Decompositions in algebra

Gent, D.M.H. van

CHAPTER 3

Indecomposable algebraic integers

3.1 Introduction

This chapter is based on [18]. In number theory, in particular the theory of the geometry of numbers, one equips a number field K with an inner product, turning any order R in K into a lattice in $\mathbb{R}\otimes_{\mathbb{Q}}K$. After normalizing this inner product, we may define it on an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ as

$$\langle \alpha, \beta \rangle = \frac{1}{[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]} \sum_{\sigma\colon \mathbb{Q}(\alpha,\beta)\to\mathbb{C}} \sigma(\alpha)\cdot\overline{\sigma(\beta)},$$

where the sum ranges over all ring homomorphisms from $\mathbb{Q}(\alpha,\beta)$ to $\mathbb{C}$. We write $\overline{\mathbb{Z}}$ for the ring of integers of $\overline{\mathbb{Q}}$, i.e. the integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}}$, and we call its elements the algebraic integers. Although $\overline{\mathbb{Z}}$ is not of finite rank, we may still meaningfully call it a lattice in the sense of Chapter 2.

Theorem 3.2.10. *The abelian group $\overline{\mathbb{Z}}$ equipped with the inner product from Definition 3.2.5 is a Hilbert lattice. Its shortest non-zero vectors are precisely the roots of unity, which all have length 1, and its packing radius, see Definition 2.6.1, is $1/2$.*

We will treat this lattice structure on $\overline{\mathbb{Z}}$ as intrinsically interesting. The theory in this chapter is motivated by the closest vector problem for $\overline{\mathbb{Z}}$. Since $\overline{\mathbb{Z}}$ has infinite rank, it may be that a closest vector does not exist. Formally we ask the question: 'Does there exist an algorithm that, given $n \in \mathbb{Z}_{>0}$, some $r \in \mathbb{R}_{>0}\cap\overline{\mathbb{Q}}$ and $\alpha \in \overline{\mathbb{Q}}$, decides whether there exist n distinct elements $\beta \in \overline{\mathbb{Z}}$ such that $\|\alpha-\beta\| < r$ and if so computes n such β?' Since $\overline{\mathbb{Z}}$ is enumerable, once we know such β exist we can find them. However, it is certainly of interest to compute β efficiently. The following result derived from classical capacity theory by T. Chinburg, for which we give a direct proof in Section 3.6, answers the question affirmatively for $r > 1$.

Corollary 3.6.7. *Suppose $r \in \mathbb{R}$ and $\alpha \in \overline{\mathbb{Q}}$. If $r > 1$, then there exist infinitely many $\beta \in \overline{\mathbb{Z}}$ such that $\|\alpha-\beta\| < r$.*

The proof is sufficiently constructive that we are able to derive an algorithm to compute arbitrarily many such β, see Proposition 3.6.10. This result also gives an upper bound on the covering radius.

Theorem 3.6.9. *The covering radius of $\overline{\mathbb{Z}}$, see Definition 2.6.1, is between $\sqrt[4]{1/2}$ and 1.*

Our main result is the following theorem, which is complementary to Corollary 3.6.7.

Theorem 3.11.2. *Suppose $r \in \mathbb{R}$ and $\alpha \in \overline{\mathbb{Q}}$. If $r < \sqrt[4]{\mathrm{e}/4}$, then there exist only finitely many $\beta \in \overline{\mathbb{Z}}$ such that $\|\alpha - \beta\| < r$.*

Again, one can algorithmically enumerate all such β, solving the problem for $r < \sqrt[4]{\mathrm{e}/4}$. This leaves a gap for r between $\sqrt[4]{\mathrm{e}/4}$ and 1 for which we do not know an answer to the decision problem.

Next we consider the related problem of computing the indecomposable vectors of $\overline{\mathbb{Z}}$, see Definition 2.4.1. A consequence of Corollary 3.6.7 is that for every $d \in \mathbb{Z}_{>0}$ there exist only finitely many indecomposable algebraic integers of degree up to d. We will prove the following effective upper and lower bounds.

Theorem 3.7.7. *There are least* $\exp(\frac{1}{4}(\log 2)d^2 + O(d \log d))$ *and at most* $\exp(\frac{1}{2}(1 + \log 2)d^2 + O(d \log d))$ *indecomposable algebraic integers of degree up to d.*

A decomposition of $\alpha \in \overline{\mathbb{Z}}$ corresponds to a lattice point with distance at most $\|\alpha/2\|$ to $\alpha/2$, and non-trivial decompositions exist if and only if there are at least 3 such lattice points. Hence deciding whether a lattice point is indecomposable is easier than the closest vector problem. It is also a good challenge problem for our algorithms. To this end, we derive the following numerical results.

Theorem 3.14.1. *There are exactly* 2 *indecomposable algebraic integers of degree* 1*, there are exactly* 14 *of degree* 2*, and there are at least* 354 *and at most* 588 *of degree* 3*.*

It would be interesting to study other lattice invariants of $\overline{\mathbb{Z}}$, but most constructions seem to fail to generalize to infinite rank, like the determinant and the dual lattice. One that does survive is the isometry group. For $\overline{\mathbb{Z}}$ it certainly contains $\mu(\overline{\mathbb{Z}}) \rtimes \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, see Lemma 3.2.13, but we do not know whether that is all.

3.2 The lattice of algebraic integers

We will write $\overline{\mathbb{Q}}$ for an algebraic closure of $\mathbb{Q}$. An *algebraic integer* is an element $\alpha \in \overline{\mathbb{Q}}$ for which there exists a monic $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$. The algebraic integers form a subring of $\overline{\mathbb{Q}}$, which we denote $\overline{\mathbb{Z}}$. In this section we will prove that $\overline{\mathbb{Z}}$ together with a natural choice of square-norm is a Hilbert lattice.

Definition 3.2.1. For a ring K we define the *fundamental set* to be the set $\mathrm{X}(K)$ of ring homomorphisms from K to $\mathbb{C}$. For a ring L with subring K and $\sigma \in \mathrm{X}(K)$ we define $\mathrm{X}_\sigma(L) = \{\rho \in \mathrm{X}(L) \mid \rho|_K = \sigma\}$.

Lemma 3.2.2. *Let $\alpha \in \overline{\mathbb{Q}}$ and $\mathbb{Q}(\alpha) \subseteq L \subseteq \overline{\mathbb{Q}}$ subfields with $[L:\mathbb{Q}] < \infty$. Then the quantities*

$$\prod_{\sigma \in \mathrm{X}(L)} |\sigma(\alpha)|^{1/[L:\mathbb{Q}]} \quad \text{and} \quad \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(L)} |\sigma(\alpha)|^2$$

are in $\mathbb{R}_{\geq 0}$, equal to zero if and only if $\alpha = 0$, and do not depend on the choice of L. □

Definition 3.2.3. We define the maps $N, q \colon \overline{\mathbb{Q}} \to \mathbb{R}_{\geq 0}$ by

$$N(\alpha) = \prod_{\sigma \in \mathrm{X}(\mathbb{Q}(\alpha))} |\sigma(\alpha)|^{1/[\mathbb{Q}(\alpha):\mathbb{Q}]} \quad \text{and}$$
$$q(\alpha) = \frac{1}{[\mathbb{Q}(\alpha):\mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(\mathbb{Q}(\alpha))} |\sigma(\alpha)|^2.$$

Lemma 3.2.4. *For $\alpha, \beta \in \overline{\mathbb{Q}}$ we have $q(\alpha+\beta) + q(\alpha-\beta) = 2q(\alpha) + 2q(\beta)$.*

Proof. By Lemma 3.2.2 the restriction of q to $L = \mathbb{Q}(\alpha, \beta)$ is given by $q(\gamma) = \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(L)} |\sigma(\gamma)|^2$. The norm $|\cdot|$ on $\mathbb{C}$ satisfies the parallelogram law and we may apply this term-wise to the sum defining q to obtain the lemma. □

Definition 3.2.5. For $\alpha, \beta \in \overline{\mathbb{Q}}$ we write $\langle \alpha, \beta \rangle$ for the inner product on $\overline{\mathbb{Q}}$ induced by q as given by Theorem 2.2.5 and Lemma 3.2.4. Explicitly, it is given by

$$\langle \alpha, \beta \rangle = \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(L)} \sigma(\alpha)\overline{\sigma(\beta)}$$

for any field $\mathbb{Q}(\alpha, \beta) \subseteq L \subseteq \overline{\mathbb{Q}}$ with $[L:\mathbb{Q}] < \infty$.

Lemma 3.2.6 (AM-GM inequality, Theorem 5.1 in [7])**.** *Let $n \in \mathbb{Z}_{\geq 1}$ and $x_1, \ldots, x_n \in \mathbb{R}_{\geq 0}$. Then*

$$\sqrt[n]{x_1 \cdots x_n} \leq \frac{x_1 + \cdots + x_n}{n},$$

with equality if and only if $x_1 = x_2 = \cdots = x_n$. □

Definition 3.2.7. An element $\delta \in \overline{\mathbb{Q}}$ is called *uniform* if $|\sigma(\delta)| = |\tau(\delta)|$ for all $\sigma, \tau \in \mathrm{X}(\overline{\mathbb{Q}})$.

Lemma 3.2.8. *For all $\alpha \in \overline{\mathbb{Q}}$ we have $N(\alpha)^2 \leq q(\alpha)$ with equality if and only if α is uniform.*

Proof. This follows from a straightforward application of Lemma 3.2.6:

$$\begin{aligned} q(\alpha) &= \frac{1}{[\mathbb{Q}(\alpha):\mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(\mathbb{Q}(\alpha))} |\sigma(\alpha)|^2 \\ &\geq \Big(\prod_{\sigma \in \mathrm{X}(\mathbb{Q}(\alpha))} |\sigma(\alpha)|^2 \Big)^{1/[\mathbb{Q}(\alpha):\mathbb{Q}]} = N(\alpha)^2, \end{aligned}$$

with equality if and only if $|\sigma(\alpha)|^2 = |\rho(\alpha)|^2$ for all $\sigma, \rho \in \mathrm{X}(\mathbb{Q}(\alpha))$. □

Proposition 3.2.9. *If $\alpha \in \overline{\mathbb{Z}}$, then $q(\alpha) \leq 1$ if and only if $\alpha = 0$ or α is a root of unity. If α is a root of unity, then $q(\alpha) = 1$.*

Proof. Let $\alpha \in \overline{\mathbb{Z}}$. The 'if' part of the implication follows directly from the definition. For the 'only if' part, suppose α is non-zero. If $q(\alpha) \leq 1$, then $N(\alpha)^2 \leq 1$ by Lemma 3.2.8. Then $N(\alpha)^{[\mathbb{Q}(\alpha):\mathbb{Q}]} = |N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)| \in \mathbb{Z}_{\geq 1}$, so $N(\alpha)^2 = q(\alpha) = 1$. By Lemma 3.2.8 we have $|\sigma(\alpha)| = 1$ for all $\sigma \in \mathrm{X}(\mathbb{Q}(\alpha))$, so α is a root of unity by Kronecker's theorem (Corollary 5.6 in [38]). □

Theorem 3.2.10. *The abelian group $\overline{\mathbb{Z}}$ equipped with the inner product from Definition 3.2.5 is a Hilbert lattice. Its shortest non-zero vectors are precisely the roots of unity, which all have length* 1*, and its packing radius, see Definition 2.6.1, is* $1/2$.

Proof. By Lemma 3.2.4 and Proposition 3.2.9 respectively the group $\overline{\mathbb{Z}}$ together with q satisfies the parallelogram law and is discrete, so indeed it is a Hilbert lattice. The remaining statements follow also from Proposition 3.2.9. □

We may write $\|x\|$ for $\sqrt{q(x)}$, the *2-norm* of $x \in \overline{\mathbb{Q}}$. Similarly, we may think of $N(x)$ as the *0-norm* of x, in the sense that $\lim_{p \to 0} \|x\|_p = N(x)$.

Lemma 3.2.11. *Suppose $\alpha, \delta \in \overline{\mathbb{Q}}$ and δ is uniform. Then $q(\alpha\delta) = q(\alpha)q(\delta)$. If also $\alpha, \delta \in \overline{\mathbb{Z}}$ and $\alpha\delta$ is indecomposable, then α is indecomposable.*

Proof. Let $L \supseteq \mathbb{Q}(\alpha, \delta)$. Then for all $\sigma \in \mathrm{X}(L)$ we have $q(\delta) = |\sigma(\delta)|^2$. Moreover,

$$q(\alpha\delta) = \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(L)} |\sigma(\alpha\delta)|^2 = \frac{1}{[L:\mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(L)} |\sigma(\alpha)|^2 \cdot q(\delta) = q(\alpha)q(\delta).$$

Now suppose $\alpha, \delta \in \overline{\mathbb{Z}}$ and let $(\beta, \gamma) \in \mathrm{dec}(\alpha)$. Then $\alpha\delta = \beta\delta + \gamma\delta$ and

$$q(\alpha\delta) = q(\alpha)q(\delta) \geq (q(\beta) + q(\gamma))q(\delta) = q(\beta\delta) + q(\gamma\delta),$$

so $(\beta\delta, \gamma\delta) \in \operatorname{dec}(\alpha\delta)$. If $\alpha\delta$ is indecomposable, then $\delta \neq 0$ and $0 \in \{\beta\delta, \gamma\delta\}$, so $0 \in \{\beta, \gamma\}$ and (β, γ) must be a trivial decomposition. Hence α is indecomposable. □

Definition 3.2.12. Write μ_∞ for the group of roots of unity in $\overline{\mathbb{Z}}$ and $\mathrm{Gal}(\overline{\mathbb{Q}})$ for the group of ring automorphisms of $\overline{\mathbb{Q}}$. Note that $\mathrm{Gal}(\overline{\mathbb{Q}})$ naturally acts on μ_∞, and write $\mu_\infty \rtimes \mathrm{Gal}(\overline{\mathbb{Q}})$ for their semi-direct product with respect to this action.

Lemma 3.2.13. *The group $\mu_\infty \rtimes \mathrm{Gal}(\overline{\mathbb{Q}})$ acts faithfully on the Hilbert lattice $\overline{\mathbb{Z}}$, where μ_∞ acts by multiplication and $\mathrm{Gal}(\overline{\mathbb{Q}})$ by application.*

Proof. Let $\alpha \in \overline{\mathbb{Z}}$, $\zeta \in \mu_\infty$ and $\rho \in \mathrm{Gal}(\overline{\mathbb{Q}})$. Let K be the normal closure of $\mathbb{Q}(\zeta, \alpha)$ and $n = [K : \mathbb{Q}]$.

First we show that the individual group actions on $\overline{\mathbb{Z}}$ are well-defined. Clearly $\zeta\alpha \in \overline{\mathbb{Z}}$ and note that ζ is uniform with $q(\zeta) = 1$. Hence multiplication by ζ is an isometry, i.e. preserves length, by Lemma 3.2.11. Recall that automorphisms preserve integrality and thus $\rho(\alpha) \in \overline{\mathbb{Z}}$. Since K is normal over $\mathbb{Q}$ we have $\rho K = K$ and thus $\mathrm{X}(K) \circ \rho = \mathrm{X}(K)$. Hence applying ρ to α simply results in a reordering of the terms in the sum defining q with respect to K, and thus ρ is an isometry.

Note that for $(\chi, \sigma), (\xi, \tau) \in \mu_\infty \rtimes \mathrm{Gal}(\overline{\mathbb{Q}})$ we have

$$(\chi, \sigma)\big((\xi, \tau)\,\alpha\big) = \chi \cdot \sigma(\xi \cdot \tau(\alpha)) = (\chi\sigma(\xi))((\sigma\tau)(\alpha)) = \big((\chi, \sigma) \cdot (\xi, \tau)\big)\,\alpha,$$

so the semi-direct product acts on $\overline{\mathbb{Z}}$ as well. Finally, suppose (ζ, ρ) acts as the identity. Note that $\mathrm{Gal}(\overline{\mathbb{Q}})$ fixes 1, so letting (ζ, ρ) act on 1 shows that $\zeta = 1$, and thus $\rho = \mathrm{id}$. Hence the action is faithful. □

Question 3.2.14. Is $\mu_\infty \rtimes \mathrm{Gal}(\overline{\mathbb{Q}})$ the entire isometry group of $\overline{\mathbb{Z}}$?

Proposition 3.2.15. *Let $\alpha \in \overline{\mathbb{Z}}$, $r \in \mathbb{Z}_{\geq 0}$ and $s \in \mathbb{Z}_{>0}$ such that $r/s \leq 1$. Then any root β of $X^s - \alpha^r$ satisfies $q(\beta) \leq q(\alpha)^{r/s}$.*

Proof. Let β be a root of $X^s - \alpha^r$, let $K = \mathbb{Q}(\alpha, \beta)$ and $n = [K : \mathbb{Q}]$. The case $r = 0$ follows from Proposition 3.2.9, so suppose $r > 0$. Then

$$\begin{aligned} q(\beta) &= \frac{1}{n} \sum_{\sigma \in \mathrm{X}(K)} |\sigma(\beta)|^2 = \frac{1}{n} \sum_{\sigma \in \mathrm{X}(K)} |\sigma(\beta^s)|^{2/s} = \frac{1}{n} \sum_{\sigma \in \mathrm{X}(K)} |\sigma(\alpha^r)|^{2/s} \\ &= \frac{1}{n} \sum_{\sigma \in \mathrm{X}(K)} \big(|\sigma(\alpha)|^2\big)^{r/s} \leq \Big(\frac{1}{n} \sum_{\sigma \in \mathrm{X}(K)} |\sigma(\alpha)|^2\Big)^{r/s} = q(\alpha)^{r/s}, \end{aligned}$$

where the inequality is $n^{-1/r}\|x\|_r \leq n^{-1/s}\|x\|_s$ from Lemma 2.2.14 applied to the vector $x = (|\sigma(\alpha)|^{2/s})_{\sigma \in \mathrm{X}(K)}$, using that $0 < r \leq s$. □

3.3 Indecomposable algebraic integers

We will now focus on the indecomposables of the lattice $\overline{\mathbb{Z}}$.

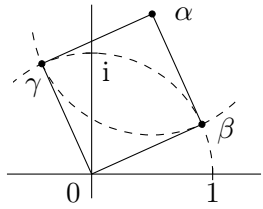

Figure 3.1: Integral $\alpha = \frac{1}{2}(1 + \mathrm{i}\sqrt{7})$ with $q(\alpha) = 2$.

Proposition 3.3.1. *Let $\alpha \in \overline{\mathbb{Z}}$. If $0 < q(\alpha) < 2$, then α is indecomposable. If $q(\alpha) = 2$, then α is decomposable if and only if it is the sum of two roots of unity. Such roots of unity are necessarily orthogonal, unique up to reordering, and of degree at most 2 over $\mathbb{Q}(\alpha)$.*

Proof. If $0 < q(\alpha) < 2$, then α is indecomposable by combining Theorem 3.2.10 and Lemma 2.4.4. Suppose $q(\alpha) = 2$. If $\alpha = \zeta + \xi$ for roots of unity $\zeta, \xi \in \overline{\mathbb{Q}}$, then $q(\alpha) = 2 = q(\zeta) + q(\xi)$, so $(\zeta, \xi) \in \mathrm{dec}(\alpha)$ is non-trivial. Conversely, suppose $(\beta, \gamma) \in \mathrm{dec}(\alpha)$ is non-trivial. By Theorem 3.2.10 we have $q(\beta), q(\gamma) \geq 1$. Then $0 \leq q(\alpha) - q(\beta) - q(\gamma) = 2 - q(\beta) - q(\gamma) \leq 0$, so we must have $q(\beta) = q(\gamma) = 1$. It follows that β and γ are orthogonal, and by Proposition 3.2.9 they are roots of unity.

Suppose $(\beta, \gamma) \in \mathrm{dec}(\alpha)$ is non-trivial. For any $\sigma \in \mathrm{X}(\mathbb{Q}(\alpha))$ and $\rho \in \mathrm{X}_\sigma(\mathbb{Q}(\alpha, \beta))$ the points 0, $\rho(\alpha)$, $\rho(\beta)$ and $\rho(\gamma)$ form the vertices of a rhombus with unit length sides, as can be seen in Figure 3.1. It follows that $\{\rho(\beta), \rho(\gamma)\}$ is uniquely determined by $\rho(\alpha) = \sigma(\alpha)$. As ρ is uniquely determined by $\rho(\beta)$ there are at most two elements in $\mathrm{X}_\sigma(\mathbb{Q}(\alpha, \beta))$, in other words $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \leq 2$. □

Remark 3.3.2. Proposition 3.3.1 gives us a way to decide whether an $\alpha \in \overline{\mathbb{Z}}$ with $q(\alpha) = 2$ is indecomposable, as it puts an upper bound on the degree of the roots of unity, leaving only finitely many to check. Knowledge of $\mathbb{Q}(\alpha)$ can further reduce this number.

Example 3.3.3. There exist $\alpha \in \overline{\mathbb{Z}}$ with $q(\alpha) = 2$ which are indecomposable. Consider $f = X^2 - X + 2$ with root $\alpha \in \overline{\mathbb{Z}}$, as in Figure 3.1. Note that the roots of f in $\mathbb{C}$ are $\frac{1}{2}(1 \pm \mathrm{i}\sqrt{7})$ with absolute value $\frac{1}{2}\sqrt{1^2 + 7} = \sqrt{2}$, so $q(\alpha) = 2$. Suppose $(\beta, \gamma) \in \mathrm{dec}(\alpha)$ is a non-trivial decomposition. Proposition 3.3.1 shows that β and γ are roots of unity. Note that $|\alpha^2| = 2$ under

all embeddings of α in $\mathbb{C}$, and $\alpha^2 = |\alpha|^2 \cdot \beta\gamma$. Hence $\alpha^2/2 = \frac{1}{2}\alpha - 1$ is a root of unity. Either one notes that $\alpha^2/2$ is not even integral, or that $\alpha^2/2 = \pm 1$, as those are the only roots of unity in $\mathbb{Q}(\alpha)$, which is clearly absurd. Hence we have a contradiction and α is indecomposable.

Lemma 3.3.4. *Let $\mathbb{Q} \subseteq K \subseteq L \subseteq \overline{\mathbb{Q}}$ be fields with $[L : \mathbb{Q}] < \infty$. Then for all $\alpha \in K$ and $\beta \in L$ we have*

$$[L : K] \cdot \langle \alpha, \beta \rangle = \langle \alpha, \mathrm{Tr}_{L/K}(\beta) \rangle.$$

Proof. Recall for $\sigma \in \mathrm{X}(K)$ the definition $\mathrm{X}_\sigma(L) = \{\rho \in \mathrm{X}(L) \mid \rho|_K = \sigma\}$ from Definition 3.2.1. For all $\sigma \in \mathrm{X}(K)$ and $\beta \in L$ we have $\sigma(\mathrm{Tr}_{L/K}(\beta)) = \sum_{\rho \in \mathrm{X}_\sigma(L)} \rho(\beta)$. Then with $\alpha \in K$ and $\beta \in L$ we have

$$\begin{aligned}
[L : K] \cdot \langle \alpha, \beta \rangle &= \frac{[L : K]}{[L : \mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(K)} \sum_{\rho \in \mathrm{X}_\sigma(L)} \rho(\alpha)\overline{\rho(\beta)} \\
&= \frac{1}{[K : \mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(K)} \sigma(\alpha) \overline{\sum_{\rho \in \mathrm{X}_\sigma(L)} \rho(\beta)} \\
&= \frac{1}{[K : \mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(K)} \sigma(\alpha)\overline{\sigma(\mathrm{Tr}_{L/K}(\beta))} \\
&= \langle \alpha, \mathrm{Tr}_{L/K}(\beta) \rangle,
\end{aligned}$$

as was to be shown. □

One could phrase Lemma 3.3.4 in terms of adjoint linear maps. For number fields $K \subseteq L$, the linear map $t_{L/K} = [L : K]^{-1} \cdot \mathrm{Tr}_{L/K} : L \to K$, the *trace*, is adjoint to the inclusion $K \to L$ with respect to the induced inner products.

Proposition 3.3.5. *Roots of unity $\zeta, \xi \in \overline{\mathbb{Z}}$ are orthogonal, i.e. $\langle \zeta, \xi \rangle = 0$, if and only if $\zeta^{-1}\xi$ does not have square-free order.*

Proof. Let $K = \mathbb{Q}(\zeta^{-1}\xi)$. We have $[K : \mathbb{Q}] \cdot \langle \zeta, \xi \rangle = [K : \mathbb{Q}] \cdot \langle 1, \zeta^{-1}\xi \rangle = \mathrm{Tr}_{K/\mathbb{Q}}(\zeta^{-1}\xi)$ by Lemma 3.2.13 and Lemma 3.3.4. Recall that the trace of an n-th root of unity equals $\mu(n)$, the Möbius function, which is zero precisely when n has a square divisor in $\mathbb{Z}_{>1}$. □

For $\alpha, \beta \in \overline{\mathbb{Z}}$ we say β *divides* α, and write $\beta \mid \alpha$, if there exists some $\gamma \in \overline{\mathbb{Z}}$ such that $\alpha = \beta\gamma$. We write $\beta \nmid \alpha$ if β does not divide α. Recall from Definition 3.2.7 that for $\delta \in \overline{\mathbb{Z}}$ we say δ is uniform if $|\sigma(\delta)| = |\tau(\delta)|$ for all $\sigma, \tau \in \mathrm{X}(\overline{\mathbb{Q}})$.

Proposition 3.3.6. *If $\alpha \in \overline{\mathbb{Z}}$ is such that $\sqrt{2} \mid \alpha$ or $\sqrt{3} \mid \alpha$, then $\alpha \notin \mathrm{indec}(\overline{\mathbb{Z}})$.*

Proof. Let $\zeta \in \overline{\mathbb{Q}}$ be a primitive 8-th root of unity, which we may choose such that $\zeta + \zeta^{-1} = \sqrt{2}$. Thus $(\zeta, \zeta^{-1}) \in \mathrm{dec}(\sqrt{2})$, because $\langle \zeta, \zeta^{-1} \rangle = 0$ by Proposition 3.3.5. Moreover, $\sqrt{2}$, ζ and ζ^{-1} are all uniform. For any $\beta \in \overline{\mathbb{Z}}$ we get from Lemma 3.2.11 that

$$q(\zeta\beta) + q(\zeta^{-1}\beta) = (q(\zeta) + q(\zeta^{-1})) \cdot q(\beta) = q(\sqrt{2}) \cdot q(\beta) = q(\sqrt{2}\beta),$$

so $\sqrt{2}\beta$ has a non-trivial decomposition.

With ξ a primitive twelfth root of unity we have $\xi + \xi^{-1} = \sqrt{3}$ with ξ, ξ^{-1} and $\sqrt{3}$ uniform. We have a decomposition because $\langle \xi, \xi^{-1} \rangle = \langle 1, \xi^{-2} \rangle = \frac{1}{2} \geq 0$, so the argument from before applies. □

Lemma 3.3.7. *If $\alpha \in \overline{\mathbb{Z}}$ is such that $\sqrt{2} \nmid \alpha \mid 2$ and α is uniform, then $\alpha \in \mathrm{indec}(\overline{\mathbb{Z}})$.*

Proof. By assumption we may write $2 = \alpha\gamma$ for some non-zero $\gamma \in \overline{\mathbb{Z}}$. Note that γ is not a unit, since otherwise $\sqrt{2} \mid 2 \mid \alpha$. Now let $(\beta, \alpha - \beta) \in \mathrm{dec}(\alpha)$. Then by Lemma 2.4.3 and Lemma 3.2.11 we have $q(\alpha) \geq q(\alpha - 2\beta) = q(\alpha - \alpha\beta\gamma) = q(\alpha) \cdot q(1 - \beta\gamma)$, so $q(1 - \beta\gamma) \leq 1$. As γ is not a unit we have $\beta\gamma \neq 1$, so $\beta\gamma = 1 - \zeta$ for some root of unity ζ of order say n by Proposition 3.2.9. Suppose n is not a power of 2. Then $1 - \zeta$ and 2 are coprime. As $2 \mid 2\beta = \alpha(1 - \zeta)$ we have that $2 \mid \alpha$, which contradicts $\sqrt{2} \nmid \alpha$. Hence n is a power of 2. If $n > 2$, then $1 - \zeta \mid \sqrt{2}$ so $\sqrt{2} \mid \alpha$, which is again a contradiction. Therefore $n = 1$ or $n = 2$, which correspond to the trivial decompositions with $\beta = 0$ and $\beta = \alpha$ respectively. We conclude that α is indecomposable. □

Proposition 3.3.8. *It holds that*

$$2\sqrt{2} \leq \sup\{q(\alpha) \mid \alpha \in \overline{\mathbb{Z}} \text{ is indecomposable}\}.$$

Proof. We will prove that for each $r \in \mathbb{Q} \cap [1, 3/2)$ there exists $\alpha \in \mathrm{indec}(\overline{\mathbb{Z}})$ such that $q(\alpha) = 2^r$.

Consider $\beta = \frac{1+\sqrt{-7}}{2}$ as in Example 3.3.3 and write $\overline{\beta} = 1 - \beta$ for its conjugate. Write $r = \frac{a}{b}$ with integers $a \geq b > 0$ and let $\gamma \in \overline{\mathbb{Z}}$ be a zero of $X^b - \beta$. Now take $\alpha = \overline{\beta} \cdot \gamma^{a-b}$. We will show α satisfies the conditions to Lemma 3.3.7. Because $|\sigma(\alpha)| = |\sigma(\beta)|^r = 2^{r/2}$ for all $\sigma \in \mathrm{X}(\overline{\mathbb{Q}})$, and hence α is uniform, we then have that α is indecomposable and $q(\alpha) = 2^r$.

Note that $\alpha \cdot \gamma^{2b-a} = \overline{\beta} \cdot \beta = 2$, so $\alpha \mid 2$. Let $v \colon K \to \mathbb{R} \cup \{\infty\}$ be a valuation over 2 for some number field K which is Galois over $\mathbb{Q}$ containing

the relevant elements. Because $0 = v(1) = v(\overline{\beta} + \beta) \geq \min\{v(\overline{\beta}), v(\beta)\}$, we have $v(\beta) = 0$ or $v(\overline{\beta}) = 0$. By potentially composing v with an automorphism swapping β and $\overline{\beta}$ we obtain a valuation v' such that $v'(\overline{\beta}) = 0$. We have $1 = v'(2) = v'(\beta \cdot \overline{\beta}) = v'(\beta)$ and thus $v'(\gamma) = 1/b$. Then $v'(\alpha) = r - 1 < 1/2 = v'(\sqrt{2})$, from which we conclude that $\sqrt{2} \nmid \alpha$. Thus α satisfies the conditions to Lemma 3.3.7, as was to be shown. □

3.4 Enumeration of degree-2 indecomposables

The indecomposables of $\overline{\mathbb{Z}}$ of degree 1 are 1 and -1. In this section we compute the indecomposables of degree 2. The fields of degree 2 over $\mathbb{Q}$ are $\mathbb{Q}(\sqrt{d})$ for $d \in \mathbb{Z} \setminus \{1\}$ square-free. The following lemma is easily verified by separating the cases d negative and positive.

Lemma 3.4.1. *Let $d \in \mathbb{Z} \setminus \{1\}$ be square-free and let $a, b \in \mathbb{Q}$. Then $q(a + b\sqrt{d}) = a^2 + |d| \cdot b^2$.* □

Lemma 3.4.2. *Let $\alpha \in \overline{\mathbb{Z}}$ and suppose one of the following holds:*

1. *the real part of α^2 is at least 2 under every embedding $\mathbb{Q}(\alpha) \to \mathbb{C}$;*
2. *the real part of α^2 is at most -2 under every embedding $\mathbb{Q}(\alpha) \to \mathbb{C}$;*
3. *$\alpha = (1 + \sqrt{d})/2$ with $d \in \mathbb{Z}$ square-free such that $9 \leq d \leq 25$.*

Then α has a non-trivial decomposition in a degree 2 extension of $\mathbb{Q}(\alpha)$.

Proof. Let $K = \mathbb{Q}(\alpha)$ and $\gamma = \alpha^2/4$. Let $f = X^2 - \alpha X + 1 \in K[X]$, let $\beta \in \overline{\mathbb{Z}}$ be a root of f and write $L = K(\beta)$. Then $(\beta - \alpha/2)^2 = \beta^2 - \alpha\beta + \alpha^2/4 = \alpha^2/4 - 1 = \gamma - 1$. For 1 and 3 we will show $q(\beta - \alpha/2) \leq q(\alpha/2)$. Then $(\beta, \alpha - \beta)$ is a decomposition of α by Lemma 2.4.3, and since neither 0 nor α is a root of f we conclude that this decomposition is non-trivial.

1. Let $\sigma \in \mathrm{X}(L)$. For $\delta \in L$ write $\mathrm{Re}_\sigma(\delta)$ and $\mathrm{Im}_\sigma(\delta)$ for the real respectively imaginary part of $\sigma(\delta)$. By assumption $\mathrm{Re}_\sigma(\gamma) \geq 1/2$. Thus $\mathrm{Re}_\sigma(\gamma - 1)^2 = (\mathrm{Re}_\sigma(\gamma) - 1)^2 \leq \mathrm{Re}_\sigma(\gamma)^2$. As $\mathrm{Im}_\sigma(\gamma - 1)^2 = \mathrm{Im}_\sigma(\gamma)^2$ we may conclude that $|\sigma(\gamma - 1)| \leq |\sigma(\gamma)|$. Then

$$q(\beta - \alpha/2) = \frac{1}{[L : \mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(L)} |\sigma(\gamma - 1)| \leq \frac{1}{[L : \mathbb{Q}]} \sum_{\sigma \in \mathrm{X}(L)} |\sigma(\gamma)| = q(\alpha/2),$$

as was to be shown.

2. Let $\mathrm{i} \in \overline{\mathbb{Q}}$ be a primitive fourth root of unity. Then $\mathrm{i}\alpha$ satisfies the conditions to 1, hence it has a non-trivial decomposition $(\beta, \mathrm{i}\alpha - \beta)$, where β is a root of $X^2 - \mathrm{i}\alpha X + 1$. In turn, $(-\mathrm{i}\beta, \alpha + \mathrm{i}\beta)$ is a non-trivial decomposition of α, where $-\mathrm{i}\beta$ is a root of $X^2 - \alpha X - 1$. In particular $-\mathrm{i}\beta$ is of degree at most 2 over $\mathbb{Q}(\alpha)$.

3. Since $d > 0$ the field K is totally real. Let $\gamma_1, \gamma_2 \in \mathbb{R}$ be the images of γ under $\mathrm{X}(K)$ such that $\gamma_1 < \gamma_2$. Because $9 \leq d \leq 25$ we have $\gamma_1 = (\sqrt{d}-1)^2/16 \leq 1$ and $\gamma_2 = (\sqrt{d}+1)^2/16 \geq 1$. Hence

$$\begin{aligned} q(\beta - \alpha/2) &= \frac{1}{2}\big(|\gamma_1 - 1| + |\gamma_2 - 1|\big) = \frac{1}{2}\big((1-\gamma_1) + (\gamma_2 - 1)\big) \\ &= \frac{2\sqrt{d}}{16} \leq \frac{1+d}{16} = q(\alpha/2), \end{aligned}$$

as was to be shown. □

Theorem 3.4.3. *The indecomposable elements of $\overline{\mathbb{Z}}$ of degree 2 up to conjugacy and sign are $\sqrt{-1}$, $\frac{1+\sqrt{-7}}{2}$, $\frac{1+\sqrt{-3}}{2}$ and $\frac{1+\sqrt{5}}{2}$, for a total of 14 indecomposables.*

Proof. First note that the 4 listed elements indeed are indecomposable: We treated $(1+\sqrt{-7})/2$ in Example 3.3.3, and the remaining 3 have square-norm less than 2, so Proposition 3.3.1 applies. Since conjugation and multiplication by -1 are isometries by Lemma 3.2.13, all 14 are indecomposable.

Let $\alpha \in \overline{\mathbb{Z}}$ be of degree 2 over $\mathbb{Q}$. It remains to show that α, up to conjugation and sign, admits a non-trivial decomposition or is one of the 4 listed indecomposables. Since α is of degree 2 over $\mathbb{Q}$ it is an element of $\mathbb{Q}(\sqrt{d})$ for some square-free $d \in \mathbb{Z}\setminus\{1\}$. Then we may write $\alpha = (a+b\sqrt{d})/2$ for some $a, b \in \mathbb{Z}$ with $a+b \in 2\mathbb{Z}$ and by conjugating and changing sign we may assume $a, b \geq 0$. If $a \geq 2$ we have

$$q(\alpha/2-1) = \Big(\frac{a}{4}-1\Big)^2 + |d|\Big(\frac{b}{4}\Big)^2 = \Big(\Big(\frac{a}{4}\Big)^2 + |d|\Big(\frac{b}{4}\Big)^2\Big) + \Big(1-\frac{a}{2}\Big) \leq q(\alpha/2),$$

so $(1, \alpha - 1)$ is a decomposition of α. Since $\alpha \neq 1$, this decomposition is non-trivial. Similarly we get a decomposition $(\sqrt{d}, \alpha - \sqrt{d})$ if $b \geq 2$, so either this decomposition is non-trivial or $\alpha = \sqrt{d}$.

First suppose $\alpha = \sqrt{d}$. If $|d| < 2$ then $d = -1$, and $\sqrt{-1}$ is listed. Otherwise $\alpha^2 = d$ satisfies the hypotheses of Lemma 3.4.2.1 or Lemma 3.4.2.2, so $\sqrt{d}$ is not indecomposable.

For $\alpha \neq \sqrt{d}$ the remaining cases are $\alpha = (1+\sqrt{d})/2$, which is integral only if $d \equiv 1 \bmod 4$. If $d \leq -9$ the real part of α^2 is $(1+d)/4 \leq -2$ under either embedding, so α satisfies the conditions to Lemma 3.4.2.2. If $-9 < d < 9$ we have $d \in \{-7, -3, 5\}$ and thus $\alpha = (1+\sqrt{d})/2$ is listed. For $9 \leq d \leq 25$ we may apply Lemma 3.4.2.3. The remaining case is $25 < d$, where we have that $\sigma(\alpha^2) = [(1 \pm \sqrt{d})/2]^2 \geq (\sqrt{d}-1)^2/4 \geq 2$ for all $\sigma \in \mathrm{X}(\mathbb{Q}(\sqrt{d}))$, so Lemma 3.4.2.1 applies. Hence α is either listed or not indecomposable. □

It is interesting to note that all non-trivial decompositions of $\alpha \in \overline{\mathbb{Z}}$ of degree 2 over $\mathbb{Q}$ that are produced in Theorem 3.4.3 live in a field extension of degree at most 2 over $\mathbb{Q}(\alpha)$.

3.5 Geometry of numbers

In this section we gather some known results about the geometry of numbers.

Definition 3.5.1. Let K be a number field. We write $K_{\mathbb{R}} = \mathbb{R} \otimes_{\mathbb{Q}} K$ and $K_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{Q}} K$.

Recall for a number field K the definition of $\mathrm{X}(K)$, the set of ring homomorphisms from K to $\mathbb{C}$.

Lemma 3.5.2. *We have an isomorphism of $\mathbb{C}$-algebras $\Phi_K \colon K_{\mathbb{C}} \to \mathbb{C}^{\mathrm{X}(K)}$ given by*

$$\Phi_K(z \otimes \alpha) = (z \cdot \sigma(\alpha))_{\sigma \in \mathrm{X}(K)}.$$

We have a natural inclusion $K_{\mathbb{R}} \to K_{\mathbb{C}} \to \mathbb{C}^{\mathrm{X}(K)}$, and its image is given by the subspace of elements invariant under the involution $(x_\sigma)_\sigma \mapsto (\overline{x_{\overline{\sigma}}})_\sigma$. This inclusion induces an isomorphism of $\mathbb{R}$-algebras $K_{\mathbb{R}} \cong \mathbb{R}^r \times \mathbb{C}^s$ for integers $r, s \geq 0$ such that $r = \#\{\sigma \in \mathrm{X}(K) \mid \sigma[K] \subseteq \mathbb{R}\}$ and $r + 2s = [K : \mathbb{Q}]$. □

Definition 3.5.3. We equip $K_{\mathbb{C}}$ with the inner product induced by the standard Hermitian inner product on $\mathbb{C}^{\mathrm{X}(K)}$ and $K_{\mathbb{R}}$ with its restriction, turning $K_{\mathbb{R}}$ into a real inner product space. Since $K_{\mathbb{R}}$ is an inner product space we have an induced measure on $K_{\mathbb{R}}$ we denote vol.

Remark 3.5.4. For a number field K and $\alpha \in K$ we have

$$\|\alpha\|^2 = \frac{1}{[K : \mathbb{Q}]} \|\Phi_K(\alpha)\|^2.$$

In fact, $K_{\mathbb{R}}$ is the universal Hilbert space of the lattice $\overline{\mathbb{Z}} \cap K$. Note that the norm on $K_{\mathbb{R}}$ is not the 'standard' norm on $\mathbb{R}^r \times \mathbb{C}^s$. In terms of the latter vector space it is given by

$$(x_1, \ldots, x_r, z_1, \ldots, z_s) \mapsto \sqrt{|x_1|^2 + \cdots + |x_r|^2 + 2|z_1|^2 + \cdots + 2|z_s|^2}.$$

Theorem 3.5.5 (Proposition 4.26 in [38])**.** *Let R be an order in a number field K. Then $\Phi_K[R]$ is a full rank lattice in $K_{\mathbb{R}}$ with determinant $|\Delta(R)|^{1/2}$, where $\Delta(R)$ is the discriminant of R.* □

Definition 3.5.6. For a commutative ring R and $d \in \mathbb{Z}_{\geq 0}$ we write $R[X]_d = \{f \in R[X] \mid \deg(f) < d\}$.

Lemma 3.5.7. *The functor $-[X]_d$ commutes with finite products.* □

Lemma 3.5.8. *For a number field K we have an isomorphism of real vector spaces $K_{\mathbb{R}}[X]_d \cong (\mathbb{R}[X]_d)^r \times (\mathbb{C}[X]_d)^s$ for all $d \in \mathbb{Z}_{\geq 0}$ induced by the isomorphism $K_{\mathbb{R}} \cong \mathbb{R}^r \times \mathbb{C}^s$ of Lemma 3.5.2.* □

Theorem 3.5.9 (Minkowski, Theorem 4.19 in [38])**.** *Let $n \in \mathbb{Z}_{\geq 0}$, let $\Lambda \subseteq \mathbb{R}^n$ be a full rank lattice and let $S \subseteq \mathbb{R}^n$ be a symmetric convex body. If $\mathrm{vol}(S) > 2^n \det(\Lambda)$, then there exists a non-zero element in $\Lambda \cap S$.* □

Definition 3.5.10. For all $\alpha \in \overline{\mathbb{Q}}$ the set $\mathrm{X}(\overline{\mathbb{Q}}) \cdot \alpha$ is finite. Hence we may equip $\overline{\mathbb{Q}}$ with the *max-norm*

$$|x|_\infty = \max_{\sigma \in \mathrm{X}(\overline{\mathbb{Q}})} |\sigma(x)|.$$

We extend this definition to the universal Hilbert space containing $\overline{\mathbb{Q}}$, and in turn restrict it to $K_{\mathbb{C}}$ and $K_{\mathbb{R}}$ for any number field K.

Lemma 3.5.11. *For $\alpha \in \overline{\mathbb{Q}}$ we have $\|\alpha\| \leq |\alpha|_\infty$ and for $n \geq 0$ we have $|\alpha^n|_\infty = |\alpha|_\infty^n$.* □

3.6 Szegő capacity theory

In this section we will give a proof of a specialization of a theorem on capacity theory due to Szegő. As a corollary (Corollary 3.6.7) to this theorem T. Chinburg derives a solution to the closest vector problem for large radii as discussed in the introduction of this chapter. We will present the proof in a manner to be explicit enough to derive an algorithm.

Definition 3.6.1. Let X be a metric space with metric d and let $S \subseteq X$ be a subset. A *rounding function from X to S* is a map $\lfloor \cdot \rceil \colon X \to S$ for which there exists some constant $\varepsilon \in \mathbb{R}_{\geq 0}$ such that for all $x \in X$ we have $d(x, \lfloor x \rceil) \leq \varepsilon$. We call such an ε an *error constant* for $\lfloor \cdot \rceil$.

Example 3.6.2. For $\mathbb{Z}$ in $\mathbb{Q}$ with the metric induced by the usual absolute value we may round to a nearest integer, giving a rounding function with error constant $1/2$. For a naive rounding map for an arbitrary order R with basis $(\alpha_i)_i$ of a number field K with metric induced by q we may simply send $\sum_i x_i \alpha_i \in K$ with $x_i \in \mathbb{Q}$ to $\sum_i \lfloor x_i \rceil \alpha_i \in R$. An error constant for this rounding function is for example $\frac{1}{2} \sum_{i=1}^n |\alpha_i|_\infty$. The same method works for R in $K_{\mathbb{R}}$.

Definition 3.6.3. Let A be a commutative ring, let $c \in A$, and let $|\cdot|$ be a norm on A. We define the *induced c-norm on* $A[X]$ to be the norm

$$f = \sum_{k=0}^{\infty} f_k \cdot (X-c)^k = \sum_{k=0}^{\infty} f_k Y^k \mapsto \max_k |f_k|$$

for $Y = X - c$. Let $R \subseteq A$ be a subring and $[\cdot] : A \to R$ a rounding function. We say this rounding function is *translation invariant* if $[a+r] = [a] + r$ for all $a \in A$ and $r \in R$. We recursively define the *induced rounding function with respect to c* to be the rounding function $\lfloor \cdot \rceil : A[X] \to R[X]$ with respect to the c-norm on $A[X]$ given by $\lfloor 0 \rceil = 0$ and

$$\lfloor aX^n + f \rceil \mapsto [a]X^n + \left\lfloor (a - [a])(X^n - Y^n) + f \right\rceil$$

for all $a \in A$ and $f \in A[X]_n$.

We will verify that this is indeed a rounding function.

Proposition 3.6.4. *Using the same notation as in Definition 3.6.3, the map* $\lfloor \cdot \rceil : A[X] \to R[X]$ *is a rounding function with the same error constant as the rounding function* $[\cdot] : A \to R$*. If the latter is translation invariant, then so is the former.*

Proof. Let ε be the error constant for $[\cdot]$ and $Y = X - c$. We with induction on n that $\lfloor \cdot \rceil$ restricts to a rounding function $A[X]_{n+1} \to R[X]_{n+1}$ with error constant ε. Clearly $\|0 - \lfloor 0 \rceil\| = 0 \leq \varepsilon$. Suppose $n \in \mathbb{Z}_{\geq 0}$ and consider $aX^n + f$ for $a \in A$ and $f \in A[X]_n$. Write

$$g = (a - [a])(X^n - Y^n) + f \in A[X]_n.$$

Then by the induction hypothesis

$$\|f - \lfloor f \rceil\| = \|(a - [a])Y^n + (g - \lfloor g \rceil)\| = \max\{|a - [a]|, \|g - \lfloor g \rceil\|\} \leq \varepsilon,$$

as was to be shown. Hence $\lfloor \cdot \rceil : A[X] \to R[X]$ is a rounding function with error constant ε.

Suppose $[\cdot]$ is translation invariant. To show $\lfloor \cdot \rceil$ is translation invariant, it suffices to show with induction to n that for all $a \in A$, $b \in R$, $f \in A[X]_n$ and $g \in R[X]_n$ we have $\lfloor (aX^n + f) + (bX^n + g) \rceil = \lfloor aX^n + f \rceil + (bX^n + g)$. The base case reduces to translation invariance of $[\cdot]$. For $n \geq 0$ we have

$$\begin{aligned}
&\lfloor (aX^n + f) + (bX^n + g) \rceil \\
&\quad = [a+b]X^n + \lfloor ((a+b) - [a+b])(X^n - Y^n) + f + g \rceil \\
&\quad = ([a] + b)X^n + \lfloor (a - [a])(X^n - Y^n) + f \rfloor + g \\
&\quad = \lfloor aX^n + g \rceil + (bX^n + g),
\end{aligned}$$

as was to be shown. □

Recall the the max-norm from Definition 3.5.10.

Theorem 3.6.5 (Szegő)**.** *Let R be an order of a number field K and let $r > 1$. Then for each $c \in K$ there exists a monic non-constant $g \in R[X]$ such that for all $z \in K_{\mathbb{C}}$ satisfying $|g(z)|_\infty < r$ we have $|z - c|_\infty < r$.*

This theorem is a special case of a theorem of Szegő, adapted from [40]. For simplicity we take $c \in K$ instead of $c \in K_{\mathbb{R}}$. The proof of this theorem will be sufficiently constructive that one can easily distill an algorithm from it.

Proof. Let $[\cdot] : K \to R$ be some translation invariant rounding function, for example as in Example 3.6.2, and let ε be its error constant. Let $\lfloor \cdot \rceil$ be the induced rounding function with respect to c. Let $d \in \mathbb{Z}_{>0}$ such that $dc \in R$, which exists since $c \in \mathbb{Q}R$. Successively choose $b, n \in \mathbb{Z}_{>0}$ such that

$$(1)\ 2\varepsilon r^{-b} \leq r - 1, \quad (2)\ b! \cdot d^b \mid n \quad \text{and} \quad (3)\ r^{n-1} \geq 2.$$

We claim $g = \lfloor (X - c)^n \rceil$ satisfies the conclusion to the theorem.

Write $f = (X - c)^n = \sum_k f_k X^k$. It follows from (2) that for all $k \leq b$ we have $d^k \mid \frac{b! d^b}{k!} \mid \binom{n}{n-k}$. Hence for all $k \geq n - b$ we have $f_k = \binom{n}{n-k} c^{n-k} \in R$. Thus by translation invariance we have $e \colon = f - g \in K[X]_{n-b}$. Let $\mathrm{X}(K)$ act on $K[X]$ coefficient-wise and fix $\sigma \in \mathrm{X}(K)$. Let $z \in \mathbb{C}$ such that $s := |z - \sigma(c)| \geq r$. Then

$$\left| \frac{\sigma(e)(z)}{\sigma(f)(z)} \right| \leq s^{-n} \sum_{i=0}^{n-b-1} \varepsilon \cdot s^i \leq \frac{\varepsilon s^{-b}}{s - 1} \leq \frac{c r^{-b}}{r - 1} \overset{(1)}{\leq} \frac{1}{2}.$$

It follows that

$$\left| \frac{\sigma(g)(z)}{\sigma(f)(z)} \right| = \left| 1 - \frac{\sigma(e)(z)}{\sigma(f)(z)} \right| \geq \frac{1}{2} \quad \text{and}$$
$$|\sigma(g)(z)| \geq \frac{|\sigma(f)(z)|}{2} \geq \frac{r^n}{2} \overset{(3)}{\geq} r.$$

Thus, if $|\sigma(g)(z)| < r$, then $|z - \sigma(c)| < r$. Taking the maximum over all $\sigma \in \mathrm{X}(K)$ proves the theorem for $c \in K$. □

Theorem 3.6.6 (Szegő)**.** *Suppose $r \in \mathbb{R}$ and $\alpha \in \overline{\mathbb{Q}}$. If $r > 1$, then there exist infinitely many $\beta \in \overline{\mathbb{Z}}$ such that $|\alpha - \beta|_\infty < r$.*

Proof. Consider $K = \mathbb{Q}(\alpha)$ and let $R \subseteq K$ be some order of K. By Theorem 3.6.5 there exists some monic non-constant $g \in R[X]$ such that for all

$z \in K_{\mathbb{C}}$ satisfying $|g(z)|_\infty < r$ we have $|z - \alpha|_\infty < r$. Now $g^n - 1 \in R[X]$ is monic and non-constant for all $n \in \mathbb{Z}_{\geq 1}$, so

$$S = \{\beta \in \overline{\mathbb{Z}} \mid (\exists\, n \in \mathbb{Z}_{\geq 1})\ g^n(\beta) = 1\}$$

is infinite. Let $\beta \in S$ and $L = K(\beta)$. It suffices to show that $|\alpha - \beta|_\infty < r$. We have that

$$|g(\beta)|_\infty^n = |g(\beta)^n|_\infty = |1|_\infty = 1,$$

so $|g(\beta)|_\infty < r$. Thus by definition of g we have $|\alpha - \beta|_\infty < r$. □

Combined with Lemma 3.5.11 we obtain the following.

Corollary 3.6.7. *Suppose $r \in \mathbb{R}$ and $\alpha \in \overline{\mathbb{Q}}$. If $r > 1$, then there exist infinitely many $\beta \in \overline{\mathbb{Z}}$ such that $\|\alpha - \beta\| < r$.* □

Proposition 3.6.8. *If $\alpha \in \overline{\mathbb{Z}}$ satisfies $\|\alpha\| > 2$, then α has infinitely many decompositions in $\overline{\mathbb{Z}}$.*

Proof. Let $\gamma = \alpha/2$. By Corollary 3.6.7 there are infinitely many $\beta \in \overline{\mathbb{Z}}$ such that $\|\gamma - \beta\| < \|\gamma\|$ as $\|\gamma\| = \|\alpha\|/2 > 1$. By Lemma 2.4.3 each such β gives a decomposition $(\beta, \alpha - \beta)$ of α. □

It follows from this proposition, as we will show later in the form of Proposition 3.7.4, that there are only finitely many indecomposables in $\overline{\mathbb{Z}}$ of a given degree.

Theorem 3.6.9. *The covering radius of $\overline{\mathbb{Z}}$, see Definition 2.6.1, is between $\sqrt[4]{1/2}$ and 1.*

Proof. By Proposition 3.3.8 we have $2^{3/4} \leq \sup\{\|\alpha\| \mid \alpha \in \mathrm{indec}(\overline{\mathbb{Z}})\}$ and consequently we get the lower bound $2^{-1/4} \leq \sup\{\|\alpha/2\| \mid \alpha \in \mathrm{indec}(\overline{\mathbb{Z}})\}$. For any $\alpha \in \mathrm{indec}(\overline{\mathbb{Z}})$ we have by Lemma 2.4.3 for all $x \in \overline{\mathbb{Z}}$ that $\|\alpha/2\| \leq \|\alpha/2 - x\|$, and thus $\alpha/2 \in \overline{\mathrm{Vor}}(\overline{\mathbb{Z}})$ by Corollary 2.6.12. Therefore $2^{-1/4} \leq r(\overline{\mathbb{Z}})$ by Proposition 2.6.10. For all $r > 1$ and $\alpha \in \overline{\mathbb{Q}}$ there exist $\beta \in \overline{\mathbb{Z}}$ such that $\|\alpha - \beta\| < r$ by Corollary 3.6.7. Taking the limit of r down to 1 and noting that $\overline{\mathbb{Q}} = \mathbb{Q} \cdot \overline{\mathbb{Z}}$ is dense in the Hilbert space of $\overline{\mathbb{Z}}$ proves the theorem. □

Proposition 3.6.10. *There exists an algorithm that, given $n \in \mathbb{Z}_{>0}$, some $r \in \mathbb{R} \cap \overline{\mathbb{Q}}$ and $\alpha \in \overline{\mathbb{Q}}$, decides whether $r > 1$ and if so computes n distinct $\beta \in \overline{\mathbb{Z}}$ such that $\|\alpha - \beta\| < r$, each represented by their minimal polynomial over $\mathbb{Q}(\alpha)$.*

Proof. Since $r \in \overline{\mathbb{Q}}$ we may decide whether $r = 1$, and if it is not we may approximate r to arbitrary precision so that we may decide whether $r > 1$. We may compute an error constant $\varepsilon \in \mathbb{Q}_{>1}$ for the rounding function and then the polynomial g as in Theorem 3.6.5. For sufficiently many m we then compute the irreducible factors of $g^m - 1$ over $\mathbb{Q}(\alpha)$ as in [31], following the proof of Theorem 3.6.6. □

Corollary 3.6.11. *There is an algorithm that takes as input an $n \in \mathbb{Z}_{\geq 0}$ and an element $\alpha \in \overline{\mathbb{Z}}$ given by its minimal polynomial, and decides whether $\|\alpha\| > 2$ and if so computes n non-trivial decompositions $(\beta, \gamma) \in \mathrm{dec}(\alpha)$, each represented by the minimal polynomial of β over $\mathbb{Z}[\alpha]$.*

Proof. We apply Proposition 3.6.10 with $\alpha/2$ in the place of α and $\|\alpha/2\|$ in the place of r. Note that $r \in \mathbb{R} \cap \overline{\mathbb{Q}}$. □

3.7 Bounds on indecomposable algebraic integers

In this section we will prove an effective upper bound on the total number of indecomposable algebraic integers of a given degree. In particular, we will show that this number is finite. We do this by constructing a complete list of candidates for indecomposability among all algebraic integers of given degree. We also give a lower bound on the number of indecomposables.

Proposition 3.7.1. *Suppose $\alpha \in \mathrm{indec}(\overline{\mathbb{Z}})$ has minimal polynomial $f = \sum_{k=0}^{n} f_{n-k} X^k \in \mathbb{Z}[X]$. Then $|f_k| \leq \binom{n}{k} 2^k$ for all $0 \leq k \leq n$.*

Proof. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}^\times$ be the roots of f. We have Maclaurin's inequalities (Theorem 11.2 in [7])

$$s_1 \geq s_2^{1/2} \geq s_3^{1/3} \geq \cdots \geq s_n^{1/n}, \quad \text{where } s_k = \binom{n}{k}^{-1} \cdot \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I|=k}} \prod_{i \in I} |\alpha_i|.$$

By Proposition 3.6.8 we have that $\|\alpha\| \leq 2$. Then by Lemma 2.2.14 we have

$$s_1 = \frac{1}{n} \sum_i |\alpha_i| \leq \Big(\frac{1}{n} \sum_i |\alpha_i|^2 \Big)^{1/2} = \|\alpha\| \leq 2.$$

Then $|f_k| \leq \binom{n}{k} s_k \leq \binom{n}{k} s_1^k \leq \binom{n}{k} 2^k$ for all k, as was to be shown. □

Corollary 3.7.2. *Suppose $\alpha \in \mathrm{indec}(\overline{\mathbb{Z}})$ has degree at most m. Then there exists a monic polynomial $g = \sum_{k=0}^{m} g_{m-k} X^k \in \mathbb{Z}[X]$ of degree m such that $g(\alpha) = 0$ and $|g_k| \leq \binom{m}{k} 2^k$ for all $0 \leq k \leq m$.*

Proof. Let f as in Proposition 3.7.1 and $g = X^{m-n} \cdot f$. Then $|g_k| = |f_k| \leq \binom{n}{k} 2^k \leq \binom{m}{k} 2^k$. □

Proposition 3.7.3. *Considered as functions of $n \in \mathbb{Z}_{\geq 1}$, the following hold:*

1. $$\log(n!) = n \log n - n + O(\log n);$$
2. $$\log\Big(\prod_{k=1}^{n} k^k\Big) = \tfrac{1}{2} n^2 \log n - \tfrac{1}{4} n^2 + O(n \log n);$$
3. $$\log\Big(\prod_{k=0}^{n} (k!)\Big) = \tfrac{1}{2} n^2 \log n - \tfrac{3}{4} n^2 + O(n \log n);$$
4. $$\log\Big(\prod_{k=0}^{n} \binom{n}{k}\Big) = \tfrac{1}{2} n^2 + O(n \log n).$$

Proof. 1. This is Stirling's approximation, which is classical.

2. Note that $f(x) = x \log x$ is an increasing function on $\mathbb{R}_{\geq 1}$. Hence

$$\begin{aligned} \log\Big(\prod_{k=1}^{n} k^k\Big) = \sum_{k=1}^{n} f(k) &\leq \int_1^{n+1} f(x)\,\mathrm{d}x = \Big[\tfrac{1}{2} x^2 \log(x) - \tfrac{1}{4} x^2\Big]_{x=1}^{n+1} \\ &= \tfrac{1}{2} n^2 \log(n) - \tfrac{1}{4} n^2 + O(n \log(n)). \end{aligned}$$

We analogously get the same estimate for a lower bound by considering $\int_1^n f(x)\,\mathrm{d}x$.

3. From 1 and 2 we get

$$\begin{aligned} \log\Big(\prod_{k=0}^{n} (k!)\Big) &= \sum_{k=1}^{n} \Big(k \log(k) - k + O(\log(k))\Big) \\ &= \big(\tfrac{1}{2} n^2 \log(n) - \tfrac{1}{4} n^2\big) - \tfrac{1}{2} n^2 + O(n \log(n)). \end{aligned}$$

4. We first rewrite the binomials in terms of factorials and then apply 1 and 3, so that

$$\begin{aligned} \log\Big(\prod_{k=0}^{n} \binom{n}{k}\Big) = \log\left(\frac{(n!)^n}{\big(\prod_{k=0}^{n} (k!)\big)^2}\right) &= n \log(n!) - 2 \log\Big(\prod_{k=0}^{n} (k!)\Big) \\ &= (n^2 \log(n) - n^2) - 2(\tfrac{1}{2} n^2 \log n - \tfrac{3}{4} n^2) + O(n \log n) \\ &= \tfrac{1}{2} n^2 + O(n \log n), \end{aligned}$$

as was to be shown. □

Proposition 3.7.4. *Let $n \in \mathbb{Z}_{\geq 1}$. There are at most*

$$n \prod_{k=1}^{n} \left(2\binom{n}{k}2^k + 1\right) = \exp\left(\tfrac{\log(2)+1}{2}\, n^2 + O(n\log(n))\right)$$

indecomposable elements in $\overline{\mathbb{Z}}$ of degree up to n.

Proof. By Corollary 3.7.2 every indecomposable of degree at most n is the root of a monic polynomial $f = \sum_{k=0}^{n} f_{n-k}X^k$ such that $|f_k| \leq \binom{n}{k}2^k$ for all $0 \leq k \leq n$. Hence every such polynomial corresponds to at most n indecomposables. For every $0 < k \leq n$ there are $2\binom{n}{k}2^k + 1$ choices for f_k, and $f_0 = 1$, proving the first upper bound. We may bound $2\binom{n}{k}2^k + 1 \leq 3\binom{n}{k}2^k$, so that by Proposition 3.7.3.4 we get

$$\begin{aligned} n \prod_{k=1}^{n} \left(2\binom{n}{k}2^k + 1\right) &\leq n \cdot 3^n \cdot 2^{\binom{n+1}{2}} \cdot \prod_{k=0}^{n} \binom{n}{k} \\ &= \exp\left(\tfrac{\log(2)+1}{2}\, n^2 + O(n\log(n))\right), \end{aligned}$$

as was to be shown. □

For $f \in \mathbb{Q}[X]$ monic write $q(f)$ for the average of the square length of the roots of f in $\mathbb{C}$, such that for all $\alpha \in \overline{\mathbb{Z}}$ with minimal polynomial $f_\alpha \in \mathbb{Q}[X]$ we get $q(\alpha) = q(f_\alpha)$. Note that $f = (X+2)^n$, although it is not irreducible, has $q(f) = 4$ and attains the bounds of Proposition 3.7.1. However, that does not imply that Proposition 3.7.4 cannot be improved, as it is not clear that all combinations of coefficients occur for polynomials f with $q(f) \leq 4$. Some small degree numerical results might suggest improvements can be made.

degree	1	2	3	4
# monic $f \in \mathbb{Z}[X]$ s.t. $(\forall k)\ \lvert f_k\rvert \leq \binom{n}{k}2^k$	5	81	5525	1786785
# monic $f \in \mathbb{Z}[X]$ s.t. $q(f) \leq 4$	5	49	989	48422
# $\alpha \in \overline{\mathbb{Z}}$ s.t. $q(\alpha) \leq 4$	5	39	739	40354

We also have the following lower bound.

Proposition 3.7.5. *Let $n \in \mathbb{Z}_{\geq 1}$. There are at least*

$$\exp\left(\frac{\log 2}{4}n^2 + O(n\log n)\right)$$

indecomposable algebraic integers of degree n.

Proof. Let $n \in \mathbb{Z}_{\geq 1}$ and recall the definition of $\mathbb{Z}[X]_n$ from Definition 3.5.6. Consider the set

$$S_n = \left\{ f = \sum_{k=0}^{n-1} f_k X^k \in 2X\mathbb{Z}[X]_{n-1} + 2 \;\middle|\; (\forall k)\ |f_k|(\sqrt{2})^k n \leq (\sqrt{2})^{n-1} \right\}.$$

For $f \in S_n$ consider $g = X^n - f$ and note that g is irreducible by Eisenstein's criterion. Consider the ball $D \subseteq \mathbb{C}$ of radius $r = (\sqrt{2})^{1-1/n} < \sqrt{2}$ around 0. For all z on the boundary of D we have

$$|f(z)| \leq \sum_{k=0}^{n-1} |f_k||z|^k \leq \sum_{k=0}^{n-1} |f_k|(\sqrt{2})^k \overset{\text{(i)}}{\leq} \sum_{k=0}^{n-1} \frac{(\sqrt{2})^{n-1}}{n} = (\sqrt{2})^{n-1} = |z|^n,$$

where (i) is strict for n sufficiently large due to $|f_0|n = 2n < (\sqrt{2})^{n-1}$. Hence by Rouché's theorem (Theorem 4.18 in [1]) the polynomials X^n and g have the same number of roots in D. It follows that all roots of g in $\mathbb{C}$ have length less than $\sqrt{2}$. Thus $q(\alpha) < 2$ for all roots $\alpha \in \overline{\mathbb{Z}}$ of g, so α is indecomposable by Proposition 3.3.1.

We conclude that for n sufficiently large there are at least $n \cdot \#S_n$ indecomposable algebraic integers of degree n, so it remains to prove a lower bound on $\#S_n$. Note that the coefficients of $f \in S_n$ satisfy independent inequalities, so we may simply give a lower bound per coefficient. Let $B = n - 3\log_2(n) - 2$, which is positive for n sufficiently large. For $k > B$ we consider only $f_k = 0$ and get a lower bound of 1 for this coefficient. For $0 < k \leq B$ we have

$$2\left\lfloor \frac{(\sqrt{2})^{n-k-1}}{2n} \right\rfloor + 1 \geq 2\Big(\frac{(\sqrt{2})^{n-k-1}}{2n} - 1\Big) + 1 = \frac{(\sqrt{2})^{n-k-1}}{n} - 1 = \text{(ii)}$$

choices for f_k. Then for n sufficiently large we have

$$\frac{n}{(\sqrt{2})^{n-k-2}} \leq \frac{n}{n^{3/2}} \leq \sqrt{2} - 1, \quad \text{so that} \quad \text{(ii)} \geq \frac{(\sqrt{2})^{n-k-2}}{n}.$$

Hence S_n contains, for n sufficiently large, at least

$$\begin{aligned} \prod_{k=1}^{B} \frac{(\sqrt{2})^{n-k-2}}{n} &= \exp\Big(\frac{\log 2}{2} \sum_{k=1}^{B} (n-k-2) - B\log n\Big) \\ &= \exp\Big(\frac{\log 2}{4} n^2 + O(n\log n)\Big) \end{aligned}$$

elements, from which the proposition follows. □

Corollary 3.7.6. *Let $n \in \mathbb{Z}_{\geq 1}$. There are at least*

$$\exp\Big(\frac{\log 2}{4}n^2 + O(n \log n)\Big)$$

indecomposable algebraic integers of degree up to n. □

From the upper and lower bound we may now conclude the following.

Theorem 3.7.7. *There are least* $\exp(\frac{1}{4}(\log 2)d^2 + O(d \log d))$ *and at most* $\exp(\frac{1}{2}(1 + \log 2)d^2 + O(d \log d))$ *indecomposable algebraic integers of degree up to d.* □

3.8 Fekete capacity theory

In this section we present a proof of a special case of Fekete's theorem using Minkowski's convex body theorem. Fekete's theorem can be thought of as a partial converse to Theorem 3.6.6 of Szegő. Although this does not give us a converse to Corollary 3.6.7, using similar techniques as in this section we will later prove Theorem 3.11.2 mentioned in the introduction. The goal of this section is to showcase the proof technique we will use to prove Theorem 3.11.2 so that we may later improve clarity by brevity. Recall the definition of the norm $|\cdot|_\infty$ from Definition 3.5.10.

Theorem 3.8.1 (Fekete)**.** *Suppose $r \in \mathbb{R}$ and $\alpha \in \overline{\mathbb{Q}}$. If $r < 1$, then there exist only finitely many $\beta \in \overline{\mathbb{Z}}$ such that $|\beta - \alpha|_\infty \leq r$.*

Just like for Szegő's theorem, it is possible to derive an algorithmic counterpart to Fekete's theorem. Combining Theorem 3.8.1 and Theorem 3.6.6, the point $r = 1$ is still a singularity. For $\alpha \in \overline{\mathbb{Z}}$ and $r = 1$ clearly all $\beta \in \alpha + \mu_\infty$ satisfy $|\beta - \alpha|_\infty \leq r$. However, when $\alpha \notin \overline{\mathbb{Z}}$ we do not know what happens in general. We start with a volume computation.

Definition 3.8.2. Let A be an $\mathbb{R}$-algebra equipped with a real inner product. We equip $A[Y]$ with an inner product

$$\Big\langle \sum_{k=0}^{\infty} f_k Y^k, \sum_{k=0}^{\infty} g_k Y^k \Big\rangle = \sum_{k=0}^{\infty} \langle f_k, g_k \rangle,$$

which is the 'standard' inner product when we naturally identify $A[Y]$ with $A^{(\mathbb{Z}_{\geq 0})}$. For $n \in \mathbb{Z}_{\geq 0}$ we equip $A[Y]_n$, as defined in Definition 3.5.6, with the restriction of this inner product.

Remark 3.8.3. Obviously $\mathbb{R}$ is an $\mathbb{R}$-algebra with a real inner product. We identify $\mathbb{C}$ with $\mathbb{R}^2$ by choosing $\mathbb{R}$-basis $\{1, \mathrm{i}\}$, and equip $\mathbb{C}$ with the inner product induced by the natural inner product on $\mathbb{R}^2$. For a number field K we remark that $K_{\mathbb{R}}$ has a real inner product as in Definition 3.5.3.

Lemma 3.8.4. *Let A be an $\mathbb{R}$-algebra of dimension $d < \infty$. For all $a, b \in \mathbb{R}$, $c \in A$ and $n \in \mathbb{Z}_{\geq 0}$ we have an $\mathbb{R}$-linear transformation ϕ on $A[X]_n$ given by $f \mapsto bf(a(X - c))$ with $\det \phi = (a^{n(n-1)/2} \cdot b^n)^d$.*

Proof. Note that ϕ is trivially an $\mathbb{R}$-linear transformation. Choose an $\mathbb{R}$-basis $\{e_1, \ldots, e_d\}$ for A. Writing ϕ as a matrix with respect to the basis $\{e_i X^j \mid 1 \leq i \leq d, 0 \leq j < n\}$ for $A[X]_n$ we note that ϕ is a lower triangular matrix with diagonal entries $b, ba, ba^2, \ldots, ba^{n-1}$, each occurring with multiplicity d. The determinant of ϕ is then simply the product of the diagonal. □

Lemma 3.8.5. *Let $\mathbb{F}$ be either $\mathbb{R}$ or $\mathbb{C}$ and let $r \in \mathbb{R}_{>0}$. For $n \in \mathbb{Z}_{\geq 0}$ consider*

$$S_n(r) = \{f \in \mathbb{F}[Y]_n \mid (\forall\, z \in \mathbb{C})\ |z| \leq r \Rightarrow |f(z)| \leq r\}.$$

Then as function of n we have

$$\log \mathrm{vol}(S_n(r)) \geq -\tfrac{1}{2} n^2 \cdot [\mathbb{F} : \mathbb{R}] \cdot \log r + O(n \log n).$$

Proof. Write $S_n = S_n(1)$. By applying the transformation $f \mapsto rf(r^{-1}Y)$ to $\mathbb{F}[Y]_n$ we bijectively map S_n to $S_n(r)$. From Lemma 3.8.4 it follows that $\log \mathrm{vol}(S_n(r)) = -\frac{1}{2} n^2 \cdot [\mathbb{F} : \mathbb{R}] \cdot \log r + \log \mathrm{vol}(S_n) + O(n \log n)$. It remains to prove $\log \mathrm{vol}\, S_n \geq O(n \log n)$.

First suppose $\mathbb{F} = \mathbb{R}$. Consider the set

$$T_n = \Big\{ \sum_{k=0}^{n-1} f_k Y^k \in \mathbb{R}[Y]_n \;\Big|\; \sum_{k=0}^{n-1} |f_k| \leq 1 \Big\}.$$

Note that for all $f \in T_n$ and $z \in \mathbb{C}$ such that $|z| \leq 1$ we have $|f(z)| \leq \sum_{k=0}^{n-1} |f_k| \leq 1$, so $f \in S_n$. Hence $T_n \subseteq S_n$ and $\mathrm{vol}(T_n) \leq \mathrm{vol}(S_n)$. With Proposition 3.7.3.1 we compute $\log \mathrm{vol}(T_n) = \log(2^n/n!) = O(n \log n)$, from which the lemma follows for $\mathbb{F} = \mathbb{R}$.

For $\mathbb{F} = \mathbb{C}$, note that we have an isometry $\mathbb{R}[X]_n^2 \to \mathbb{C}[X]_n$ given by $(f, g) \mapsto f + \mathrm{i} \cdot g$. For $f, g \in \frac{1}{2} T_n$ and $z \in \mathbb{C}$ such that $|z| \leq 1$ we have $|f(z) + \mathrm{i} \cdot g(z)| \leq |f(z)| + |g(z)| \leq \frac{1}{2} + \frac{1}{2} = 1$, so $f + \mathrm{i} \cdot g \in S_n$. Hence $\log \mathrm{vol}(S_n) \geq \log(\mathrm{vol}(\frac{1}{2} T_n)^2) = 2 \log \mathrm{vol}(T_n) - 2n \log 2 = O(n \log n)$, from which the lemma follows for $\mathbb{F} = \mathbb{C}$. □

Theorem 3.8.6. *Let R be an order of a number field K and let $0 < r < 1$. For all $c \in K_{\mathbb{R}}$ there exists a non-zero $g \in R[X]$ such that for all $z \in K_{\mathbb{R}}$, if $|z - c|_\infty \leq r$ then $|g(z)|_\infty \leq r$.*

Proof. Write $d = [K : \mathbb{Q}]$. Let $n \in \mathbb{Z}_{\geq 0}$ and consider the lattice $\Lambda_n = R[X]_n$ in the inner product space $K_{\mathbb{R}}[Y]_n$, where $Y = X - c$. Note that $\dim_{\mathbb{R}} K_{\mathbb{R}}[Y]_n = dn$ and that Λ_n is a full-rank lattice in $K_{\mathbb{R}}[Y]_n$ with $\det(\Lambda_n) = |\Delta(R)|^{n/2}$ by Lemma 3.8.4 and Theorem 3.5.5. Consider

$$S_n = \left\{ f \in K_{\mathbb{R}}[Y]_n \;\middle|\; (\forall\, \sigma \in \mathrm{X}(K))\,(\forall\, z \in \mathbb{C})\ |z| \leq r \Rightarrow |\sigma(f)(z)| \leq r \right\}$$

and note that it is both symmetric and convex. Moreover, it follows from Lemma 3.8.5 that $\log \mathrm{vol}(S_n) \geq -\frac{1}{2} n^2 d \log r + O(n \log n)$. Hence

$$\log\left(\frac{\mathrm{vol}(S_n)}{2^{dn} \cdot \det(\Lambda_n)}\right) \geq -\tfrac{1}{2} n^2 d \log r + O(n \log n).$$

Because $-\frac{1}{2} d \log r > 0$ there exists some n sufficiently large such that $\mathrm{vol}(S_n) > 2^{dn} \det(\Lambda_n)$. By Theorem 3.5.9 there then exists some non-zero $g \in \Lambda_n \cap S_n$ which as polynomial in X satisfies the requirements. □

Proof of Theorem 3.8.1. Let $K = \mathbb{Q}(\alpha)$ and let $R \subseteq K$ be some order of K. Then by Theorem 3.8.6 there exists some non-zero $g \in R[X]$ such that for all $z \in K_{\mathbb{R}}$, if $|z - \alpha|_\infty \leq r$ then $|g(z)|_\infty \leq r$. Suppose $\beta \in \overline{\mathbb{Z}}$ satisfies $|\beta - \alpha|_\infty \leq r$. Then $|g(\beta)|_\infty \leq r$, or equivalently $|\rho(g(\beta))| \leq r$ for all $\rho \in \mathrm{X}(L)$. Hence

$$|N_{L/\mathbb{Q}}(g(\beta))| = \prod_{\rho \in \mathrm{X}(L)} |\rho(g(\beta))| \leq r^{[L:\mathbb{Q}]} < 1.$$

As $g(\beta) \in \overline{\mathbb{Z}}$, we must then have $g(\beta) = 0$. As β must be a root of g and g is non-zero, there can only be finitely many β. □

3.9 Reduction to exponentially bounded polynomials

We now prepare to prove the main theorem. If there are only finitely many decompositions of an algebraic integer α, then certainly there exists a non-zero polynomial $f \in \mathbb{Z}[X]$ such that $f(\beta) = 0$ for all decompositions $(\beta, \alpha - \beta)$ of α. The goal is to exhibit such a polynomial when α is short using a lattice argument, similarly to the proof of Theorem 3.8.1. In this section we derive an analytic sufficient condition for a polynomial f to have this property.

Definition 3.9.1. Let K be a number field. We define $\mathcal{S}(K) = \mathrm{X}(K) \times \mathbb{C}$, the coproduct (i.e. disjoint union) of measurable spaces of $\#\,\mathrm{X}(K)$ copies of $\mathbb{C}$, where $\mathbb{C}$ has the standard Lebesgue measurable space structure. We write $\mathcal{M}(K)$ for the set of probability measures μ on $\mathcal{S}(K)$, i.e. all measures μ such that $\mu(\mathcal{S}(K)) = 1$.

Definition 3.9.2. Let K be a number field and $r \in \mathbb{R}_{>0}$. For $f \in K_{\mathbb{R}}[Y]$ we say f is *exponentially bounded at radius* r if for all $\mu \in \mathcal{M}(K)$ satisfying $\int |z|^2 \,\mathrm{d}\mu(\sigma, z) < r^2$ it holds that $\int \log|\sigma(f)(z)| \,\mathrm{d}\mu(\sigma, z) < 0$.

Proposition 3.9.3. *Let $\alpha \in \overline{\mathbb{Z}}$, $K = \mathbb{Q}(\alpha)$ and $r > \|\alpha/2\|$. If $f \in \mathcal{O}_K[X]$ is exponentially bounded at radius $r \in \mathbb{R}_{>0}$ as polynomial in the variable $Y = X - \alpha/2$, then for all $(\beta, \gamma) \in \mathrm{dec}(\alpha)$ we have $f(\beta) = 0$.*

Proof. Suppose $(\beta, \gamma) \in \mathrm{dec}(\alpha)$. Then $\|\beta - \alpha/2\| \leq \|\alpha/2\| < r$ by Lemma 2.4.3. Let $L = K(\beta)$ and

$$B = \{(\rho|_K, \rho(\beta - \alpha/2)) \,|\, \rho \in \mathrm{X}(L)\} \subseteq \mathcal{S}(K),$$

which has $\#B = [L : \mathbb{Q}]$ and $\#(B \cap (\{\sigma\} \times \mathbb{C})) = [L : K]$ for all $\sigma \in \mathrm{X}(K)$. Let $\mu \in \mathcal{M}(K)$ be the uniform probability measure on B and write f_Y for f as a polynomial in the variable Y. Because $\int |x|^2 \,\mathrm{d}\mu(\sigma, x) = \|\beta - \alpha/2\|^2 < r^2$ and f_Y is exponentially bounded at radius r we get

$$\begin{aligned}\log\left(N(f(\beta))^{[L:\mathbb{Q}]}\right) &= \log \prod_{\rho \in \mathrm{X}(L)} |\rho(f(\beta))| = \sum_{\rho \in \mathrm{X}(L)} \log|\rho(f_Y(\beta - \alpha/2))| \\ &= [L : \mathbb{Q}] \cdot \int \log|\sigma(f_Y)(x)| \,\mathrm{d}\mu(\sigma, x) < 0.\end{aligned}$$

We conclude that $N(f(\beta)) < 1$. Since $f(\beta)$ is integral we have $f(\beta) = 0$, as was to be shown. □

Example 3.9.4. The set of polynomials of $K_{\mathbb{R}}$ exponentially bounded at radius r is closed under multiplication and is symmetric. However, we will show that it is not convex.

Let $r = 1$ and $K = \mathbb{Q}$. For all $c \in (-1, 1)$ the constant polynomial c is trivially exponentially bounded at any positive radius, in particular at radius 1. Also the polynomial Y^2 is exponentially bounded: For any $\mu \in \mathcal{M}(K)$ such that $\int |z|^2 \,\mathrm{d}\mu(\sigma, z) < 1$ we have

$$\int \log|z^2| \,\mathrm{d}\mu(\sigma, z) \leq \log \int |z|^2 \,\mathrm{d}\mu(\sigma, z) < \log 1 = 0.$$

Here the first inequality is Jensen's inequality for integrals. When μ has finite support, this comes down to Lemma 3.2.6. For $c \in (-1, 1)$ and

$k \in \mathbb{Z}_{\geq 0}$ the product cY^{2k} of exponentially bounded polynomials at radius 1 is exponentially bounded at radius 1. We claim that $\frac{1}{4}(1 + Y^{2k})$ for k sufficiently large, which is a convex combination of $\frac{1}{2}$ and $\frac{1}{2}Y^{2k}$, is not exponentially bounded at radius 1. Taking $\mu \in \mathcal{M}(\mathbb{Q})$ with weight $\frac{1}{5}$ at 2 and remaining weight at 0 we have $\int |z|^2 \,\mathrm{d}\mu(\sigma, z) = \frac{4}{5} < 1$, yet $\int \log|\frac{1}{4}(1 + Y^{2k})| \,\mathrm{d}\mu(\sigma, z) = \frac{1}{5}\log(1 + 2^{2k}) - \log 4 \to \infty$ as $k \to \infty$. We conclude that the set of exponentially bounded polynomials at radius 1 is not convex. A similar argument works for all radii and number fields.

Lemma 3.9.5. *Let $D \subseteq \mathbb{C}$ be a convex subset and let $f\colon D \to \mathbb{C}$ be analytic. Then for distinct $x, y \in D$ we have*

$$\left|\frac{f(x) - f(y)}{x - y}\right| \leq \sup_{z \in D} |f'(z)|.$$

Proof. Let $\gamma\colon [0,1] \to D$ be the parametrization of the straight line connecting x and y, which is well-defined since D is convex. First note that

$$\begin{aligned}\int_0^1 f'(\gamma(t)) \,\mathrm{d}t &= \int_0^1 f'(tx + (1-t)y) \,\mathrm{d}t \\ &= \frac{1}{x - y}\Big[f(tx + (1-t)y)\Big]_{t=0}^{1} \\ &= \frac{f(x) - f(y)}{x - y}.\end{aligned}$$

Then

$$\begin{aligned}\left|\frac{f(x) - f(y)}{x - y}\right| = \left|\int_0^1 f'(\gamma(t)) \,\mathrm{d}t\right| &\leq \int_0^1 \big|f'(\gamma(t))\big| \,\mathrm{d}t \\ &\leq \int_0^1 \big(\sup_{z \in D} |f'(z)|\big) \,\mathrm{d}t = \sup_{z \in D} |f'(z)|,\end{aligned}$$

as was to be shown. □

We will now translate the measure theoretic property of Definition 3.9.2 to an analytic one. Our results in the coming sections only depend on the 'if' part of the following equivalence.

Theorem 3.9.6. *Let K be a number field, $0 < r < 1$ and $f \in K_{\mathbb{R}}[Y]$. Then f is exponentially bounded at radius r if and only if there exists an $a \in \mathbb{R}_{>0}$ such that for all $\sigma \in \mathrm{X}(K)$ and $z \in \mathbb{C}$ we have*

$$|\sigma(f)(z)| \leq \exp(a(|z|^2 - r^2)).$$

Proof. ($\Leftarrow$) Suppose such a exists. Let $\mu \in \mathcal{M}(K)$ such that

$$\int |z|^2 \,\mathrm{d}\mu(\sigma, z) < r^2.$$

Then

$$\int \log|\sigma(f)(z)| \,\mathrm{d}\mu(\sigma, z) \leq \int a(|z|^2 - r^2) \,\mathrm{d}\mu(\sigma, z) < ar^2 - ar^2 = 0,$$

so f is exponentially bounded at radius r.

($\Rightarrow$) Let $D_0 = \{z \in \mathbb{C} \,|\, |z| < r\}$ and $D_\infty = \{z \in \mathbb{C} \,|\, |z| > r\}$. For $c \in \{0, \infty\}$ let

$$A_c = \big\{a \in \mathbb{R} \,\big|\, (\forall\, \rho \in \mathrm{X}(K))\, (\forall\, z \in D_c)\ |\rho(f)(z)| \leq \exp(a(|z|^2 - r^2))\big\}.$$

Firstly, we show that A_0 is non-empty. Let $\rho \in \mathrm{X}(K)$ and $z_0 \in D_0$, and let $\mu \in \mathcal{M}(K)$ be the measure with weight 1 at (ρ, z_0). Then $\int |x|^2 \,\mathrm{d}\mu(\sigma, x) = |z_0|^2 < r^2$, so by exponential boundedness

$$|\rho(f)(z_0)| = \exp\Big(\int \log|\sigma(f)(x)| \,\mathrm{d}\mu(\sigma, x)\Big) < 1.$$

It follows that $0 \in A_0$, and even $(-\infty, 0] \subseteq A_0$. This argument also shows that $\rho(f)$ is bounded by 1 on the boundary of D_0, the circle of radius r.

Secondly, we show that A_∞ is non-empty. Since $\exp(|z|^2 - r^2)$ grows faster than any polynomial, there exists some $b > r$ such that $|\rho(f)(z)| \leq \exp(|z|^2 - r^2)$ for all $|z| \geq b$. Write $B = \{z \in \mathbb{C} \,|\, |z| \leq b\}$. Let $\rho \in \mathrm{X}(K)$ and $z \in B \cap D_\infty$, and write $g = \rho(f)$ and $\theta = z/|z|$. As remarked at the end of the previous paragraph we have $|g(r\theta)| \leq 1$, so that

$$\begin{aligned}
\log|g(z)| &\leq \log(1 + |g(z) - g(r\theta)|) \\
&\leq |g(z) - g(r\theta)| \\
&= \frac{|z|^2 - r^2}{|z| + r} \cdot \left|\frac{g(z) - g(r\theta)}{z - r\theta}\right| \\
&\overset{*}{\leq} (|z|^2 - r^2) \cdot \frac{\sup_{x \in B} |g'(x)|}{2r} \\
&\leq a(|z|^2 - r^2),
\end{aligned}$$

where $*$ follows from Lemma 3.9.5 and a is the maximum of 1 and all $(2r)^{-1} \sup_{x \in B} |\rho(f)'(x)|$ for $\rho \in \mathrm{X}(K)$. Thus $a \in A_\infty$.

Thirdly, we show that $A_0 \cap A_\infty$ is non-empty. Suppose for the sake of contradiction that $A_0 \cap A_\infty$ is empty. Clearly A_0 and A_∞ are closed.

Hence there exist reals that are neither in A_0 nor A_∞, and let a be such a real number. It follows that $a > 0$. In turn, there exist $z_0 \in D_0$ and $z_\infty \in D_\infty$ with $\rho_0, \rho_\infty \in \mathrm{X}(K)$ such that $|\rho_0(f)(z_0)| > \exp(a(|z_0|^2 - r^2))$ and $|\rho_\infty(f)(z_\infty)| > \exp(a(|z_\infty|^2 - r^2))$. Choose some $t \in (0,1)$ such that $(1-t)|z_0|^2 + t|z_\infty|^2 < r^2$ and let μ be the measure that assigns weight $1-t$ to (ρ_0, z_0) and weight t to (ρ_∞, z_∞). Then $\int |z|^2 \,\mathrm{d}\mu(\sigma, z) < r^2$ and thus

$$0 > \int \log|\sigma(f)(z)| \,\mathrm{d}\mu(\sigma, z) = (1-t)\log|\rho_0(f)(z_0)| + t\log|\rho_\infty(f)(z_\infty)|.$$

Taking the limit of t up to $s \in \mathbb{R}$ such that $(1-s)|z_0|^2 + s|z_\infty|^2 = r^2$ we get

$$\begin{aligned} 0 &\geq (1-s)\log|\rho_0(f)(z_0)| + s\log|\rho_\infty(f)(z_\infty)| \\ &> a((1-s)|z_0|^2 + s|z_\infty|^2 - r^2) = 0, \end{aligned}$$

a contradiction. Hence $A_0 \cap A_\infty$ is non-empty, as was to be shown.

Note that $D_0 \cup D_\infty$ is dense in $\mathbb{C}$, so any positive $a \in A_0 \cap A_\infty$ gives the inequality we set out to prove. Suppose $a \in A_0 \cap A_\infty$ is such that $a \leq 0$. Thus $|\rho(f)(z)| \leq \exp(a(|z|^2 - r^2)) \leq 1$ for all $z \in D_\infty$ and $\rho \in \mathrm{X}(K)$, so $\rho(f)$ is a constant function. However, as $|\rho(f)(z)| < 1$ for $z \in D_0$ as shown before, this constant is strictly less than 1. Let $c \in (0,1)$ be a constant that bounds $\rho(f)$ for all $\rho \in \mathrm{X}(K)$. Then $-r^{-2}\log c \in A_0 \cap A_\infty$ is positive. Hence $A_0 \cap A_\infty$ always contains a positive element. □

3.10 Volume computation

The next step is to compute the volume of a symmetric convex set of exponentially bounded polynomials. As in Lemma 3.8.5 it suffices for the sake of volume computation to consider the case where the radius is 1 and the base field is $\mathbb{R}$. In view of Theorem 3.9.6, we consider the unit-ball of the following norm.

Definition 3.10.1. Let $\mathbb{F}$ be either $\mathbb{R}$ or $\mathbb{C}$. We equip $\mathbb{F}[Y]$ with the *exp-norm*

$$\|f\|_{\mathrm{e}} = \max_{z \in \mathbb{C}} \frac{|f(z)|}{\exp(|z|^2)},$$

not to be confused with $\|-\|_p$ for $p = \mathrm{e}$ from Definition 2.2.11.

Lemma 3.10.2. *Consider the map* $\phi\colon \mathbb{Z}_{\geq 0} \to \mathbb{R}_{\geq 0}$ *given by*

$$\phi(n) = \begin{cases} \left(\frac{n}{2}\right)! & \text{if } n \text{ is even} \\ \left(\frac{n-1}{2}\right)! \cdot \sqrt{\frac{n+1}{2}} & \text{if } n \text{ is odd} \end{cases}.$$

Then we have

$$\log\Big(\prod_{k=0}^{n}\phi(k)\Big) = \tfrac{1}{4}n^2\log n - (\tfrac{3}{8}+\tfrac{1}{4}\log 2)n^2 + O(n\log n)$$

and for all $x \in \mathbb{R}_{\geq 0}$ *and* $m \in \mathbb{Z}_{\geq 0}$ *we have*

$$\frac{x^{2m+1}}{\phi(2m+1)} \leq \frac{1}{2}\bigg(\frac{x^{2m}}{\phi(2m)} + \frac{x^{2m+2}}{\phi(2m+1)}\bigg).$$

Proof. Writing out the product we have

$$\begin{aligned}\prod_{k=0}^{n}\phi(k) &= \bigg(\prod_{m=0}^{\lfloor n/2\rfloor}\phi(2m)\bigg)\bigg(\prod_{m=0}^{\lfloor (n-1)/2\rfloor}\phi(2m+1)\bigg)\\ &= \bigg(\prod_{m=0}^{\lfloor n/2\rfloor} m!\bigg)\bigg(\prod_{m=0}^{\lfloor (n-1)/2\rfloor} m!\bigg)\bigg(\prod_{m=0}^{\lfloor (n-1)/2\rfloor}\sqrt{m+1}\bigg).\end{aligned}$$

We then apply Proposition 3.7.3 to compute

$$\begin{aligned}\log\Big(\prod_{k=0}^{n}\phi(k)\Big) &= \lfloor\tfrac{n}{2}\rfloor^2\big(\tfrac{1}{2}\log\lfloor\tfrac{n}{2}\rfloor - \tfrac{3}{4}\big) + \lfloor\tfrac{n-1}{2}\rfloor^2\big(\tfrac{1}{2}\log\lfloor\tfrac{n-1}{2}\rfloor - \tfrac{3}{4}\big)\\ &\quad + \lfloor\tfrac{n-1}{2}\rfloor\big(\log\lfloor\tfrac{n-1}{2}\rfloor - 1\big) + O(n\log n)\\ &= \big(\tfrac{n}{2}\big)^2\big(\tfrac{1}{2}\log\tfrac{n}{2} - \tfrac{3}{4}\big) + \big(\tfrac{n}{2}\big)^2\big(\tfrac{1}{2}\log\tfrac{n}{2} - \tfrac{3}{4}\big) + O(n\log n)\\ &= \tfrac{1}{4}n^2\log n - (\tfrac{3}{8}+\tfrac{1}{4}\log 2)n^2 + O(n\log n),\end{aligned}$$

proving the first part. For the second, let $m \in \mathbb{Z}_{\geq 0}$ and $x \in \mathbb{R}_{\geq 0}$. Then

$$\begin{aligned}\frac{1}{\phi(2m)} + \frac{x^2}{\phi(2m+2)} &= \frac{1}{m!}\Big(\Big(1 - \frac{x}{\sqrt{m+1}}\Big)^2 + \frac{2x}{\sqrt{m+1}}\Big)\\ &\geq \frac{1}{m!}\frac{2x}{\sqrt{m+1}} = 2\cdot\frac{x}{\phi(2m+1)},\end{aligned}$$

from which the second part follows. □

Recall the notation $R[X]_n$ from Definition 3.5.6, the subset of $R[X]$ of polynomials of degree strictly less than n.

Proposition 3.10.3. *Write* $S = \{f \in \mathbb{R}[Y] \mid \|f\|_{\mathrm{e}} \leq 1\}$. *Then for* $n \in \mathbb{Z}_{\geq 0}$ *we have*

$$\log \operatorname{vol}(S \cap \mathbb{R}[Y]_n) \geq -\tfrac{1}{4}n^2\log n + (\tfrac{3}{8}+\tfrac{1}{4}\log 2)n^2 + O(n\log n).$$

Proof. Consider ϕ as in Lemma 3.10.2 and define

$$T = \Big\{ \sum_{i=0}^{\infty} f_i Y^i \in \mathbb{R}[Y] \;\Big|\; (\forall i)\ |f_i| \leq \frac{1}{2\phi(i)} \Big\}.$$

Then for all $f \in T$ and $z \in \mathbb{C}$ we have using Lemma 3.10.2 that

$$\begin{aligned} |f(z)| &\leq \sum_{i=0}^{\infty} |f_i| \cdot |z|^i \leq \sum_{i=0}^{\infty} \frac{|z|^i}{2\phi(i)} \\ &= \frac{1}{2}\left[\sum_{k=0}^{\infty} \frac{|z|^{2k}}{k!} + \sum_{k=0}^{\infty} \frac{|z|^{2k+1}}{\phi(2k+1)} \right] \\ &\leq \frac{1}{2}\left[\sum_{k=0}^{\infty} \frac{|z|^{2k}}{k!} + \sum_{k=0}^{\infty} \frac{1}{2}\left(\frac{|z|^{2k}}{k!} + \frac{|z|^{2k+2}}{(k+1)!} \right) \right] \\ &\leq \sum_{k=0}^{\infty} \frac{|z|^{2k}}{k!} = \exp|z^2|, \end{aligned}$$

so $f \in S$ and $T \subseteq S$. Then by Lemma 3.10.2 we have

$$\begin{aligned} \log \mathrm{vol}(T \cap \mathbb{R}[Y]_n) &= -n\log 2 - \log\Big(\prod_{k=0}^{n-1} \phi(k) \Big) \\ &= -\tfrac{1}{4}n^2 \log n + (\tfrac{3}{8} + \tfrac{1}{4}\log 2)n^2 + O(n \log n), \end{aligned}$$

from which the proposition follows. □

Proposition 3.10.3 is sufficient for our purposes. It may interest a reader that the lower bound of Proposition 3.10.3 is actually an equality, which we will show in the remainder of this section.

Theorem 3.10.4 (Brunn–Minkowski inequality, Theorem 4.1 in [16])**.** *Let $n \in \mathbb{Z}_{\geq 1}$ and let $A, B \subseteq \mathbb{R}^n$ be bounded non-empty measurable sets. Then for all $t \in [0,1]$ such that*

$$(1-t)A + tB = \{(1-t)a + tb \,|\, a \in A,\, b \in B\}$$

is measurable we have the inequality

$$\mathrm{vol}((1-t)A + tB)^{1/n} \geq (1-t)\mathrm{vol}(A)^{1/n} + t\mathrm{vol}(B)^{1/n}. \quad \square$$

We will only apply this theorem to compact subsets of $\mathbb{R}^n$, which are indeed measurable and bounded. Moreover, for $A, B \subseteq \mathbb{R}^n$ compact and $t \in (0,1)$ also the set $(1-t)A + tB$ is compact, hence measurable.

Corollary 3.10.5. *Let $n \in \mathbb{Z}_{\geq 0}$, let $V \subseteq \mathbb{R}^n$ be a subspace and let $S \subseteq \mathbb{R}^n$ be a symmetric convex body. Then the map that sends $x \in \mathbb{R}^n$ to $\mathrm{vol}_V(V \cap (S - x))$ takes a maximum at 0.*

Proof. Let $x \in \mathbb{R}^n$ and write $m = \dim V$ and $H_x = V \cap (S - x)$. If $m = 0$ the corollary holds trivially, so suppose $m > 0$. Note that $H_{-x} = -H_x$ since S and V are symmetric. Because S and V are convex we have $\frac{1}{2}H_x + \frac{1}{2}H_{-x} \subseteq H_0$. Hence by Theorem 3.10.4 we have

$$\begin{aligned}\mathrm{vol}(H_0)^{1/m} &\geq \mathrm{vol}(\tfrac{1}{2}H_x + \tfrac{1}{2}H_{-x})^{1/m} \\ &\geq \tfrac{1}{2}\mathrm{vol}(H_x)^{1/m} + \tfrac{1}{2}\mathrm{vol}(H_{-x})^{1/m} \\ &= \mathrm{vol}(H_x)^{1/m},\end{aligned}$$

from which the corollary follows. □

Recall the definition of $\oplus$ from Definition 2.5.1.

Corollary 3.10.6. *Let $n \in \mathbb{Z}_{\geq 0}$, let $U, V \subseteq \mathbb{R}^n$ be subspaces such that $U \oplus V = \mathbb{R}^n$ and write π for the projection $U \oplus V \to U$. If $S \subseteq \mathbb{R}^n$ is a symmetric convex body, then $\mathrm{vol}_{\mathbb{R}^n}(S) \leq \mathrm{vol}_U(\pi S) \cdot \mathrm{vol}_V(S \cap V)$.*

Proof. By Corollary 3.10.5 we have

$$\begin{aligned}\mathrm{vol}(S) &= \int_{\pi S} \mathrm{vol}_V(V \cap (S - x))\,\mathrm{d}x \\ &\leq \int_{\pi S} \mathrm{vol}_V(V \cap S)\,\mathrm{d}x \\ &= \mathrm{vol}_U(\pi S) \cdot \mathrm{vol}_V(V \cap S).\end{aligned}$$

□

Theorem 3.10.7. *Write $S = \{f \in \mathbb{R}[Y] \mid \|f\|_{\mathrm{e}} \leq 1\}$. Then for $n \in \mathbb{Z}_{\geq 0}$ we have*

$$\log \mathrm{vol}(S \cap \mathbb{R}[Y]_n) = -\tfrac{1}{4}n^2 \log n + (\tfrac{3}{8} + \tfrac{1}{4}\log 2)n^2 + O(n \log n).$$

Proof. We already proved a lower bound in Proposition 3.10.3, so it remains to prove an upper bound. We will inductively show that

$$\mathrm{vol}(S \cap \mathbb{R}[Y]_n) \leq 2^n \prod_{k=1}^{n-1} \Big(\frac{2\mathrm{e}}{k}\Big)^{k/2}.$$

It then follows from Proposition 3.7.3 that

$$\begin{aligned}\log \mathrm{vol}(S \cap \mathbb{R}[Y]_n) &\leq n \log 2 + \frac{1}{2}\sum_{k=1}^{n-1} k\big(\log(2\mathrm{e}) - \log k\big) \\ &= -\tfrac{1}{4}n^2 \log n + (\tfrac{3}{8} + \tfrac{1}{4}\log 2)n^2 + O(n \log n).\end{aligned}$$

For $n = 0$ and $n = 1$ the inequality certainly holds. Now suppose the inequality holds for $n \geq 1$. Write $\mathbb{R}[Y]_{n+1} = (\mathbb{R}Y^n) \oplus \mathbb{R}[Y]_n$ and let $\pi\colon \mathbb{R}[Y]_{n+1} \to \mathbb{R}Y^n$ be the projection map. By Corollary 3.10.6 it suffices to show for $n > 0$ that $\mathrm{vol}(\pi(S \cap \mathbb{R}[Y]_{n+1})) \leq 2(\frac{n}{2\mathrm{e}})^{-n/2}$. We do this by proving

$$\pi(S \cap \mathbb{R}[Y]_{n+1}) \overset{\text{(i)}}{\subseteq} S \cap (\mathbb{R}Y^n) \overset{\text{(ii)}}{\subseteq} [-1, +1]\Big(\frac{2\mathrm{e}}{n}\Big)^{n/2} Y^n.$$

(i) Suppose $f \in \mathbb{R}[Y]_{n+1}$ and $\|f\|_{\mathrm{e}} < \|\pi(f)\|_{\mathrm{e}}$. Since $\pi(f)$ is a monomial, the function $z \mapsto |\pi(f)(z)| \exp(-|z|^2)$ takes its maximum on a circle of radius say r. Then for all z on this circle we have

$$|f(z)| \leq \|f\|_{\mathrm{e}} \exp(r^2) < \|\pi(f)\|_{\mathrm{e}} \exp(r^2) = |\pi(f)(z)|.$$

Hence by Rouché's theorem (Theorem 4.18 in [1]), the polynomial $f - \pi(f)$ has as many roots as $\pi(f)$ in the disk $\{z \in \mathbb{C} \,|\, |z| \leq r\}$, counting multiplicities. However, since $f - \pi(f)$ has degree at most $n - 1$ and $\pi(f)$ has n such roots, this is a contradiction. Hence $\|\pi(f)\|_{\mathrm{e}} \leq \|f\|_{\mathrm{e}}$, from which (i) follows.

(ii) Consider the map $g\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ given by $x \mapsto x^n \exp(-x^2)$. Then

$$\frac{\mathrm{d}g}{\mathrm{d}x} = x^{n-1}(n - 2x^2)\exp(-x^2) = 0 \iff x = 0 \ \vee \ x = \sqrt{n/2}.$$

Hence g takes a maximum at $(n/2)^{1/2}$, so we conclude that $\|Y^n\|_{\mathrm{e}} = g((n/2)^{1/2}) = (\frac{n}{2\mathrm{e}})^{n/2}$. Thus $\max\{c \in \mathbb{R} \,|\, cY^n \in S\} = (\frac{2\mathrm{e}}{n})^{n/2}$, as was to be shown.

The theorem now follows by induction. □

3.11 Proof of the main theorem

We are now ready to give a proof of Theorem 3.11.2.

Proposition 3.11.1. *Let R be an order of a number field K, let $\alpha \in K$ and $0 < r^2 < \frac{1}{2}\exp(\frac{1}{2})$. Then there exists some non-zero $f \in R[X]$ such that $f(X - \alpha)$ is exponentially bounded at radius r.*

Proof. Let $n \in \mathbb{Z}_{\geq 1}$ and $d = [K : \mathbb{Q}]$. Write $Y = X - \alpha$ and consider the real vector space $K_{\mathbb{R}}[Y]_n$, which we equip with an inner product as in Definition 3.8.2 with respect to the variable Y. By Theorem 3.5.5 and Lemma 3.8.4 the lattice $R[X]_n$ in $K_{\mathbb{R}}[Y]_n$ is full rank and has determinant $\det(R[Y]_n) = |\det(R)|^n = |\Delta(R)|^{n/2}$. For $b \in \mathbb{R}_{\geq 0}$ consider

$$\begin{aligned} S_n &= \{f \in K_{\mathbb{R}}[Y]_n \,|\, (\forall\, \sigma \in \mathrm{X}(K),\, z \in \mathbb{C})\ |\sigma(f)(z)| \leq \exp(bn(|z|^2 - r^2))\} \\ &= \{f \in K_{\mathbb{R}}[Y]_n \,|\, (\forall\, \sigma \in \mathrm{X}(K))\ \|\exp(bnr^2)\sigma(f)((bn)^{-1/2}Y)\|_{\mathrm{e}} \leq 1\}. \end{aligned}$$

We have a natural orthogonal decomposition $K_{\mathbb{R}} \cong \mathbb{R}^u \times \mathbb{C}^v$ for some $u, v \in \mathbb{Z}_{\geq 0}$ which in turn gives an orthogonal decomposition $K_{\mathbb{R}}[Y]_n = (\mathbb{R}[Y]_n)^u \times (\mathbb{C}[Y]_n)^v$. Note that S_n is simply a product over $\sigma \in \mathrm{X}(K)$ of

$$S_n(\sigma) = \{f \in \mathbb{F}[Y]_n \mid \| \exp(bnr^2) \cdot \sigma(f)((bn)^{-1/2} \cdot Y)\|_{\mathrm{e}} \leq 1\}$$

where $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$ depending on whether $\sigma(K) \subseteq \mathbb{R}$. Then using Lemma 3.8.4 and Proposition 3.10.3 we compute

$$\begin{aligned}\log \mathrm{vol}(S_n) &\geq d\Big(\big(-\tfrac{1}{4}n^2 \log n + (\tfrac{3}{8} + \tfrac{1}{4}\log 2)n^2\big) + \big(\tfrac{1}{4}n^2 \log(bn) - bn^2r^2\big)\Big) \\ &\quad + O(n \log n) \\ &= dn^2 \cdot \varepsilon(b) + O(n \log n),\end{aligned}$$

with $\varepsilon(b) = \frac{1}{4}\log(2b) + \frac{3}{8} - r^2 b$. Choosing $b = (2r)^{-2}$ we get $\varepsilon(b) = \frac{1}{4}(\frac{1}{2} - \log(2r^2)) > 0$. Hence

$$\log\Big(\frac{\mathrm{vol}(S_n)}{2^{dn} \cdot |\Delta(R)|^{n/2}}\Big) \geq dn^2 \cdot \varepsilon(b) + O(n \log n) \to \infty \quad (\text{as } n \to \infty).$$

Thus by Minkowski's theorem there exists for n sufficiently large some non-zero $g \in S_n \cap R[X]$. Because $g \in S_n$, this polynomial is exponentially bounded at radius r by Theorem 3.9.6. □

Theorem 3.11.2. *Suppose $r \in \mathbb{R}$ and $\alpha \in \overline{\mathbb{Q}}$. If $r < \sqrt[4]{\mathrm{e}/4}$, then there exist only finitely many $\beta \in \overline{\mathbb{Z}}$ such that $\|\alpha - \beta\| < r$.*

Proof. Let $\gamma = \alpha/2$, let $K = \mathbb{Q}(\gamma)$ and let R be some order in K. Choose $r \in \mathbb{R}_{>0}$ such that $\|\gamma\| < r < \sqrt[4]{\mathrm{e}/4}$. Then by Proposition 3.11.1 there exists some non-zero polynomial $f \in R[X]$ which as polynomial in $Y = X - \gamma$ is exponentially bounded at radius r. Hence by Proposition 3.9.3 all $(\beta, \alpha - \beta) \in \mathrm{dec}(\alpha)$ satisfy $f(\beta) = 0$. As f has only finitely many roots, the theorem follows. □

From the proof of Theorem 3.11.2 one easily derives the following result.

Proposition 3.11.3. *There exists an algorithm that, given some $r \in \mathbb{R} \cap \overline{\mathbb{Q}}$ and $\alpha \in \overline{\mathbb{Q}}$, decides whether $r < \sqrt[4]{\mathrm{e}/4}$ and if so computes all $\beta \in \overline{\mathbb{Z}}$ such that $\|\alpha - \beta\| \leq r$, each represented by their minimal polynomial over $\mathbb{Q}(\alpha)$.*

Proof. Clearly $r \neq \sqrt[4]{\mathrm{e}/4}$ as the latter is not algebraic. However, both are computable, and after finitely many steps of approximation we can decide whether $r < \sqrt[4]{\mathrm{e}/4}$. We have an explicit formula for a lower bound on the volume of the set S as defined in the proof of Proposition 3.10.3. So moreover

we can compute a sufficiently large n such that Minkowski's theorem, as in the proof of Proposition 3.11.1, guarantees the existence of a non-zero lattice point in S. We may then simply enumerate all lattice points to eventually find a polynomial f as in Proposition 3.11.1. We determine using [31] the monic irreducible factors of f and decide which factors g have a root β satisfying $\|\alpha - \beta\| \leq r$. □

Corollary 3.11.4. *There is an algorithm that takes as input an element $\alpha \in \overline{\mathbb{Z}}$ given by its minimal polynomial, and decides whether $\|\alpha\| < \sqrt[4]{4\mathrm{e}}$ and if so, computes all non-trivial $(\beta, \gamma) \in \mathrm{dec}(\alpha)$, each represented by the minimal polynomial of β over $\mathbb{Q}(\alpha)$.*

Proof. We apply Proposition 3.11.3 with $\alpha/2$ in the place of α and $\|\alpha/2\|$ in the place of r. By Lemma 2.4.3 each β found gives a decomposition $(\beta, \alpha - \beta)$. Note that we can filter out the trivial decompositions. □

3.12 Remarks on the proof of the main theorem

In this section we briefly discuss the proof of Theorem 3.11.2 and make some practical remarks for explicit computation.

The proof of Theorem 3.11.2 proceeds in the following steps:

1. We determine a sufficient condition for a polynomial to have all lattice points close to α as roots.
2. We translate this condition into an analytic one.
3. We determine the volume of a symmetric convex set of polynomials satisfying this condition.
4. We apply Minkowski's convex body theorem to find integral polynomials in this set.

Theorem 3.9.6 suggests that step (2) can hardly be improved upon. By Theorem 3.10.7 we correctly computed the volume of our symmetric convex set in step (3). However, in order to make it convex we fixed the constant a that comes out of Theorem 3.9.6. It is easy to verify that we indeed made an optimal choice of a in Proposition 3.11.1, although that does not guarantee we chose the best convex subset. If the weakest link in the proof is step (4), we likely require a completely different approach. It should be noted however that Minkowski's convex body theorem is powerful enough to prove the classical Theorem 3.8.6.

One could also ask for stronger results in the case we are only interested in decompositions of lattice points, i.e. when $\alpha \in \frac{1}{2}\overline{\mathbb{Z}}$. A piece of information we can exploit is the following symmetry: For all $\alpha \in \overline{\mathbb{Z}}$ we have an involution $x \mapsto \alpha - x$ on $\overline{\mathbb{Z}}$ which induces action on $\mathrm{dec}(\alpha)$, given by $(\beta, \gamma) \mapsto (\gamma, \beta)$.

Lemma 3.12.1. *Let $\alpha \in \overline{\mathbb{Z}}$ and let $\mathbb{Z}[\alpha] \subseteq R$ be an order of $\mathbb{Q}(\alpha)$. For all $f \in R[X]$ such that $f(\beta) = 0$ for all $(\beta, \gamma) \in \mathrm{dec}(\alpha)$, also $g = f(\alpha - X) \in R[X]$ satisfies $g(\beta) = 0$ for all $(\beta, \gamma) \in \mathrm{dec}(\alpha)$.* □

Lemma 3.12.1 turns the involution on $\overline{\mathbb{Z}}$ into an R-algebra automorphism on $R[X]$. We can incorporate this automorphism in our proof of Theorem 3.11.2.

Proposition 3.12.2. *Let $\alpha \in \overline{\mathbb{Z}}$, let $\mathbb{Z}[\alpha] \subseteq R$ be an order of $K = \mathbb{Q}(\alpha)$ and let $r \in \mathbb{R}_{>0}$. For all $f \in R[X]$ such that f as a polynomial in $Y = X - \alpha/2$ is exponentially bounded at radius r, so is $f(X) \cdot f(\alpha - X) \in K[Y^2]$.*

Proof. Note that the involution $X \mapsto \alpha - X$ is with respect to Y given by $Y \mapsto -Y$. Hence if f as a polynomial in Y is exponentially bounded at radius r, then so is $f(\alpha - X)$. As noted in Example 3.9.4, the set of polynomials exponentially bounded at r is closed under multiplication. Hence $g = f(X) \cdot f(\alpha - X)$ is exponentially bounded at radius r. Now g is invariant under $Y \mapsto -Y$, meaning all coefficients at odd degree monomials in Y are zero, i.e. $g \in K[Y^2]$. □

An interesting question to ask is how dissimilar f and $f(\alpha - X)$ can be for exponentially bounded f. Certainly both should have β as root for all $(\beta, \gamma) \in \mathrm{dec}(\alpha)$ by Lemma 3.12.1. In the context of finding 'small' f algorithmically it seems that often f and $f(\alpha - X)$ are the same (up to sign).

As a consequence of Proposition 3.12.2, when proving a specialization of Theorem 3.11.2 to $\alpha \in \frac{1}{2}\overline{\mathbb{Z}}$ we may look at the lattice $R[X(\alpha - X)]$ in $K_{\mathbb{R}}[Y^2]$ instead of $R[X]$ in $K_{\mathbb{R}}[Y]$. The effect is two-fold. Firstly, it simplifies the volume computation of Proposition 3.10.3, as we no longer require the ad-hoc function ϕ from Lemma 3.10.2. Secondly, any integral polynomial in our symmetric body can be found in a lower dimensional lattice in Proposition 3.11.1. This follows from the suggested changes to Proposition 3.10.3, but can heuristically be seen as follows. If f is a solution in the original lattice $R[X]$, then $f(X) \cdot f(\alpha - X)$ is a solution in our new lattice $R[X(\alpha - X)]$ at the same dimension. However, as discussed before, f is likely to be an element of $R[X(\alpha - X)]$ anyway, and if so we would have found f at half the dimension in $R[X(\alpha - X)]$. Neither of these changes have an effect on the quality of our theoretical results. However, when we want to compute decompositions in practice, the latter 'dimension reduction' is very useful.

3.13 Computational example

We will now work out an example proving an algebraic integer α is indecomposable.

Showing that α is indecomposable will be trivial when $\|\alpha\| \leq \sqrt{2}$ as we have seen in Proposition 3.3.1, so we will choose α such that $\|\alpha\| > \sqrt{2} \approx 1.414$. On the other hand, the algorithm from Proposition 3.11.3 terminates faster the smaller $\|\alpha\|$ is, so for this example we will consider $\alpha = \sqrt[3]{3}$ with $\|\alpha\| = 3^{1/3} \approx 1.442$.

Setup. Let $\alpha = \sqrt[3]{3}$ and let $r^2 = 6/11$, so that $\|\alpha/2\| < r < \sqrt[4]{\mathrm{e}/4}$. Write $K = \mathbb{Q}(\alpha)$ and $R = \mathbb{Z}[\alpha]$ and consider the ring $R[X]$. Writing $Y = X - \alpha/2$, we are looking for a polynomial $f \in R[X]$ such that f as polynomial in Y is exponentially bounded at radius r. However, writing $Z = X(\alpha - X)$ we may instead look for such a polynomial in $R[Z]$, as follows from Lemma 3.12.1.

Finding a polynomial. It is quite involved to systematically find short vectors in a lattice. Instead we will employ a more ad-hoc approach, more along the lines of Theorem 3.6.6. We guess that our polynomial f will be monic in Z of some degree n. We start with Z^n and then greedily subtract $\mathbb{Z}[\alpha]$-multiples of lower degree powers of Z such that the resulting polynomial in Y becomes 'small', i.e. has small coefficients under every embedding $K \to \mathbb{C}$ with lower degree terms weighing more heavily. Effectively, we are applying a rounding function in the sense of Definition 3.6.3. Note that $Z = -Y^2 + \alpha^2/4$. Similarly as in the proof of Theorem 3.6.6, taking $n = 4$ the Y^6 term becomes integral, which is useful. Thus we will try $n = 4$. We compute:

$$\begin{array}{rrrcllll}
Z^4 & & & = & Y^8 & -\alpha^2 Y^6 & +\frac{9}{8}\alpha Y^4 & -\frac{9}{16}Y^2 & +\frac{9}{256}\alpha^2 \\
 & \alpha^2 Z^3 & & = & & -\alpha^2 Y^6 & +\frac{9}{4}\alpha Y^4 & -\frac{27}{16}Y^2 & +\frac{9}{64}\alpha^2 \\
\hline
Z^4 & -\alpha^2 Z^3 & & = & Y^8 & & -\frac{9}{8}\alpha Y^4 & +\frac{9}{8}Y^2 & -\frac{27}{256}\alpha^2 \\
 & & -\alpha Z^2 & = & & & -\alpha Y^4 & +\frac{3}{2}Y^2 & -\frac{3}{16}\alpha^2 \\
\hline
Z^4 & -\alpha^2 Z^3 & +\alpha Z^2 & = & Y^8 & & -\frac{1}{8}\alpha Y^4 & -\frac{3}{8}Y^2 & +\frac{21}{256}\alpha^2
\end{array}$$

The remaining coefficients with respect to Y look pretty small in every embedding $K \to \mathbb{C}$, so we guess

$$f(Y) = Y^8 - \tfrac{1}{8}\alpha Y^4 - \tfrac{3}{8}Y^2 + \tfrac{21}{256}\alpha^2 = Z^4 - \alpha^2 Z^3 + \alpha Z^2 \in R[Z].$$

is going to be exponentially bounded at radius r as polynomial in Y.

Proving exponentially boundedness. If we take $b\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ given by

$$b(w) = w^4 + \tfrac{1}{8} \cdot 3^{1/3} \cdot w^2 + \tfrac{3}{8} \cdot w + \tfrac{21}{256} \cdot 3^{2/3},$$

then for all $\sigma \in \mathrm{X}(K)$ and $z \in \mathbb{C}$ we have $|\sigma(f)(z)| \leq b(|z|^2)$. To prove that f is exponentially bounded at radius r it suffices to find $a \in \mathbb{R}$ such that $b(w) \leq \exp(a(w - r^2))$ for all $w \in \mathbb{R}_{\geq 0}$. Because $b(0) = \frac{21}{256}3^{2/3}$, we must have $a \leq -\log(b(0))/r^2 \approx 3.4$. We will try $a = 3$ for simplicity. Consider the function $B(w) = b(w) \cdot \exp(-a(w - r^2))$, for which we want to show $B(w) \leq 1$ for all w. Then

$$0 = B'(w) = \exp(-a(w - r^2))(b'(w) - ab(w))$$

if and only if $ab(w) - b'(w) = 0$. Since the latter is simply a polynomial equation we will find using standard techniques that it has no positive real roots. We compute:

$$\begin{aligned} ab(w) - b'(w) &= 3w^4 - 4w^3 + \tfrac{3}{8}3^{1/3}w^2 + (\tfrac{9}{8} - \tfrac{1}{4}3^{1/3})w + (\tfrac{63}{256}3^{2/3} - \tfrac{3}{8}) \\ &> 3w^4 - 4w^3 + \tfrac{3}{5}w^2 + \tfrac{3}{4}w + \tfrac{1}{4}. \end{aligned}$$

For $1 \leq w$ we get $ab(w) - b'(w) > 3w^4 - 4w^3 + \frac{3}{2} = w^2(3^{1/2}w - 2 \cdot 3^{-1/2})^2 + (\frac{3}{2} - \frac{4}{3}w^2) \geq 0$ and for $0 < w \leq 1$ we get $ab(w) - b'(w) > 3w^4 - 4w^3 + \frac{3}{2}w^2 = 3w^2(w^2 - \frac{4}{3}w + \frac{1}{2}) \geq 3w^2(w - 2^{-1/2})^2 \geq 0$. Hence B has no local maxima besides possibly at 0, and because $B(w) \to 0$ as $w \to \infty$ we conclude that B takes a maximum at 0. Therefore b is bounded by $w \mapsto \exp(a(w - r^2))$ and thus f is exponentially bounded at radius r.

Finding decompositions. Writing f as a polynomial in X we get

$$\begin{aligned} f &= X^8 - 4\alpha X^7 + 7\alpha^2 X^6 - 21X^5 + 13\alpha X^4 - 5\alpha^2 X^3 + 3X^2 \\ &= X^2 \cdot (\alpha - X)^2 \cdot (X^4 - 2\alpha X^3 + 2\alpha^2 X^2 - 3X + \alpha). \end{aligned}$$

By Proposition 3.9.3 all decompositions of α can be found among the roots of f. The factors X and $\alpha - X$ correspond to the trivial decompositions $(0, \alpha)$ and $(\alpha, 0)$ of α. The polynomial $h = X^4 - 2\alpha X^3 + 2\alpha^2 X^2 - 3X + \alpha$ is irreducible as it is Eisenstein at the prime (α). Let $\beta \in \overline{\mathbb{Z}}$ be a root of h. By Lemma 3.2.8 we have $\|\beta\| \geq N(\beta) = N(h(0)) = 3^{1/3} = \|\alpha\|$. We can only have $\|\beta\|^2 + \|\alpha - \beta\|^2 \leq \|\alpha\|^2$ if $\|\alpha - \beta\| = 0$, i.e. $\alpha = \beta$, which is impossible. Hence α is indecomposable by Lemma 2.4.3.

3.14 Enumeration of degree-3 indecomposables

In this section we discuss our attempt to compute the indecomposable algebraic integers of degree 3 and derive Theorem 3.14.1. We will refer to tables of computational results, which can be found in the appendix, and are obtained by a computer program [19] written in Sage [41].

We will write $f_\alpha \in \mathbb{Z}[x]$ for the minimal polynomial of $\alpha \in \overline{\mathbb{Z}}$. We will consider α up to 'trivial isometries' of $\overline{\mathbb{Z}}$, namely those of $\mu_\infty \rtimes \mathrm{Gal}(\overline{\mathbb{Q}})$ as in Lemma 3.2.13. Using Proposition 3.7.1 we compute a set of 5525 polynomials among which we can find all minimal polynomials of the indecomposable algebraic integers of degree 3. Among those 5525 polynomials f only 700 are in fact irreducible with $q(\alpha) \leq 4$ for all roots α of f. We already eliminated the Galois action by considering minimal polynomials instead of elements, and by choosing only one element of each μ_∞-orbit $\{f, -f(-x)\}$ we eliminate the action of μ_∞, and end up with 'only' 350 polynomials to check. Of those 350, there are 27 polynomials f_α such that $q(\alpha) < 2$, so that α is indecomposable by Proposition 3.3.1.

Small degree decompositions. For 95 polynomials f, the roots α of f have a non-trivial decomposition in the ring of integers of $\mathbb{Q}(\alpha)$. For 116 of the remaining polynomials f_α we can find a non-trivial decomposition $(\beta, \alpha - \beta)$ of α with β in the ring of integers of a degree 2 extension of $\mathbb{Q}(\alpha)$. Of those 116 there are 84 for which the minimal polynomial g_β of β over $\mathbb{Q}(\alpha)$ is of the form $x^2 - \alpha x \pm 1$, a polynomial we encountered in the proof of Lemma 3.4.2. The remaining 32 polynomials and corresponding decompositions can be found in Table 1. We are now left with 112 polynomials to check.

Large degree decompositions. To find decompositions in higher degree extensions we implemented a lattice algorithm. Since we are interested in finding only one decomposition instead of all of them, and since verifying whether something is a decomposition is computationally easy, we can get away with a lot of heuristics. For $(\beta, \alpha - \beta) \in \mathrm{dec}(\alpha)$ we have, on average of squares over all embeddings of $\mathbb{Q}(\alpha, \beta)$ in $\mathbb{C}$, that $|\beta - \alpha/2| \leq \sqrt{q(\alpha/2)} = r$ by Lemma 2.4.3. Hence if we write $g_\beta = \sum_i c_i (x - \alpha/2)^i$ we have that $\sum_i |c_i| r^i$ should be small. It is useful for our lattice algorithm to instead consider the 2-norm $(\sum_i r^i \sum_\sigma |\sigma(c_i)|^2)^{1/2}$ and hope this does not affect the quality of our results for the worse. We enumerate small polynomials $\varepsilon \in \mathbb{Q}(\alpha)[x]$ of degree less than $d \in \mathbb{Z}_{>0}$ such that $(x - \alpha/2)^d - x^d + \varepsilon$ is in the lattice of integral polynomials, and thus $(x - \alpha/2)^d + \varepsilon$ is monic, integral and small. We then verify for each of those whether they induce a decomposition of α. The 41 polynomials f_α for which this method has found a non-trivial decomposition $(\beta, \alpha - \beta)$ of α with g_β of degree greater than 2 are listed in Table 2 together with the polynomial g_β found. This leaves 71 polynomials to check and gives an upper bound of $6 \cdot 98 = 588$ on the number of indecomposable algebraic integers of degree 3.

Indecomposables. On the other hand, we want to prove that certain α are indecomposable. To this end, we implemented a lattice algorithm similar

to that of Proposition 3.11.3. To hopefully speed up the algorithm we also apply the dimension reducing symmetry trick discussed from Lemma 3.12.1. Writing R for the ring of integers of $\mathbb{Q}(\alpha)$ and $z = x(\alpha - x)$, we enumerate short $g \in R[z]$ for which we verify whether g as polynomial in $y = x - \alpha/2$ is exponentially bounded. The 32 polynomials f_α for which we found such a g proving indecomposability of α are listed in Table 3. We present g in factored form for compactness. This leaves 39 polynomials undetermined and gives a lower bound of $6 \cdot 59 = 354$ on the number of indecomposable algebraic integers of degree 3.

Theorem 3.14.1. *There are exactly* 2 *indecomposable algebraic integers of degree* 1*, there are exactly* 14 *of degree* 2*, and there are at least* 354 *and at most* 588 *of degree* 3*.*

Proof. The degree 1 case is obvious: 1 and -1 are the only indecomposable integers. The degree 2 case is Theorem 3.4.3. The bounds for degree 3 are the result of the computation in this section. □