Bounds on roots of unity in orders

Tristan Tillij

Master's thesis
Under supervision of Prof. Dr. H.W. Lenstra Jr.
Defended on August 25, 2017

Mathematisch Instituut
Universiteit Leiden

Contents

Introduction

An *order* is a commutative ring whose additive group is isomorphic to $\mathbb{Z}^n$ for some nonnegative integer n, called its *rank*. This thesis presents bounds on the number and multiplicative order of *roots of unity* in an order, in terms of its rank. The main results are the following four closely related theorems.

I Theorem. *An order of rank n has at most $6^{\frac{n}{2}}$ roots of unity if n is even, and at most $2 \cdot 6^{\frac{n-1}{2}}$ roots of unity if n is odd, and these upper bounds are sharp.*

These bounds are attained by $\mathbb{Z}[\zeta_3]^{\frac{n}{2}}$ for all even n, and by $\mathbb{Z} \times \mathbb{Z}[\zeta_3]^{\frac{n-1}{2}}$ for all odd n.

II Theorem. *Let $e(n)$ denote the maximum of the exponents of the groups of roots of unity of orders of rank n. Then $\ln e(n) \sim \sqrt{n \ln n}$ as $n \longrightarrow \infty$.*

Of particular interest are *connected* orders, that is, nonzero orders that are not products of two nonzero rings.

III Theorem. *A connected order of rank n has at most 2^n roots of unity if $n \neq 2, 4$. For $n = 2$ and $n = 4$ it has at most 6 and 18 roots of unity, respectively, and all these upper bounds are sharp.*

For each $n \neq 2, 4$ the bound of 2^n is attained by the subring of $\mathbb{Z}^n$ generated by its roots of unity. For $n = 2$ and $n = 4$ the bounds are attained by $\mathbb{Z}[\zeta_3]$ and the subring of $\mathbb{Z}[\zeta_3]^2$ generated by its third roots of unity. We show that these rings are indeed connected in section 3.

IV Theorem. *Let $e_c(n)$ denote the maximum of the exponents of the groups of roots of unity of connected orders of rank n. Then $\ln e_c(n) \sim \sqrt{n \ln n}$ as $n \longrightarrow \infty$.*

We prove theorems I and III in section 4, and theorems II and IV in section 5. For the latter two we use two classical results from analytic number theory; the prime number theorem and Landau's theorem. In section 3 we show that for all four theorems we may restrict our attention to *reduced* orders. Reduced orders are those in which 0 is the unique nilpotent element.

V Theorem. *For every order there exists a reduced order of the same rank with the same group of roots of unity, and for every connected order there exists a reduced connected order of the same rank with the same group of roots of unity.*

This is proved in section 3. Here we also develop some theory on the subrings of orders generated by roots of unity.

The main concern of section 2 is the proof of the following characterization of reduced orders.

VI Theorem. *A ring is a reduced order if and only if it is isomorphic to a subring of finite index of a finite product of rings of integers.*

This makes reduced orders the subject of algebraic number theory. In this section we also collect some results from commutative algebra particular to orders that are used throughout the later sections.

Section 6 presents a result that is of a more theoretical nature.

VII Theorem. *The tensor product of two connected orders over $\mathbb{Z}$ is again connected.*

Its proof requires some more background in algebraic number theory, which we summarize there. Every order is a finite product of connected orders, so this implies that the *primitive idempotents* of the tensor product $A \otimes_{\mathbb{Z}} B$ of two orders A and B are the pure tensors of the primitive idempotents of A and B.

This raises the question whether the same is true for the roots of unity. That is, whether the roots of unity of the tensor product $A \otimes_{\mathbb{Z}} B$ are the pure tensors of the roots of unity of A and B. In general they are not, but, as before, restricting our attention to connected orders turns out to be interesting. For an order A denote its group of roots of unity by $\mu(A)$. We leave the following question to the reader.

VIII Question. *Let A and B be connected orders. Is the natural map $\mu(A) \times \mu(B) \longrightarrow \mu(A \otimes_{\mathbb{Z}} B)$ surjective?*

Finally I would like to express my gratitude to my advisor Hendrik Lenstra Jr. His ideas and guidance have been invaluable in shaping this thesis, and his support and enthusiasm made sure this project stayed a pleasure to work on.

I would also like to thank to Abtien Javan Peykar for the many fruitful discussions, both on the thesis matter itself and on the process of writing.

1 Definitions and examples

Throughout this thesis all rings are commutative and with identity. Subrings contain the identity and homomorphisms respect the identity. A zero divisor in a ring R is an element $r \in R$ for which multiplication by r is not injective. We adopt the convention that zero is a natural number, and that when taking intersections or products of ideals in a given ring R, the intersection and product of an empty collection of ideals is R. Also, all tensor products will be over $\mathbb{Z}$, so we omit this from the notation.

1.1 Definition. An *order* is a commutative ring $(A, +, \cdot)$ for which there exists a natural number n such that $(A, +) \cong \mathbb{Z}^n$. The number n is called the *rank* of A and is denoted by $\operatorname{rk} A$.

This uniquely determines the rank because $\mathbb{Z}^m \cong \mathbb{Z}^n$ only if $m = n$.

1.2 Examples. If $f \in \mathbb{Z}[X]$ is monic then $\mathbb{Z}[X]/(f)$ is an order of rank $\deg f$. If K is a number field then its ring of integers $\mathcal{O}_K$ is an order of rank $[K : \mathbb{Q}]$. If G is a finite group then the group ring $\mathbb{Z}[G]$ is an order of rank $\#G$. Subrings and finite products of orders are again orders, and hence so are fibred products of orders, as are tensor products of orders over $\mathbb{Z}$.

A note must be made on terminology. By a *ring of integers* we will always mean the integral closure of $\mathbb{Z}$, or equivalently the maximal order, in a number field. This excludes for example such rings as $\mathbb{Z}[\sqrt{-3}]$.

Let R be a commutative ring and E a commutative $\mathbb{Q}$-algebra that is finite-dimensional as a $\mathbb{Q}$-vector space.

1.3 Definition. A *root of unity* of R is an element of $R^\times$ of finite multiplicative order. The group of all roots of unity of R is denoted by $\mu(R)$.

1.4 Definition. If G is a group and p is a prime number, define

$$G_p := \{g \in G : \ (\exists k \in \mathbb{N})(g^{p^k} = 1)\}.$$

1.5 Examples. Let $p \neq 2$ be prime. Then $\mu(\mathbb{Z}[\zeta_p]) = \langle -\zeta_p \rangle$ and $\mu(\mathbb{Z}[\zeta_p])_2 = \langle -1 \rangle$. In general, if G is a finite abelian group then G_p is its Sylow-p subgroup.

1.6 Definition. An *idempotent* of R is an element $e \in R$ satisfying $e^2 = e$. An idempotent $e \in R$ is *primitive* if $e \neq 0$ and $ee' \in \{0, e\}$ for all idempotents $e' \in R$. A ring is *connected* if it has precisely two idempotents.

1.7 Examples. The only idempotents of $\mathbb{Z}$ are 0 and 1, so $\mathbb{Z}$ is connected. More generally domains are connected as $e(e-1) = 0$ implies $e = 0$ or $e = 1$.

Also $\mathbb{Z}[X]/(X^2-1)$ is connected, whereas $\mathbb{Z}[X]/(X^2-X)$ has the additional idempotents X and $1-X$. A product of two nonzero rings is never connected; pairs of idempotents are idempotents of the product.

1.8 Definition. An element $x \in R$ is *nilpotent* if there exists $n \in \mathbb{N}$ with $x^n = 0$, and similarly an ideal $I \subset R$ is *nilpotent* if there exists $n \in \mathbb{N}$ with $I^n = 0$. The ideal $\mathcal{N}(R)$ of nilpotent elements of R is the *nilradical* of R, and R is *reduced* if $\mathcal{N}(R) = 0$. The quotient $R/\mathcal{N}(R)$ is denoted by R_{red}.

1.9 Examples. In the quotient $\mathbb{Z}[X]/(f)$, where f is monic, the nilpotent elements are the common multiples of the irreducible factors of f. For any ring R its quotient R_{red} is reduced.

For a polynomial $f = \sum_{k=0}^{m} a_k X^k \in R[X]$ we denote its formal derivative by $f' = \sum_{k=1}^{m} k a_k X^{k-1}$.

1.10 Definition. A polynomial $f \in R[X]$ is *separable* over R if

$$fR[X] + f'R[X] = R[X].$$

An element $x \in E$ is called *separable* if it is a zero of some $f \in \mathbb{Q}[X]$ separable over $\mathbb{Q}$. The set E_{sep} of all separable elements of E is the *separable closure of* $\mathbb{Q}$ in E, and E is *separable* if $E = E_{\mathrm{sep}}$.

In section 3 we will see that E_{sep} is in fact a subring of E.

1.11 Examples. For any $n \in \mathbb{N}$ the polynomial $X^n - 1$ is separable over R if and only if $n \in R^\times$, and $X^2 - X$ is separable over any ring. Hence in any finite-dimensional $\mathbb{Q}$-algebra roots of unity and idempotents are separable, and 0 is the only nilpotent separable element as X^n is separable only if $n = 1$.

2 Preliminaries

We establish some general facts on the structure of the set of prime ideals of orders, assuming basic commutative algebra (see [1]). The main result of this section is theorem VI, which we prove at the end of this section. We first recall two well-known facts that we will often need, both in this section and in later ones. Let φ denote Euler's totient function.

2.1 Proposition. *For every positive integer k we have $\varphi(k) \geq \left(\frac{k}{2}\right)^{\frac{\ln 2}{\ln 3}}$.*

Proof. For every odd prime p we have $p - 1 \geq p^{\frac{\ln 2}{\ln 3}}$ because the left hand side grows faster than the right hand side and equality holds for $p = 3$. Hence for every $m > 0$ we have

$$\varphi(p^m) = p^{m-1}(p-1) \geq p^{m-1+\frac{\ln 2}{\ln 3}} \geq (p^m)^{\frac{\ln 2}{\ln 3}}.$$

As both $\varphi(k)$ and $k^{\frac{\ln 2}{\ln 3}}$ are multiplicative functions, it follows that for all odd $k > 0$ we have $\varphi(k) \geq k^{\frac{\ln 2}{\ln 3}}$. For $p = 2$, for all $m > 0$ we have

$$\varphi(2^m) = 2^{m-1} \geq \left(\frac{2^m}{2}\right)^{\frac{\ln 2}{\ln 3}}.$$

Multiplicativity of φ now implies that $\varphi(k) \geq \left(\frac{k}{2}\right)^{\frac{\ln 2}{\ln 3}}$ for every $k > 0$. □

2.2 Lemma. *The group of roots of unity of a number field is finite cyclic of even order.*

Proof. Let K be a number field of degree n. For every $k \in \mathbb{N}$ the primitive k-th roots of unity of K are precisely the roots of the k-th cyclotomic polynomial Φ_k in K. Of course Φ_k has at most $\deg \Phi_k = \varphi(k)$ roots in K, and Φ_k has no roots if $k > 2n^{\frac{\ln 3}{\ln 2}}$ as then $\deg \Phi_k = \varphi(k) > n$ by proposition 2.1. This shows that the group of roots of unity of a number field is finite, and that for every divisor d of its order it has at most $\varphi(d)$ elements of order d, hence it is cyclic. Its order is even because -1 has order 2. □

Throughout this section let A be an order of rank n and let $E := A \otimes \mathbb{Q}$.

2.3 Proposition. *The order A is integral over $\mathbb{Z}$ and E is Artinian.*

Proof. As $A \cong \mathbb{Z}^n$ is finitely generated as a $\mathbb{Z}$-module, so is $\mathbb{Z}[a]$ for every $a \in A$. Hence A is integral over $\mathbb{Z}$, see also [1, proposition 5.1, p. 59]. Also E is finitely generated as a $\mathbb{Q}$-module, so it is a finite-dimensional $\mathbb{Q}$-vector space and its ideals are subspaces. In a descending chain of subspaces the dimension is descending, so every such chain in E stabilizes. □

2.4 Lemma. (Going-up) *Let B be a subring of A and $\mathfrak{q} \subset B$ prime. Then there exists a prime $\mathfrak{p} \subset A$ such that $\mathfrak{q} = \mathfrak{p} \cap B$.*

Proof. Because $B \subset A$ is integral, see [1, theorem 5.10, p. 62]. □

2.5 Proposition. *Let R be a ring and $P \subset R$ a minimal prime. Then every $p \in P$ is a zero divisor.*

Proof. The unique prime of R_P is PR_P, so $\frac{p}{1} \in R_P$ is nilpotent for every $p \in P$. This implies there exist $r \in R - P$ and $m \in \mathbb{N}$ such that $rp^m = 0$. □

2.6 Proposition. *A prime $\mathfrak{p} \subset A$ is minimal (maximal) if and only if $\mathfrak{p} \cap \mathbb{Z}$ is.*

Proof. Because A is integral over $\mathbb{Z}$ we have $\dim A \leq \dim \mathbb{Z} = 1$, hence every prime is minimal or maximal. If $\mathfrak{p} \subset A$ is minimal then it consists of zero divisors, so $\mathfrak{p} \cap \mathbb{Z} = 0$ because A is torsion free. If $\mathfrak{p} \subset A$ is maximal then $A/\mathfrak{p}$ is a field that is finitely generated as a $\mathbb{Z}$-module. In particular it does not contain $\mathbb{Q}$, hence its characteristic is positive and so $\mathfrak{p} \cap \mathbb{Z} \neq 0$. □

2.7 Corollary. *Let B be a subring of A and $\mathfrak{p} \subset A$ prime. Then $\mathfrak{p} \cap B$ is minimal (maximal) if and only if $\mathfrak{p}$ is.*

2.8 Corollary. *A prime $\mathfrak{p} \subset A$ is minimal if and only if $A/\mathfrak{p}$ is an order.*

2.9 Proposition. *The nilradical $\mathcal{N}(E)$ of E is nilpotent, and E has only finitely many prime ideals, all of which are maximal.*

Proof. Because E is Artinian, see [1, propositions 8.1, 8.3 and 8.4, p. 89]. □

2.10 Corollary. *For every prime $\mathfrak{p} \subset E$ the quotient $E/\mathfrak{p}$ is a number field.*

2.11 Corollary. *There exists $m \in \mathbb{N}$ such that the canonical map $E \longrightarrow \prod_{\mathfrak{p}} E/\mathfrak{p}^m$, where $\mathfrak{p}$ ranges over the prime ideals of E, is an isomorphism.*

2.12 Proposition. 1. *If A is reduced then E is reduced.*
2. *The canonical map $A \longrightarrow E$ is injective.*
3. *The mapping $\mathfrak{p} \longmapsto \mathfrak{p} \cap A$ is a bijection between the set of primes of E and the set of minimal primes of A.*

Proof. 1, 2: Because A is torsion-free and $E \cong S^{-1}A$, where $S = \mathbb{Z} - \{0\}$.
3: Primes of E map to primes of A not meeting $\mathbb{Z} - \{0\}$; by proposition 2.6 these are minimal. Conversely, if $\mathfrak{q}$ is a minimal prime of A then $\mathfrak{q}E$ is a prime of E and $\mathfrak{q}E \cap A = \mathfrak{q}$. □

Because of the second statement we will often consider A a subring of E without further mention.

Proof of theorem VI. Rings of integers are reduced orders, and subrings and finite products of reduced orders are again reduced orders. This proves one direction.

For the other, suppose A is a reduced order and let $E := A \otimes \mathbb{Q}$. The image of A in the number field $E/\mathfrak{p}$ is contained in its ring of integers $\mathcal{O}_{E/\mathfrak{p}}$, because A is integral over $\mathbb{Z}$ by proposition 2.3. Because A is reduced, so

is E by proposition 2.12, so by proposition 2.9 and the Chinese remainder theorem we have $E \cong \prod_{\mathfrak{p}} E/\mathfrak{p}$, where $\mathfrak{p}$ ranges over the finitely many primes of E. This yields the second equality in

$$\operatorname{rk} A = \dim_{\mathbb{Q}} E = \dim_{\mathbb{Q}} \prod_{\mathfrak{p}} E/\mathfrak{p} = \operatorname{rk} \prod_{\mathfrak{p}} \mathcal{O}_{E/\mathfrak{p}},$$

which shows that the image of A in $\prod_{\mathfrak{p}} \mathcal{O}_{E/\mathfrak{p}}$ is of finite index. □

3 Subrings generated by roots of unity

The main result of this section is theorem V, which tells us it suffices to prove theorems I through IV for reduced orders. Before its proof we establish a few results on subrings of orders generated by roots of unity; some such subrings allow useful descriptions as *fibred products*. We also give a few examples of connected orders of low rank with relatively many roots of unity, which we will see again in section 4.

This section builds on a classical result, known as the Jordan-Chevalley decomposition. We need it only for finite-dimensional $\mathbb{Q}$-algebras.

3.1 Theorem. (Jordan-Chevalley) *Let E be a finite-dimensional $\mathbb{Q}$-algebra. The subset $E_{\mathrm{sep}} \subset E$ is a subring of E, and the natural map $E_{\mathrm{sep}} \longrightarrow E_{\mathrm{red}}$ is a ring isomorphism and induces an isomorphism $E \cong \mathcal{N}(E) \oplus E_{\mathrm{sep}}$ of $\mathbb{Q}$-vector spaces.*

Proof. Omitted, see [2, theorem 1.1, p. 1]. □

We note two consequences. For the remainder of this section let A be a nonzero order and $E := A \otimes \mathbb{Q}$, so E is a finite-dimensional $\mathbb{Q}$-algebra. First of all we see that $E_{\mathrm{sep}} \cong E_{\mathrm{red}}$, so for every prime $\mathfrak{p} \subset E$ and every positive integer m we have $(E/\mathfrak{p}^m)_{\mathrm{sep}} \cong E/\mathfrak{p}$.

3.2 Corollary. *For every prime $\mathfrak{p} \subset E$ and every $m > 0$ there is a unique ring homomorphism $E/\mathfrak{p} \longrightarrow E/\mathfrak{p}^m$ that is a section of the quotient map.*

Second, as noted in example 1.11 we have $\mu(A) \subset E_{\mathrm{sep}}$. For a ring R and a subset $S \subset R$ let $\mathbb{Z}[S]$ denote the subring of R generated by S.

3.3 Corollary. *The subring $\mathbb{Z}[\mu(A)]$ of A is reduced.*

This will be a key ingredient in the proof of theorem V.

3.4 Proposition. *Let p be a prime number. There is precisely one prime $\mathfrak{p} \subset \mathbb{Z}[\mu(A)_p]$ lying over p, and its residue field is $\mathbb{F}_p$.*

Proof. Let $\mathfrak{p} \subset \mathbb{Z}[\mu(A)_p]$ be a prime lying over p and let $\zeta \in \mu(A)_p$ and $k \in \mathbb{N}$ be such that $\zeta^{p^k} = 1$. Then $\zeta \equiv 1 \pmod{\mathfrak{p}}$ as $\zeta^{p^k} - 1^{p^k} \equiv (\zeta - 1)^{p^k} \pmod{p}$, so $\mathfrak{p}$ is the kernel of the unique ring homomorphism $\mathbb{Z}[\mu(A)_p] \longrightarrow \mathbb{F}_p$. □

3.5 Proposition. *Let p be prime. Then $\mathbb{Z}[\mu(A)_p]$ is reduced and connected.*

Proof. If $\mathfrak{q} \subset \mathbb{Z}[\mu(A)_p]$ is minimal $\mathbb{Z}[\mu(A)_p]/\mathfrak{q}$ is an order so $\mathfrak{q}+(p) \neq \mathbb{Z}[\mu(A)_p]$, so $\mathfrak{q}$ is contained in the unique prime lying over p. Hence if $e \in \mathbb{Z}[\mu(A)_p]$ is idempotent then either $e \in \mathfrak{q}$ for every minimal prime $\mathfrak{q}$, or $1 - e \in \mathfrak{q}$ for every minimal prime $\mathfrak{q}$, and so either e or $1 - e$ is nilpotent. Then either $e = 0$ or $e = 1$ and hence $\mathbb{Z}[\mu(A)_p]$ is connected. □

3.6 Example. The order $C := \mathbb{Z}[\zeta_3] \times \mathbb{Z}[\zeta_3]$ contains the connected subring $D := \mathbb{Z}[\mu(C)_3]$. Because $\#\mu(C) = 6 \times 6 = 2^2 \times 3^2$ we have $2 \times 3^2 \mid \#\mu(D)$. As $C = \mathbb{Z}[\mu(C)]$ and C is not connected, we see that $\#\mu(D) = 2 \times 3^2 = 18$.

The order D features prominently in the proof of theorem III. It can be described alternatively as a *fibred product* of two orders.

3.7 Definition. Let R, S and T be rings and $f : R \longrightarrow T$, $g : S \longrightarrow T$ ring homomorphisms. The *fibred product* of R and S with respect to f and g is

$$R \times_T S := \{(r, s) \in R \times S : f(r) = g(s)\}.$$

This is a subring of $R \times S$. The maps f and g are absent from the notation; they will always be clear from the context. Note that the fibred product of two connected rings over a nonzero ring is again connected. Also, the fibred product of two rings over a finite ring of m elements is of index dividing m in the Cartesian product.

3.8 Proposition. *Let B be a nonzero order and p prime. If the p-th cyclotomic polynomial Φ_p has a zero in A then*

$$\mathbb{Z}[\mu(A \times B)_p] = \mathbb{Z}[\mu(A)_p] \times_{\mathbb{F}_p} \mathbb{Z}[\mu(B)_p].$$

Proof. Because $\mu(A \times B)_p = \mu(A)_p \times \mu(B)_p$ and because the unique ring homomorphisms from $\mathbb{Z}[\mu(A)_p]$ and $\mathbb{Z}[\mu(B)_p]$ to $\mathbb{F}_p$ map $\mu(A)_p$ and $\mu(B)_p$ respectively to 1, we see that $\mathbb{Z}[\mu(A \times B)_p] \subset \mathbb{Z}[\mu(A)_p] \times_{\mathbb{F}_p} \mathbb{Z}[\mu(B)_p]$.

For the converse note that for every $(\alpha, \beta) \in \mathbb{Z}[\mu(A)_p] \times_{\mathbb{F}_p} \mathbb{Z}[\mu(B)_p]$ there exist $a, b \in \mathbb{Z}$ with $a \equiv b \pmod{p}$ such that $(\alpha, a), (b, \beta) \in \mathbb{Z}[\mu(A \times B)_p]$, so

$$(\alpha, \beta) + (0, a - b) = (\alpha, a) + (b, \beta) - (b, b) \in \mathbb{Z}[\mu(A \times B)_p],$$

where $a-b$ is a multiple of p. So it suffices to show that $(0, p) \in \mathbb{Z}[\mu(A \times B)_p]$. Let $\zeta \in A$ be a zero of Φ_p. Then $\zeta^p = 1$ so $\zeta \in \mu(A)_p$ and $(0, p) = \Phi_p((\zeta, 1)) \in \mathbb{Z}[\mu(A \times B)_p]$. □

3.9 Example. With C and D as in example 3.6 we find that $D = \mathbb{Z}[\zeta_3] \times_{\mathbb{F}_3} \mathbb{Z}[\zeta_3]$ because Φ_3 has a zero in $\mathbb{Z}[\zeta_3]$. This shows D is a subring of C of index 3. In particular it is the only connected subring of C containing $\mu(C)_3$.

Finally we prove theorem V. The proof is somewhat involved, so we first establish an intermediate result.

3.10 Lemma. *Let K be a number field and d a positive integer. Then there exists a field extension $L \supset K$ with $[L : K] = d$ and $\mu(L) = \mu(K)$.*

Proof. It suffices to prove the lemma for d prime. Let $L \supset K$ be a field extension of prime degree p with $\mu(L) \neq \mu(K)$. Let $\zeta \in L$ be a generator of $\mu(L)$ and k its order, so that $L = K[\zeta] \cong K[X]/(f)$ for some f dividing the k-th cyclotomic polynomial. Then the subfield $\mathbb{Q}(\zeta) \subset L$ is of degree $\varphi(k)$, so $\varphi(k)$ divides $[L : \mathbb{Q}] = p[K : \mathbb{Q}]$, which happens for only finitely many values of k by proposition 2.1. Of course Φ_k has only finitely many divisors for any given k, so up to isomorphism there are only finitely many extensions $L \supset K$ with $[L : K] = p$ and $\mu(L) \neq \mu(K)$. As there are infinitely many extensions of K of degree p that are pairwise nonisomorphic as fields, this implies there exists an extension $L \supset K$ of degree p with $\mu(L) = \mu(K)$. □

To prove theorem V, for a given order A we construct a reduced order A' of the same rank with $\mu(A') = \mu(A)$, and we show that if A is connected then so is this reduced order A'.

Proof of theorem V. Let A be an order, let $E := A \otimes \mathbb{Q}$, let $m \in \mathbb{N}$ be such that $\mathcal{N}(E)^m = 0$ and let $F := \mathbb{Z}[\mu(A)] \otimes \mathbb{Q}$, which is reduced by corollary 3.3 and proposition 2.12. For every prime $\mathfrak{q} \subset F$ and every prime $\mathfrak{p} \subset E$ lying over $\mathfrak{q}$ the residue field $E/\mathfrak{p}$ is an $F/\mathfrak{q}$-module, hence so is $E/\mathfrak{p}^m$ by corollary 3.2. For every prime $\mathfrak{q} \subset F$ there is a prime $\mathfrak{p} \subset E$ lying over $\mathfrak{q}$ by lemma 2.4, so the sum

$$n_\mathfrak{q} := \sum_{\mathfrak{p}|\mathfrak{q}} \dim_{F/\mathfrak{q}} E/\mathfrak{p}^m$$

is positive for every $\mathfrak{q} \subset F$. Let $L_\mathfrak{q} \supset F/\mathfrak{q}$ be a field extension of degree $n_\mathfrak{q}$ with $\mu(L_\mathfrak{q}) = \mu(F/\mathfrak{q})$, which exists by lemma 3.10, and let $\mathcal{O} := \prod_\mathfrak{q} \mathcal{O}_{L_\mathfrak{q}}$. Then $F \cap \mathcal{O} = \prod_\mathfrak{q} \mathcal{O}_{F/\mathfrak{q}}$ and $\mathbb{Z}[\mu(A)]$ is a subring of finite index, say d, in this intersection because F is reduced and therefore

$$(F \cap \mathcal{O}) \otimes \mathbb{Q} \cong (F \otimes \mathbb{Q}) \cap (\mathcal{O} \otimes \mathbb{Q}) \cong F = \mathbb{Z}[\mu(A)] \otimes \mathbb{Q}.$$

The subring $A' := \mathbb{Z}[\mu(A)] + d\mathcal{O}$ of $\mathcal{O}$ is of finite index as it contains $d\mathcal{O}$. By choice of the $n_\mathfrak{q}$ we have $\operatorname{rk} A' = \operatorname{rk} A$, and it is clear that $\mu(A) \subset \mu(A')$.

Also $A' \cap F \subset \mathbb{Z}[\mu(A)]$ because if $y := a + dx \in F$ for some $a \in \mathbb{Z}[\mu(A)]$ and $x \in \mathcal{O}$, then $x = \frac{y-a}{d} \in F \cap \mathcal{O}$, so $dx \in \mathbb{Z}[\mu(A)]$ and hence also $y \in \mathbb{Z}[\mu(A)]$. By construction of the $L_{\mathfrak{q}}$ we have equality in

$$\mu(A') \subset \mu(\mathcal{O}) = \mu(F),$$

which shows that $\mu(A') \subset F \cap A' = A$, so indeed $\mu(A') = \mu(A)$.

To see that A' is connected if A is, note that if $e \in A'$ is idempotent then $e \in F \cap \mathcal{O} \subset F$. Because $A' \cap F \subset \mathbb{Z}[\mu(A)] \subset A$ this shows that $e \in A$. □

4 Bounds on the number of roots of unity

In this section we prove theorems I and III, establishing sharp bounds on the number of roots in unity of an order in general, and in a connected order in particular, given its rank. Theorem I is at this point a direct application of the results of the previous sections. We first use lemma 3.10 to give a characterization of the groups that occur as the group of roots of unity of an order of a given rank.

4.1 Proposition. *Let n be a positive integer and G a group. Then G is isomorphic to the group of roots of unity of a ring of integers of rank n if and only if G is finite cyclic of even order and $\varphi(\#G) \mid n$.*

Proof. Let A be a ring of integers of rank n. Then it is contained in the number field $E := A \otimes \mathbb{Q}$ of degree n, so its group of roots of unity is finite cyclic of even order by lemma 2.2. Let $\zeta \in \mu(A)$ be a generator and $k = \#\mu(A)$ its order, so that its minimal polynomial over $\mathbb{Q}$ is the k-th cyclotomic polynomial Φ_k. Then the subfield $\mathbb{Q}(\zeta) \subset E$ is of degree $\deg \Phi_k = \varphi(k)$, so $\varphi(k)$ divides $[E : \mathbb{Q}] = n$.

Conversely, if G is finite cyclic of even order, say k, then $G \cong \mu(\mathbb{Z}[\zeta_k])$, where $\mathbb{Z}[\zeta_k]$ is the ring of integers of $\mathbb{Q}(\zeta_k)$. If $n = d\varphi(k)$ then by lemma 3.10 there exists a field extension $L \supset \mathbb{Q}(\zeta_k)$ with $[L : \mathbb{Q}(\zeta_k)] = d$ and $\mu(L) = \mu(\mathbb{Q}(\zeta_k))$, so $\mathcal{O}_L$ is a ring of integers of rank n with $\mu(\mathcal{O}_L) \cong G$. □

For the remainder of this section let A be an order of rank n, let $k := \#\mu(A)$ and let $E := A \otimes \mathbb{Q}$.

4.2 Proposition. *If $n = 2$ and $k > 2^n$ then $A \cong \mathbb{Z}[\zeta_3]$.*

Proof. First suppose that A is not reduced. Then $\operatorname{rk} \mathbb{Z}[\mu(A)] < 2$ as $\mathbb{Z}[\mu(A)]$ is reduced, and hence embeds into $A_{\mathrm{red}} := A/\mathcal{N}(A)$. So $\mathbb{Z}[\mu(A)] \cong \mathbb{Z}$, but $\mathbb{Z}[\mu(A)]$ contains $k > 4$ roots of unity, a contradiction. Hence A is reduced.

Then it follows from theorem VI that A is of finite index in a ring of integers as otherwise it is isomorphic to a subring of $\mathbb{Z} \times \mathbb{Z}$ with $k > 4$ roots of unity, which is impossible. From proposition 4.1 it follows that $\varphi(k)$ divides $\operatorname{rk} A = 2$, so $k = 6$ as $k > 4$. Then $E \cong \mathbb{Q}(\zeta_3)$ and A is isomorphic to a subring of $\mathbb{Z}[\zeta_3]$ containing ζ_3. □

Proof of theorem I. We proceed by induction on the rank to show that for every order A we have $\#\mu(A) \leq m(\operatorname{rk} A)$, where

$$m(n) := \begin{cases} 6^{\frac{n}{2}} & \text{if } n \text{ is even} \\ 2 \cdot 6^{\frac{n-1}{2}} & \text{if } n \text{ is odd} \end{cases}.$$

The base case $n = 0$ is clear, so let A be an order of rank $n > 0$.

If A is a domain and $k := \#\mu(A)$ then $\varphi(k) \mid n$ and so $k \leq 2n^{\frac{\ln 3}{\ln 2}}$ by proposition 2.1, and we are done because $2n^{\frac{\ln 3}{\ln 2}} \leq m(n)$. If A is not a domain then without loss of generality, by theorem V we may assume that A is reduced, and so it follows from theorem VI that A is of finite index in a product $B \times C$ of nonzero orders. By induction hypothesis

$$\#\mu(B)\#\mu(C) \leq m(\operatorname{rk} B)m(\operatorname{rk} C) \leq m(\operatorname{rk} B + \operatorname{rk} C),$$

and so $\#\mu(A) \leq m(\operatorname{rk} A)$. This concludes the induction step.

Equality holds for $\mathbb{Z}[\zeta_3]^{\frac{n}{2}}$ if n is even, and for $\mathbb{Z} \times \mathbb{Z}[\zeta_3]^{\frac{n-1}{2}}$ if n is odd, so $m(n)$ is a sharp upper bound for every $n \in \mathbb{N}$. □

Somewhat surprisingly, these are the only orders, up to isomorphism, that attain the upper bound.

4.3 Proposition. *Let A be an order. Then $\#\mu(A) = m(\operatorname{rk} A)$ if and only if there exist $a, b \in \mathbb{N}$ with $a \leq 1$ such that $A \cong \mathbb{Z}^a \times \mathbb{Z}[\zeta_3]^b$.*

Proof. One direction is easily verified, so suppose that $\#\mu(A) = m(\operatorname{rk} A)$, and let $n := \operatorname{rk} A$. Then A must be reduced as otherwise

$$\#\mu(A) = \#\mu(\mathbb{Z}[\mu(A)]) \leq m(\operatorname{rk} \mathbb{Z}[\mu(A)]) \leq m(\operatorname{rk} A_{\text{red}}) < m(\operatorname{rk} A).$$

So A is of finite index in a finite product of rings of integers by theorem VI. We proceed by induction on the number of rings in the product.

If A is of finite index in a single ring of integers then it is a domain, so $\#\mu(A) \leq 2n^{\frac{\ln 3}{\ln 2}}$ by propositions 4.1 and 2.1, where $2n^{\frac{\ln 3}{\ln 2}} \leq m(n)$ with equality iff $n \in \{1, 2\}$. The base case now follows from proposition 4.2.

If A is of finite index in a product of multiple rings of integers, then it is of finite index in a product $B \times C$ of nonzero orders, and we have

$$\#\mu(A) \leq \#\mu(B)\#\mu(C) \leq m(\operatorname{rk} B)m(\operatorname{rk} C) \leq m(\operatorname{rk} A).$$

If the second inequality is an equality then by induction hypothesis we have $B \cong \mathbb{Z}^{a_1} \times \mathbb{Z}[\zeta_3]^{b_1}$ and $C \cong \mathbb{Z}^{a_2} \times \mathbb{Z}[\zeta_3]^{b_2}$ with $a_1, a_2 \leq 1$. If also the third inequality is an equality then $\operatorname{rk} B$ and $\operatorname{rk} C$ are not both odd and hence $a_1 + a_2 \leq 1$, so A is isomorphic to a subring of $\mathbb{Z}^a \times \mathbb{Z}[\zeta_3]^b$ with $a \leq 1$. Finally, if also the first inequality is an equality then $\mu(A) = \mu(B \times C)$ and hence A is isomorphic to a subring of $\mathbb{Z}^a \times \mathbb{Z}[\zeta_3]^b$ containing all its roots of unity. As $1, -1, \zeta_3 \in \mu(\mathbb{Z}[\zeta_3])$ and $1, -1 \in \mu(\mathbb{Z})$, the identities

$$(\zeta_3 + 1)^6 = 1 \qquad \text{and} \qquad (1 + (-1))^6 = 0,$$

imply that it contains all idempotents of $\mathbb{Z}^a \times \mathbb{Z}[\zeta_3]^b$, so $A \cong \mathbb{Z}^a \times \mathbb{Z}[\zeta_3]^b$. □

The proof of theorem III requires some more preparation, mostly to deal with the exceptional bounds for orders of ranks 2 and 4. For the remainder of this section assume that A is connected. Recall from example 3.6 the connected order $D := \mathbb{Z}[\mu(\mathbb{Z}[\zeta_3] \times \mathbb{Z}[\zeta_3])_3]$.

4.4 Proposition. *If $n = 4$ and $k > 2^n$ then $A \cong D$.*

Proof. If A is not reduced then $\mathbb{Z}[\mu(A)]$ is reduced and of rank less than 4, and then $k \leq 12$ by theorem I, a contradiction. So A is reduced, hence of finite index in a product of rings of integers $\mathcal{O}$. At least one of these rings of integers B must have $\#\mu(B) > 2^{\operatorname{rk} B}$, and from proposition 4.1 it then follows that $\operatorname{rk} B = 2$. By proposition 4.2 this implies $B \cong \mathbb{Z}[\zeta_3]$, so $\mathcal{O} \cong \mathbb{Z}[\zeta_3] \times C$ for some order C of rank 2. Note that $(\zeta_3, -1) \notin A$ as $\Phi_3((\zeta_3, -1)) = (0, 1) \notin A$, so $\#\mu(\mathcal{O}) \geq 2\#\mu(A) > 32$. Then $\#\mu(C) > 4$ so also $C \cong \mathbb{Z}[\zeta_3]$, and A is a connected subring of $\mathcal{O} = \mathbb{Z}[\zeta_3] \times \mathbb{Z}[\zeta_3]$ with $\#\mu(A) = 18$. This means A contains $\mu(\mathcal{O})_3$, and as we saw in example 3.6 this implies $A \cong D$. □

Proof of theorem III. We proceed by induction on the rank to show that for every connected order A we have $\#\mu(A) \leq m_c(\operatorname{rk} A)$, where

$$m_c(n) := \begin{cases} 2^n + 2 & \text{if } n \in \{2, 4\} \\ 2^n & \text{otherwise} \end{cases}.$$

The base case $n = 1$ is clear, so let A be a connected order of rank $n > 1$.

If A is a domain and $k := \#\mu(A)$ then $\varphi(k) \mid n$ and so $k \leq 2n^{\frac{\ln 3}{\ln 2}}$ by proposition 2.1. We have $2n^{\frac{\ln 3}{\ln 2}} > m_c(n)$ only if $n = 3$, in which case $k = 2$ because $\varphi(k) \mid n$ by proposition 4.1, so we are done. If A is not a domain then without loss of generality, by theorem V we may assume A is reduced, and so it follows from theorem VI that A is of finite index in a product $B \times C$ of nonzero orders. If $\#\mu(B) \leq 2^{\operatorname{rk} B}$ and $\#\mu(C) \leq 2^{\operatorname{rk} C}$ then

$$\#\mu(A) \leq \#\mu(B)\#\mu(C) \leq 2^{\operatorname{rk} B + \operatorname{rk} C} = 2^{\operatorname{rk} A} \leq m_c(\operatorname{rk} A),$$

and we are done. If not then without loss of generality $\#\mu(B) > 2^{\operatorname{rk} B}$, so by induction hypothesis $\operatorname{rk} B \in \{2, 4\}$ and $\#\mu(B) = 2^{\operatorname{rk} B} + 2$. Then by propositions 4.2 and 4.4 either $B \cong \mathbb{Z}[\zeta_3]$ or $B \cong D$, either way B contains a zero of Φ_3, say ζ. If $(\zeta, -1) \in A$ then also $\Phi_3((\zeta, -1)) = (0, 1) \in A$, contradicting the fact that A is connected, so we find that

$$\#\mu(A) \leq \frac{1}{2}\#\mu(B)\#\mu(C) \leq \frac{1}{2}(2^{\operatorname{rk} B} + 2)m_c(\operatorname{rk} C) \leq m_c(\operatorname{rk} B + \operatorname{rk} C),$$

where the last inequality is a matter of checking a few cases. Of course $\operatorname{rk} B + \operatorname{rk} C = \operatorname{rk} A$, so this shows that $\#\mu(A) \leq m_c(\operatorname{rk} A)$.

For $n \notin \{2, 4\}$ the upper bound is attained by $\mathbb{Z}[\mu(\mathbb{Z}^n)_2]$, which is connected by proposition 3.5. For $n = 2$ and $n = 4$ it is attained by $\mathbb{Z}[\zeta_3]$ and D, respectively, so $m_c(n)$ is a sharp upper bound for every $n > 0$. □

Propositions 4.2 and 4.4 tell us that $\mathbb{Z}[\zeta_3]$ and D are the unique connected orders, up to isomorphism, for which the upper bound is attained when $n = 2$ and $n = 4$, respectively. For every other $n > 0$ there are, up to isomorphism, precisely $\lfloor \frac{n}{2} \rfloor + 1$ connected orders of the rank n that attain the upper bound.

4.5 Proposition. *Let A be a connected order. Then $\#\mu(A) = 2^{\operatorname{rk} A}$ if and only if there exist $a, b \in \mathbb{N}$ such that $A \cong \mathbb{Z}[\mu(\mathbb{Z}^a \times \mathbb{Z}[i]^b)_2]$.*

Proof. As $\mathbb{Z}[\mu(A)]$ contains $2^{\operatorname{rk} A}$ roots of unity it follows from theorem III that $\operatorname{rk} \mathbb{Z}[\mu(A)] = \operatorname{rk} A$ and so $\mathbb{Z}[\mu(A)] \otimes \mathbb{Q} = E$. Then A is reduced because $\mathbb{Z}[\mu(A)]$ is, so E is a finite product of number fields. Let K be one of these number fields. As $\mu(A) = \mu(A)_2$ and $E = \mathbb{Q}(\mu(A))$ we have $K = \mathbb{Q}(\mu(K)_2)$, and because $\mu(K)_2$ is finite cyclic by lemma 2.2 this implies $K \cong \mathbb{Q}(\zeta_{2^k})$ for some $k > 0$. Then $\#\mu(K) \leq 2^{\operatorname{rk} K}$, so from $\#\mu(A) = 2^{\operatorname{rk} A}$ it follows that also $\#\mu(K) = 2^{\operatorname{rk} K}$, which implies $k \leq 2$. This shows A is isomorphic to a subring of finite index of $B := \mathbb{Z}^a \times \mathbb{Z}[i]^b$ for some $a, b \in \mathbb{N}$, that moreover contains $\mu(B)_2$. It remains to show that $\mathbb{Z}[\mu(B)_2]$ is the unique connected subring of B containing $\mu(B)_2$.

Let C be a connected subring of B containing $\mu(B)_2$. As $\Phi_2 = X + 1$ has a root in every order, repeated application of proposition 3.8 shows that

$$\mathbb{Z}[\mu(B)_2] = \underbrace{\mathbb{Z} \times_{\mathbb{F}_2} \cdots \times_{\mathbb{F}_2} \mathbb{Z}}_{a \text{ times}} \times_{\mathbb{F}_2} \underbrace{\mathbb{Z}[i] \times_{\mathbb{F}_2} \cdots \times_{\mathbb{F}_2} \mathbb{Z}[i]}_{b \text{ times}}.$$

It follows that for every $x \in C$ there exists an idempotent $e \in B$ such that $x + e \in \mathbb{Z}[\mu(B)] \subset C$. Then also $e \in C$ and so $e \in \{0, 1\}$ because C is connected. Hence $x \in \mathbb{Z}[\mu(B)_2]$, which shows that $C = \mathbb{Z}[\mu(B)_2]$. □

5 Bounds on the exponent

In this section we establish bounds on the exponent of the group of roots of unity of an order in terms of its rank. In particular we prove theorems II and IV. We do so by first determining sharp lower bounds for the rank of an order given the exponent of its group of roots of unity, and then the same for connected orders.

5.1 Lemma. *If m and n are positive integers that do not divide each other, i.e. $m \nmid n$ and $n \nmid m$, then $\Phi_m\mathbb{Z}[X] + \Phi_n\mathbb{Z}[X] = \mathbb{Z}[X]$.*

Proof. Let $d := \gcd(m, n)$ and let a and b be positive integers such that $an - bm = d$. Then $\Phi_m(x)$ divides $\frac{x^{bm}-1}{x^d-1}$ and $\Phi_n(x)$ divides $\frac{x^{an}-1}{x^d-1}$, so

$$u(x) := -\frac{x^d}{\Phi_m(x)}\frac{x^{bm}-1}{x^d-1} \qquad \text{and} \qquad v(x) := \frac{1}{\Phi_n(x)}\frac{x^{an}-1}{x^d-1},$$

are polynomials with integer coefficients. Since $bm + d = an$ we find that

$$u(x)\Phi_m(x) + v(x)\Phi_n(x) = -x^d\frac{x^{bm}-1}{x^d-1} + \frac{x^{an}-1}{x^d-1} = 1. \qquad \square$$

As noted before the exponent of the group of roots of unity of a nonzero order is even. Define

$$\mathcal{Q} := \{p^k : \ p \text{ is prime and } k \in \mathbb{N}_{>0} \text{ and } p^k \neq 2\} \cup \{12\},$$

where the latter is simply the natural number 12. For every finite subset $\mathcal{E} \subset \mathcal{Q}$ define $A_\mathcal{E} := \prod_{q\in\mathcal{E}} \mathbb{Z}[\zeta_q]$.

5.2 Proposition. *Let $e > 2$ be even and let A be an order with $\exp\mu(A) = e$ of minimal rank. Then $A \cong A_\mathcal{E}$ for some nonempty finite subset $\mathcal{E} \subset \mathcal{Q}$ with $\gcd(q, q') = 1$ for all $q, q' \in \mathcal{E}$.*

Proof. Let $\zeta \in \mu(A)$ be of order e. Then $\mathbb{Z}[\zeta] \subset A$ is of finite index by minimality of $\operatorname{rk} A$, so A is reduced because $\mathbb{Z}[\zeta]$ is. Let $E := A \otimes \mathbb{Q}$ so that $\mathbb{Q}(\zeta) = E \cong \prod_\mathfrak{p} E/\mathfrak{p}$, where $\mathfrak{p}$ ranges over the primes of E. The $E/\mathfrak{p}$ are number fields, and $\mathbb{Q}(\zeta)$ maps surjectively to each one so they are cyclotomic fields. It follows that $\mathbb{Z}[\zeta]$ maps surjectively to the ring of integers of each one, which implies that $B := \prod_\mathfrak{p} \mathcal{O}_{E/\mathfrak{p}}$ is also an order with $\exp\mu(B) = e$ of minimal rank.

Let $k_1, \ldots, k_m \in \mathbb{N}$ be such that $B \cong \prod_{i=1}^m \mathbb{Z}[\zeta_{k_i}]$, and note that $k_i > 2$ for all i. For each i, if $k_i = qk_i'$ for some $q \in \mathcal{Q}$ and $k_i' > 2$ with $(q, k_i') = 1$, then

$$\begin{aligned} \exp\mu(\mathbb{Z}[\zeta_{k_i}]) &= \exp\mu(\mathbb{Z}[\zeta_q] \times \mathbb{Z}[\zeta_{k_i'}]), \\ \operatorname{rk}\mathbb{Z}[\zeta_{k_i}] &= \varphi(k_i) \geq \varphi(q) + \varphi(k_i') = \operatorname{rk}(\mathbb{Z}[\zeta_q] \times \mathbb{Z}[\zeta_{k_i'}]). \end{aligned}$$

Minimality of $\operatorname{rk} B$ then implies that equality holds, and hence that $k_i = 12$. Of course if $k_i = 2q$ for some $q \in \mathcal{Q}$ with $(q, 2) = 1$ then $\mathbb{Z}[\zeta_{k_i}] = \mathbb{Z}[\zeta_q]$, which shows that in any case $\mathbb{Z}[\zeta_{k_i}] = \mathbb{Z}[\zeta_q]$ for some $q \in \mathcal{Q}$.

Minimality of $\operatorname{rk} B$ now implies that $B \cong A_{\mathcal{E}}$ for a nonempty finite subset $\mathcal{E} \subset \mathcal{P}$ with $\gcd(q, q') = 1$ for all $q, q' \in \mathcal{E}$. Because $\zeta \in \mu(B)$ is of order e its minimal polynomial f is of the form $f = \prod_{q \in \mathcal{E}} \Phi_{c_q q}$ where $c_q \in \{1, 2\}$ and $\gcd(q, c_q) = 1$. Because $\gcd(q, q') = 1$ for all $q, q' \in \mathcal{E}$, by lemma 5.1 the $\Phi_{c_q q}$ are pairwise comaximal and hence by the Chinese remainder theorem

$$\mathbb{Z}[\zeta] \cong \mathbb{Z}[X]/(f) \cong \prod_{q \in \mathcal{E}} \mathbb{Z}[X]/(\Phi_{c_q q}) \cong \prod_{q \in \mathcal{E}} \mathbb{Z}[\zeta_q] \cong B,$$

which implies that also $A \cong B \cong A_{\mathcal{E}}$. □

From this it is easy to determine the lower bound for all even e; define

$$n(e) := \begin{cases} -1 + \sum_{p|e} \varphi(p^{e_p}) & \text{if } e_2 = 1 \text{ and } e > 2 \\ \sum_{p|e} \varphi(p^{e_p}) & \text{otherwise} \end{cases}$$

5.3 Proposition. *Let A be a nonzero order with $e := \exp \mu(A)$. Then $\operatorname{rk} A \geq n(e)$, and this lower bound is sharp.*

Proof. For $e = 2$ this is clear. Given an even number $e = \prod_{p|e} p^{e_p} > 2$ let A be an order with $\exp \mu(A) = e$ of minimal rank. Then by proposition 5.2 we have $A \cong A_{\mathcal{E}}$ for some nonempty finite subset $\mathcal{E} \subset \mathcal{Q}$ with $\gcd(q, q') = 1$ for all $q, q' \in \mathcal{E}$. It follows that

$$e = \exp \mu(A_{\mathcal{E}}) = \operatorname{lcm}(2, \prod_{q \in \mathcal{E}} q),$$

so writing $e = \prod_{p|e} p^{e_p}$ this shows that either $\mathcal{E} = \{p^{e_p} : p \mid e \text{ and } p^{e_p} \neq 2\}$, or $e_2 = 2$ and $e_3 = 1$ and $\mathcal{E} = \{p^{e_p} : p \mid \frac{e}{12}\} \cup \{12\}$. In either case we have

$$\operatorname{rk} A_{\mathcal{E}} = \sum_{q \in \mathcal{E}} \varphi(q) = n(e).$$ □

The minimum of $\operatorname{rk} A$ for connected orders A with a given exponent e does not differ much from the minimum for orders in general. Define

$$n_c(e) := \begin{cases} n(e) & \text{if } e = 12 \text{ or } e \text{ is twice a prime power} \\ 1 + n(e) & \text{otherwise} \end{cases},$$

where 1 is also considered a prime power.

5.4 Proposition. *Let A be a connected order with $e := \exp \mu(A)$. Then $\operatorname{rk} A \geq n_c(e)$, and this lower bound is sharp.*

Proof. For $e = 2$ this is clear, and $n(e)$ is a lower bound for every even e by proposition 5.3. The connected orders $\mathbb{Z}[\zeta_{12}]$ and $\mathbb{Z}[\zeta_{p^k}]$ show that $n_c(e) = n(e)$ if $e = 12$ or e is twice a prime power.

So suppose $e \neq 12$ and e is not twice a prime power. By proposition 5.2 every order A with $\exp \mu(A) = e$ and $\operatorname{rk} A$ minimal is isomorphic to $A_{\mathcal{E}}$ for some subset $\mathcal{E} \subset \mathcal{Q}$ with $\gcd(q, q') = 1$ for all $q, q' \in \mathcal{E}$, so we have

$$e = \exp \mu(A_{\mathcal{E}}) = \operatorname{lcm}(2, \prod_{q \in \mathcal{E}} q).$$

Then $\#\mathcal{E} > 1$ as $e \neq 12$ and e is not twice a prime power, so $A_{\mathcal{E}}$ is not connected and therefore $n_c(e) > n(e)$.

Write $e = \prod_{p|e} p^{e_p}$ and let $\mathcal{E} = \{p^{e_p} : p \mid e \text{ and } p^{e_p} \neq 2\}$. By proposition 3.4 there is a unique ring homomorphism $\mathbb{Z}[\zeta_{p^{e_p}}] \longrightarrow \mathbb{F}_p$ for every prime power p^{e_p}, and it maps $\zeta_{p^{e_p}}$ to 1. Taking the fibred product $\mathbb{Z} \times_B A_{\mathcal{E}}$ with respect to these maps, where $B := \prod_{p|e} \mathbb{F}_p$, we get a connected order of rank $n(e) + 1$ because the $\mathbb{F}_p$ are finite and nonzero. Moreover, for every $\zeta \in \mu(A_{\mathcal{E}})$ whose p-th component is a power of $\zeta_{p^{e_p}}$ for every p dividing e, the pair $(1, \zeta) \in \mathbb{Z} \times A_{\mathcal{E}}$ is a root of unity in the fibred product $\mathbb{Z} \times_B A_{\mathcal{E}}$. This implies $\exp \mu(\mathbb{Z} \times_B A_{\mathcal{E}}) = \exp \mu(A_{\mathcal{E}}) = e$, and so $n_c(e) = 1 + n(e)$. □

From these lower bounds on the rank in terms of the exponent we determine upper bounds on the exponent in terms of the rank using a classical result by Landau and the prime number theorem. For every $x > 1$ let

$$\pi(x) := \sum_{p \leq x} 1 \qquad \text{and} \qquad \theta(x) := \sum_{p \leq x} \ln p,$$

where p ranges over primes only. These are known as the prime counting function and the first Chebyshev function, respectively.

5.5 Theorem. (Prime number theorem)

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1 \qquad \textit{and} \qquad \lim_{x \to \infty} \frac{\theta(x)}{x} = 1.$$

Proof. Omitted, see [3, sections 18, 24 and 25]. □

For every positive integer n let $g(n)$ denote the maximum of the orders of the elements of S_n, the symmetric group on n elements. This function is known as *Landau's function*. Let $y(n)$ be the greatest integer such that $\sum_{p \leq y(n)} p \leq n$, where p again ranges over primes only.

5.6 Theorem. (Landau)

$$\lim_{n\to\infty} \frac{y(n)}{\sqrt{n \ln n}} = 1 \qquad \textit{and} \qquad \lim_{n\to\infty} \frac{\ln g(n)}{\sqrt{n \ln n}} = 1.$$

Proof. Omitted, see the main result of section 61 of [3] and its proof. □

The second limit is known as Landau's theorem.

Proof of theorems II and IV. We first show that $\limsup_{n\to\infty} \frac{\ln e(n)}{\sqrt{n \ln n}} \leq 1$, where $e(n)$ is the maximum of the exponents of the groups of roots of unity of orders of rank n. Let A be an order of rank $n \geq 4$ with $\exp \mu(A) = e(n)$, and let $e(n) = \prod_p p^{e_p}$. In this proof all sums and products indexed by p will range over primes p dividing $e(n)$. By proposition 5.2 we have

$$n + 1 \geq \sum_p \varphi(p^{e_p}) \geq \sum_{p \geq \sqrt{n}} \varphi(p^{e_p}) \geq \left(1 - \frac{1}{\sqrt{n}}\right) \sum_{p \geq \sqrt{n}} p^{e_p},$$

and because $n \geq 4$ some rearranging yields $\sum_{p\geq\sqrt{n}} p^{e_p} \leq n(1 + \frac{3}{\sqrt{n}})$. This implies that the symmetric group on $n' := \lfloor n\left(1 + \frac{3}{\sqrt{n}}\right) \rfloor$ elements contains a product $\prod_{p\geq\sqrt{n}} \sigma_p$ of disjoint cycles $\sigma_p \in S_{n'}$ with $\operatorname{ord} \sigma_p = p^{e_p}$, and hence an element of order $\prod_{p\geq\sqrt{n}} p^{e_p}$. This means $\prod_{p\geq\sqrt{n}} p^{e_p} \leq g(n')$.

From proposition 5.2 we also find that $\varphi(p^{e_p}) \leq n + 1$ for every prime p dividing e, and hence that $p^{e_p} \leq 2n + 2$. It follows that

$$\ln \prod_{p<\sqrt{n}} p^{e_p} \leq \sum_{p<\sqrt{n}} \ln(2n + 2) \leq \pi(\sqrt{n}) \ln(2n + 2) \leq c(\sqrt{n}) \frac{\sqrt{n}}{\ln \sqrt{n}} \ln(2n + 2),$$

for some function c satisfying $\lim_{x\to\infty} c(x) = 1$, by the prime number theorem. Because $n \geq 4$ we have $\frac{\ln(2n+2)}{\ln \sqrt{n}} < 4$, so

$$\ln e(n) = \ln \prod_{p<\sqrt{n}} p^{e_p} + \ln \prod_{p\geq\sqrt{n}} p^{e_p} < 4c(\sqrt{n})\sqrt{n} + \ln g(n').$$

The desired inequality now readily follows from the fact that $\lim_{n\to\infty} \frac{n'}{n} = 1$ and Landau's theorem, which together yield the last equality in

$$\limsup_{n\to\infty} \frac{\ln e(n)}{\sqrt{n \ln n}} \leq \limsup_{n\to\infty} \frac{4c(\sqrt{n})\sqrt{n} + \ln g(n')}{\sqrt{n \ln n}} = 1.$$

To see that $\liminf_{n\to\infty} \frac{\ln e(n)}{\sqrt{n \ln n}} \geq 1$, let $n > 0$ and let $m := n - \sum_{p\leq y(n)}(p - 1)$. Then the order $A(n) := \mathbb{Z}^m \times \prod_{p\leq y(n)} \mathbb{Z}[\zeta_p]$ has rank n and

$$\ln \exp \mu(A(n)) = \ln \prod_{p\leq y(n)} p = \theta(y(n)),$$

which shows that $e(n) \geq \theta(y(n))$. By Landau's theorem and the prime number theorem

$$\liminf_{n\to\infty} \frac{\ln e(n)}{\sqrt{n \ln n}} \geq \liminf_{n\to\infty} \frac{\theta(y(n))}{\sqrt{n \ln n}} = \lim_{n\to\infty} \frac{\theta(y(n))}{y(n)} \frac{y(n)}{\sqrt{n \ln n}} = 1,$$

which proves theorem II, that $\lim_{n\to\infty} \frac{\ln e(n)}{\sqrt{n \ln n}} = 1$. Theorem IV now follows immediately from proposition 5.4. □

6 Tensor products of orders

This section provides some context for question VIII, the most notable result being theorem VII. To prove theorem VII we first prove that $\mathcal{O}_K \otimes \mathcal{O}_K$ is connected if $\mathbb{Q} \subset K$ is a finite Galois extension. Then we extend the result to the tensor product of any pair of connected orders. This requires a few results from algebraic number theory which we now summarize.

6.1 Theorem. (Minkowski) *Let $K \neq \mathbb{Q}$ be a number field. Then there exists a prime $p \in \mathbb{Z}$ that is ramified in K.*

Proof. Omitted, see [4, proposition 2.14, p. 204, corollary 2.12, p. 202]. □

For the remainder of this section let $\mathbb{Q} \subset K$ be a finite Galois extension with Galois group $G := \mathrm{Gal}(K/\mathbb{Q})$.

6.2 Definition. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a nonzero prime. The *inertia group* of $\mathfrak{p}$ is

$$I_\mathfrak{p} := \{\sigma \in G : (\forall x \in \mathcal{O}_K)(\sigma(x) \equiv x \bmod \mathfrak{p})\}.$$

These are the field automorphisms of K that fix $\mathfrak{p}$ and induce the identity on $\mathcal{O}_K/\mathfrak{p}$.

6.3 Proposition. *Let $\mathfrak{p} \subset \mathcal{O}_K$ be a nonzero prime and let $K^{I_\mathfrak{p}}$ be the fixed field of $I_\mathfrak{p}$. Then $\mathfrak{p} \cap \mathcal{O}_{K^{I_\mathfrak{p}}}$ does not ramify in $\mathbb{Q} \subset K^{I_\mathfrak{p}}$.*

Proof. Omitted, see [4, proposition 9.6, p. 57]. □

6.4 Proposition. *The Galois group G is generated by the inertia groups of all nonzero prime ideals of $\mathcal{O}_K$.*

Proof. The fixed field K^I of the group I generated by the inertia groups is the intersection of the fixed fields of the inertia groups. By proposition 6.3 every prime is unramified in K^I. By theorem 6.1 the only unramified extension of $\mathbb{Q}$ is $\mathbb{Q}$, so by Galois theory I is the entire Galois group. □

6.5 Proposition. *The tensor product $\mathcal{O}_K \otimes \mathcal{O}_K$ is connected.*

Proof. Let $e = \sum x_i \otimes y_i \in \mathcal{O}_K \otimes \mathcal{O}_K$ be idempotent, let $\mathfrak{p} \subset \mathcal{O}_K$ be a nonzero prime and let $\sigma \in I_\mathfrak{p}$. Because the multiplication map

$$\psi : \mathcal{O}_K \otimes \mathcal{O}_K \longrightarrow \mathcal{O}_K : x \otimes y \longmapsto xy,$$

is a ring homomorphism also $\psi(e)$ and $\psi((\mathrm{id} \otimes \sigma)(e))$ are idempotents in $\mathcal{O}_K$, hence each is either 0 or 1. As $\sigma(x) - x \in \mathfrak{p}$ for all $x \in \mathcal{O}_K$ we see that

$$\psi((\mathrm{id} \otimes \sigma)(e)) - \psi(e) = \sum x_i \sigma(y_i) - \sum x_i y_i = \sum x_i(\sigma(y_i) - y_i) \in \mathfrak{p},$$

which implies $\psi((\mathrm{id} \otimes \sigma)(e)) = \psi(e)$. For every $\tau \in G$ also $(\mathrm{id} \otimes \tau)(e)$ is idempotent, from which it follows that also

$$\psi((\mathrm{id} \otimes \sigma\tau)(e)) = \psi((\mathrm{id} \otimes \sigma)((\mathrm{id} \otimes \tau)(e))) = \psi((\mathrm{id} \otimes \tau)(e)).$$

By proposition 6.4 the inertia groups of the nonzero primes of $\mathcal{O}_K$ together generate G, which shows that $\psi((\mathrm{id} \otimes \tau)(e)) = \psi(e)$ for all $\tau \in G$. Hence

$$K \otimes K \longrightarrow \prod_{\tau \in G} K : z \longmapsto (\psi((\mathrm{id} \otimes \tau)(z))_{\tau \in G},$$

maps e to 0 or 1, and this map is surjective by the Chinese remainder theorem as the kernels $\ker(\psi \circ (\mathrm{id} \otimes \tau))$ are pairwise distinct maximal ideals. Comparing dimensions then shows that it is injective, so $e = 0$ or $e = 1$. □

We recall two simple facts from commutative algebra.

6.6 Proposition. *Let A and B be orders and $I, J \subset A$ ideals. Then*

$$(A \otimes B)/(I \otimes B) \cong (A/I) \otimes B \qquad \text{as rings, and}$$
$$(I \otimes B) \cap (J \otimes B) = (I \cap J) \otimes B \qquad \text{as submodules of } A \otimes B.$$

Proof. Because $B \cong \mathbb{Z}^n$ is free over $\mathbb{Z}$ it is flat, so the exact sequences

$$0 \longrightarrow \mathfrak{p} \longrightarrow A \longrightarrow A/\mathfrak{p} \longrightarrow 0,$$

$$0 \longrightarrow \mathfrak{p} \cap \mathfrak{q} \longrightarrow A \longrightarrow (A/\mathfrak{p}) \times (A/\mathfrak{q})$$

remain exact when taking tensor products with B. □

6.7 Lemma. *Let R be a ring. If R is connected the so is R_{red}.*

Proof. Let $e \in R$ be such that $\overline{e} \in R_{\mathrm{red}}$ is idempotent. Then $e^2 - e \in \mathcal{N}(R)$ so there exists some $k \geq 1$ such that $e^k(1-e)^k = 0$. Let $f := e^k$ and $g = (1-e)^k$, so that $fg = 0$ and $\overline{f}, \overline{g} \in R_{\mathrm{red}}$ are also idempotent. Note that $f + g - 1 \in \mathcal{N}(R)$ so $f + g$ is a unit, and that for $u := (f+g)^{-1}$ we have

$$uf = uf \cdot u(f+g) = (uf)^2 + u^2 fg = (uf)^2,$$

so uf is idempotent hence $uf \in \{0, 1\}$. If $uf = 0$ then $0 = f = e^k$ so $\overline{e} = 0$. If $uf = 1$ then $f = u^{-1} = f + g$ so $0 = g = (1-e)^k$ and hence $\overline{e} = 1$. □

6.8 Lemma. *If A and B are orders such that A is connected and $(A/\mathfrak{p}) \otimes B$ is connected for every minimal prime $\mathfrak{p} \subset A$, then $A \otimes B$ is connected.*

Proof. Let $e \in A \otimes B$ be idempotent. Then $e + (\mathfrak{p} \otimes B) \in (A \otimes B)/(\mathfrak{p} \otimes B)$ is idempotent for every minimal prime $\mathfrak{p} \subset A$. Then it equals either 0 or 1 because $(A \otimes B)/(\mathfrak{p} \otimes B) \cong (A/\mathfrak{p}) \otimes B$ is connected. For $i \in \{0, 1\}$ let $\mathfrak{q}_i$ denote the intersection of all minimal primes $\mathfrak{p} \subset A$ with $e \equiv i \pmod{\mathfrak{p} \otimes B}$. Then $\mathfrak{q}_0 \cap \mathfrak{q}_1 = \mathcal{N}(A)$ and $\mathfrak{q}_0 + \mathfrak{q}_1 = A$ because $e \in \mathfrak{q}_0$ and $1 - e \in \mathfrak{q}_1$, so by the Chinese remainder theorem $A_{\mathrm{red}} \cong A/\mathfrak{q}_0 \times A/\mathfrak{q}_1$. Note that A_{red} is connected by lemma 6.7 because A is, so either $\mathfrak{q}_0 = A$ or $\mathfrak{q}_1 = A$. This means either $e \in \mathfrak{p} \otimes B$ for every minimal prime $\mathfrak{p} \subset A$, or $1 - e \in \mathfrak{p} \otimes B$ for every minimal prime $\mathfrak{p} \subset A$. It follows that either e or $1 - e$ is contained in

$$\bigcap_{\mathfrak{p}} (\mathfrak{p} \otimes B) = \Big(\bigcap_{\mathfrak{p}} \mathfrak{p}\Big) \otimes B = \mathcal{N}(A) \otimes B,$$

the intersections running over all finitely many minimal primes of A, and hence either e or $1 - e$ is nilpotent. It follows that either $e = 0$ or $e = 1$, so $A \otimes B$ is connected. □

Proof of theorem VII. Let $\mathfrak{p} \subset A$ and $\mathfrak{q} \subset B$ be minimal primes. Then $A/\mathfrak{p}$ and $B/\mathfrak{q}$ embed into the rings of integers $\mathcal{O}_L$ and $\mathcal{O}_M$ of their respective fields of fractions L and M, which are number fields. Let K be a finite Galois extension into which both L and M embed. Then we have injections

$$(A/\mathfrak{p}) \otimes (B/\mathfrak{q}) \longrightarrow \mathcal{O}_L \otimes \mathcal{O}_M \longrightarrow \mathcal{O}_K \otimes \mathcal{O}_K,$$

because these rings are all free over $\mathbb{Z}$, and hence flat. The last tensor product is connected by proposition 6.5, so $(A/\mathfrak{p}) \otimes (B/\mathfrak{q})$ is also connected.

For every minimal prime $\mathfrak{p} \subset A$ the quotient $A/\mathfrak{p}$ is an order. As B is connected and $(A/\mathfrak{p}) \otimes (B/\mathfrak{q})$ is connected for every minimal $\mathfrak{q} \subset B$, it follows from lemma 6.8 that $(A/\mathfrak{p}) \otimes B$ is connected. Because A is connected, applying lemma 6.8 again now shows that $A \otimes B$ is connected. □

This implies that every primitive idempotent of $A \otimes B$ is a pure tensor of primitive idempotents of A and B, which raises the question of whether the same is true for the roots of unity of the tensor product. That is, given two orders A and B, is the natural map

$$\mu(A) \times \mu(B) \longrightarrow \mu(A \otimes B),$$

is surjective? As mentioned in the introduction, in general it is not; for $A = B = \mathbb{Z}^2$ we have $A \otimes B \cong \mathbb{Z}^4$ so $\#\mu(A) \times \#\mu(B) = \#\mu(A \otimes B) = 16$. As $(-1) \otimes (-1) = 1 \otimes 1$ the map is not injective, so it is not surjective.

For *connected* orders, however, it is not immediately clear whether the natural map is surjective in general. We leave the reader with the following question.

VIII Question. *Let A and B be connected orders. Is the natural map $\mu(A) \times \mu(B) \longrightarrow \mu(A \otimes B)$ surjective?*

References

[1] M.F. Atiyah and I.G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company. Westview Press, 1969. ISBN: 978-0201003611.

[2] H.W. Lenstra Jr. and A. Silverberg. *Algorithms for commutative algebras over the rational numbers*. 2015. URL: https://arxiv.org/abs/1509.08843.

[3] E. Landau. *Handbuch der Lehre von der Verteilung der Primzahlen*. B.G. Teubner, 1909.

[4] J. Neukirch. *Algebraic Number Theory*. A Series of Comprehensive Studies in Mathematics. Springer-Verlag, 1999. ISBN: 978-3642084737.