 0 such that $\alpha_1^{b_1} \cdot ... \cdot \alpha_n^{b_n} = 1$, but every proper subset of $\alpha_1, ..., \alpha_n$ is multiplicatively independent, then for every $1 \leq i \leq n$*

$$|b_i| \leq 58\frac{(n-1)!e^{n-1}}{(n-1)^{n-1}}d^n(\log d)\prod_{j\neq i}\mathrm{h}(\alpha_j)$$

[1] An explicit description of what we mean by that is given at the end of this chapter

This can be found in [LM04, corollary 3.2].

2.3 Modular curves

We now want to introduce the modular curves $X_0(N)$, fundamental for the definition of a special variety.

Definition 2.3.1. Let N be a positive integer, we define the congrunece subgroup $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ as

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| c \equiv 0(N) \right\}$$

For $N = 1$ we notice that $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$ and we may want to find a description for the cosets of $\Gamma_0(N)$ in $\Gamma_0(1)$.

Remark 2.3.2. If $\sigma_0 = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$ we can notice that

$$\Gamma_0(N) = (\sigma_0^{-1} \mathrm{SL}_2(\mathbb{Z})\sigma_0) \cap \mathrm{SL}_2(\mathbb{Z})$$

Proposition 2.3.3. *Given the set of matrices with integer coefficients*

$$C(N) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| ad = N, 0 \leq b < d, (a, b, d) = 1 \right\}$$

there is a bijection between $C(N)$ and the right cosets of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$ given by

$$\sigma \mapsto (\sigma_0^{-1} \mathrm{SL}_2(\mathbb{Z})\sigma) \cap \mathrm{SL}_2(\mathbb{Z})$$

Corollary 2.3.4. $[\Gamma_0(1) : \Gamma_0(N)] = |C(N)| = N \prod_{p|N} \left(1 + \frac{1}{p}\right)$

While the modular curve $Y_0(N) := {}^{\mathcal{H}}\!/_{\Gamma_0(N)}$ is not compact, it can be shown that, if $\mathcal{H}^* = \mathcal{H} \cup \{\infty\} \cup \mathbb{Q}$, the quotient $X_0(N) := {}^{\mathcal{H}^*}\!/_{\Gamma_0(N)}$ is a compact Riemann surface. If we consider $N = 1$, $\{\infty\}$ and $\mathbb{Q}$ form a unique class in the quotient $X_0(1)$, identified with the point ∞. It can be shown that the j-invariant gives a biolomorphism $j : X_0(1) \to \mathbb{P}^1(\mathbb{C})$ such that $j(\infty) = \infty$; in particular, j is holomorphic on $\mathcal{H}$ and $\mathrm{SL}_2(\mathbb{Z})$-invariant. To express the holomorphicity condition at infinity, we can use the following expansion:

Proposition 2.3.5. *Let $z \in \mathcal{H}$ and $q = e^{2\pi i z}$. The j function admits the Fourier expansion*

$$j(z) = \frac{1}{q} + 744 + 196884q + ... = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n$$

where the c_n are integers for all $n \in \mathbb{N}$.

Remark 2.3.6. The expansion above is well defined, because the matrix $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ belongs to $\mathrm{SL}_2(\mathbb{Z})$, so $j(z+1) = j(\gamma z) = j(z)$ and there is a factorization of j through the map $q = e^{2\pi i z}$.

The map q sends $\infty \mapsto 0$, defining an expansion of j around ∞. In particular, every function $\mathrm{SL}_2(\mathbb{Z})$-invariant has a factorization through q, so we can consider such a function to be holomorphic at ∞ if its Laurent series in q is holomorphic. In a similar way, we can define functions meromorphic at ∞ and define their order.

We now want to extend this argument to all the groups $\Gamma_0(N)$. First of all, since $[\Gamma_0(1) : \Gamma_0(N)] < +\infty$, if $\pi : X_0(N) \to X_0(1)$ is the projection, there are a finite number of elements $x \in X_0(N)$ such that $\pi(x) = \infty$; these elements will be called *cusps*. If $x \in X_0(N)$ is a cusp, then $\{\gamma x | \gamma \in \Gamma_0(1)\}$ is the set of the cusps of $X_0(N)$. As we noticed for $\Gamma_0(1)$, the element $\gamma = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$ is such that for every $\delta \in \Gamma_0(1)$ one can verify that $\delta^{-1}\gamma\delta \in \Gamma_0(N)$. Moreover, if a function $f : \mathcal{H} \to \mathbb{C}$ is $\Gamma_0(N)$-invariant, we can see that $f(z+N) = f(\gamma z) = f(z)$ and for every $\delta \in \Gamma_0(1)$, $(f \circ \delta)(z+N) = f(\delta(z+N)) = f(\delta\gamma z) = f((\delta\gamma\delta^{-1})(\delta z)) = f(\delta z)$, hence every $f \circ \delta$ is invariant for the translation by N. This means that every function $f \circ \delta$ factors through the map $q_N = e^{\frac{2\pi i z}{N}}$, so that we can define an expansion of f around every cusp. We can now give the following definition:

Definition 2.3.7. A function $f : \mathcal{H} \to \mathbb{C}$ is said to be a *weakly modular form of weight* 0 *for the group* $\Gamma_0(N)$ if it is $\Gamma_0(N)$-invariant and meromorphic on $\mathcal{H}$ and at the cusps.

Proposition 2.3.8. *$j(Nz)$ is a weakly modular form of weight* 0 *for* $\Gamma_0(N)$.

Proof. If $\sigma_0 = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$, we can write $j(Nz) = j(\sigma_0 z)$. If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, we can compute

$$\sigma_0\gamma\sigma_0^{-1} = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} N^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & Nb \\ \frac{c}{N} & d \end{pmatrix} = \gamma'$$

Hence $\sigma_0\gamma = \gamma'\sigma_0$, and thus $j(N\gamma z) = j(\sigma_0\gamma z) = j(\gamma'\sigma_0 z) = j(\gamma'(Nz))$. Then if $\gamma \in \Gamma_0(N)$ we have that $\gamma' \in \Gamma_0(1)$, so $j(N\gamma z) = j(Nz)$, hence $j(Nz)$ is $\Gamma_0(N)$-invariant.
$j(Nz)$ is holomorphic on $\mathcal{H}$ because $N\mathcal{H} = \mathcal{H}$ and $j(z)$ is holomorphic. So we just need to prove that it is meromorphic at the cusps. Let $\gamma \in \Gamma_0(1)$;

by proposition 2.3.3 there exists $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(N)$ such that $j(N\gamma z) = j(\sigma_0 \gamma z) = j(\sigma z)$, then we have $q(\sigma z) = e^{\sigma z} = e^{2\pi i \frac{az+b}{d}} = \zeta_d^b q^{\frac{a}{d}} = \zeta_N^{ab} q_N^{a^2}$. Hence

$$j(N\gamma z) = \frac{\zeta_N^{-ab}}{q_N^{a^2}} + \sum_{n=0}^{\infty} c_n \zeta_N^{nab} q_N^{na^2}$$

which completes the proof. □

Proposition 2.3.9. *Every weakly modular form f of weight 0 for $\Gamma_0(1)$ is a rational function of $j(z)$. Moreover, if it is holomorphic on $\mathcal{H}$, it is a polynomial of $j(z)$.*

Proof. First of all, we notice that if f is holomorphic on $\mathcal{H}$ and at ∞, then it is constant, because it is holomorphic on $X_0(1) \cong \mathbb{P}^1(\mathbb{C})$. So, let us consider the case in which f is holomorphic on $\mathcal{H}$ with a pole at ∞. Write $f = \sum_{n=-k}^{\infty} c_n q^n$, where $k > 0$, and notice that there exists a polynomial $P(x)$ such that $f - P(j)$ is holomorphic at ∞. To see this, it is sufficient to notice that $f - c_{-k} j^k = \sum_{n=-k+1}^{\infty} c'_n q^n$, so we can iterate the argument k times. Hence $f - P(j) = d$ is constant, so $f = P(j) + d$. If f is meromorphic, then it has a finite number of poles, because it is meromorphic on $X_0(1) = \mathbb{P}^1(\mathbb{C})$, which is compact. We know that j is surjective, so for every $w \in \mathcal{H}$ there exists $c_w \in \mathbb{C}$ such that $j(z) - c_w$ is holomorphic on $\mathcal{H}$, has a unique simple pole at ∞ and vanishes at w. Then w is a simple zero, because $\sum_{z \in \mathbb{P}^1(\mathbb{C})} \operatorname{ord}_z(j - c) = 0$. Hence if w is a pole of f of order r_w, the function $f(z)(j(z) - c_w)^{r_w}$ has no pole at w, in particular the function $f(z) \prod_{w \text{ pole of } f} (j(z) - c_w)^{r_w}$ is a weakly modular form holomorphic on $\mathcal{H}$, so it is a polynomial of j. This proves that f is a rational function of j. □

We can now define the following polynomial

$$\Phi_N(x, j) := \prod_{\sigma \in C(N)} (x - j(\sigma z)) = \prod_{i=1}^{|C(N)|} (x - j(N\gamma_i z))$$

We can notice that applying an element $\gamma \in \Gamma_0(1)$ to the coefficients of the polynomial $\Phi_N(x, j)$, we just have a permutation of the $j(N\gamma_i z)$, hence, as they are symmetric functions of the roots, they are invariant under $\Gamma_0(1)$. Moreover, the coefficients are holomorphic on $\mathcal{H}$, because they are polynomials of holomorphic functions. So, by the previous proposition, they are polynomials of $j(z)$, thus we can see $\Phi_N(x, j)$ as a polynomial in two variables $\Phi_N(x, y)$ evalued in $y = j(z)$.

Definition 2.3.10. Given the polynomial defined above, the equation $\Phi_N(x, y) = 0$ is called the *modular equation.*

In this thesis we will often refer to a modular curve as a modular equation for some N.

Proposition 2.3.11. *Let N be a positive integer, then*

- $\Phi_N(x, y) \in \mathbb{Z}[x, y]$.
- $\Phi_N(x, y)$ *is irreducible.*
- *If $N > 1$ then $\Phi_N(x, y) = \Phi_N(y, x)$.*
- *If N is not a perfect square,* $\deg \Phi_N(x, x) > 1$ *and its leading coefficient is ± 1.*
- *If $N = p$ is prime, then $\Phi_N(x, y) \equiv (x^p - y)(x - y^p)$ $(mod\ p)$.*

2.4 Ring class fields and the j-invariant

Definition 2.4.1. An extension of number fields L/K, is called *abelian* if it is a Galois extension and $\mathrm{Gal}\left(L/K\right)$ is an abelian group.

Definition 2.4.2. An extension of number fields L/K, is called *unramified* if every prime $P \in \mathcal{O}_K$ is unramified in $\mathcal{O}_L$.

Theorem 2.4.3. *Let K be a number field, then there exists a maximal abelian unramified extension L/K.*

Definition 2.4.4. The extension L of the previous theorem is called the *Hilbert class field* of K.

In this section we are going to describe the connections between the Hilbert class field, the class group and the j invariant.

Lemma 2.4.5. *Let L/K be a Galois extension, let $P \subset \mathcal{O}_K$ be a prime and $Q \subset \mathcal{O}_L$ an unramified prime containing P. There is a unique $\sigma_Q \in \mathrm{Gal}\left(L/K\right)$ such that $\sigma_Q(\alpha) \equiv \alpha^{N(P)} (mod\ Q)$ for every $\alpha \in \mathcal{O}_L$.*

Proof. Since P is unramified, the inertia group $E(Q|P)$ is trivial, then the decomposition group is $D(Q|P) \cong \mathrm{Gal}\left(\frac{\mathcal{O}_L}{Q} \Big/ \frac{\mathcal{O}_K}{P}\right)$, which is cyclic generated by the Frobenius element $\bar{\sigma}(x) = x^{N(P)}$, which is the desired element. □

Remark 2.4.6. It is not difficult to notice that σ_Q as in the previous lemma has the following properties:

- If $\tau \in \mathrm{Gal}\left(L/K\right)$ then $\tau\sigma_Q\tau^{-1} = \sigma_{\tau(Q)}$.
- The order of σ_Q is the inertia degree $f(Q|P)$, since it is the cardinality of the decomposition group.
- P splits completely in L if and only if $\sigma_Q = id$, i.e. if and only if the decomposition group is trivial.

Definition 2.4.7. Let L/K be an unramified abelian extension and $P \subset \mathcal{O}_K$ be a prime. We define the *Artin symbol* $\left(\frac{L/K}{P}\right)$ as the automorphism σ_Q of a prime $Q \subset \mathcal{O}_L$ above P.

Remark 2.4.8. The Artin symbol is well defined, because if $Q, Q' \subset \mathcal{O}_L$ are two different primes above P we know that there exists $\tau \in \mathrm{Gal}\left(L/K\right)$ such that $\tau(Q) = Q'$, so $\sigma_{Q'} = \tau\sigma_Q\tau^{-1} = \sigma_Q$, where the last equality holds because L/K is abelian.

By unique factorization of ideals, we can extend the definition of the Artin symbol to all fractional ideals.

Definition 2.4.9. Let L/K be an unramified abelian extension and $\mathfrak{a} \subset K$ a fractional ideal. The *Artin symbol* of $\mathfrak{a} = \prod P_i^{r_i}$ si

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{P_i|\mathfrak{a}} \left(\frac{L/K}{P_i}\right)^{r_i}$$

This definition allows us to define a map from fractional ideals to the Galois group, whose importance lies in the following theorem:

Theorem 2.4.10. *Let K be a number field and L its Hilbert class field. The Artin map*

$$\left(\frac{L/K}{\cdot}\right) : \mathcal{F}(K) \to \mathrm{Gal}\left(L/K\right)$$

is surjective and its kernel is $\mathcal{P}(K)$, hence there is an isomorphism

$$Cl(\mathcal{O}_K) \cong \mathrm{Gal}\left(L/K\right)$$

Corollary 2.4.11. *Let K be a number field, L its Hilbert class field and h_K the class number of K, then $h_K = [L : K]$.*

Let K be a complex quadratic field, we now want to find a similar statement for a generic order $\mathcal{O} \subset K$. The main problem is that the conductor might not allow to find a proper unramified extension. However, thanks to proposition 2.1.19, a generalization of the Artin map can be defined, leading to the following theorem:

Theorem 2.4.12. *Let $\mathcal{O}$ be an order of K of conductor f. There exists a unique abelian extension L/K such that all primes of K ramified in L divide f and there is an isomorphism*

$$Cl(\mathcal{O}) \cong \mathcal{F}_K(f)/\mathcal{P}_{K,\mathbb{Z}}(f) \cong \mathrm{Gal}\left(L/K\right)$$

Definition 2.4.13. The unique field given by the previous theorem is called the *ring class field* of $\mathcal{O}$.

Corollary 2.4.14. *Let $\mathcal{O} \subset K$ be an order in a complex quadratic field and $L \supset K$ be its ring class field, we have $[L : K] = h_{\mathcal{O}}$.*

Class field theory is linked to the j-invariant thanks to the following theorem:

Theorem 2.4.15. *Let $\mathcal{O}$ be an order in a quadratic imaginary field K and let $\mathfrak{a}$ be a proper fractional ideal of $\mathcal{O}$. The j invariant $j(\mathfrak{a})$ is an algebraic integer and $K(j(\mathfrak{a}))$ is the ring class field of $\mathcal{O}$.*

The j-invariant of every proper ideal in a quadratic order is a singular modulus. Conversely, every singular modulus σ comes from a proper ideal in a quadratic order, indeed, if $\sigma = j(\tau)$ with $\tau \in K$, let $ax^2 + bx + c \in \mathbb{Z}[x]$ be a polynomial with τ as a root and $(a, b, c) = 1$, then $a\tau \in \mathcal{O}_K$, because $0 = a(a\tau^2 + b\tau + c) = (a\tau)^2 + b(a\tau) + ac$, so $j(\tau) = j(\langle 1, \tau\rangle) = j(\langle a, a\tau\rangle)$ and $\mathfrak{a} = \langle a, a\tau\rangle$ is a proper ideal in the order $\mathcal{O} = \{\alpha \in K | \alpha\mathfrak{a} \subseteq \mathfrak{a}\} = \langle 1, a\tau\rangle$. This is the order $\mathcal{O}_\sigma$ associated to the singular modulus σ.

Corollary 2.4.16. *Every singular modulus σ is an algebraic integer and $[K(\sigma) : K] = |Cl(\mathcal{O}_\sigma)|$.*

CHAPTER 3

Special varieties and Ax-Schanuel

In this chapter we are going to introduce the idea of special variety, where "special" depends on the context; in particular we will treat the case of the modular curves and the case of the multiplicative groups.

The concept of special variety is similar to that of torsion subvariety considered in the Manin-Mumford conjecture.

Definition 3.0.1. Let A be an abelian variety over a field K. $B \subseteq A$ is a *torsion subvariety* if it is a translate of an abelian subvariety by a torsion point, i.e. there exists a torsion point $b \in A$ and an abelian subvariety $B_0 \in A$ such that $B = b + B_0$.

If $X \subseteq A$ is an algebraic variety, we can consider the torsion subvarieties of X to be ordered by inclusion. Then, a maximal torsion subvariety is a torsion subvariety that is not contained in any other torsion subvariety of X.

Theorem 3.0.2 (Manin-Mumford conjecture)**.** *Let A be an abelian variety, $X \subseteq A$ an algebraic variety, then X admits only finitely many maximal torsion subvarieties.*

This conjecture was proved by Michel Raynaud in 1983 [Ray83]. The André-Oort conjecture generalizes it by introducing special varieties.

3.1 Special varieties

Special varieties can be introduced in a general context, but we will restrict to the case of subvarieties of $\mathbb{C}^n$ both because they are easier to study and because it will be sufficient for our treatment.

We will identify the points of the modular curve $Y_0(1)(\mathbb{C})$ with $\mathbb{C}$ and the multiplicative group $\mathbb{G}_m(\mathbb{C})$ with $\mathbb{C}^*$

Definition 3.1.1. A *weakly special subvariety* of X is a subvariety of the following form:

- $\mathbf{X = \mathbb{C}^n}$: let $n_0, ..., n_k \subseteq \{1, 2, ..., n\}$ be a partition, then $M = M_0 \times M_1 \times ... \times M_k$ is the sought subvariety, where M_0 is a point in $\mathbb{C}^{n_0}$ and M_i is a modular curve in $\mathbb{C}^{n_i}$ for $i \geq 1$ ($\mathbb{C}^{n_i}$ is the product of the coordinates contained in n_i). Alternatively, M is given by a system of equations of the form: $x_i = c$ for some $c \in \mathbb{C}$, or a modular equation $\Phi_N(x_i, x_j) = 0$ for some i, j and $N \in \mathbb{N}$ (with any two of them not lying in the same plane).

- $\mathbf{X = (\mathbb{C}^*)^n}$: a subvariety T defined by a finite system of equations $\prod_{i=1}^{n} x_i^{a_{ij}} = \xi_j$ with $a_{ij} \in \mathbb{Z}$ not all 0 for every $j = 1, ..., k$.

- $\mathbf{X = \mathbb{C}^n \times (\mathbb{C}^*)^m}$: a product of two weakly special subvarieties $M \times T$, with $M \subseteq \mathbb{C}^n$ and $T \subseteq (\mathbb{C}^*)^m$.

Definition 3.1.2. A *special point* of X is a point of the following form:

- $\mathbf{X = \mathbb{C}^n}$: a point such that each coordinate is a singular modulus.

- $\mathbf{X = (\mathbb{C}^*)^n}$: a torsion point, i.e. a point such that each coordinate is a root of unity.

- $\mathbf{X = \mathbb{C}^n \times (\mathbb{C}^*)^m}$: a point such that its projections on $\mathbb{C}^n$ and $(\mathbb{C}^*)^m$ are special points.

Definition 3.1.3. A *special subvariety* of X is a subvariety of the following form:

- $\mathbf{X = \mathbb{C}^n}$: a weakly special subvariety such that $n_0 = \emptyset$ or M_0 is a special point. Alternatively, a subvariety defined by a system of equations of the form: $x_i = c$ with c singular modulus, or a modular equation $\Phi_N(x_i, x_j) = 0$ for some i, j and $N \in \mathbb{N}$ (with any two of them not lying in the same plane).

- $\mathbf{X = (\mathbb{C}^*)^n}$: a weakly special subvariety such that ξ_j is a root of unity for every j.

- $\mathbf{X = \mathbb{C}^n \times (\mathbb{C}^*)^m}$: a product of two special subvarieties $M \times T$, with $M \subseteq \mathbb{C}^n$ and $T \subseteq (\mathbb{C}^*)^m$.

Theorem 3.1.4 (André-Oort conjecture)**.** *Every subvariety of $\mathbb{C}^n$ has finitely many maximal special subvarieties.*

This conjecture was proved by Jonathan Pila in 2011 [Pil11], while for the general case of Shimura varieties Pila, Tsimerman and others published a preprint of a possible solution in Semptember 2021 [PST$^+$21]. The André-Oort conjecture has a further generalization, which is the Zilber-Pink conjecture. Let us call $X = \mathbb{C}^n \times (\mathbb{C}^*)^m$.

Definition 3.1.5. Let $W \subseteq X$ be a subvariety. A subvariety $A \subseteq W$ is called an *atypical component* of W in X if there exists a special subvariety $T \subseteq X$ such that $A \subseteq W \cap T$ and $\dim A > \dim W + \dim T - \dim X$.

Example 3.1.6. Every proper special subvariety of X is an atypical component of itself in X, indeed if $T \subset X$ is special, $T \subseteq T$ and $\dim T > 2\dim T - \dim X$ since $\dim X > \dim T$.

Conjecture 3.1.7 (Zilber-Pink)**.** *Let $W \subseteq X$ be a subvariety. There are only finitely many maximal atypical components of W in X.*

3.2 Ax-Schanuel and the j function

We now want to give some Ax-Schanuel results in the mixed modular-multiplicative setting we are working in. To explain what we mean, let us first consider the following:

Conjecture 3.2.1 (Schanuel)**.** *Let $z_1, ..., z_n \in \mathbb{C}$ be linearly independent over $\mathbb{Q}$, then the field $\mathbb{Q}(z_1, ..., z_n, e^{z_1}, ..., e^{z_n})$ has transcendence degree at least n over $\mathbb{Q}$.*

Even if this conjecture is far from being proved, there are different results that prove special or analogous cases. For example, the Lindemann-Weierstrass theorem is a special case of Schanuel's conjecture which only considers algebraic numbers.

Theorem 3.2.2 (Lindemann-Weierstrass)**.** *Let $z_1, ..., z_n \in \bar{\mathbb{Q}}$ be linearly independent over $\mathbb{Q}$, then $e^{z_1}, ..., e^{z_n}$ are algebraically independent over $\mathbb{Q}$.*

A statement analogous to the Schanuel conjecture for power series, was proved by James Ax in 1971 [Ax71]. This theorem is commonly known as Ax-Schanuel and is the following:

Theorem 3.2.3 (Ax-Schanuel)**.** *Let $f_1, ..., f_n \in \mathbb{C}[[z_1, ..., z_m]]$ be linearly independent over $\mathbb{Q}$ modulo $\mathbb{C}$, i.e. $f_1 - f_1(0), ..., f_n - f_n(0)$ are linearly independent over $\mathbb{Q}$, then*

$$\operatorname{trdeg}_{\mathbb{Q}} \mathbb{Q}(f_1, ..., f_n, e^{f_1}, ..., e^{f_n}) \geq n + \operatorname{rank} \left(\frac{\partial f_i}{\partial z_j} \right)_{i,j}$$

If we consider the special case in which $m = 1$ and $f_i(0) = 0$ for every i, we get another conjecture of Schanuel, similar to the original one.

Theorem 3.2.4. *Let $f_1, ..., f_n \in \mathbb{C}[[z]]$ be linearly independent over $\mathbb{Q}$ and without constant terms, then*

$$\operatorname{trdeg}_{\mathbb{C}(z)} \mathbb{C}(z)(f_1, ..., f_n, e^{f_1}, ..., e^{f_n}) \geq n$$

Remark 3.2.5. Given a power series $f \in \mathbb{C}[[z]]$, if the constant term is equal to 0, then the function e^f is well defined as $\sum_{i=0}^{\infty} \frac{f^i}{i!}$. Indeed, f^i contains only terms of degree at least i, so e^f is a power series in which every term is a finite sum of the terms of the power series f^i.

For our purposes, we want to give a geometric implication of this theorem. This has been observed by Tsimerman in his work [Tsi15] proving Ax-Schanuel through o-minimality.

Let us consider the exponential map $\exp : \mathbb{C}^n \to (\mathbb{C}^*)^n$ such that $\exp(z_1, ..., z_n) = (e^{z_1}, ..., e^{z_n})$, then let us define the set $D_n := \{(\mathbf{x}, \mathbf{y}) \in \mathbb{C}^n \times (\mathbb{C}^*)^n | \mathbf{y} = \exp(\mathbf{x})\}$, which is the graph of exp, and define the projections π_a, π_m from $\mathbb{C}^n \times (\mathbb{C}^*)^n$ respectively to $\mathbb{C}^n$ and $(\mathbb{C}^*)^n$.

Theorem 3.2.6. *Let $U \subseteq D_n$ be an irreducible complex analytic subspace such that $\pi_m(U)$ does not lie in a weakly special subvariety of $(\mathbb{C}^*)^n$, then*

$$\dim U^{zar} \geq \dim U + n$$

where U^{zar} denotes the Zariski closure of U in $\mathbb{C}^n \times (\mathbb{C}^*)^n$.

Proof. Since U is an analytic space (and lies in D_n), there is an open set $B \subseteq \mathbb{C}^n$ and an analytic function $f : B \to \mathbb{C}^n$ such that $U = (f, \exp \circ f)(B)$. One can verify that

$$\dim U = \operatorname{rank} \left(\frac{\partial f_i}{\partial z_j} \right)_{i,j}$$

and

$$\dim U^{zar} = \operatorname{trdeg}_{\mathbb{C}} \mathbb{C}(f_1, ..., f_n, e^{f_1}, ..., e^{f_n})$$

If we menage to prove that $f_1, .., f_n$ are linearly independent over $\mathbb{Q}$ modulo $\mathbb{C}$, we can apply Ax-Schanuel (since analytic functions are power series) and complete the proof. However, $f_1, .., f_n$ are linearly independent modulo $\mathbb{C}$ if and only if $e^{f_1}, ..., e^{f_n}$ are multiplicatively independent modulo $\mathbb{C}$, that means that they don't satisfy any relation of the form $x_1^{a_1} \cdot ... \cdot x_n^{a_n} = \xi$. In particular, we can conclude that $f_1, .., f_n$ are linearly independent over $\mathbb{Q}$ modulo $\mathbb{C}$ if and only if $(e^{f_1}, ..., e^{f_n})$ doesn't lie in any weakly special subvariety of $(\mathbb{C}^*)^n$, that follows from the hypothesis. □

Corollary 3.2.7. *Let $V \subseteq C^n \times (\mathbb{C}^*)^n$ be an irreducible subvariety, let U be a connected irreducible component of $V \cap D_n$, assume that $\pi_m(U)$ is not contained in a weakly special subvariety of $(\mathbb{C}^*)^n$, then*

$$\dim V \geq \dim U + n$$

In recent years, Pila and Tsimerman proved a modular version of Ax-Schanuel [PT+16], an equivalent theorem obtained replacing exp with j. We now give the setting to state the theorem. Let us consider $\mathcal{H}$ as an open subset of $\mathbb{P}^1(\mathbb{C})$ and let us define $j : \mathcal{H}^n \to \mathbb{C}^n$ as the product of j on every component. Let $\Gamma \subset \mathbb{P}^1(\mathbb{C})^n \times \mathbb{C}^n$ be the graph of j, then we have the following:

Theorem 3.2.8. *Let $V \subseteq \mathbb{P}^1(\mathbb{C})^n \times \mathbb{C}^n$ be an algebraic subvariety, and let U be an irreducible component of $V \cap \Gamma$. If the projection of U to $\mathbb{C}^n$ is not contained in a proper weakly special subvariety, then*

$$\dim V = \dim U + n$$

Eventually, we prove a result in the mixed modular-multiplicative setting, that will be necessary to complete the proof of theorem 1.0.4. This can be considered a mixed "weak complex Ax"; the reader can find a description of it in [HP16, conjecture 5.10].

From now on we will call

$$X_{n,m} := \mathbb{C}^n \times (\mathbb{C}^*)^m \quad \text{and} \quad U_{n,m} := \mathcal{H}^n \times \mathbb{C}^m$$

then we have a function $\pi : U_{m,n} \to X_{n,m}$ such that

$$\pi(z_1, ..., z_n, u_1, ..., u_m) = (j(z_1), ..., j(z_n), \exp(u_1), ..., \exp(u_m))$$

where $\exp(u) = e^{2\pi i u}$.

Definition 3.2.9. An *algebraic subvariety* of $U_{n,m}$ will be a complex-analytically irreducible component of $Y \cap U_{n,m}$, where $Y \subseteq \mathbb{C}^n \times \mathbb{C}^m$ is an algebraic subvariety.

Definition 3.2.10. A *weakly special subvariety* of $U_{n,m}$ is an irreducible component of $\pi^{-1}(W)$, where W is a weakly special subvariety of $X_{n,m}$.

Definition 3.2.11. A *special subvariety* of $U_{n,m}$ is an irreducible component of $\pi^{-1}(W)$, where W is a special subvariety of $X_{n,m}$.

Theorem 3.2.12. *Let $V \subseteq X_{n,m}$ and $W \subseteq U_{n,m}$ be algebraic subvarieties and $A \subseteq W \cap \pi^{-1}(V)$ a complex-analytically irreducible component, then*

$$\dim A = \dim V + \dim W - \dim(X_{m,n})$$

unless A is contained in a proper weakly special subvariety of U.

This theorem leads to a mixed form of "weak complex Ax", stated in [HP16], which is a consequence of Ax-Schanuel. As multiplicative [Ax71] and modular [PT$^+$16] Ax-Schanuel imply respectively multiplicative and modular weak complex Ax, mixed Ax-Schanuel given above implies mixed weak complex Ax.

Theorem 3.2.13 (Weak complex Ax)**.** *Let $U' \subseteq U_{n,m}$ be a weakly special subvariety and let $X' = \pi(U')$. If $V \subseteq X'$ and $W \subseteq U'$ are algebraic subvarieties and A is a complex analytically irreducible component of $W \cap \pi^{-1}(V)$, then*

$$\dim A = \dim V + \dim W - \dim X'$$

unless A is contained in a proper weakly special subvariety of U'.

We now give some definitions in order to state the most convinient form of weak complex Ax for our purpose.

Definition 3.2.14. Let $V \subseteq X_{n,m}$ be a subvariety.

- A *component* with respect to V is a complex analytically irreducible component of $W \cap \pi^{-1}(V)$ for some algebraic variety $W \subseteq U_{n,m}$.
- Let A be a component with respect to V. We define its *defect* to be $\partial(A) := \dim Zcl(A) - \dim A$, where $Zcl(A)$ denotes the Zariski closure of A.
- A component with respect to V is *optimal* if there is no strictly larger component B with respect to V with $\partial B \leq \partial A$.
- A component A with respect to V is *geodesic* if it is a component of $W \cap \pi^{-1}(V)$ for some weakly special subvariety $W \subseteq U_{n,m}$.

Theorem 3.2.15 (Weak complex Ax, second form)**.** *Let $V \subseteq X_{n,m}$ be a subvariety. An optimal component with respect to V is geodesic.*

The proof that the two versions of weak complex Ax are equivalent is the same of that of [HP16].

CHAPTER 4

o-minimality: the Theorem of Pila and Wilkie

In this chapter we will define o-minimal structures with the aim of introducing the Pila-Wilkie theorem. This will allow to underline how model theory applies to number theory.

4.1 o-minimal structures

Definition 4.1.1. Let R be a set, a *structure* on R is a sequence $S_0, S_1, S_2, ...$ of sets such that $S_n \subseteq \mathcal{P}(R^n)$, their elements are called *definable* sets and have the following properties:

- if $A \in S_n$ then $\bar{A} \in S_n$
- if $A, B \in S_n$ then $A \cup B \in S_n$
- if $A \in S_n$ and $B \in S_m$ then $A \times B \in S_{m+n}$
- for every $1 \leq i, j \leq n$ the set $\{(x_1, ..., x_n) \in R^n | x_i = x_j\} \in S_n$
- if $\pi : R^{n+1} \to R^n$ is the projection map, then $A \in S_{n+1} \Longrightarrow \pi(A) \in S_n$

Definition 4.1.2. We say that a map $f : R^n \to R^m$ is *definable* if its graph is definable, i.e. if $\{(x, y) \in R^{n+m} | y = f(x)\} \in S_{n+m}$

We now want to consider the case where $R = \mathbb{R}$, in particular we would like to study structures where sets defined by equations and inequalities of polynomials are definable. In addition, we would like these structures to be compatible with the properties of $\mathbb{R}$ as an ordered ring. For that reason, we

are going to give the following new definition of structure when $\mathbb{R}$ is the base set.

Definition 4.1.3. A *structure over* $\mathbb{R}$ is a structure with the following additional properties:

- the operations $+, \cdot : \mathbb{R}^2 \to \mathbb{R}$ are definable
- $\{x\}$ is definable $\forall x \in \mathbb{R}$
- the relation $<$ is definable, that is for every n and every $1 \leq i, j \leq n$ the set $\{(x_1, ..., x_n) \in \mathbb{R}^n | x_i < x_j\}$ is definable

Definition 4.1.4. We will call *semi-algebraic* set a subset of $\mathbb{R}^n$ of the form

$$\left\{ (x_1, ..., x_n) \in \mathbb{R}^n \;\middle|\; \begin{array}{llll} f_1(x_1, ..., x_n) > 0, & ... & f_s(x_1, ..., x_n) > 0, \\ g_1(x_1, ..., x_n) = 0, & ... & g_t(x_1, ..., x_n) = 0 \end{array} \right\}$$

where $f_1, ..., f_s, g_1, ..., g_t \in \mathbb{R}[x_1, ..., x_n]$.

Remark 4.1.5. It is not difficult to show with some calculations that all the semi-algebraic sets are definable in every structure over $\mathbb{R}$.

Definition 4.1.6. An *o-minimal structure* is a structure over $\mathbb{R}$ whose definable sets in $\mathbb{R}$ are only the semi-algebraic sets. In other words, the only definable sets in $\mathbb{R}$ are the following:

- $\emptyset$
- the intervals (a, b) with $a, b \in \mathbb{R} \cup \{\pm\infty\}$
- $\{x\}$ for every $x \in \mathbb{R}$
- finite unions of the previous sets

One may wonder wether the semi-algebraic sets form an o-minimal structure or not. We can see that all the properties are easy to verify but the closure under projection. However, we have the following result:

Theorem 4.1.7 (Tarski-Seidenberg)**.** *Let $A \subseteq \mathbb{R}^{n+1}$ be a semi-algebraic set, let $\pi : \mathbb{R}^{n+1} \to \mathbb{R}^n$ be the projection map, then $\pi(A)$ is a semi-algebraic set in $\mathbb{R}^n$.*

Corollary 4.1.8. *The sequence $(S_n)_n$, where S_n is the set of the semi-algebraic sets of $\mathbb{R}^n$, form an o-minimal structure, that will be denoted by $\mathbb{R}_{alg}$.*

We may also want to study structures where sets defined by equations and inequalities of analytic functions are definable.

Definition 4.1.9. A set $A \subseteq \mathbb{R}^n$ is called *semi-analytic at the point* $y \in \mathbb{R}^n$ if y has an open neighborhood U such that $U \cap A$ is a finite union of sets of the form

$$\left\{ (x_1, ..., x_n) \in \mathbb{R}^n \;\middle|\; \begin{array}{llll} f_1(x_1, ..., x_n) > 0, & ... & f_s(x_1, ..., x_n) > 0, \\ g_1(x_1, ..., x_n) = 0, & ... & g_t(x_1, ..., x_n) = 0 \end{array} \right\}$$

where $f_1, ..., f_s, g_1, ..., g_t$ are real analytic functions.

Definition 4.1.10. A set $A \subseteq \mathbb{R}^n$ is called *semi-analytic* if it is semi-analytic at every point $x \in \mathbb{R}^n$.

Unfortunately, semi-analytic sets don't form an o-minimal structure. That is due to the fact that the projection of a semi-analytic set is not neccesarily semi-analytic. Then, we have to introduce some other sets.

Definition 4.1.11. A set $A \subseteq \mathbb{R}^n$ is called *subanalytic at the point* $y \in \mathbb{R}^n$ if y has an open neighborhood U such that $U \cap A$ is the projection, thorugh the map $\pi : \mathbb{R}^{n+m} \to \mathbb{R}^n$, of a bounded semi-analytic set $S \subseteq \mathbb{R}^{n+m}$, for some $m \in \mathbb{N}$.

Definition 4.1.12. A set $A \subseteq \mathbb{R}^n$ is called *subanalytic* if it is subanalytic at every point $x \in \mathbb{R}^n$.

Definition 4.1.13. A set $A \subseteq \mathbb{R}^n$ is called *globally subanalytic* (or *finitely subanalytic*) if its image under the map

$$(x_1, ..., x_n) \longmapsto \left(\frac{x_1}{\sqrt{1 + x_1^2}} \;,\; ... \;,\; \frac{x_n}{\sqrt{1 + x_n^2}} \right)$$

from $\mathbb{R}^n$ to $\mathbb{R}^n$ is subanalytic in $\mathbb{R}^n$.

The importance of the subanalytic sets is expressed by the following theorem of Van den Dries [VdD86]:

Theorem 4.1.14. *Let S_n be the set of the finitely subanalytic sets in $\mathbb{R}^n$, then $(S_n)_{n \in \mathbb{N}}$ is an o-minimal strucutre denoted with $\mathbb{R}_{an}$.*

The more common name "globally subanalityc" comes from a different definition which has been proven to be equivalent to the previous one.

Definition 4.1.15. A set $A \subseteq \mathbb{R}^n$ is called *globally subanalytic* if it is subanalytic in $\mathbb{P}^n(\mathbb{R})$, where $\mathbb{R}^n$ is identified with the open set $U_0 = \{(x_0 : ... : x_n) | x_0 \neq 0\}$.

The o-minimal structure $\mathbb{R}_{an}$ can be further extended to a larger structure $\mathbb{R}_{an,\exp}$ in which the exponential function is definable. Van den Dries and others in [vdDMM94, 5.13] proved the following theorem:

Theorem 4.1.16. $\mathbb{R}_{an,\exp}$ *is an o-minimal structure.*

Subsequently, Peterzil and Starchenko introduced many results extending the theory of o-minimality to complex numbers. A complex set is said to be definable if it is definable considered in real coordinates; similarily, a complex function is definable if its graph is a definable set. In [PS04], they proved the following theorem:

Theorem 4.1.17. *The Weierstrass $\wp$ function is definable in the o-minimal structure $\mathbb{R}_{an,\exp}$.*

Corollary 4.1.18. *The j function is definable in the o-minimal structure $\mathbb{R}_{an,\exp}$.*

4.2 The Pila-Wilkie theorem

In recent years, thanks to Jonathan Pila and Alex James Wilkie, o-minimality has been applied to number theory through their important counting theorem. Their result is a generalization of the previous Bombieri-Pila theorem [BP89], which counts rational points of bounded height in transcendental curves. Pila and Wilkie managed to prove the same statement for definable sets in some o-minimal structures.

Definition 4.2.1. Let $X \subseteq \mathbb{R}^n$, we will denote by $X(\mathbb{Q}, T)$ the set of the points $x \in X \cap \mathbb{Q}^n$ such that $H(x_i) \leq T$ for every $i = 1, ..., n$, where $H(x_i)$ is the multiplicative height of x_i.

Definition 4.2.2. Let $X \subseteq \mathbb{R}^n$, we will denote by X^{alg} the union of all the segments of algebraic curves contained in X. Moreover, we will write $X^{tr} = X \setminus X^{alg}$.

Theorem 4.2.3 (Pila-Wilkie)**.** *Let $X \subseteq \mathbb{R}^n$ be a definable set in some o-minimal structure, then for every $\epsilon \in \mathbb{R}^+$ there exists a constant $c(X, \epsilon)$ such that*

$$|X^{tr}(\mathbb{Q}, T)| \leq c(X, \epsilon)T^{\epsilon}$$

Pila and Wilkie proved this theorem in 2006 [PW$^+$06], generalizing the previous result of Bombieri and Pila of 1989, which is the following:

Theorem 4.2.4. *Let $C \subset \mathbb{R}^2$ be a real analytic plane compact curve.*

- *Suppose that C is transcendental, then for every $\epsilon > 0$ there is a constant $k(C, \epsilon)$ such that*

$$\left| C \cap \frac{1}{N}\mathbb{Z}^2 \right| \leq k(C, \epsilon)N^{\epsilon}$$

- *Suppose that C is a segment of an irreducible plane algebraic curve of degree d, then for every $\epsilon > 0$ there is a constant $k(C, \epsilon)$ such that*

$$\left| C \cap \frac{1}{N}\mathbb{Z}^2 \right| \leq k(C, \epsilon) N^{\frac{1}{d}+\epsilon}$$

In the proof of theorem 1.0.4 we will need to bound the quadratic points (corresponding to singular moduli), then the Pila-Wilkie theorem, in this form, is not sufficient, since its statement involves only the rational numbers. Indeed, we will use a stronger version proved by Pila in 2009 [Pil09].

Definition 4.2.5. Let $X \subseteq \mathbb{R}^n$, we will denote by $X(\mathbb{Q}, d, T)$ the set of the points $x \in X$ such that $[\mathbb{Q}(x_i) : \mathbb{Q}] \leq d$ and $H(x_i) \leq T$ for every $i = 1, ..., n$.

Theorem 4.2.6. *Let $X \subseteq \mathbb{R}^n$ be definable in some o-minimal structure, let d be a positive integer, then for every $\epsilon > 0$ there exists a constant $c(X, \epsilon, d)$ such that*

$$|X^{tr}(\mathbb{Q}, d, T)| \leq c(X, \epsilon, d) T^{\epsilon}$$

Actually, also this version of the theorem is not enough, because singular moduli correspond to imaginary quadratic points, but we can consider their projection on $\mathbb{R}$, which for each point gives two points at most quadratic.

CHAPTER 5

Proof of the main theorem

The proof of theorem 1.0.4 will be given by proving at first a different theorem stating that distinct rational "translates" of the j-function are multiplicatively independent modulo constant. We now give a more precise statement of this theorem.

Definition 5.0.1. Let $f_1, ..., f_n : \mathcal{H} \to \mathbb{C}$ be functions, they will be called *multiplicatively independent modulo constants* if there are no $k_1, ..., k_n \in \mathbb{Z}$ not all 0 and $c \in \mathbb{C}$ such that $\prod_{i=1}^{n} f_i^{k_i} = c$.

Let's consider the functions $j(g_1 z), ..., j(g_n z) : \mathcal{H} \to \mathbb{C}$ for some $g_1, ..., g_n \in \mathrm{GL}_2^+(\mathbb{Q})$. We know that $j(g_i z), j(g_k z)$ are identically equal if and only if $[g_i] = [g_k]$ in the quotient $\mathrm{PSL}_2(\mathbb{Z}) \backslash \mathrm{PGL}_2^+(\mathbb{Q})$. We will prove the following:

Theorem 5.0.2. *Let $g_1, ..., g_n \in \mathrm{GL}_2^+(\mathbb{Q})$. If the functions $j(g_1 z), ..., j(g_n z)$ are pairwise distinct, then they are multiplicatively independent modulo constants.*

The key to prove this will be to show that there exists a $z \in \mathcal{H}$ such that one and only one of these functions vanishes in z. To do this, we need some further tools.

5.1 Trees of lattices

When we consider the set of the lattices up to scaling, we can define a structure of graph on it, in particular a regular connected tree, which will allow us to prove theorem 5.0.2.

Let us define the sets

$$T_{\mathbb{Q}} := \mathrm{PSL}_2(\mathbb{Z}) \backslash \mathrm{PGL}_2^+(\mathbb{Q}) \quad \text{and} \quad T_p := \mathrm{PSL}_2(\mathbb{Z}_p) \backslash \mathrm{PGL}_2(\mathbb{Q}_p)$$

There is a map $T_{\mathbb{Q}} \to T_p$ given by the inclusions $\mathbb{Z} \subset \mathbb{Z}_p$ and $\mathbb{Q} \subset \mathbb{Q}_p$. This map is well defined, because two classes $[g], [h] \in T_{\mathbb{Q}}$, for $g, h \in \mathrm{PGL}_2^+(\mathbb{Q})$, are the same class if there is $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$ such that $\gamma g = h$, but $\mathrm{PSL}_2(\mathbb{Z}) \subset \mathrm{PSL}_2(\mathbb{Z}_p)$, then $[g]_p = [h]_p$, where $[g]_p$ is the image of $[g]$ in T_p.

Remark 5.1.1. The map defined above is not injective, because there may be such a γ that belongs to $\mathrm{PSL}_2(\mathbb{Z}_p) \setminus \mathrm{PSL}_2(\mathbb{Z})$. For example, let $a \neq 1$ be a quadratic residue modulo p, hence $\sqrt{a}, \frac{1}{\sqrt{a}} \in \mathbb{Z}_p$ and therefore $\begin{pmatrix} \sqrt{a} & 0 \\ 0 & \frac{1}{\sqrt{a}} \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}_p)$, so

$$[I]_p = \left[\begin{pmatrix} \sqrt{a} & 0 \\ 0 & \frac{1}{\sqrt{a}} \end{pmatrix} \right]_p = \left[\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \right]_p$$

but $[I] \neq \left[\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \right]$ in $T_{\mathbb{Q}}$.

If we consider the product over the primes of the maps $T_{\mathbb{Q}} \to T_p$ we get an inclusion $T_{\mathbb{Q}} \subset \prod_{p \text{ prime}} T_p$. Indeed, given $[g], [h] \in T_{\mathbb{Q}}$, if we have that $[g]_p = [h]_p$ for every p, the matrix gh^{-1} belongs to $\mathrm{PSL}_2(\mathbb{Z}_p)$ for every p, i.e. the coefficients of gh^{-1} are rational numbers belonging to Z_p for every p, hence $gh^{-1} \in \mathrm{PSL}_2(\mathbb{Z})$ and $[g] = [h]$.

The set $T_{\mathbb{Q}}$ may be identified with the set of the $\mathbb{Z}$-lattices in $\mathbb{Q}^2$ up to scaling. This can be seen taking the lattice generated by ge_1, ge_2, with e_1, e_2 being the canonical basis, for every $g \in \mathrm{PGL}_2^+(\mathbb{Q})$. The correspondence is well defined because g and h generate the same lattice (up to scaling) if and only if gh^{-1} generates $\mathbb{Z}^2$, i.e. $gh^{-1} \in \mathrm{PSL}_2(\mathbb{Z})$. Likewise, T_p may be identified with the set of the $\mathbb{Z}_p$-lattices in $\mathbb{Q}^2$ up to scaling.

We can define a graph structure on T_p by taking its points as nodes and by saying that two lattices are connected by an edge if there exists a cyclic p-isogeny between them, i.e. if one can scale one to be inside the other with index p.

Definition 5.1.2. We say that a graph is a *tree* if there are no cycles in it.

Definition 5.1.3. We call a graph *regular* if every node has the same degree. A graph whose nodes have degree n will be called an *n-regular graph.*

Proposition 5.1.4. *The graph T_p is a $(p+1)$-regular connected tree.*

Proof. Let us first prove that it is connected. Let $(a_1, b_1)\mathbb{Z}_p \oplus (a_2, b_2)\mathbb{Z}_p$ be a generic lattice. We know that every number in $\mathbb{Q}_p$ is the product of a power of p and an invertible element of $\mathbb{Z}_p$, hence we can write the lattice as $(p^{k_1}\alpha_1, p^{h_1}\beta_1)\mathbb{Z}_p \oplus (p^{k_2}\alpha_2, p^{h_2}\beta_2)\mathbb{Z}_p$. Since $\mathbb{Z}_p = \beta_i^{-1}\mathbb{Z}_p$ for $i = 1, 2$, we may assume that $\beta_1 = \beta_2 = 1$, by renaming $\alpha_i\beta_i^{-1}$ as α_i. Without loss of generality, we can also suppose that $h_1 \geq h_2$, then we have

$$\begin{aligned}
&(p^{k_1}\alpha_1, p^{h_1})\mathbb{Z}_p \oplus (p^{k_2}\alpha_2, p^{h_2})\mathbb{Z}_p = \\
&(p^{k_1}\alpha_1 - p^{k_2+h_1-h_2}\alpha_2, p^{h_1} - p^{h_1})\mathbb{Z}_p \oplus (p^{k_2}\alpha_2, p^{h_2})\mathbb{Z}_p = \\
&(c, 0)\mathbb{Z}_p \oplus (p^{k_2}\alpha_2, p^{h_2})\mathbb{Z}_p
\end{aligned}$$

Again, we can write $c = p^\ell\gamma$, with $\gamma \in \mathbb{Z}_p^*$. We have two cases:

1. $\boldsymbol{\ell \leq k_2}$ **:** in this case we simply have that

$$\begin{aligned}
&(p^\ell\gamma, 0)\mathbb{Z}_p \oplus (p^{k_2}\alpha_2, p^{h_2})\mathbb{Z}_p = \\
&(p^\ell, 0)\mathbb{Z}_p \oplus (p^{k_2}\alpha_2, p^{h_2})\mathbb{Z}_p = \\
&(p^\ell, 0)\mathbb{Z}_p \oplus (0, p^{h_2})\mathbb{Z}_p
\end{aligned}$$

   which is an orthogonal lattice.

2. $\boldsymbol{\ell > k_2}$ **:** in this case we cannot chose a simpler basis, then the lattice will have the form $(p^\ell, 0)\mathbb{Z}_p \oplus (p^{k_2}, p^{h_2}\alpha_2^{-1})\mathbb{Z}_p$.

It is now easy to notice that every two lattices of type 1 are always connected, because we just need to scale each coordinate by a factor p a proper number of times. Moreover, we can see that every lattice of type 2 is connected to a lattice of type 1, because we can multiply the second coordinate by p until $k_2 \geq \ell$, obtaining a lattice of type 1. Then T_p is connected.
To prove that it is a tree, suppose that there is a cycle $L_1, L_2, ..., L_n, L_{n+1} = L_1$, where $n > 2$ and $L_i \neq L_j$ for every $1 \leq i < j \leq n$, then, since L_i considered up to scaling, we can fix a scale so that $L_1 \subset L_2 \subset ... \subset L_n \subset L_{n+1} = cL_1 = \frac{1}{p^k}L_1$, where $c \in \mathbb{Q}_p$ and $k = -v_p(c) > 0$. We know that $[L_{i+1} : L_i] = p$ for every i, then $p^{2k} = [L_{n+1} : L_1] = \prod_{i=1}^{n}[L_{i+1} : L_i] = p^n$.

Lemma 5.1.5. *For every $i \leq 1$ we have ${}^{L_i}\!/_{L_1} \cong {}^{\mathbb{Z}}\!/_{p^{i-1}\mathbb{Z}}$.*

Proof. We prove this lemma by induction. If $i = 1$ is trivial and it is also true for $i = 2$ because there is a cyclic p-isogeny between L_1 and L_2. Suppose that ${}^{L_i}\!/_{L_1} \cong {}^{\mathbb{Z}}\!/_{p^{i-1}\mathbb{Z}}$ for a fixed $i \geq 2$ and for all the previous, then ${}^{L_i}\!/_{L_1} < {}^{L_{i+1}}\!/_{L_1}$ and $\left[{}^{L_{i+1}}\!/_{L_1} : {}^{L_i}\!/_{L_1}\right] = [L_{i+1} : L_i] = p$. Hence, either ${}^{L_{i+1}}\!/_{L_1} \cong$

$\mathbb{Z}/p^i\mathbb{Z}$, which is our goal, or $L_{i+1}/L_1 \cong \mathbb{Z}/p^{i-1}\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. In the latter case, we would have

$$\mathbb{Z}/p^{i-2}\mathbb{Z} \cong L_{i-1}/L_1 < L_{i+1}/L_1 \cong \mathbb{Z}/p^{i-1}\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

and so

$$L_{i+1}/L_{i-1} \cong \frac{L_{i+1}/L_1}{L_{i-1}/L_1} \cong \left(\mathbb{Z}/p\mathbb{Z}\right)^2$$

Hence $pL_{i+1} \subseteq L_{i-1}$, but $[L_{i+1} : pL_{i+1}] = p^2 = [L_{i+1} : L_{i-1}]$, so $[L_{i-1} : pL_{i+1}] = 1$, i.e. $pL_{i+1} = L_{i-1}$, which means that they are the same lattice up to scale, but this is absurd by assumption. □

Now, by the lemma, we get that

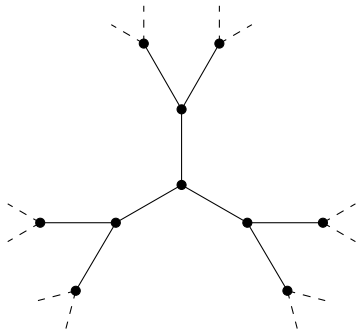
$$\left(\mathbb{Z}/p^k\mathbb{Z}\right)^2 \cong p^{-k}L_1/L_1 = L_{n+1}/L_1 \cong \mathbb{Z}/p^n Z$$

which is absurd, hence there can't be any cycle.
Eventually, to prove that T_p is $(p+1)$-regular, we just need to notice that, given a lattice L, every adjacent lattice can be scaled to a unique proper sublattice of L of index p. All these lattices will also contain pL, then there is a correspondence between them and the subgroups of order p of $L/pL \cong \left(\mathbb{Z}/p\mathbb{Z}\right)^2$. To count these subgroups, we just need to count the elements of order p and notice that there are $p-1$ of them in every orbit, then there are $\frac{p^2-1}{p-1} = p+1$ subgroups, which corresponds to the nodes adjacent to L. □

The lattices in $T_{\mathbb{Q}}$ and T_p are defined to be inside $\mathbb{Q}^2$ and $\mathbb{Q}_p^2$ respectively, but we can chose an element $\tau \in \mathbb{C}$ so that $1, \tau$ are a basis of $\mathbb{Q}^2$ inside $\mathbb{C}$. The difference with the previous definition is that a lattice embedded in $\mathbb{C}$ might have a structure of ideal in some ring in addition to that of $\mathbb{Z}$-module. In particular, this happens if and only if τ is imaginary quadratic, i.e. if the lattice considered gives rise to a CM elliptic curve.

Let us examine the lattice $\Lambda = \mathbb{Z} \oplus \omega\mathbb{Z}$, with $\omega = e^{\frac{2\pi i}{3}}$, root of the polynomial $x^2 + x + 1$, whose j-invariant is equal to 0. The quotient $E_0 = \mathbb{C}/\Lambda$ is a CM curve and its ring of endomorphisms is $\mathbb{Z}[\omega]$ itself. Then, every curve isogenous to E_0 has also ring of endomorphisms $\mathbb{Z}[\omega]$, so, up to nomalizing its lattice, we can consider it to be inside $\mathbb{Z}[\omega] \otimes \mathbb{Q} = \mathbb{Q}(\omega)$. On the other hand, every lattice $L \subset \mathbb{Q}(\omega)$ (up to scaling) has its curve E_L isogenous to the curve E_0, indeed we can scale it so that it contains $\mathbb{Z}[\omega]$ and $L/\mathbb{Z}[\omega]$ is cyclic. Then we can define $T'_{\mathbb{Q}}$ to be the set of the lattices in $\mathbb{Q}(\omega)$ up to scaling, and corrispondingly $T'_p := \{L \otimes \mathbb{Z}_p | L \in T'_{\mathbb{Q}}\}$. T'_p is just the set T_p, where $\mathbb{Q}_p^2$ is identified with $\mathbb{Q}(\omega) \otimes \mathbb{Z}_p$.

Remark 5.1.6. We can notice that both T_p and T'_p are $p+1$-regular connected trees (as in the picture below), hence they are completely symmetric in every node. In particular, if we choose a correspondence between them, we can send the base node $\mathbb{Z}_p^2$ of T_p in every node of T'_p. However, this choice doesn't determine the correspondence between the other vertices of the graph. For instance, every node adjacent to the base node of T_p can be sent in every node adjacent to the image of the base node in T'_p.



Remark 5.1.7. In $T'_{\mathbb{Q}}$, one can decide that $\mathbb{Z}[\omega]$ corresponds to $\mathbb{Z}^2$ in $T_{\mathbb{Q}}$, then in T'_p the lattice $\mathbb{Z}[\omega] \otimes \mathbb{Z}_p$ corresponds to $\mathbb{Z}_p^2$ in T_p. However, this doesn't determine the correspondence between other latticese and edges, in particular, that depends on the choice of correspondence of basis between $\mathbb{Z}[\omega]$ and $\mathbb{Z}^2$.

Remark 5.1.8. Let $\mathbb{Z}[\omega] \otimes \mathbb{Z}_p$ correspond to $\mathbb{Z}_p^2$ as in the previous remark, then every $L \in T_p$ adjacent to $\mathbb{Z}_p^2$ can be sent in every $L' \in T'_p$ adjacent to $\mathbb{Z}[\omega] \otimes \mathbb{Z}_p$ with a proper choice of basis for $\mathbb{Z}^2$, i.e. with a proper choice of a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. In addition, every $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma' \equiv \gamma \pmod{p}$ gives the same correspondence. To see this, set a default correspondence between lattices and identify L' with its preimage in T_p, then $L' = \gamma L$ and up to scale we can consider them to contain $\mathbb{Z}^2$ with index p. Let $\gamma' = \gamma + p\delta$, we have $\gamma' L = (\gamma + p\delta)L \subset \gamma L + \mathbb{Z}^2 = L'$. Conversely, we have that $(\gamma')^{-1} = \gamma^{-1} + p\delta'$, so $(\gamma')^{-1}L' = (\gamma^{-1} + p\delta')L' \subset \gamma^{-1}L' + \mathbb{Z}^2 = L$, that is $L' \subset \gamma' L$, and so $L' = \gamma' L$. Hence, L can be sent to L' with a proper choice of $\bar{\gamma} \in \mathrm{SL}_2\left(\mathbb{Z}/p\mathbb{Z}\right)$.

Let us now study the curves isomorphic to E_0 in $T'_{\mathbb{Q}}$. In particular, we want to prove the following proposition:

Proposition 5.1.9. *For every prime p, there exists a node $N' \in T'_p$ adiacent to the lattice $\mathbb{Z}[\omega] \otimes \mathbb{Z}_p$ such that every other lattice $L \in T'_{\mathbb{Q}}$ for which the shortest path from $\mathbb{Z}[\omega] \otimes \mathbb{Z}_p$ to $L \otimes \mathbb{Z}_p$ goes through N' is not isomorphic to E_0, i.e. it is not of the form $\Lambda \otimes \mathbb{Z}_p$ with $\mathbb{C}/\Lambda \cong E_0$.*

Proof. Let $L \in T'_{\mathbb{Q}}$ such that $E_L \cong E_0$, then up to scale $L \supset \mathbb{Z}[\omega]$ and $L/\mathbb{Z}[\omega]$ is the kernel of an endomorphism of E_0, that is the kernel of the multiplication by

$\alpha \in \mathbb{Z}[\omega]$. This kernel is $\frac{Z[\omega]}{(\alpha)} \cong \frac{(\alpha^{-1})}{\mathbb{Z}[\omega]}$ and looking to the corresponding maps in $\mathbb{Q}_p$ the kernel becomes $\frac{(\alpha^{-1})\otimes\mathbb{Z}_p}{\mathbb{Z}[\omega]\otimes\mathbb{Z}_p}$. This means that the endomorphisms (and so the lattices isomorphic to E_0) correspond to some elements of the fractional ideal group of $\mathbb{Z}[\omega] \otimes \mathbb{Z}_p$ (providing the endomorphisms giving the kernels) quotiented out by the fractional principal ideals of $\mathbb{Z}_p$ (scaling). We know that $\mathbb{Z}[\omega] \otimes \mathbb{Z}_p = \frac{\mathbb{Z}[x]}{(x^2+x+1)} \otimes \mathbb{Z}_p \cong \frac{\mathbb{Z}_p[x]}{(x^2+x+1)}$, then we have 3 different cases:

- $\mathbf{p \equiv 1 (3)}$: in this case $x^2 + x + 1$ splits modulo p, then by Hensel's lemma also splits in $\mathbb{Z}_p[x]$ and $\omega, \bar{\omega} \in \mathbb{Z}_p$ are different roots of it. Then $\mathbb{Z}[\omega]\otimes\mathbb{Z}_p \cong \frac{\mathbb{Z}_p[x]}{(x-\omega)} \times \frac{\mathbb{Z}_p[x]}{(x-\bar{\omega})} \cong \mathbb{Z}_p^2$. So its ideal group is isomorphic to $\mathbb{Z}^2$ and quotiented by the diagonal. This means that the lattices isomorphic to E_0 are the same of $\mathbb{Z}$ and are adjacent if and only if they are represented by consecutive numbers (multiplication by p).

- $\mathbf{p \equiv 2 (3)}$: in this case x^2+x+1 doesn't split in $\mathbb{Z}_p$, so $\mathbb{Z}[\omega]\otimes\mathbb{Z}_p = \mathbb{Z}_p[\omega]$ and its maximal ideal is (p), then its ideal group is isomorphic to $\mathbb{Z}$ (powers of p). But since $p \in \mathbb{Q}_p^*$ (and so $(p) \in \mathcal{F}(\mathbb{Z}_p)$), the lattices isomorphic to E_0 are just $\mathbb{Z}$ quotiented by $\mathbb{Z}$, so there is just one such lattice, that is $\mathbb{Z}[\omega]$.

- $\mathbf{p = 3}$: in this case $x^2+x+1 = (x-1)^2+3(x-1)+3$, so it is irreducible by Eisenstein, then $\mathbb{Z}[\omega]\otimes\mathbb{Z}_3 = \mathbb{Z}_3[\omega]$ and since $(3) = (1-\omega)^2$ is totally ramified in $\mathbb{Z}[\omega]$, so it is in $\mathbb{Z}_3[\omega]$. Hence the ideal group is equal to $\mathbb{Z}$ (exponents of $1-\omega$) and quotienting by the ideals of $\mathbb{Z}_3$, i.e. the powers of (3), corresponds to quotienting by $2\mathbb{Z}$, since the valuation of 3 is 2. So, there are just 2 lattices isomorphic to E_0. In addition, these two nodes are connected, since we can get from one to the other by multiplying by $1-\omega$, which is a cyclic 3-isogeny.

Since T'_p is a $(p+1)$-regular tree and $p \geq 2$, every node has at least 3 adjacent nodes, but in all cases above, $\mathbb{Z}[\omega]\otimes\mathbb{Z}_p$ (which is isomorphic to E_0) can have at most 2 other lattices isomorphic to E_0 adjacent to it. In particular, there is N' adjacent to $\mathbb{Z}[\omega]\otimes\mathbb{Z}_p$ which is not isomorphic to E_0. In second and third case we obviously conclude by considering this node. In the first case, if there were a node L isomorphic to E_0 with shortest path to $\mathbb{Z}[\omega]\otimes\mathbb{Z}_p$ passing through N', there would be a path from L to $\mathbb{Z}[\omega]\otimes\mathbb{Z}_p$ passing only through nodes isomorphic to E_0, because these nodes form a connected line in T'_p. But since T'_p is a tree, this would imply that this path passes through N', which is absurd. □

5.2 Rational translates of j are independent

We have introduced some properties of trees of lattices, so we are now ready to prove theorem 5.0.2. We will do that by proving the following:

Proposition 5.2.1. *Let $g_1, ..., g_n \in \mathrm{GL}_2^+(\mathbb{Q})$ such that the functions $j(g_1 z), ..., j(g_n z)$ are pairwise distinct, then there exists $z \in \mathcal{H}$ such that $j(g_i z) = 0$ for exactly one i.*

Proof. We first suppose that there exists a prime number p such that the images of $g_1, ..., g_n$ in T_p are distinct. If u_i is the image of g_i in T_p for every i, we may assume that u_1 and u_2 are two nodes with maximal distance. Then, there is a unique node $N \in T_p$ adjacent to u_1 such that every path from u_1 to any other u_i goes through N (because T_p is a tree). Furthermore, we can assume that $g_1 = I$, because we can consider the functions $j(g_i z)$ to be defined over $g_1^{-1}\mathcal{H} = \mathcal{H}$. We can now take a map from T_p to T'_p sending $\mathbb{Z}_p^2$ to $\mathbb{Z}[\omega] \otimes \mathbb{Z}_p$, in addition, by remark 5.1.8, we can send N to the node N' of proposition 5.1.9, so that u_i is never isomorphic to E_0 for $i \neq 0$. Hence, taking $z = \omega$, we get $j(g_1 z) = j(\omega) = 0$ and for $i > 1$ we get $j(g_i z) \neq 0$, because the image of $g_i = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in T'_p is $\langle a\omega + b, c\omega + d\rangle \ncong E_0$ and

$$j(g_i\omega) = j\left(\frac{a\omega + b}{c\omega + d}\right) = j\left(\langle \frac{a\omega + b}{c\omega + d}, 1\rangle\right) = j(\langle a\omega + b, c\omega + d\rangle) \neq 0$$

Let us now prove the proposition without the simplifying assumption. Since $j(g_1 z), ..., j(g_n z)$ are all distinct, the classes of g_i in $T_{\mathbb{Q}}$ are all distinct, then for every $i \neq j$ there exist a prime p such that $u_i \neq u_j$ in T_p. This means that while there is no p separating $g_1, ..., g_n$, there exists a $k \in \mathbb{N}$ such that, if we consider the first k primes $2 = p_1, ..., p_k$, they are distinct, i.e. for every g_i, g_j there is a $q < p_k$ such that they are distinct in T_q. Let $S = \{g_1, ..., g_n\}$, let $v_1 \in T_2 = T_{p_1}$ be an extremal node (just as u_1 in the simple case above), then we call $S_1 \subset S$ the set of the g_i whose image is v_1. Similarly, we can take an extremal node $v_2 \in T_3 = T_{p_2}$ among the images of elements of S_1, then we can define $S_2 \subset S_1$ to be the set of the elements of S_1 whose image is v_2. In particular, for every $1 \leq t \leq k$ we can consider the set $S_t \subset S_{t-1}$ of the elements whose image in T_{p_t} is an extremal node v_t among the images of elements of S_{t-1} (with $S_0 = S$). By the choice of k, we know that S_k has just one element, then, as in the simple case, we may assume that this node is the image of g_1 and that $g_1 = I$. For every $1 \leq t \leq k$ there exists a unique node $N_t \in T_{p_t}$ adjacent to v_t through which all the paths from v_t to other images of S_{t-1} go. By a proper choice of a basis for $\mathbb{Z}^2 \in T_{\mathbb{Q}}$, the map from T_{p_t} to T'_{p_t} sending $\mathbb{Z}_{p_t}^2$ to $\mathbb{Z}[\omega] \otimes \mathbb{Z}_{p_t}^2$, sends also N_t to N'_t as in proposition 5.1.9, for every t. Indeed, by remark 5.1.8 and by Chinese remainder theorem, the choice of a

basis for every p_t corresponds to the choice of an element in $\mathrm{SL}_2\left(\mathbb{Z}/(\prod p_t)\mathbb{Z}\right)$. We can choose a proper matrix in $\mathrm{SL}_2(\mathbb{Z})$ that projects to the right element because the projection $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2\left(\mathbb{Z}/R\mathbb{Z}\right)$ is surjective for every natural number R. For $i > 1$, let us consider $t < k$ such that $g_i \in S_t \setminus S_{t+1}$: the image of g_i in $T'_{p_{t+1}}$ is connected to v_{t+1} via N'_{t+1}, so g_i is not isomorphic to E_0. Hence, as in the simple case, $j(g_1\omega) = j(\omega) = 0$ and $j(g_i\omega) \neq 0$ for every $i > 1$. □

Now, to prove theorem 5.0.2, let us suppose that the functions $j(g_1 z), ..., j(g_n z)$ are not multiplicatively independent modulo constant, then there exist $k_1, ..., k_n \in \mathbb{Z}$ and $c \in \mathbb{C}$ such that $\prod_{i=1}^n j(g_i z)^{k_i} = c$. We notice that $c \neq 0$ because $j(g_i z)$ are meromorphic functions, hence their product vanishes on a set of measure zero. Let $\bar{z} \in \mathcal{H}$ be an element such that $j(g_i \bar{z}) = 0$ and $j(g_t \bar{z}) \neq 0$ for every $t \neq i$, for some $1 \leq i \leq n$. Without loss of generality, we may consider $k_t \neq 0$ (otherwise we can just take a subset of the functions) and $k_i > 0$ (up to invert), hence $0 = j(g_i \bar{z})^{k_i} \cdot \prod_{t \neq i} j(g_t \bar{z})^{k_t} = \prod_{t=1}^n j(g_t \bar{z})^{k_t} = c$, which is absurd. This concludes the proof of the theorem.

5.3 Singular-dependent n-tuples in atypical components

Let $X = X_{n,n} = \mathbb{C}^n \times (\mathbb{C}^*)^n$ and let us consider the "diagonal" $V = V_n = \{(\mathbf{x}, \mathbf{x}) \in X | \mathbf{x} \in (\mathbb{C}^*)^n\}$. Since V is defined by n minimal equations, $\dim V = \operatorname{codim} V = n$. If we consider a singular-dependent n-tuple $(x_1, ..., x_n)$, we can notice that it is a special point (and so a special subvariety of dimension 0) in $\mathbb{C}^n$; moreover it satisfies an equation of the form $\prod_{i=1}^n x_i^{a_i} = 1$, hence it is contained in a special subvariety T of $(\mathbb{C}^*)^n$ of dimension $n-1$. In particular, $\mathbf{x} = (x_1, ..., x_n, x_1, ..., x_n)$ is contained in the special subvariety $\{\mathbf{x}\} \times T$ of X of dimension $0 + (n-1) = n - 1$. Hence, we obtain that

$$\dim(\{\mathbf{x}\}) = 0 > -1 = n + (n-1) - 2n = \dim V + \dim(\{\mathbf{x}\} \times T) - \dim X$$

so $\mathbf{x}$ is an atypical point of V in X.

Lemma 5.3.1. *A singular-dependent n-tuple may not be contained in an atypical component of V of positive dimension.*

Proof. Let $\mathbf{x} = (x_1, ..., x_n)$ be a singular-dependent n-tuple. $\mathbf{x}$ can never be contained in a special subvariety of $X_{0,n} = (\mathbb{C}^*)^n$ defined by two minimal equations, indeed, if we have the equations $\mathbf{y}^{\mathbf{a}} = \prod_{i=1}^n y_i^{a_i} = \zeta_\alpha$ and $\mathbf{y}^{\mathbf{b}} = \prod_{i=1}^n y_i^{b_i} = \zeta_\beta$ such that $(a_i, ..., a_n) \neq r(b_1, ..., b_n)$ for every $r \in \mathbb{Q}$, we get $\mathbf{c} = b_1\mathbf{a} - a_1\mathbf{b} \neq (0, ..., 0)$, but $c_1 = 0$. Hence, if $\mathbf{x}$ satisfies both the equations,

$\mathbf{x}^{\alpha\beta\mathbf{c}} = 1$, which gives a multiplicative dependence between $x_2, .., x_n$, contradicting the minimality of the relation of the singular-dependent n-tuple.
We now notice that the special varieties of the form $M \times (\mathbb{C}^*)^n$ or $\mathbb{C}^n \times T$ cannot contain an atypical component of V, indeed

$$(M \times (\mathbb{C}^*)^n) \cap V = \{(\mathbf{x}, \mathbf{x}) | \mathbf{x} \in M \cap (\mathbb{C}^*)^n\} = \tilde{M}$$

and

$$(\mathbb{C}^n \times T) \cap V = \{(\mathbf{x}, \mathbf{x}) | \mathbf{x} \in T\} = \tilde{T}$$

so

$$\dim(\tilde{M}) \leq \dim M = \dim(M \times (\mathbb{C}^*)^n) - n = \dim(M \times (\mathbb{C}^*)^n) + \dim V - \dim X$$

and

$$\dim(\tilde{T}) = \dim T = \dim(\mathbb{C}^n \times T) - n = \dim(\mathbb{C}^n \times T) + \dim V - \dim X$$

Hence, if $(\mathbf{x}, \mathbf{x})$ is contained in a positive dimensional atypical component of V, it must be given by a special subvariety of the form $M \times T$, with M proper special subvariety and T special subvariety defined by one equation $\prod_{i=1}^n y_i^{a_i} = \zeta_\alpha$ (i.e. it has dimension $n-1$). Then we have that

$$\begin{aligned} \dim((M \times T) \cap V) &\geq \dim(M \times T) + \dim V - \dim X = \\ &= \dim M + (n-1) + n - 2n = \dim M - 1 \end{aligned}$$

So it gives an atypical component if $\dim((M \times T) \cap V) \geq \dim M$, but

$$\dim M \leq \dim((M \times T) \cap V) = \dim(M \cap T) \leq \dim M$$

therefore $M \cap (\mathbb{C}^*)^n \subseteq T$, since M is irreducible (it is a product of irreducible varieties). We know that $\mathbf{x} \in T$, then we must have that $a_i \neq 0$ for every i, otherwise $\mathbf{x}$ wouldn't be a singular-dependent n-tuple. Since M is a positive dimensional special subvariety of $\mathbb{C}^n$, $M = M_0 \times M_1 \times ... \times M_k$ with $k \geq 1$, like in definition 3.1.3. Since $\mathbf{x} \in M$, WLOG $n_1 = \{1, 2, ..., s\}$ and $\mathbf{x}$ is contained in the curve $M_1 \times \{(x_{s+1}, ..., x_n)\}$. M_1 can be parametrized by $(j(q_1 z), ..., j(q_s z))$ with $z \in \mathbb{C}$ and $q_1, ..., q_s \in \mathrm{GL}_2^+(\mathbb{Q})$, then $j(q_1 z), ..., j(q_s z)$ would be multiplicatively dependent modulo constant ($\prod_{i=1}^s j(q_i z)^{-a_i} = \zeta_\alpha^{-1} \prod_{i=s+1}^n x_i^{a_i}$ with $a_1, ...a_s$ not all 0), hence by theorem 5.0.2 two of them are identically equal. In particular, there exist $x_i = x_j$ for some $i \neq j$, but this contradicts the minimality of the relations of the singular-dependent n-tuple. □

5.4 The proof

In this section we finally give the proof of theorem 1.0.4.

We already noticed, at the end of the second chapter, that every singular modulus is the j-invariant of a proper ideal of a quadratic order. Let the discriminant Δ_τ associated to a complex quadratic number $\tau \in \mathcal{H}$ be the same of the discriminant associated to the correspondent singular modulus $j(\tau)$. If τ is a quadratic complex number, $ax^2 + bx + c \in \mathbb{Z}[x]$ the polynomial with τ as a root and $(a, b, c) = 1$, $j(\tau)$ is the j-invariant of the proper fractional ideal $\langle 1, \tau \rangle$ in the order $\langle 1, a\tau \rangle$, hence we can consider the discriminant of a singular modulus to be, equivalently, the discriminant of its preimage τ or the discriminant of its associated order, because $\Delta(\langle 1, a\tau \rangle) = \Delta_{a\tau} = \Delta_\tau$.

Remark 5.4.1. With the notation above, one can show that the discriminant $\Delta_{j(\tau)} = \Delta_\tau$ is the discriminant of the polynomial $ax^2 + bx + c$.

Definition 5.4.2. Let $\sigma = j(\tau)$ be a singular modulus, we define its *complexity* as $\Delta(\sigma) = |\Delta_\tau|$.

Definition 5.4.3. Let $\sigma = (\sigma_1, ..., \sigma_n)$ be a n-tuple of singular moduli, then we define its *complexity* as $\Delta(\sigma) = \max\{|\Delta(\sigma_1)|, ..., |\Delta(\sigma_n)|\}$.

Definition 5.4.4. Let $\mathbf{x} = (x_1, ..., x_n) \in \bar{\mathbb{Q}}^n$, then we define the height of $\mathbf{x}$ as $\mathrm{h}(\mathbf{x}) := \max\{\mathrm{h}(x_1), ..., \mathrm{h}(x_n)\}$. Likewise $\mathrm{H}(\mathbf{x}) := \max\{\mathrm{H}(x_1), ..., \mathrm{H}(x_n)\}$.

We now define a particular set that will be the key of the proof. Let F_j be the standard fundamental domain of the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$, and $F_{\exp}$ the standard fundamental domain of the action of $2\pi i\mathbb{Z}$ on $\mathbb{C}$ by translation. Let us consider the set

$$Y := \left\{(z, u, r, s) \in F_j^n \times F_{\exp}^n \times \mathbb{R}^n \times \mathbb{R} \;\middle|\; j(z) = \exp(u),\ r \cdot u = 2\pi i s\right\}$$

where $j(z) = \exp(u) = e^u$ means that for every $k = 1, ..., n$ we have $j(z_k) = \exp(u_k)$. The way we defined Y is such that the former two components (z, u) are in the preimage of the set V defined in the previous section through the map $(j, \exp)$; the latter two components keep track of the multiplicative relation of the singular moduli, which becomes a linear relation in the preimage of exp. Let us now consider the projection of Y defined as following:

$$Z := \left\{(z, r, s) \in F_j^n \times \mathbb{R}^n \times \mathbb{R} \;\middle|\; \exists u \in F_{\exp}^n,\ (z, u, r, s) \in Y\right\}$$

It is not difficult to notice that there is a 1-1 correspondence between singular dependent n-tuples and the points $(z, r, s) \in Z$ such that $[\mathbb{Q}(z_i) : \mathbb{Q}] = 2$ for every $i = 1, ..., n$ and $(r, s) \in \mathbb{Z}^{n+1}$ have no common divisors and $r \neq (0, ..., 0)$. We will call this points *singular points of* Z.

Proposition 5.4.5. *Let us suppose that there are infinitely many singular dependent n-tuples, then there exists a constant $c > 0$ such that frequently in $T > 0$ there are at least $cT^{\frac{1}{4n^2}}$ singular points of Z with height at most T.*

Proof. Let $\sigma \in V$ be a singular dependent n-tuple, then its preimage through $(j, \exp)$ is a point $\tau = (z_1, ..., z_n, u_1, ..., u_n) \in F_j^n \times F_{\exp}^n$ and there exist $r_1, ..., r_n, s \in \mathbb{Z}$ such that $(z, u, r, s) \in Y$. We know that $\sum_{i=1}^{n} r_i u_i = 2\pi i s$, in particular

$$1 = \sigma_1^{r_1} \cdot ... \cdot \sigma_n^{r_n} = j(z_1)^{r_1} \cdot ... \cdot j(z_n)^{r_n} = (e^{u_1})^{r_1} \cdot ... \cdot (e^{u_n})^{r_n}$$

hence, if $d = [\mathbb{Q}(\sigma_1, ..., \sigma_n) : \mathbb{Q}]$, by proposition 2.2.10 there exists a constant c_1 dependent on n such that

$$|r_i| \leq c_1 d^n (\log d) \prod_{k \neq i} \mathrm{h}(\sigma_k) \tag{5.1}$$

By proposition 2.2.7, given $\epsilon > 0$, there exists a constant c_2 such that $\mathrm{h}(\sigma_k) \leq c_2 |\Delta_{\sigma_k}|^{\epsilon}$ for every k, then $\mathrm{h}(\sigma_k) \leq |\Delta(\sigma)|^{\epsilon}$. In addition, by proposition 2.2.9 we know that for every $\epsilon > 0$ there exists a constant c_3 such that

$$[\mathbb{Q}(\sigma_i) : \mathbb{Q}] = |Cl(\mathcal{O}_{\sigma_i})| \leq c_3 |\Delta_{\sigma_i}|^{\frac{1}{2}+\epsilon} \leq c_3 |\Delta(\sigma)|^{\frac{1}{2}+\epsilon}$$

hence we have that $d \leq c_3^n |\Delta(\sigma)|^{\frac{n}{2}+n\epsilon}$, so 5.1 becomes

$$\mathrm{H}(r_i) = |r_i| \leq c_4 |\Delta(\sigma)|^{\frac{n^2}{2}+(n^2+n+1)\epsilon} \log(\Delta(\sigma)) \leq c_5 |\Delta(\sigma)|^{n^2}$$

for some constants c_4, c_5 and for a suitable choice of ϵ. A bound on s can be found by noticing that $u_i \in F_{\exp}$, then $|\operatorname{Im}\{u_i\}| \leq 2\pi i$, so using the linear dependence $\sum_{i=1}^{n} r_i u_i = 2\pi i s$ we easily see that $\mathrm{H}(s) = |s| \leq \sum_{i=1}^{n} |r_i| \leq n\,\mathrm{H}(r)$. Finally, since $z_1, ..., z_n$ are quadratic integers, by proposition 2.2.8 we know that $\mathrm{H}(z) \leq 2\Delta(\sigma)$. Then there exists a constant c_6 such that $\mathrm{H}(z, r, s) \leq c_6 |\Delta(\sigma)|^{n^2}$.

By Northcott's theorem (2.2.6), there are singular points of Z arbitrarily high, thus with arbitrarily high complexity. Let $(z, r, s) \in Z$ be a singular point with complexity Δ, if it is given by a singular dependent n-tuple σ where $|\Delta_{\sigma_i}| = \Delta$, by proposition 2.2.9 for every ϵ there exists a constant c_7 such that $[\mathbb{Q}(\sigma_i) : \mathbb{Q}] = Cl(\mathcal{O}_{\sigma_i}) \geq c_7 |\Delta|^{\frac{1}{2}-\epsilon}$. By taking $\epsilon = \frac{1}{4}$ we have $[\mathbb{Q}(\sigma_i) : \mathbb{Q}] \geq c_7 |\Delta|^{\frac{1}{4}}$, then σ_i has at least $c_7 \Delta^{\frac{1}{4}}$ conjugates. Every automorphisms sends a singular dependent n-tuple to another singular dependent n-tuple; we can assume that σ is the n-tuple with the highest complexity among all its conjugates (if necessary, by increasing Δ), then there are at least $c_7 \Delta^{\frac{1}{4}}$ singular dependent n-tuples with complexity at most Δ. By taking $T = c_6 \Delta(\sigma)^{n^2}$, we see that this is equivalent to saying that there are at least $cT^{\frac{1}{4n^2}}$ singular points of Z with height at most T, for a suitable constant c_8. $\square$

Let us now consider the map $\rho : F_j^n \times \mathbb{R}^{n+1} \to \mathbb{R}^{2n} \times \mathbb{R}^{n+1}$ taking real coordinates, this is clearly injective, then there is a bijection $Z \longleftrightarrow \rho(Z)$. We can notice that if the height of the singular points of Z is bounded then also the height of the points of $\rho(Z)$ must be bounded and vice versa. In particular, let (z, r, s) be a singular point of Z, then if $z_k = x_k + iy_k$, $\rho(z, r, s) = (x, y, r, s)$. Since it is a singular point, z_k is quadratic, i.e. $x_k \in \mathbb{Q}$ and $[\mathbb{Q}(y_k) : \mathbb{Q}] \leq 2$, hence the degree of the points of $\rho(Z)$ is bounded by 2. By point 3 of proposition 2.2.6 we have that

$$\begin{aligned}
\mathrm{h}(x) &= \mathrm{h}\left(\frac{1}{2} \cdot 2x\right) \leq \mathrm{h}(2x) + \log 2 \leq \mathrm{h}(x + iy) + \mathrm{h}(x - iy) + 2\log 2 = \\
&= \mathrm{h}(z) + \mathrm{h}(\bar{z}) + \log 4 = 2\,\mathrm{h}(z) + \log 4 \\
\mathrm{h}(y) &= \mathrm{h}\left(\frac{1}{2i} \cdot 2iy\right) \leq \mathrm{h}(2iy) + \log 2 \leq \mathrm{h}(iy + x) + \mathrm{h}(iy - x) + 2\log 2 = \\
&= \mathrm{h}(z) + \mathrm{h}(\bar{z}) + \log 4 = 2\,\mathrm{h}(z) + \log 4
\end{aligned}$$

because z and $\bar{z}$ are conjugates over $\mathbb{Q}$. Moreover, we have that

$$\mathrm{h}(z) = \mathrm{h}(x + iy) \leq \mathrm{h}(x) + \mathrm{h}(y) + \log 2 \leq 2\,\mathrm{h}(x, y) + \log 2$$

thus we have

$$\mathrm{H}(x, y) \leq 4\,\mathrm{H}(z)^2 \qquad \mathrm{H}(z) \leq 2\,\mathrm{H}(x, y)^2 \tag{5.2}$$

This implies that, by proposition 5.4.5, the number of special points of $\rho(Z)$ with height at most T is at least $cT^{\frac{1}{8n^2}}$ for a suitable constant c.

Now, we can notice that Z is a definable set in the o-minimal structure $R_{an,\exp}$, because it is the projection of Y, which is definable since it defined by algebraic equations and by the functions exp and j. Indeed, exp and j are definable functions thanks to corollary 4.1.18. Hence, we can apply theorem 4.2.6, the algebraic version of Pila-Wilkie, to the set $\rho(Z)$ and obtain that

$$|\rho(Z)^{tr}(\mathbb{Q}, 2, T)| \leq c'T^{\epsilon}$$

for some constant c' depending on ϵ. By taking $\epsilon < \frac{1}{8n^2}$, we notice that, if there are infinitely many singular points of $\rho(Z)$, then infinitely many of them must lie in $\rho(Z)^{alg}$, because they are at least $cT^{\frac{1}{8n^2}} - c'T^{\epsilon}$, which tends to ∞ as T tends to ∞.

Let us now consider the set

$$\tilde{Z} = \{(z, u) \in \mathcal{H}^n \times \mathbb{C}^n | \exists (r, s) \in \mathbb{R}^{n+1}, (z, u, r, s) \in Y\}$$

it is not difficult to notice that $\tilde{Z} = \pi^{-1}(V)$, where π is the same of that in chapter 3, because one can always find an r such that the linear combination of the imaginary parts of u is zero. We need the following lemma:

Lemma 5.4.6. *Let us suppose that $\rho(Z)^{alg}$ contains infinitely many singular points, then there is an algebraic variety $Y \subset \mathcal{H}^n \times \mathbb{C}^n$ which intersect $\pi^{-1}(V)$ in a positive dimensional component A which contains singular points and is atypical in dimension, i.e.*

$$\dim A > \dim Y + \dim V - \dim X$$

As explained by Pila and Tsimerman in their article, this lemma can be proven with the same strategies used in [HP12] and [HP16].

Lemma 5.4.7. *Let $W \subseteq X$ be a weakly special subvariety containing a special point, then it is a special subvariety.*

Proof. W is a product $S \times T$ of weakly special subvarieties of $\mathbb{C}^n$ and $(\mathbb{C}^*)^n$ respectively. Likewise, a special point is a product of special points. We just need to prove the statement separately for S and T. If $(x_1, ..., x_n) \in T$ is a special point, then x_i is a root of unity for every i, therefore, for every equation defining T we have $x_1^{a_1} \cdot ... \cdot x_n^{a_n} = \xi$ and so ξ is a root of unity, hence T is special. Now, if $S = M_0 \times ... \times M_k$, like in definition 3.1.1, either $M_0 = \emptyset$ (which means that S is special) or $M_0 \subset \mathbb{C}^{m_0}$ is a point. Since there is a special point $(x_1, ..., x_n) \in S$, its coordinates in $\mathbb{C}^{m_0}$ are the same of M_0, hence M_0 is a special point and S is special. □

We now consider the algebraic subvariety Y and the component A given by lemma 5.4.6. If we take a component B with respect to V containing A which is maximal among those such that $\partial(B) \leq \partial(A)$, we can notice that B is an optimal component (as defined at the end of chapter 3). Hence, by weak complex Ax 3.2.15, B is also a geodesic component, so the Zariski closure W of B in X is a weakly special subvariety and therefore special, by lemma 5.4.7. We have that

$$\dim W - \dim B = \partial(B) \leq \partial(A) \leq \dim Y - \dim A < \dim V - \dim X$$

and so B is an atypical component of V. Hence, by lemma 5.3.1, we got a contradiction, in particular, there can't be infinitely many singular dependent n-tuples. This completes the proof.

Bibliography

[Ax71] James Ax. On schanuel's conjectures. *Annals of mathematics*, pages 252–268, 1971.

[BP89] Enrico Bombieri and Jonathan Pila. The number of integral points on arcs and ovals. *Duke Mathematical Journal*, 59(2):337–357, 1989.

[Cox11] David A Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011.

[HP12] Philipp Habegger and Jonathan Pila. Some unlikely intersections beyond andré–oort. *Compositio Mathematica*, 148(1):1–27, 2012.

[HP16] Philipp Habegger and Jonathan Pila. O-minimality and certain atypical intersections. In *Annales scientifiques de l'ENS*, volume 49. Société Mathématique de France, 2016.

[LM04] Thomas Loher and David Masser. Uniformly counting points of bounded height. *Acta Arithmetica*, 111:277–297, 2004.

[Pau14] Roland Paulin. An explicit andré-oort type result for $\mathbb{P}^1(\mathbb{C}) \times \mathbb{G}_m(\mathbb{C})$ based on logarithmic forms. *arXiv preprint arXiv:1403.2949*, 2014.

[Pil09] Jonathan Pila. On the algebraic points of a definable set. *Selecta Mathematica*, 15(1):151–170, 2009.

[Pil11] Jonathan Pila. O-minimality and the André-Oort conjecture for $\mathbb{C}^n$. *Ann. of Math. (2)*, 173(3):1779–1840, 2011.

[PS04] Ya'acov Peterzil and Sergei Starchenko. Uniform definability of the weierstrass $\wp$ functions and generalized tori of dimension one. *Selecta Math.(NS)*, 10(4):525–550, 2004.

[PST+21] Jonathan Pila, Ananth Shankar, Jacob Tsimerman, Hélène Esnault, and Michael Groechenig. Canonical heights on shimura varieties and the andré-oort conjecture. *arXiv preprint arXiv:2109.08788*, 2021.

[PT+16] Jonathan Pila, Jacob Tsimerman, et al. Ax–schanuel for the j-function. *Duke Mathematical Journal*, 165(13):2587–2605, 2016.

[PT17] Jonathan Pila and Jacob Tsimerman. Multiplicative relations among singular moduli. *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)*, 17(4):1357–1382, 2017.

[PW+06] Jonathan Pila, Alex James Wilkie, et al. The rational points of a definable set. *Duke Mathematical Journal*, 133(3):591–616, 2006.

[PZ08] Jonathan Pila and Umberto Zannier. Rational points in periodic analytic sets and the manin–mumford conjecture. *Rendiconti Lincei-Matematica e Applicazioni*, 19(2):149–162, 2008.

[Ray83] Michel Raynaud. Sous-variétés d'une variété abélienne et points de torsion. In *Arithmetic and geometry*, pages 327–352. Springer, 1983.

[Tsi15] Jacob Tsimerman. Ax-schanuel and o-minimality. *O-minimality and Diophantine geometry*, 421:216, 2015.

[VdD86] Lou Van den Dries. A generalization of the tarski-seidenberg theorem, and some nondefinability results. *Bulletin (New Series) of the American Mathematical Society*, 15(2):189–193, 1986.

[vdDMM94] Lou van den Dries, Angus Macintyre, and David Marker. The elementary theory of restricted analytic fields with exponentiation. *Annals of Mathematics*, 140(1):183–205, 1994.