Chapter 4

The Schinzel–Zassenhaus Conjecture

4.1 Statement

At the end of Chapter 1, we stated the following widely open *Lehmer Conjecture*.

Conjecture 4.1.1 (Lehmer Conjecture)**.** *There exists a constant $c > 0$ such that each algebraic number $\alpha \in \overline{\mathbb{Q}}^*$, which is not a root of unity, satisfies*

$$h(\alpha) \geq \frac{c}{\deg(\alpha)}. \tag{4.1.1}$$

The assumption of the conjecture is reasonable: $h(\alpha) = 0$ if α is 0 or a root of unity.

A similar but weaker conjecture is the *Schinzel–Zassenhaus Conjecture*.

Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic integer, and $f \in \mathbb{Z}[X]$ be the minimal polynomial of α with leading coefficient 1. Denote by $d := \deg(\alpha) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, and write $\alpha_1 = \alpha, \ldots, \alpha_d \in \mathbb{C}$ for the Galois conjugates of α. Then $f(X) = (X - \alpha_1) \cdots (X - \alpha_d)$.

Definition 4.1.2. *The **house** of α, denote by $\lceil \alpha \rceil$, is* $\max_{i=1}^{d} |\alpha_i|$.

Now we are ready to state the *Schinzel–Zassenhaus Conjecture*, recently proved by Dimitrov.

Theorem 4.1.3. *There exists a constant $c > 0$ such that each algebraic integer $\alpha \in \overline{\mathbb{Q}}^*$, which is not a root of unity, satisfies*

$$\log \lceil \alpha \rceil \geq \frac{c}{\deg(\alpha)}. \tag{4.1.2}$$

In fact, Dimitrov's proof shows that one can take $c = \log 2/4$.

The goal of this chapter is to present the proof of Theorem 4.1.3. Before doing this, let us start by explaining how the Lehmer Conjecture implies the Schinzel–Zassenhaus Conjecture. Roughly speaking, $h(\alpha)$ is the *average* of $\log^+ |\alpha_i|$, while $\log \lceil \alpha \rceil$ is the *maximum* of $\log^+ |\alpha_i|$. Here, $\log^+(\cdot)$ is defined to be $\max\{\log(\cdot), 0\}$.

Proof of Conjecture 4.1.1 implying Theorem 4.1.3. Let $\alpha \in \overline{\mathbb{Q}}^*$ be an algebraic integer which is not a root of unity. Let $f \in \mathbb{Z}[X]$ be its minimal polynomial with leading coefficient 1. Denote by $d = \deg(\alpha)$. Let the real number $c > 0$ be from Conjecture 4.1.1.

We claim that $\sum_{i=1}^{d} \log^+ |\alpha_i| \geq c$. To show this, we use the Mahler measure.[1] By Proposition 1.3.14, we have $\deg(\alpha) h(\alpha) = \log M(f)$. By Jensen's Lemma (Lemma 1.3.9), we have $\log M(f) = \sum_{i=1}^{d} \log^+ |\alpha_i|$. Thus (4.1.1) yields the desired lower bound.

[1] This is an overkill. One only needs some argument from the proof of Proposition 1.3.14 to achieve this. Nevertheless since we had much discussion on the Mahler measure in Chapter 1, we present the proof in this way which looks "cleaner". Moreover, this is a good recall the of link of the current formulation of the Lehmer Conjecture to the one in most references where the Mahler measure is involved.

Up to sign, $|\alpha_1 \cdot \cdots \cdot \alpha_d|$ is the constant term of $f \in \mathbb{Z}[X]$. So $|\alpha_1 \cdot \cdots \cdot \alpha_d| \geq 1$ since $\alpha \neq 0$. So there exists $i \in \{1, \ldots, d\}$ such that $\log |\alpha_i| \geq 0$. Thus $\log \lceil \overline{\alpha} \rceil = \max_{1 \leq i \leq d} \log^+ |\alpha_i|$.

The previous two paragraphs then imply that $d \log \lceil \overline{\alpha} \rceil \geq c$. Hence we are done. □

We close this section by a simple property of the house.

Lemma 4.1.4. *Let $\alpha \in \overline{\mathbb{Q}}^*$ be an algebraic integer. Then we have*

(i) $\lceil \overline{\alpha} \rceil \geq 1$;

(ii) $\lceil \overline{\alpha} \rceil = 1$ *if and only if* α *is a root of unity.*

Proof. Up to sign, $|\alpha_1 \cdot \cdots \cdot \alpha_d|$ is the constant term of $f \in \mathbb{Z}[X]$. So $|\alpha_1 \cdot \cdots \cdot \alpha_d| \geq 1$ since $\alpha \neq 0$. Thus $\lceil \overline{\alpha} \rceil = \max |\alpha_i| \geq 1$. This proves (i).

For (ii), the "if" direction is clearly true. Now we prove the "only if" direction. Assume $\lceil \overline{\alpha} \rceil = 1$. Then $|\alpha_i| = 1$ for each $i \in \{1, \ldots, d\}$. For each positive integer k, set $f_k(X) := \prod_{i=1}^{d} (X - \alpha_i^k)$. The Galois conjugates of the algebraic integer α^k are precisely $\alpha_1^k, \ldots, \alpha_d^k$. Hence $f_k \in \mathbb{Z}[X]$. Thus the absolute value of each coefficient of f_k is $\leq 2^d$ because $|\alpha_i^k| = 1$ for each i and k. As d is independent of k, the set $\{f_k : k \in \mathbb{Z}_{>0}\}$ is a finite set. So $\{\alpha^k : k \in \mathbb{Z}_{>0}\}$ is a finite set. Hence $\alpha^l = 1$ for some $l \in \mathbb{Z}_{>0}$. We are done. □

4.2 Transfinite diameter

Let $K \subseteq \mathbb{C}$ be a non-empty *compact* set.

4.2.1 Basic definition and properties

The *diameter* of K, denoted by $d_2(K)$, is defined to be $\max_{z_1, z_2 \in K} |z_1 - z_2|$. We extend this notion now. Let $n \geq 2$. For $z_1, \ldots, z_n \in K$, denote by

$$V(z_1, \ldots, z_n) := \det \begin{bmatrix} 1 & z_1 & \cdots & z_1^{n-1} \\ 1 & z_2 & \cdots & z_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & z_n & \cdots & z_n^{n-1} \end{bmatrix} = \prod_{1 \leq i < j \leq n} (z_j - z_i).$$

Definition 4.2.1. *For $n \geq 2$, define*

$$d_n(K) := \max_{z_1, \ldots, z_n \in K} |V(z_1, \ldots, z_n)|^{1/\binom{n}{2}}.$$

In other words, $d_n(K)$ is the maximum of the *geometric mean* of the distances of n points in K. This observation leads to the following lemma, whose proof we leave to the exercise class.

Lemma 4.2.2. *We have $d_2(K) \geq d_3(K) \geq \cdots \geq d_n(K) \geq \cdots \geq 0$.*

Thus the limit $\lim_{n \to \infty} d_n(K)$ exists.

Definition 4.2.3. *The **transfinite diameter** of K is defined to be*

$$d_\infty(K) := \lim_{n \to \infty} d_n(K).$$

Example 4.2.4. *(i) If K is a finite set, then $d_\infty(K) = 0$. Indeed, $d_{\#K+1}(K) = 0$.*

(ii) The converse of (i) is not true. Let $K = \{0\} \cup \{\frac{1}{n} : n \in \mathbb{Z}_{>0}\}$. *As the geometric mean is at most the arithmetic mean, it is not hard to show that* $d_n(K) \to 0$. *Hence* $d_\infty(K) = 0$.

To get a better feeling of the transfinite diameter, let us compute a slightly more complicated example.

Lemma 4.2.5. *Consider the unit circle* $S^1 = \{e^{i\theta} : 0 \le \theta < 2\pi\} \subseteq \mathbb{C}$. *We have* $d_\infty(S^1) = 1$.

Proof. Let us show that $d_\infty(S^1) \ge 1$. Let ζ_n be a primitive n-th root of unity. Then $V(1, \zeta_n, \dots, \zeta_n^{n-1}) \neq 0$ by definition. Next $V(1, \zeta_n, \dots, \zeta_n^{n-1})$ is an algebraic integer because by the determinant expansion it is a sum of products of algebraic integers. Moreover, $V(1, \zeta_n, \dots, \zeta_n^{n-1}) \in \mathbb{Q}$ since it is invariant under the Galois group. Thus $V(1, \zeta_n, \dots, \zeta_n^{n-1}) \in \mathbb{Z}$ and is non-zero. Thus $|V(1, \zeta_n, \dots, \zeta_n^{n-1})| \ge 1$. So $d_n(S^1) \ge |V(1, \zeta_n, \dots, \zeta_n^{n-1})|^{2/n(n-1)} \ge 1$. This implies $d_\infty(S^1) \ge 1$.

Now let us show that $d_\infty(S^1) \le 1$. For any $z_1, \dots, z_n \in S^1$, by the determinant expansion we have $|V(z_1, \dots, z_n)|^{2/n(n-1)} \le (2n!)^{2/n(n-1)} \le (2n^n)^{2/n(n-1)} = n^{2/(n-1)} 2^{2/n(n-1)}$. Thus $d_n(S^1) \le n^{2/(n-1)} 2^{2/n(n-1)}$. Taking $n \to \infty$, we get $d_\infty(S^1) \le 1$. □

Remark 4.2.6. *(i) One can show that* $d_n(S^1)$ *is attained at the points* $1, \zeta_n, \dots, \zeta_n^{n-1}$.

(ii) The second part of the proof also works for $K = \overline{D(0,1)}$, *the closed unit disk. Then combined with the first part, we also have* $d_\infty(\overline{D(0,1)}) = 1$.

(iii) The last observation is not a coincidence. In fact, as a consequence of the maximum principal, we have $d_\infty(K) = d_\infty(\partial K)$ *for any non-empty compact region* $K \subseteq \mathbb{C}$.

It is a natural question to compute $d_\infty([0,1])$ for the real interval $[0,1]$. It turns out that the analysis involved is quite complicated. In this course, we do this computation by relating the transfinite diameter to the *Chebyshev constant* introduced later on (Definition-Lemma 4.2.9).

We end this subsection with some properties of the transfinite diameter.

Lemma 4.2.7. *We have:*

(i) $d_\infty(\lambda K) = |\lambda| d_\infty(K)$ *for each* $\lambda \in \mathbb{C}$;

(ii) $d_\infty(\lambda + K) = d_\infty(K)$ *for each* $\lambda \in \mathbb{C}$;

(iii) $d_\infty(K') \le d_\infty(K)$ *if* $K' \subseteq K$;

In fact, the same statements hold true if d_∞ is replaced by d_n for any $n \ge 2$. The proof of this lemma is an easy observation.

In this course, we also need the following lemma for the proof of the Polya–Bertrandias theorem. It allows to replace K by a "nicer" compact subset of $\mathbb{C}$.

Lemma 4.2.8. *For each* $\epsilon > 0$, *set* $K_\epsilon := \{w \in \mathbb{C} : |w - z| \le \epsilon \text{ for some } z \in K\}$. *Then*

$$\lim_{\epsilon \to 0} d_\infty(K_\epsilon) = d_\infty(K).$$

The following inequality is useful to prove Lemma 4.2.8: For positive numbers δ and $a_1, \dots, a_n$, we have $\prod_{j=1}^n (a_j + \delta) - \prod_{j=1}^n a_j \le (A + \delta)^n - A^n$ where $A = \max_j a_j$.

4.2.2 Transfinite diameter and Chebyshev constant

For each positive integer n, set

$$\tau_n(K) := \left(\min_{\substack{P\in\mathbb{C}[X] \text{ monic,} \\ \deg P = n}} \max_{z\in K} |P(z)| \right)^{1/n}. \tag{4.2.1}$$

Definition-Lemma 4.2.9. *The limit*

$$\tau(K) = \lim_{n\to\infty} \tau_n(K)$$

exists. It is called the ***Chebyshev constant*** *of K.*

Proof. Let $a := \liminf_{n\geq 1} \tau_n(K)$ and $b := \limsup_{n\geq 1} \tau_n(K)$. Our goal is to show that $a = b$.

Let $\epsilon > 0$. Then there exists $n \geq 1$ such that $\tau_n(K) \leq a + \epsilon$. So there exists a monic polynomial $P \in \mathbb{C}[X]$ with $\deg P = n$ such that $|P(z)| \leq (a+\epsilon)^n$ for all $z \in K$. Now fix $z_0 \in K$, and let $Q(z) := (z - z_0)^l P(z)^k$. Then $|Q(z)| \leq d_2(K)^l (a+\epsilon)^{nk}$ for all $z \in K$. But $Q \in \mathbb{C}[X]$ is a monic polynomial of degree $l + nk$. So

$$\tau_{l+nk}(K)^{l+nk} \leq d_2(K)^l (a+\epsilon)^{nk} \tag{4.2.2}$$

for all non-negative integres l and k.

Next, there exists an increasing sequence $\{n_i \in \mathbb{Z}_{>0}\}_{i\geq 1}$ such that $b = \lim_{i\to\infty} \tau_{n_i}(K) = b$. Write $n_i = l_i + nk_i$ with $l_i \in \{0, \ldots, n-1\}$. Then (4.2.2) yields

$$\tau_{n_i}(K) \leq d_2(K)^{\frac{l_i}{n_i}} (a+\epsilon)^{\frac{n_i - l_i}{n_i}}.$$

Notice that l_i is bounded when $i \to \infty$. Hence letting $i \to \infty$ we obtain $b \leq a + \epsilon$. As $\epsilon > 0$ is arbitrary, we then have $b = a$. Now we are done. □

Proposition 4.2.10. $\tau(K) = d_\infty(K)$.

Proof. We prove this in two steps.

First, let us establish the following inequality: For each positive integer n, we have

$$\tau_n(K)^n \leq \frac{d_{n+1}(K)^{\frac{n(n+1)}{2}}}{d_n(K)^{\frac{n(n-1)}{2}}} \leq (n+1)\tau_n(K)^n. \tag{4.2.3}$$

By definition of d_{n+1} (recall that K is compact), $d_{n+1}(K) = |V(z_1, \ldots, z_{n+1})|^{2/n(n+1)}$ for some $z_1, \ldots, z_{n+1} \in K$. By definition of τ_n, there exists a monic $P \in \mathbb{C}[X]$ with $\deg P = n$ such that $\tau_n(K)^n = \max_{z\in K} |P(z)|$. Now we have

$$\begin{aligned}
d_{n+1}(K)^{\frac{n(n+1)}{2}} = |V(z_1, \ldots, z_{n+1})| &= \left| \det \begin{bmatrix} 1 & z_1 & \cdots & z_1^{n-1} & z_1^n \\ 1 & z_2 & \cdots & z_2^{n-1} & z_2^n \\ \vdots & \vdots & & \vdots & \\ 1 & z_n & \cdots & z_n^{n-1} & z_n^n \end{bmatrix} \right| \\
&= \left| \det \begin{bmatrix} 1 & z_1 & \cdots & z_1^{n-1} & P(z_1) \\ 1 & z_2 & \cdots & z_2^{n-1} & P(z_2) \\ \vdots & \vdots & & \vdots & \\ 1 & z_n & \cdots & z_n^{n-1} & P(z_n) \end{bmatrix} \right| \\
&\leq |P(z_1)||V(z_2, \ldots, z_{n+1})| + \cdots + |P(z_{n+1})||V(z_1, \ldots, z_n)| \\
&\leq (n+1)\tau_n(K)^n d_n(K)^{\frac{n(n-1)}{2}}.
\end{aligned}$$

This shows the second inequality in (4.2.3). For the first inequality, by definition of d_n (recall that K is compact), $d_n(K) = |V(z_1, \dots, z_n)|^{2/n(n-1)}$ for some $z_1, \dots, z_n \in K$. Take $P(X) := \prod_{i=1}^n (X - z_i)$. Then P is monic and has degree n. So $\tau_n(K)^n \le \max_{z\in K} |P(z)|$. Take $z_0 \in K$ such that $|P(z_0)| = \max_{z\in K} |P(z)|$; such a z_0 exists since K is compact. Then

$$d_{n+1}(K)^{\frac{n(n+1)}{2}} \ge |V(z_1, \dots, z_n, z_0)| = |P(z_0)||V(z_1, \dots, z_n)| \ge \tau_n(K)^n d_n(K)^{\frac{n(n-1)}{2}}.$$

Next, take the log of (4.2.3) and sum up from 2 to n. We then obtain

$$\frac{2}{n(n+1)} \left(\log d_2(K) + \sum_{i=2}^n i \log \tau_i(K) \right) \le \log d_{n+1}(K) \le \frac{2}{n(n+1)} \left(\log(n+1)! + \log d_2(K) + \sum_{i=2}^n i \log \tau_i(K) \right)$$

When $n \to \infty$, $\frac{2}{n(n+1)} \log d_2(K) \to 0$, and $\frac{2}{n(n+1)} \log(n+1)! \le \frac{2}{n(n+1)} \log(n+1)^{n+1} \to 0$. And it is not hard to check that $\frac{2}{n(n+1)} \sum_{i=2}^n i \log \tau_i(K) \to \log \tau(K)$. Hence we are done. □

This proposition yields the following corollary, which is useful to compute the transfinite diameter.

Lemma 4.2.11. *For each $P \in \mathbb{C}[X] \setminus \mathbb{C}$ monic, we have*

$$d_\infty(P(K)) = d_\infty(K)^{\deg P}.$$

Proof. Write $d = \deg P$. By Proposition 4.2.10, we only need to prove $\tau(P(K)) = \tau(K)^d$.

For $\ge$. For $n \ge 1$, let $Q \in \mathbb{C}[X]$ be monic of degree n such that $\tau_n(P(K))^n = \max_{z\in P(K)} |Q(z)|$. Then $\tau_{nd}(K)^{nd} \le \max_{z\in K} |Q(P(z))| = \tau_n(P(K))^n$. Therefore $\tau_{nd}(K)^d \le \tau_n(P(K))$. As d is fixed, letting $n \to \infty$ yields $\tau(K)^d \le \tau(P(K))$.

For $\le$. For $n \ge 2$, there exists $Q \in \mathbb{C}[X]$ monic of degree n such that $\tau_n(K)^n = \max_{z\in K} |Q(z)|$. Write $z_1, \dots, z_n \in \mathbb{C}$ for the roots of Q. Take any $w \in P(K)$, and set $q_n(w) := \prod_{i=1}^n (w - P(z_i))$. Write $w_1, \dots, w_d$ for the roots of the polynomial $P(X) - w \in \mathbb{C}[X]$. Then we have

$$\prod_{j=1}^d Q(w_j) = \prod_{j=1}^d \prod_{i=1}^n (w_j - z_i) = \prod_{i=1}^n \prod_{j=1}^d (w_j - z_i) = (-1)^d \prod_{i=1}^n \prod_{j=1}^d (z_i - w_j) = (-1)^d \prod_{i=1}^n (P(z_i) - w).$$

Hence $\prod_{j=1}^d Q(w_j) = (-1)^{nd} q_n(w)$. Since $q_n \in \mathbb{C}[X]$ is monic of degree n, we have

$$\tau_n(P(K))^n \le \max_{w\in P(K)} |q_n(w)| = \max_{w\in P(K)} \left| \prod_{j=1}^d Q(w_j) \right| \le (\tau_n(K)^n)^d$$

Thus $\tau(P(K)) \le \tau(K)^d$ by letting $n \to \infty$. □

Corollary 4.2.12. $d_\infty([0,1]) = 1/4$.

Proof. Consider $K := [-2, 2]$ and the polynomial $P(X) = X^2 - 2$. We have $P^{-1}(K) = K$. Thus Lemma 4.2.11 yield $d_\infty(K) = d_\infty(K)^{1/2}$. Hence $d_\infty(K) \in \{0, 1\}$. Thus $d_\infty([0,1]) \in \{0, 1/4\}$ by Lemma 4.2.7 (i) and (ii).

It remains to show that $d_\infty([0,1]) > 0$. For each $n \ge 2$, consider the n points $0, 1/(n-1), \dots, (n-2)/(n-1), 1$. We have

$$\left| V\left(0, \frac{1}{n-1}, \dots, \frac{n-2}{n-1}, 1\right) \right| = \left(\frac{1}{n-1}\right)^{n-1} \left(\frac{2}{n-1}\right)^{n-2} \cdots \left(\frac{k}{n-1}\right)^{n-k} \cdots 1 = \frac{(n-1)! \cdots 2! 1!}{(n-1)^{\binom{n}{2}}}.$$

Set $h_n := \frac{((n-1)!\cdots 2!1!)^{2/n(n+1)}}{n-1}$ for each $n \geq 2$. Then $h_n \in [0,1]$ and hence $\{h_n\}$ contains a convergent subsequence. Let A be the limit of this convergent subsequence. It is easy to check that $\frac{h_{n+1}^{n+2}}{h_n^n} = \frac{(n-1)^n}{n^n}\frac{(n!)^{\frac{2}{n+1}}}{n^2}$. Taking the limit yield

$$A^2 = \frac{A^{n+2}}{A^n} = \lim_{n\to\infty} \frac{(n-1)^n}{n^n}\frac{(n!)^{\frac{2}{n+1}}}{n^2}.$$

Stirling's Formula says that $n! \sim \sqrt{2\pi n}(n/e)^n$ when $n \to \infty$. Thus $A = e^{-3/2} > 0$.

By definition, we have $d_n([0,1]) \geq h_n$. Hence $d_\infty([0,1]) \geq A > 0$. Hence we are done. □

In Dimitrov's proof of the Schinzel–Zassenhaus conjecture, the following *hedgehog* plays an important role. Let $z_1, \ldots, z_n \in \mathbb{C}^*$. The hedgehog with vertices $z_1, \ldots, z_n$, denoted by $K(z_1, \ldots, z_n)$, is defined to be $\bigcup_{i=1}^n [0,1]z_i$. A theorem of Dubini asserts that

$$d_\infty(K(z_1, \ldots, z_n)) \leq 4^{-1/n} \max_{1\leq i\leq n} |z_i|. \tag{4.2.4}$$

We shall not prove this result in our course. Instead, let us see an example. Let ζ_n be a primitive n-th root of unity, for example $\zeta_n = e^{2\pi i/n}$. Then $P(K(\zeta_n, \ldots, \zeta_n^n)) = [0,1]$ where $P = X^n$. Thus by Lemma 4.2.11 and Corollary 4.2.12, we have $d_\infty(K(\zeta_n, \ldots, \zeta_n^n)) = 4^{-1/n}$.

4.3 Rationality of power series

In this section, we discuss when a power series (*i.e.* an element in $\mathbb{C}[[X]]$) is rational (*i.e.* lies in $\mathbb{C}[X]_{(X)}$, in other words, is the quotient of two polynomials). The goal is to prove the Polya–Bertrandias theorem over $\mathbb{C}$.

Let us look at a baby example. Supposer that $f = \sum_{n\geq 0} a_n X^n \in \mathbb{Z}[[X]]$ converges for all $z \in \mathbb{C}$, and that f is represented by a holomorphic function on $D(0,r)$ with $r > 1$. Then $\limsup_n |a_n|^{1/n} \leq r^{-1} < 1$. Therefore f is a polynomial.

4.3.1 Criterion in terms of determinant

Let $f = \sum_{n\geq 0} a_n X^n \in \mathbb{C}[[X]]$.

Definition 4.3.1. *For each integer $k \geq 0$, define*

$$\Delta_k(f) := \begin{bmatrix} a_0 & a_1 & \cdots & a_k \\ a_1 & a_2 & \cdots & a_{k+1} \\ \vdots & \vdots & & \vdots \\ a_k & a_{k+1} & \cdots & a_{2k} \end{bmatrix} \in \mathrm{Mat}_{(k+1)\times(k+1)}(\mathbb{C}).$$

Theorem 4.3.2. *f is rational if and only if $\det \Delta_k(f) = 0$ for all $k \gg 1$.*

Proof. We start with "only if". Let $f = P/Q$ with $P, Q \in \mathbb{C}[X]$. Write $Q = q_0 X^d + \cdots + q_d$ with $q_0 q_d \neq 0$. Then $Qf = P$, and the coefficient of X^{d+k} is $\sum_{i=0}^d q_{d-i} a_{d-i+k}$, which equals 0 if $d + k > \deg P$. Therefore $\det \Delta_k(f) = 0$ for all $k > \deg P$.

Conversely let us prove the "if" part. If $f = 0$ we are done. If $f \neq 0$, then leet m be the smallest non-negative integer such that $a_m \neq 0$. Then f is rational if and only if $\sum_{n\geq 0} a_{n+m} X^n$ is rational. Therefore by replacing f with $\sum_{n\geq 0} a_{n+m} X^n$, we may and do assume $a_0 \neq 0$. Then $\det \Delta_0(f) \neq 0$.

Let $d \geq 0$ be the largest integer with $\det \Delta_d(f) \neq 0$. Then $\det \Delta_k(f) = 0$ for all $k \geq d+1$.

There exists $\mathbf{q} = \begin{bmatrix} q_0 \\ \vdots \\ q_d \\ 1 \end{bmatrix} \in \mathbb{C}^{d+2} \setminus \{0\}$ such that $\Delta_{d+1}(f)\mathbf{q} = \mathbf{0}$. Thus $\sum_{j=0}^{d+1} q_j a_{i+j} = 0$ for all $i \in \{0, \ldots, d+1\}$.

Set $L_k := \sum_{j=0}^{d+1} q_j a_{k+j}$. Let $Q := q_0 X^d + \cdots + q_d$. Then $fQ = P + X^D L_0 + X^{D+1} L_1 + \cdots$ with P a polynomial of degree $\leq d-1$. Thus we can conclude by the following lemma. □

Lemma 4.3.3. *$L_k = 0$ for all $k \geq 0$.*

Proof. We prove this lemma by induction on k. By choice of $\mathbf{q}$, the lemma holds true for $k \leq d+1$.

For $k \geq d+1$. Assume $L_0 = \cdots = L_{k-1} = 0$. We wish to show that $L_k = 0$. We have

$$\Delta_k(f) = \begin{bmatrix} & a_{d+1} & \cdots & a_k \\ \Delta_d(f) & \vdots & & \vdots \\ & a_{2d+1} & \cdots & a_{d+k} \\ & a_{2d+2} & \cdots & a_{d+1+k} \\ * & \vdots & & \vdots \\ & a_{d+1+k} & \cdots & a_{2k} \end{bmatrix}$$

Add to the $(k+1)$-th column the previous $d+1$ columns with weight $q_0, \ldots, q_d$, then the $(k+1)$-th column becomes $\begin{bmatrix} L_{k-d-1} & \cdots & L_{k-1} & L_k & \cdots & L_{2k-d-1} \end{bmatrix}^\intercal$. Then add to the k-th column the previous $d+1$ columns with weight $q_0, \ldots, q_d$, then the k-th column becomes $\begin{bmatrix} L_{k-d-2} & \cdots & L_{k-2} & L_{k-1} & \cdots & L_{2k-d-2} \end{bmatrix}^\intercal$. Continuing this process, we get

$$\det \Delta_k(f) = \det \begin{bmatrix} & L_0 & \cdots & L_{k-d-1} & \\ \Delta_d(f) & \vdots & & \vdots & \\ & L_d & \cdots & L_{k-1} & \\ & L_{d+1} & \cdots & L_{k-1} & L_k \\ * & \vdots & & \vdots & \vdots \\ & L_{k-1} & \cdots & * & L_{2k-k-2} \\ & L_k & \cdots & * & L_{2k-d-1} \end{bmatrix}.$$

The upper right part is 0 by induction hypothesis. The lower right part has 0 as entries above the skew-diagonal whose entries are all L_k. Thus $\det \Delta_k(f) = \pm \det \Delta_d(f) L_k^{k-d}$. Since $\Delta_k(f) = 0$ and $\Delta_d(f) \neq 0$, we then have $L_k = 0$. □

4.3.2 The Polya–Bertrandias Theorem over $\mathbb{C}$

Theorem 4.3.4. *Let $K \subseteq \mathbb{C}$ be a non-empty compact set such that $\mathbb{C} \setminus K$ is connected. Assume that $f \in \mathbb{Z}[[X]]$ satisfies:*

(i) f converges on $D(0, \epsilon)$ for some $\epsilon > 0$,

(ii) $z \mapsto f(z^{-1})$ extends to a holomorphic map on $\mathbb{C} \setminus K$.

If $d_\infty(K) < 1$, then f is rational, i.e. $f = P/Q$ with $P, Q \in \mathbb{C}[X]$.

For various reasons, it is more convenient to work with $\hat{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$, the compactified complex plane.

There exists a version for $f \in F[[X]]$ for a number field F, for which $d_\infty(K) < 1$ is replaced by a condition involving all places of F. We will include this version as reading material at the end of this chapter.

Proof. By Lemma 4.2.8, $d_\infty(K_\epsilon) \to d_\infty(K)$ when $\epsilon \to 0^+$. Fix $\epsilon > 0$ such that $d_\infty(K_\epsilon) < 1$. Next we cover $K_{\epsilon/2}$ by disks of radius $\epsilon/2$, so that we get a compact set $K' \subseteq \mathbb{C}$ with

- $K_{\epsilon/2} \subseteq K' \subseteq K_\epsilon$,
- $d_\infty(K') < 1$,
- both $\partial K'$ and K' are semi-algebraic and piecewise C^∞.

Replace K by K'. Then ∂K has nice properties, and $f(z^{-1})$ is defined and bounded on ∂K. Thus we are able to do the integral

$$\oint_{\partial K} f(z^{-1})\mathrm{d}z.$$

For $n \geq 1$, let P_n be monic of degree n such that $\tau_n(K)^n = \max_{z\in K} |P_n(z)|$. Write, for each m, $p_m^{(n)}$ the coefficient of X^m for P_n. Then $p_n^{(n)} = 1$ for all n and $p_m^{(n)} = 0$ for all $m > n$.

For each i, j, let us compute $\mathrm{Res}_\infty f(z^{-1})P_i(z)P_j(z)$.[2]

On the one hand, $\mathrm{Res}_\infty f(z^{-1})P_i(z)P_j(z) = \mathrm{Res}_0 z^{-2} f(z)P_i(z^{-1})P_j(z^{-1})$ equals the coefficient of the term z^{-1} in the expansion of $z^{-2}f(z)P_i(z^{-1})P_j(z^{-1})$ (here we need hypothesis (i)), and thus equals $\sum_{n=k+l+1} a_n p_k^{(i)} p_l^{(j)}$. Therefore we have

$$\left[\mathrm{Res}_\infty f(z^{-1})P_i(z)P_j(z)\right]_{1\leq i,j\leq k} = B_k^\intercal \begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_2 & a_3 & \cdots & a_{k+1} \\ \vdots & \vdots & & \vdots \\ a_k & a_{k+1} & \cdots & a_{2k-1} \end{bmatrix} B_k$$

where $B_k = \left[p_i^{(j)}\right]_{0\leq i,j\leq k-1}$ is upper triangular with diagonal entries 1. The matrix in the middle of the right hand side is $\Delta_{k-1}\left(\frac{f-a_0}{X}\right)$. Hence

$$\det \Delta_{k-1}\left(\frac{f-a_0}{X}\right) = \det\left[\mathrm{Res}_\infty f(z^{-1})P_i(z)P_j(z)\right]_{1\leq i,j\leq k} \tag{4.3.1}$$

and Hadamard's Inequality yields

$$\left|\det \Delta_{k-1}\left(\frac{f-a_0}{X}\right)\right| \leq \prod_{1\leq i\leq k}\left(\sum_{1\leq j\leq k} |\mathrm{Res}_\infty f(z^{-1})P_i(z)P_j(z)|^2\right)^{1/2}. \tag{4.3.2}$$

On the other hand, we have

$$\mathrm{Res}_\infty f(z^{-1})P_i(z)P_j(z) = \frac{1}{2\pi i}\oint_{\partial K} f(z^{-1})P_i(z)P_j(z)\mathrm{d}z.$$

[2] $\mathrm{Res}_\infty g := \mathrm{Res}_0 z^{-2} g(z^{-1})$.

Notice that $f(z^{-1})$ is bounded on ∂K, and $|P_n(z)|^{1/n} \le \tau_n(K) \to d_\infty(K) < 1$ when $n \to \infty$ (see Proposition 4.2.10). Write $\delta := d_\infty(K) < 1$ for simplicity. For fix $k \gg 1$, we have

$$\sum_{1\le j\le k} |\mathrm{Res}_\infty f(z^{-1})P_i(z)P_j(z)|^2 = \begin{cases} O(\delta^{2i}) & \text{if } i \gg 1 \\ O(1) & \text{if not} \end{cases}.$$

Thus one gets, by (4.3.2), $\left|\det \Delta_{k-1}\left(\frac{f-a_0}{X}\right)\right| < 1$ for $k \gg 1$. As $\det \Delta_{k-1}\left(\frac{f-a_0}{X}\right) \in \mathbb{Z}$, we thus have

$$\left|\det \Delta_{k-1}\left(\frac{f-a_0}{X}\right)\right| = 0 \quad \text{for all } k \gg 1.$$

Hence $\frac{f-a_0}{X}$ is rational by Theorem 4.3.2. So f is rational. □

For our purpose, we will use the following equivalent version of Theorem 4.3.4.

Theorem 4.3.4′. *Let $K \subseteq \mathbb{C}$ be a non-empty compact set such that $\hat{\mathbb{C}} \setminus K$ is connected. Assume that $f = \sum_{n\ge 0} a_n X^{-n} \in \mathbb{Z}[[X^{-1}]]$ satisfies:*

(i) f converges on $\{z \in \hat{\mathbb{C}} : |z| \ge M\}$ for $M \gg 1$,

(ii) $z \mapsto f(z)$ extends to a holomorphic map on $\hat{\mathbb{C}} \setminus K$.

If $d_\infty(K) < 1$, then f is rational, i.e. $f = P/Q$ with $P, Q \in \mathbb{C}[X]$.

4.4 Proof of Schinzel–Zassenhaus

Let $\alpha \ne 0$ be an algebraic integer of degree $d \ge 1$. Let $\alpha_1 = \alpha, \dots, \alpha_d \in \mathbb{C}$ be its Galois conjugates. Then the $\mathbb{Z}$-minimal polynomial of α is $f(X) := (X-\alpha_1)\cdots(X-\alpha_d)$.

Recall that the *house* of α is $\overline{|\alpha|} := \max_i |\alpha_i|$.

4.4.1 Congruence condition

Let p be a prime number. Write $\mathbf{X} = (X_1, \dots, X_d)$. Let $e_j(\mathbf{X})$ be the elementary symmetric polynomial in $\mathbf{X}$ of degree j. Write $\mathbf{X}^p = (X_1^p, \dots, X_d^p)$.

Define

$$\psi_j(\mathbf{X}) := \frac{e_j(\mathbf{X})^p - e_j(\mathbf{X}^p)}{p} \in \mathbb{Z}[\mathbf{X}]. \tag{4.4.1}$$

Lemma 4.4.1. *For any positive integer k, we have*

$$e_j(\mathbf{X})^{p^k} \equiv e_j(\mathbf{X}^{p^k}) + p\psi_j(\mathbf{X})^{p^{k-1}} \pmod{p^2}.$$

Proof. We prove the lemma by induction on k. The base step $k = 1$ is by definition of ψ_j.

Assume the lemma is proved for $k-1 \ge 1$. We wish to prove it for k. We have

$$\begin{aligned} e_j(\mathbf{X})^{p^k} &\equiv \left(e_j(\mathbf{X}^{p^{k-1}}) + p\psi_j(\mathbf{X})^{p^{k-2}}\right)^p \pmod{p^2} \quad \text{by induction hypothesis} \\ &\equiv e_j(\mathbf{X}^{p^k}) + p\psi_j(\mathbf{X}^{p^{k-1}}) \pmod{p^2} \quad \text{by the case } k = 1 \\ &\equiv e_j(\mathbf{X}^{p^k}) + p\psi_j(\mathbf{X})^{p^{k-1}} \pmod{p^2}. \end{aligned}$$

Hence we are done. □

Now set $f_k := (X-\alpha_1^k)\cdots(X-\alpha_d^k) \in \mathbb{Z}[X]$. Write $\boldsymbol{\alpha} = (\alpha_1,\dots,\alpha_d)$ and $\boldsymbol{\alpha}^p = (\alpha_1^p,\dots,\alpha_d^p)$.

Lemma 4.4.2. *We have:*

(i) $e_j(\boldsymbol{\alpha}^{p^k}) \equiv e_j(\boldsymbol{\alpha}^p) \pmod{p^2}$ *for each* j.

(ii) $f_{p^k} \equiv f_p \pmod{p^2}$.

What we need in the proof of the Schinzel–Zassenhaus conjecture is $f_4 \equiv f_2 \pmod 4$.

Proof. It is clear that (i) implies (ii). Let us prove (i).

First, $\psi_j(\boldsymbol{\alpha}) \in \mathbb{Z}$ as it is an algebraic integer which is invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Thus Fermat's Little Theorem implies $\psi_j(\boldsymbol{\alpha})^{p^{k-1}} \equiv \psi_j(\boldsymbol{\alpha}) \pmod p$.

Next $e_j(\boldsymbol{\alpha}) \in \mathbb{Z}$ as it is an algebraic integer which is invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Thus Fermat's Little Theorem implies $e_j(\boldsymbol{\alpha})^p \equiv e_j(\boldsymbol{\alpha}) \pmod p$. Hence $e_j(\boldsymbol{\alpha})^{p^k} \equiv \cdots \equiv e_j(\boldsymbol{\alpha})^{p^2} \equiv e_j(\boldsymbol{\alpha})^p \pmod{p^2}$.

Now (i) follows from Lemma 4.4.1 and the previous two paragraphs. □

4.4.2 Proof of Schinzel–Zassenhaus

Now we are ready to prove the Schinzel–Zassenhaus conjecture, Theorem 4.1.3, with $c = \log 2/4$.

Assume (4.1.2) does not hold true for $\alpha \neq 0$, *i.e.* $|\overline{\alpha}| < 2^{1/4d}$. We wish to show that α is a root of unity.

We prove this by induction on d.

If $d = 1$, then it is clearly true that $\alpha = \pm 1$.

Assume the theorem is proved for $1,\dots,d-1 \geq 1$. Now we prove it for $d \geq 2$. Use the notation of Lemma 4.4.2. By part (ii) of the said lemma, there exists $A \in \mathbb{Z}[X]$ such that $f_4 = f_2 + 4A$. By looking at the leading coefficients of f_4 and f_2, we see that $\deg A < d$.

We start by showing that

$$\frac{f_4(X)}{f_2(X)} = \prod_{1\leq i\leq d} \frac{X-\alpha_i^4}{X-\alpha_i^2} \tag{4.4.2}$$

is a square in $\mathbb{Q}(X)$. For this purpose, we will apply the Polya–Bertrandias theorem.

Set $T := A/f_2$. Let f be the Taylor expansion in T of $\left(\frac{f_4}{f_2}\right)^{1/2} = (1+4T)^{1/2}$. Then f is a power series in T, and has coefficient in $\mathbb{Z}$ since $(1+4T)^{-1/2} \in \mathbb{Z}[[T]]$ (it is here that we need the coefficient 4).

To see that f is a power series in $\mathbb{Z}[[X]]$ or $\mathbb{Z}[[X^{-1}]]$, we use the following trick. For each polynomial $P(X) = c\prod_i (X-\beta_i)$, its *reciprocal polynomial* is defined to be $P^*(X) = c\prod_i(1-\beta_i X)$ or equivalently $P^*(X) = X^{\deg P}P(1/X)$. In particular, P is monic if and only if $P^*(0) = 1$. Then

$$\frac{f_4(X)}{f_2(X)} = \frac{f_4^*(1/X)}{f_2^*(1/X)} = \frac{f_2^*(1/X) + 4A^*(1/X)}{\prod_{1\leq i\leq d}(1-\frac{\alpha_i^2}{X})} = 1 + 4\frac{A^*(1/X)}{\prod_{1\leq i\leq d}(1-\frac{\alpha_i^2}{X})}.$$

Hence $T = \dfrac{A^*(1/X)}{\prod_{1\leq i\leq d}(1-\frac{\alpha_i^2}{X})} \in \mathbb{Z}[[X^{-1}]]$.

Now we have that $f \in \mathbb{Z}[[X^{-1}]]$ by the previous two paragraphs.

We are ready to apply the Polya–Bertrandias Theorem, Theorem 4.3.4′, to f. The relevant compact set K is the Hedgehog $K(\alpha_1^2,\dots,\alpha_d^2,\alpha_1^4,\dots,\alpha_d^4)$. Its transfinite diameter is $\leq (\max\{|\overline{\alpha}|^{4d}, |\overline{\alpha}|^{8d}\}/4)^{1/n}$. Then our assumption $|\overline{\alpha}| < 2^{1/4d}$ implies that $d_\infty(K) < 1$. And f

is clearly a holomorphic map on $\hat{\mathbb{C}} \setminus K$. Thus Theorem 4.3.4′ implies that $f \in \mathbb{Q}(X)$. So f_4/f_2 is a square in $\mathbb{Q}(X)$.

Thus the polynomial terms appearing in the product on the right hand side of (4.4.2) cannot be all different. So either $\alpha_i^2 = \alpha_j^4$ for some i and j, or $\alpha_i^2 = \alpha_j^2$ for some $i \neq j$.

If $\alpha_i^2 = \alpha_j^4$ for some i and j, then by applying elements in the Galois group we can see that $\{\alpha_1^2, \ldots, \alpha_d^2\}$ and $\{\alpha_1^4, \ldots, \alpha_d^4\}$ are the same set. So $|\alpha|^2 = |\alpha|^4$. So $|\alpha| = 1$ since $\alpha \neq 0$. Thus α is a root of unity by part (ii) of Lemma 4.1.4.

If $\alpha_i^2 = \alpha_j^2$ for some $i \neq j$, then $[\mathbb{Q}(\alpha_i^2) : \mathbb{Q}] < d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Thus we can apply the induction hypothesis to conclude that α_i^2 is a root of unity. Hence α_i is a root of unity, and thus α is a root of unity.

Now we are done.