The cyclotomic ideal

Tiersma, Samuel

S.J. Tiersma

The cyclotomic ideal

Bachelor thesis

June 29, 2021

Thesis supervisor: prof. dr. H.W. Lenstra

Universiteit Leiden
Mathematisch Instituut

Foreword

I would like to sincerely thank my supervisor, prof. dr. H. W. Lenstra, for suggesting the topic of this thesis, for his friendly, enthusiastic and astute guidance during the many meetings we had, and for proofreading this thesis diligently. Of course, any errors that remain are mine.

Contents

1 Introduction

Throughout this thesis, with the exception of Section 3.3, all rings will be assumed to be commutative. Whenever we say that d divides n, write $d \mid n$ or call d a divisor of n, it is implicit that d and n are positive integers. A divisor $d \mid n$ is called proper *if $d \neq n$.*

If a group G acts on a set X (module, ring, etc.), then we denote by X^G the set (module, ring, etc.) of G-invariants.

Let C be a finite cyclic group and let n be its order. Let ζ_n be a root of unity of order n in an algebraic closure of $\mathbb{Q}$. Consider the set X of homomorphisms from the group ring $\mathbb{Z}[C]$ to the nth cyclotomic field $\mathbb{Q}(\zeta_n)$ that are injective when restricted to C. This set corresponds bijectively to the set of injective group homomorphisms from C to the unit group of $\mathbb{Q}(\zeta_n)$. The image of any map in the latter set is the subgroup $\langle \zeta_n \rangle$ of roots of unity with order dividing n. Since any automorphism of $\langle \zeta_n \rangle$ arises as the restriction of an automorphism of $\mathbb{Q}(\zeta_n)$, it follows that the automorphism group of $\mathbb{Q}(\zeta_n)$ acts by post-composition transitively on X. Therefore any two maps in X have the same kernel. This kernel is a prime ideal of $\mathbb{Z}[C]$ and is called the *cyclotomic ideal* of $\mathbb{Z}[C]$.

Now let σ be a generator of C and let $f \in X$ be given by $f(\sigma) = \zeta_n$. Since the minimal polynomial over $\mathbb{Q}$ of the primitive n-root of unity $f(\sigma)$ is the nth cyclotomic polynomial $\Phi_n \in \mathbb{Z}[X]$, it follows readily that $\ker f$ is generated by $\Phi_n(\sigma) \in \mathbb{Z}[C]$.

We conclude that the cyclotomic ideal is a principal $\mathbb{Z}[C]$-ideal generated by $\Phi_n(\vartheta)$, where ϑ is *any* generator of C. This fact implies that the cyclotomic ideal is invariant under the natural action of $\operatorname{Aut} C$ on $\mathbb{Z}[C]$. In fact, a stronger statement holds true.

Theorem 1.1. *The cyclotomic ideal is generated by its intersection with the subring $\mathbb{Z}[C]^{\operatorname{Aut} C}$.*

Theorem 1.1 is a corollary of each of the results in the following theorem.

Theorem 1.2. *The cyclotomic ideal is generated by each of the following subsets of $\mathbb{Z}[C]^{\operatorname{Aut} C}$:*

(1) (De Bruijn–Rédei, 1953) *the set of elements*

$$\sum_{\gamma \in C\colon \gamma^p = 1} \gamma,$$

where p ranges over the prime divisors of n;

(2) (Katz–Mazur, 1985) *the set of coefficients in the polynomial*

$$Y^n - 1 - \prod_{\gamma \in C} (Y - \gamma) \in \mathbb{Z}[C][Y];$$

(3) *the set of coefficients in the above polynomial at Y^t, where t ranges over the proper divisors of n.*

We will shortly make some remarks on this theorem and show that the generators in (1) and (2) are indeed contained in the cyclotomic ideal and in $\mathbb{Z}[C]^{\operatorname{Aut} C}$. Under the assumption of this fact, Theorem 1.2(2) is logically weaker than Theorem 1.2(3). We prove Theorem 1.2(3) in Section 2.3 as Theorem 2.6, and subsequently prove Theorem 1.1 as a corollary of Theorem 1.2(3). We prove Theorem 1.2(1) in Section 2.4, by showing that it is implied by Theorem 1.1. In that section, we also sketch two direct proofs of Theorem 1.2(1) that do not depend on Theorem 1.1. Finally, we show that like Theorem 1.2(1), Theorem 1.2(3) can also be derived from Theorem 1.1.

Theorem 1.2(1) was formulated by Rédei in [Ré50] and proved by De Bruijn in [DB53]. It

will be referred to as the *De Bruijn–Rédei theorem*. Each map f in X sends the element in (1) to the sum of the pth roots of unity in $\mathbb{Q}(\zeta_n)$, which is 0. Therefore the generators in (1) are contained in the cyclotomic ideal $\ker f$. Moreover, since a group automorphism preserves the order of elements, the generators in (1) are $\operatorname{Aut} C$-invariant.

Theorem 1.2(2) was established in the work [KM85, Theorem 1.12.9] of Katz and Mazur, and will be called the *Katz–Mazur theorem*. Coefficientwise application of any map in X sends the Katz–Mazur polynomial in (2) to $Y^n - 1 - \prod_{i=0}^{n-1}(Y - \zeta_n^i) = 0 \in \mathbb{Q}(\zeta_n)[Y]$. Thus each coefficient of the Katz–Mazur polynomial is contained in the cyclotomic ideal. Similarly, since the Katz–Mazur polynomial is invariant under the action of $\operatorname{Aut} C$, so are its coefficients.

One may ask whether all coefficients are necessary to generate the ideal. Result (3) provides a negative answer, by showing that $\tau(n) - 1$ coefficients suffice, where $\tau(n)$ is the number of divisors of n.

Our proof of Theorem 1.2(3) is based on a preliminary result from commutative algebra. We call an ideal I of a commutative ring A *locally principal*, if the localization $I_\mathfrak{p}$ at every prime ideal $\mathfrak{p}$ of A is a principal $A_\mathfrak{p}$-ideal.

Proposition 1.3. *Let $A \subset B$ be commutative rings with B integral over A. Let $J \subset I$ be A-ideals with I locally principal and $JB = IB$. Then we have $J = I$.*

Proposition 1.3 is proved in Section 2.1 as Proposition 2.2. In Section 2.3 we prove Theorem 1.2(3) by applying Proposition 1.3 to a certain integral embedding of $A = \mathbb{Z}[C]$ into $B = \prod_{d|n} \mathbb{Z}[\zeta_d]$. The cyclotomic ideal will assume the role of I, and J will be the ideal generated by the elements in (3). In Section 2.2 we construct the embedding at hand, and calculate the B-ideal IB needed in the application of Proposition 1.3. After that, we prove the De Bruijn–Rédei theorem in Section 2.4 from Theorem 1.1, which we will then have derived as a corollary of the Katz–Mazur theorem. In that section we also include a brief discussion of other proofs of the De Bruijn–Rédei theorem, and show how the Katz–Mazur theorem 1.2(2) can be derived from Theorem 1.1.

In Chapter 3 we broaden our attention from ideals of the group ring $\mathbb{Z}[C]$ to general modules over that ring. Note that a module over the cyclic group C of order n is the same as an abelian group together with an automorphism of order dividing n. Modules over finite cyclic groups are, for example, frequently encountered in algebraic number theory. Our main aim is to provide a proof of a result by Lenstra on units in certain subrings of a cyclic number field [Len77, Stellingen]. This result is a strengthening of one by Latimer [Lat34, Theorem 3].

Let K be an algebraic number field. Suppose K admits r real and $2s$ imaginary embeddings, so that $n = r + 2s$ is the degree of K. If R is a subring of K, we write R^* for the unit group of R and μ_R for the torsion subgroup of R^*, consisting of the roots of unity in R.

Let R be an *order* in K, that is, a subring of K whose additive group is free of rank n. The Dirichlet unit theorem states that μ_R is finite and that R^*/μ_R is a free abelian group of rank $r + s - 1$. We can thus find a so-called *fundamental system of units* $\eta_1, \eta_2, \ldots, \eta_{r+s-1} \in R^*$ such that

$$R^* = \mu_R \times \langle \eta_1 \rangle \times \langle \eta_2 \rangle \times \cdots \times \langle \eta_{r+s-1} \rangle.$$

Now assume that the extension $K/\mathbb{Q}$ is Galois, say with group G. Then G acts naturally on K and associated objects, such as the ring of integers $\mathcal{O}_K$ of K. More generally, if an order R in K is stable under G, then the ring R is a G-module. Further, the groups R^* and R^*/μ_R related to R inherit a G-module structure.

Theorem 1.4. *Let $K/\mathbb{Q}$ be a finite cyclic extension. Then the ring of integers of K has a fundamental system of units that contains a fundamental system of units for the ring of integers of each subfield of K.*

We will prove it using the following theorem.

Theorem 1.5. *Let $K/\mathbb{Q}$ be a finite cyclic extension, and C its Galois group. Let R be an order in K which is stable under the action of C. Then C acts naturally on R^* and R^*/μ_R. Moreover, for every subgroup $D \subset C$ the natural map*

$$(R^*)^D \to (R^*/\mu_R)^D$$

is surjective.

We prove Theorem 1.4 and Theorem 1.5 in Section 3.5 as Theorem 3.22 respectively Theorem 3.21. Our proof of Theorem 1.5 is based on the following result.

Proposition 1.6. *Let C be a finite cyclic group and M a C-module. Let N be the sub-C-module of M consisting of the elements of finite additive order. Assume that D is a subgroup of C such that $N^D = M^C$. Then the natural map*

$$M^D \longrightarrow (M/N)^D$$

is surjective.

Proposition 1.6 is proved in Section 3.1 as Corollary 3.2. In the proof of Theorem 1.4 we also use the following result.

Proposition 1.7. *Let C be a finite cyclic group and n its order. Let M be a C-module whose additive group is free. Then there exists a collection $(M_d)_{d|n}$ of subgroups of M with the following property. If D is a subgroup of C and m its index, then we have a direct sum decomposition*

$$M^D = \bigoplus_{d|m} M_d.$$

Proposition 1.7 is proved in Section 3.4 as Theorem 3.17. Further, in this section we show how the De Bruijn–Rédei Theorem 1.2(1) may be derived from (a strengthening of) Proposition 1.7. We sketch the several proofs of Theorem 1.2 discussed in this thesis in Figure 1.

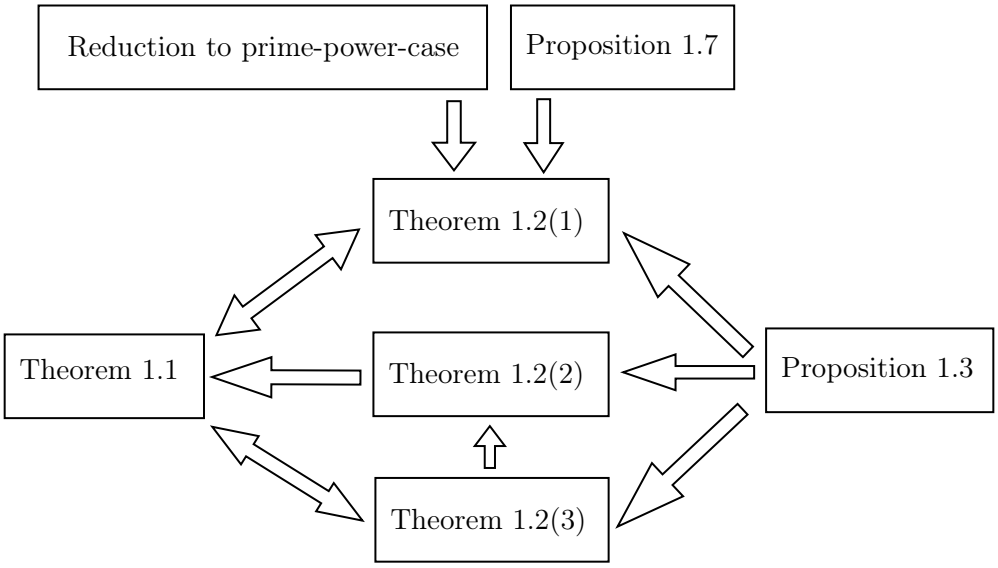

Figure 1: Diagram summarising the different proofs of Theorem 1.2. A logical implication between two results is indicated by an arrow.

For the convenience of the reader, several basic results from commutative algebra are assembled in Appendix A. The majority of proofs in this appendix is omitted. The reader can find these in our main reference [AM69], or any other textbook on commutative algebra.

2 The cyclotomic ideal

2.1 A preparatory result

In this section we prove Proposition 1.3 as Proposition 2.2.

An ideal I of a ring A is said to be *locally principal* if the localization $I_\mathfrak{p}$ at every prime ideal $\mathfrak{p}$ of A is a principal $A_\mathfrak{p}$-ideal.

Examples 2.1. (1) Any principal ideal is locally principal, for if $I = A\alpha$ is a principal ideal of a ring A and S a multiplicatively closed subset of A, then $S^{-1}I$ is the principal $S^{-1}A$-ideal generated by $\alpha/1$.

(2) A non-zero ideal I of a noetherian domain A is locally principal if and only if it is invertible, that is, there exists an A-ideal J such that the product ideal IJ is a non-zero principal ideal [Ste17, Theorem 2.7]. For example, the ideal $I = (2, 1+\sqrt{-5})$ of the Dedekind domain $\mathbb{Z}[\sqrt{-5}]$ is invertible, because I divides $(1+\sqrt{-5}) = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5})$. Since the number ring $\mathbb{Z}[\sqrt{-5}]$ is noetherian, I is locally principal. However, I is not principal, as one shows by considering the norms of its generators.

Proposition 2.2. *Let $A \subset B$ be rings, B integral over A. Let $J \subset I$ be A-ideals with I locally principal and such that $JB = IB$. Then we have $J = I$.*

Proof. First assume that A is local and B is finitely generated as an A-module. Since I is principal, we have $J = \mathfrak{a}I$ for an A-ideal $\mathfrak{a}$. If $\mathfrak{a}$ were not contained in the maximal ideal $\mathfrak{m}$ of A, then $\mathfrak{a} = A$ and $J = I$. So assume that $\mathfrak{a} \subset \mathfrak{m}$. Then $IB = JB = \mathfrak{a}IB \subset \mathfrak{m}IB \subset IB$, hence $IB = \mathfrak{m}IB$. Since I and B are both finitely generated over A, the same holds for IB. Now Nakayama's lemma yields that $IB = 0$, whence $J \subset I \subset IB = 0$ and $J = 0 = I$.

Now assume only that A is local. Let α be a generator of I. Since $\alpha \in IB = JB$, we have $\alpha = \sum_{s\in S} sj_s$ with S some finite subset of B and each $j_s \in J$. Then already in the ring $B' = A[S]$ we have $\alpha \in JB'$, that is, $IB' = JB'$. Since B' is generated as an A-algebra by finitely many elements, each integral over A, by Proposition A.1 the ring B' is finitely generated as an A-module. Now apply the previous case with B' instead of B.

Finally we prove Proposition 2.2 in its entirety. By Lemma A.6 it is sufficient to prove that $I_\mathfrak{p} = J_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$ of A. So let $\mathfrak{p}$ be a prime ideal of A. By Lemma A.4(iii) we have

$$B_\mathfrak{p}J_\mathfrak{p} = (BJ)_\mathfrak{p} = (BI)_\mathfrak{p} = B_\mathfrak{p}I_\mathfrak{p}.$$

Since by assumption $I_\mathfrak{p}$ is principal, and by Lemma A.7(ii) the ring $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$, the previous case yields that $I_\mathfrak{p} = J_\mathfrak{p}$, as was to be shown. □

Non-example. The hypothesis that I be locally principal cannot be omitted from the statement of Proposition 2.2.

For example, consider the extension $A = \mathbb{Z}[2\mathrm{i}] \subset B = \mathbb{Z}[\mathrm{i}]$ of integral domains. We leave to the reader to verify that B is integral over A. Consider the integral A-ideals $I = 2B$ and $J = 2A$. Then J is strictly contained in I, although $BI = 2B = BJ$. Thus by Proposition 2.2 the A-ideal I is not locally principal.

2.2 The cyclotomic ideal

We introduce some objects that will be referred to in the remainder of this chapter. Let C be a finite cyclic group and n its order. We fix a generator σ for C and let I be the cyclotomic ideal $\Phi_n(\sigma)\mathbb{Z}[C]$. Moreover, for every positive integer m we fix a root of unity ζ_m of order m in an algebraic closure of $\mathbb{Q}$.

We are going to embed $\mathbb{Z}[C]$ into $\prod_{d|n}\mathbb{Z}[\zeta_d]$.

For a ring R an isomorphism of R-algebras $R[X]/(X^n-1)R[X] \to R[C]$ is given by sending $X \bmod (X^n-1)$ to σ. Since the cyclotomic polynomials are pairwise coprime in $\mathbb{Q}[X]$ and it holds that $X^n-1 = \prod_{d|n}\Phi_d$, by the Chinese remainder theorem we have a natural ring isomorphism

$$\mathbb{Q}[X]/(X^n-1)\mathbb{Q}[X] \xrightarrow{\sim} \prod_{d|n}\mathbb{Q}[X]/\Phi_d\mathbb{Q}[X].$$

For a positive integer d, an isomorphism of rings $\mathbb{Q}[X]/\Phi_d\mathbb{Q}[X] \to \mathbb{Q}(\zeta_d)$ is given by sending $X \bmod \Phi_d$ to ζ_d. We obtain ring isomorphisms

$$\mathbb{Q}[C] \cong \mathbb{Q}[X]/(X^n-1)\mathbb{Q}[X] \cong \prod_{d|n}\mathbb{Q}[X]/\Phi_d\mathbb{Q}[X] \cong \prod_{d|n}\mathbb{Q}(\zeta_d),$$

whose composite sends $\sigma \in \mathbb{Q}[C]$ to the vector $(\zeta_d)_{d|n} \in \prod_{d|n}\mathbb{Q}(\zeta_d)$ and induces an injective ring homomorphism from $\mathbb{Z}[C]$ into the ring $\prod_{d|n}\mathbb{Z}[\zeta_d]$, which we regard as an inclusion.

In the following sections, we will apply Proposition 2.2 to the extension $\mathbb{Z}[C] \subset \prod_{d|n}\mathbb{Z}[\zeta_d]$ in order to show that an ideal J generated by certain elements equals the cyclotomic ideal I. This approach is summarized in the following lemma.

Lemma 2.3. *Let $J \subset I$ be a $\mathbb{Z}[C]$-ideal. Then $J = I$ if and only if $J \cdot \prod_{d|n}\mathbb{Z}[\zeta_d] = I \cdot \prod_{d|n}\mathbb{Z}[\zeta_d]$.*

Proof. It is not difficult to see, for example using Lemma A.2, that the ring $\prod_{d|n}\mathbb{Z}[\zeta_d]$ is integral over $\mathbb{Z}$, whence it is also integral over $\mathbb{Z}[C]$. The cyclotomic ideal $I = \Phi_n(\sigma)\mathbb{Z}[C]$ is principal, so locally principal as well by Example 2.1(1). Now apply Proposition 2.2 with $A = \mathbb{Z}[C]$ and $B = \prod_{d|n}\mathbb{Z}[\zeta_d]$. □

For Lemma 2.3 to be of practical use, we require an explicit description of the ideal of $\prod_{d|n}\mathbb{Z}[\zeta_d]$ generated by I.

Proposition 2.4. *We have $I \cdot \prod_{d|n}\mathbb{Z}[\zeta_d] = \prod_{d|n} I_d$, with*

$$I_d = \begin{cases} 0 & \text{if } d = n, \\ p\mathbb{Z}[\zeta_d] & \text{if } n/d = p^\alpha \text{ for } p \text{ prime and } \alpha \in \mathbb{Z}_{>0}, \\ \mathbb{Z}[\zeta_d] & \text{else.} \end{cases}$$

Since the generator $\Phi_n(\sigma) \in \mathbb{Z}[C]$ of I, when viewed as element of $\prod_{d|n}\mathbb{Z}[\zeta_d]$, equals the vector $(\Phi_n(\zeta_d))_{d|n}$, one sees that $I \cdot \prod_{d|n}\mathbb{Z}[\zeta_d] = \prod_{d|n}\Phi_n(\zeta_d)\mathbb{Z}[\zeta_d]$. Thus to establish Proposition 2.4 we need only determine the ideal $I_d = \Phi_n(\zeta_d)\mathbb{Z}[\zeta_d]$. First a useful lemma, which will also be used in Chapter 3.

Lemma 2.5. *Let $d, h \in \mathbb{Z}_{\geq 1}$ such that $d \nmid h$ and $h \nmid d$. Then $\Phi_d\mathbb{Z}[X] + \Phi_h\mathbb{Z}[X] = \mathbb{Z}[X]$.*

Proof. Using the Euclidean algorithm we find that

$$(X^d-1, X^h-1)\mathbb{Z}[X] = (X^{\gcd(d,h)}-1)\mathbb{Z}[X]. \tag{1}$$

Since neither d nor h is divisible by the other, we have that $\gcd(d,h) < d, h$. It follows that Φ_d divides $(X^d-1)/(X^{\gcd(d,h)}-1)$ and that Φ_h divides $(X^h-1)/(X^{\gcd(d,h)}-1)$. Since $\mathbb{Z}[X]$ is a domain we can cancel $X^{\gcd(d,h)}-1$ in (1). This yields the claim. □

Proof of Proposition 2.4. The case that $d = n$ is clear since the root of unity ζ_d of order $d = n$ is a zero of the cyclotomic polynomial Φ_n.

We settle the other cases, in which $n = kd$ for some $k \in \mathbb{Z}_{>1}$, by showing that for every $k \in \mathbb{Z}_{>1}$ we have $\Phi_{kd}(\zeta_d)\mathbb{Z}[\zeta_d] = p\mathbb{Z}[\zeta_d]$ if $k = p^\alpha$ for some prime number p and $\alpha \in \mathbb{Z}_{>0}$, and $\Phi_{kd}(\zeta_d)\mathbb{Z}[\zeta_d] = \mathbb{Z}[\zeta_d]$ for k that are not a power of a prime.

For every $m \in \mathbb{Z}_{\geq 1}$ we have

$$\left(\frac{X^{md}-1}{X^d-1}\right)(\zeta_d) = \left(\sum_{i=0}^{m-1} X^{id}\right)(\zeta_d) = \sum_{i=0}^{m-1} \zeta_d^{id} = m.$$

By the defining recurrence relation for the cyclotomic polynomials we have

$$(X^{md}-1)/(X^d-1) = \prod_{h \mid md,\ h \nmid d} \Phi_h.$$

For $h \in \mathbb{Z}_{>0}$ with both $d \nmid h$ and $h \nmid d$, the element $\Phi_h(\zeta_d)$ is a unit in $\mathbb{Z}[\zeta_d]$, since by Lemma 2.5 we have

$$\mathbb{Z}[\zeta_d]/\Phi_h(\zeta_d)\mathbb{Z}[\zeta_d] \cong \mathbb{Z}[X]/(\Phi_d, \Phi_h) = 0.$$

It follows that

$$\prod_{\substack{k \mid m,\\ k \neq 1}} \Phi_{kd}(\zeta_d)\mathbb{Z}[\zeta_d] = \prod_{\substack{h:\ d \mid h \mid md,\\ h \neq d}} \Phi_h(\zeta_d)\mathbb{Z}[\zeta_d] = \prod_{\substack{h \mid md,\\ h \nmid d}} \Phi_h(\zeta_d)\mathbb{Z}[\zeta_d] = \left(\frac{X^{md}-1}{X^d-1}(\zeta_d)\right)\mathbb{Z}[\zeta_d] = m\mathbb{Z}[\zeta_d].$$

From this recurrence relation our claim follows. □

2.3 The Katz–Mazur theorem

In this section we prove Theorem 1.2(3) as Theorem 2.6. We recall that C is a finite cyclic group, and n its order. Further, we have fixed a generator σ for C and let I be the cyclotomic ideal $\Phi_n(\sigma)\mathbb{Z}[C]$. Moreover, for every positive integer m we fixed a root of unity ζ_m of order m in an algebraic closure of $\mathbb{Q}$.

Theorem 2.6. *The cyclotomic ideal is generated by the coefficients at Y^t of the polynomial*

$$Y^n - 1 - \prod_{\gamma \in C} (Y - \gamma) \in \mathbb{Z}[C][Y],$$

where t ranges over the proper divisors of n.

We will give a proof of Theorem 2.6 shortly, but first state and prove the following theorem by Kummer that we will be using.

Theorem 2.7 (Kummer)**.** *Let $0 \leq k \leq m$ be integers and p a prime number. Then the multiplicity of p in the prime factorization of $\binom{m}{k}$ is equal to the number of carries involved in adding k to $m-k$ in base p.*

Proof. Denote by ord_p the p-adic valuation on $\mathbb{Z}$. For $n \in \mathbb{Z}_{\geq 0}$ we have Legendre's formula [Mol12]

$$\mathrm{ord}_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Since $\binom{m}{k} = \frac{m!}{k!(m-k)!}$, this gives

$$\mathrm{ord}_p\left(\binom{m}{k}\right) = \mathrm{ord}_p(m!) - \mathrm{ord}_p(k!) - \mathrm{ord}_p((m-k)!) = \sum_{i=1}^{\infty} \left(\left\lfloor \frac{m}{p^i} \right\rfloor - \left\lfloor \frac{k}{p^i} \right\rfloor - \left\lfloor \frac{m-k}{p^i} \right\rfloor \right).$$

The result follows since for $i \geq 1$ the ith summand equals the number of times we carry from position $i-1$ to position i when adding k and $m-k$ together in base p. □

Proof of Theorem 2.6. In the introduction we have shown that the $\mathbb{Z}[C]$-ideal J generated by such coefficients is contained in I. We can write $J \cdot \prod_{d|n} \mathbb{Z}[\zeta_d] = \prod_{d|n} J_d$, with J_d an ideal of $\mathbb{Z}[\zeta_d]$. By Lemma 2.3, to show that $I = J$ it suffices to prove that $I_d \subset J_d$ for every $d \mid n$, with I_d as in Proposition 2.4 (since $J_d \subset I_d$ is immediate from $J \subset I$).

Fix a divisor $d \mid n$. The image of the Katz–Mazur polynomial

$$Y^n - 1 - \prod_{\gamma \in C} (Y - \gamma) = Y^n - 1 - \prod_{i=0}^{n-1} (Y - \sigma^i) \in \mathbb{Z}[C][Y]$$

under coefficientwise application of the homomorphism $\mathbb{Z}[C] \to \mathbb{Z}[\zeta_d]$ sending σ to ζ_d equals

$$Y^n - 1 - \prod_{i=0}^{n-1} (Y - \zeta_d^i) = Y^n - 1 - \left(\prod_{i=0}^{d-1} (Y - \zeta_d^i) \right)^{n/d} = Y^n - 1 - (Y^d - 1)^{n/d} \in \mathbb{Z}[Y].$$

Note that J_d is the $\mathbb{Z}[\zeta_d]$-ideal generated by the coefficients Y^t of this polynomial, where t ranges over the proper divisors of n. For $0 < t < n$, the coefficient of Y^t is non-zero if and only if d divides t, and in that case it equals $\pm\binom{n/d}{t/d}$.

We now show that $I_d \subset J_d$ by distinguishing 3 cases:

(i) $n = d$;

(ii) $n/d > 1$ is a power of a prime p;

(iii) $n/d > 1$ is not a prime power.

Note that these cases are exhaustive.

(i) Trivial since $I_n = 0$.

(ii) In view of Proposition 2.4 it suffices to show that $p \in J_d$. First take $t = n/p$; then t is divisible by d. Since precisely one carry is involved when adding $(n/d)/p$ to $(n/d) - (n/d)/p$ in base p, we find that the binomial coefficient $\binom{n/d}{t/d} = \binom{n/d}{(n/d)/p} \in J_d$ is divisible by p but not by p^2.

For $t = d$ we find that $\binom{n/d}{t/d} = \binom{n/d}{1} = n/d$ is a power of p in J_d. Since $\binom{n/d}{(n/d)/p}$ and n/d have greatest common divisor p, we have $p \in J_d$ as desired.

(iii) Setting $t = d$ yields again that $n/d \in J_d$.

Let p be any prime divisor of n/d and let t be the integer such that t/d is the largest power of p dividing n/d. Similarly to (ii) we find that $\binom{n/d}{t/d}$ contains no power of p in its prime factorization.

We conclude that for every prime number p, the ideal J_d contains an integer not divisible by p, whence $J_d = \mathbb{Z}[\zeta_d]$. This finishes the proof of Theorem 2.6. □

Remark 2.8. A different version of Theorem 2.6 may be given in which t ranges over 0 and the proper divisors t of n for which n/t is odd. This version saves on the number of coefficients required to generate the cyclotomic ideal asymptotically by a factor of $\mathrm{ord}_2(n)$.

As pointed out in the introduction, the Katz–Mazur theorem implies Theorem 1.1.

Corollary 2.9. *The cyclotomic ideal is generated by its intersection with* $\mathbb{Z}[C]^{\mathrm{Aut}\, C}$. □

2.4 $\mathbb{Z}[C]^{\mathrm{Aut}\, C}$ and the De Bruijn–Rédei theorem

We recall that C is a finite cyclic group, and n its order. Further, we have fixed a generator σ for C and let I be the cyclotomic ideal $\Phi_n(\sigma)\mathbb{Z}[C]$. Moreover, for every positive integer m we fixed a root of unity ζ_m of order m in an algebraic closure of $\mathbb{Q}$.

In this section we prove the De Bruijn–Rédei theorem 1.2(1) as Theorem 2.10. There are in fact several known proofs of this theorem; a topic that will be discussed briefly at the end of the section. The proof we give derives it from Theorem 1.1 that the cyclotomic ideal be generated by its intersection with the fixed ring $\mathbb{Z}[C]^{\mathrm{Aut}\, C}$. We first study the additive structure of $A = \mathbb{Z}[C]^{\mathrm{Aut}\, C}$.

It is not difficult to see that two elements of C fall into the same orbit under the natural action of $\mathrm{Aut}\, C$ precisely when they have the same order. Thus an expression $\sum_{g\in C} a_g g \in \mathbb{Z}[C]$ is contained in the fixed ring A if and only if $a_g = a_h$ whenever $g, h \in C$ have equal order. It follows that A is free as an abelian group with basis $(\beta_d)_{d|n}$ given by

$$\beta_d = \sum_{\gamma\in C:\ \mathrm{order}(\gamma)=d} \gamma.$$

We claim that a second $\mathbb{Z}$-basis of A is given by $(\alpha_d)_{d|n}$, where

$$\alpha_d = \sum_{\gamma\in C:\ \gamma^d=1} \gamma.$$

Indeed, note the relation

$$\alpha_d = \sum_{k|d} \beta_k.$$

Möbius inversion yields that

$$\beta_d := \sum_{k|d} \mu(k)\alpha_k.$$

Since the β_d form a $\mathbb{Z}$-basis for A, so do the α_d.

The De Bruijn–Rédei theorem 2.10 asserts that the cyclotomic ideal is generated by the α_p, with $p \mid n$ a prime number.

Theorem 2.10 (De Bruijn–Rédei)**.** *Let C be a finite cyclic group, and n its order. Then the cyclotomic ideal in $\mathbb{Z}[C]$ is generated by the elements*

$$\sum_{\gamma\in C:\ \gamma^p=1} \gamma,$$

where p ranges over the prime divisors of n.

Proof. As in the introduction one shows that for $d \in \mathbb{Z}_{>1}$ dividing n the element α_d is contained in $I \cap \mathbb{Z}[C]^{\mathrm{Aut}\, C}$ (the proof given there for d that are prime goes through without that assumption). Since $\mathbb{Z}[C]^{\mathrm{Aut}\, C} = A = \bigoplus_{d|n} \mathbb{Z}\alpha_d$ and $I \cap \mathbb{Z}\alpha_1 = I \cap \mathbb{Z} = 0$, it follows that

$$I \cap \mathbb{Z}[C]^{\mathrm{Aut}\, C} = \bigoplus_{\substack{d|n,\\ d\neq 1}} \mathbb{Z}\alpha_d. \tag{2}$$

Let $d \mid n$ with $d > 1$ be given. Let p be a prime divisor of d, and let Γ be a set of representatives of the group $\{\gamma \in C \colon \gamma^d = 1\}$ modulo its subgroup $\{\gamma \in C \colon \gamma^p = 1\}$. Then we have $\alpha_d = \alpha_p \cdot \sum_{\gamma\in\Gamma} \gamma$, whence $\alpha_d \in \mathbb{Z}[C] \cdot \alpha_p$.

Since Theorem 1.1 asserts that I is generated by $I \cap \mathbb{Z}[C]^{\mathrm{Aut}\, C}$, it follows by (2) and the observation in the previous paragraph, that the α_p with $p \mid n$ prime generate I as a $\mathbb{Z}[C]$-ideal. □

We now sketch two alternative proofs of the De Bruijn–Rédei theorem.

A second proof of the De Bruijn–Rédei theorem proceeds using the method based on Proposition 1.3 that was used in establishing the Katz–Mazur theorem. One shows that for every $m \mid n$ the element α_m corresponds under the embedding $\mathbb{Z}[C] \hookrightarrow \prod_{d|n} \mathbb{Z}[\zeta_d]$ of Section 2.2 to the vector whose coordinate corresponding to a divisor d of n equals m when m divides n/d, and 0 otherwise. Therefore, on writing $\prod_{d|n} K_d$ for the ideal generated in the larger ring by the α_p with $p \mid n$ prime, we find that $K_d = \sum_{p|n/d \text{ prime}} p\mathbb{Z}[\zeta_d] = I_d$, with I_d defined as in Proposition 2.4. The proof is then concluded in the same way as in the first paragraph of the proof of Theorem 2.6.

A third, more elementary, proof of the De Bruijn–Rédei theorem may be based on the observation that the result is almost immediate when n is a prime power. Indeed, suppose $n = q^\alpha$ for a prime number q and $\alpha \in \mathbb{Z}_{>0}$. Recall that we fixed a generator σ of C. By definition $\Phi_{q^\alpha}(\sigma)$ is a generator of the cyclotomic ideal. Further, we have that $\Phi_{q^\alpha}(X) = \sum_{i=0}^{q-1} X^{iq^{\alpha-1}}$. The statement of Theorem 2.10 becomes vacuous after observing that

$$\Phi_{q^\alpha}(\sigma) = \sum_{i=0}^{q-1} \sigma^{iq^{\alpha-1}} = \sum_{\gamma\in C \colon \gamma^q=1} \gamma = \alpha_q.$$

For general n with prime factorization $n = \prod_{q|n} q^{\alpha(q)}$, the Chinese remainder theorem gives a group isomorphism $C \cong \prod_q C_q$, with C_q a cyclic group of order $q^{\alpha(q)}$. Now we have a commutative diagram (for suitably chosen isomorphisms)

$$\begin{array}{ccc} \bigotimes_{q|n} \mathbb{Z}[C_q] & \xrightarrow{\sim} & \mathbb{Z}[C] \\ \downarrow & & \downarrow \\ \bigotimes_{q|n} \mathbb{Z}[\zeta_{q^{\alpha(q)}}] & \xrightarrow{\sim} & \mathbb{Z}[\zeta_n], \end{array}$$

which allows Theorem 2.10 to be derived from the prime-power-case; we will not elaborate this however.

We have proved the De Bruijn–Rédei theorem 1.2(1) by showing that it follows from Theorem 1.1 that the cyclotomic ideal is generated by its intersection with $\mathbb{Z}[C]^{\mathrm{Aut}\, C}$. This raises the question whether Theorem 1.2(3) may also be derived from Theorem 1.1. This is possible by virtue of the observation that the coefficients of the Katz–Mazur polynomial can be regarded by Vieta's formulae as 'elementary symmetric polynomials' in the elements σ^k with $1 \leq k \leq n$ and the

basis elements α_d as 'power sums' in the σ^k; both symmetric expressions can thus be related by Newton's identities. We formalise this argument below.

Proof of the implication Theorem 1.1 $\implies$ Theorem 1.2(3). In the ring $\mathbb{Z}[T_1, \ldots, T_n]$, let $e_k = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} T_{i_1} T_{i_2} \cdots T_{i_k}$ be the kth elementary symmetric polynomial, and let $p_k = T_1^k + T_2^k + \cdots + T_n^k$ be the kth power sum. Newton's identities give that for every integer $1 \le k \le n$ we have

$$p_k - e_1 p_{k-1} + e_2 p_{k-2} - \ldots + (-1)^{k-1} e_{k-1} p_1 + (-1)^k k e_k = 0. \tag{3}$$

Consider the ring homomorphism $g : \mathbb{Z}[T_1, \ldots, T_n] \to \mathbb{Z}[C]$ given by substituting σ^k for T_k. Note that the Katz–Mazur polynomial is the result of coefficientwise application of g to the polynomial

$$Y^n - 1 - \prod_{i=1}^{n} (Y - T_i) = -1 - \sum_{t=1}^{n-1} (-1)^t e_t Y^{n-t} + (-1)^{n+1} \prod_{i=1}^{n} T_i. \tag{4}$$

Furthermore, for all $k \in \mathbb{Z}_{>0}$ we have that

$$g(p_k) = \sum_{i=0}^{n-1} \sigma^{ik} = \gcd(n, k) \alpha_{n/\gcd(n,k)}. \tag{5}$$

Recall that $A = \mathbb{Z}[C]^{\operatorname{Aut} C}$. We show by induction that for all integers $0 \le h \le n-1$ one has

$$\sum_{1 \le k \le h \colon k \mid n} \alpha_{n/k} \mathbb{Z} = \sum_{1 \le k \le h \colon k \mid n} g(e_k) A. \tag{6}$$

For $h = 0$ the statement is vacuous.

Let $1 \le m \le n-1$ be given and suppose (6) holds for $h = m-1$. If $m \nmid n$ the ideal (6) is the same for $h = m-1$ and $h = m$, so we are done by the inductive hypothesis. Therefore, we assume that $m \mid n$.

Applying g to (3) with $k = m$ gives that

$$g(p_m) - g(e_1) g(p_{m-1}) + g(e_2) g(p_{m-2}) - \ldots + (-1)^{m-1} g(e_{m-1}) g(p_1) + (-1)^m m g(e_m) = 0.$$

Let K be the ideal (6) with $h = m-1$. By (5) we have that $g(p_1), \ldots, g(p_{m-1}) \in K$, whence the above equation yields the congruence

$$g(p_m) \equiv (-1)^{m+1} m g(e_m) \bmod K. \tag{7}$$

Since $(\alpha_d)_{d \mid n}$ is a $\mathbb{Z}$-basis for A and K is generated as an abelian group by some of the α_d, we have that A/K is torsion free.

As $m \mid n$ we have by (5) that $g(p_m) = m \alpha_{n/m}$, so (7) yields that $(-1)^{m+1} m g(e_m) \equiv g(p_m) \equiv m \alpha_{n/m} \bmod K$. Since A/K is torsion free, we find the congruence $\alpha_{n/m} \equiv (-1)^{m+1} g(e_m) \bmod K$. Therefore we have by the inductive hypothesis

$$\sum_{k=1}^{m} g(e_k) A = K + g(e_m) A = \sum_{1 \le k \le m-1 \colon k \mid n} \alpha_{n/k} \mathbb{Z} + \alpha_{n/m} A = \sum_{1 \le k \le m \colon k \mid n} \alpha_{n/k} \mathbb{Z},$$

where for the last equality we used the absorbing property $\alpha_d \alpha_e = \gcd(d, e) \alpha_{\operatorname{lcm}(d,e)}$, valid for all $d, e \mid n$.

By the principle of induction it follows that (6) holds for $h = n-1$. By (2) we have

$$\sum_{0 < k < n \colon k \mid n} g(e_k) A = \sum_{1 \le k < n \colon k \mid n} \alpha_{n/k} A = \sum_{1 < k \le n \colon k \mid n} \alpha_k \mathbb{Z} = I \cap A. \tag{8}$$

But we have seen in (4) that for each integer $0 < k < n$ the coefficient of the Katz–Mazur polynomial at Y^k is $\pm g(e_{n-k})$. Since Corollary 2.9 states that the $\mathbb{Z}[C]$-ideal I is generated by $I \cap A$, taking the extension in $\mathbb{Z}[C]$ of the A-ideal (8) yields Theorem 1.2(3).

3 Fundamental systems of units

The principal aim of this chapter is to prove Theorem 1.4 and Theorem 1.5. As stated in the introduction, we will make use of two preliminary results: Proposition 1.6 and Proposition 1.7. Proposition 1.6 is proved in Section 3.1 as Corollary 3.2. Our approach to Proposition 1.7 is by formulating a similar result in a more general context, that of so-called *Pila systems* in a commutative ring acting on an object in an abelian category. The reader who is mainly interested in Theorems 1.4 and 1.5 on units in number fields and willing to take the preliminary results Propositions 1.6 and 1.7 from the introduction for granted, can start reading at Section 3.5.

3.1 Surjectivity of natural maps

In this section we prove Proposition 1.6 as Corollary 3.2. The following theorem is a generalization of Corollary 3.2. For a module M over a ring A and an element $a \in A$ we denote by $M[a]$ the submodule of M consisting of those elements that are annihilated by a.

Theorem 3.1. *Let A be a ring whose additive group is finitely generated. Let M be an A-module and denote by N the A-submodule consisting of all elements of finite additive order. Let $a \in A$ and $c \in aA$. Assume that $N[c] = M[a]$. Then the natural map*

$$M[c] \to (M/N)[c]$$

is surjective.

Proof. Let $b \in A$ be such that $c = ab$.

We claim that a acts injectively on M/N. Let $x \in M$ be such that $0 = a(x + N)$. Then $ax \in N$, so there exists $m \in \mathbb{Z}_{\neq 0}$ such that $0 = m(ax) = a(mx)$. The assumption gives that $mx \in M[a] = N[ab] \subset N$. Hence there exists $n \in \mathbb{Z}_{\neq 0}$ such that $0 = n(mx) = (nm)x$. This implies that $x \in N$, i.e., $x + N = 0 \in M/N$, as was to be shown. Note that our claim yields immediately that $(M/N)[ab] = (M/N)[b]$.

Secondly, we show that b acts bijectively on aN. To show injectivity, let $y \in N$ be such that $b(ay) = 0$. Then $y \in N[ab] = M[a]$, so $ay = 0$ as required. For surjectivity, it suffices to show that b acts surjectively on any given cyclic submodule N_0 of aN. Because A is finitely generated over $\mathbb{Z}$, and N_0 is generated by a single element of finite additive order, the module N_0 is finite. Now b acts injectively on the finite set N_0, hence surjectively. This proves our claim, and that $aN = abN$.

We will now show that the map $M[ab] \to (M/N)[ab]$ is surjective. Let $x + N$ be a coset in $(M/N)[ab] = (M/N)[b]$. Then $bx \in N$, so $abx \in aN = abN$. Hence there exists $y \in N$ such that $abx = aby$, i.e. $x - y \in M[ab]$. Since $(x - y) + N = x + N$, this finishes the proof. □

Corollary 3.2. *Let C be a finite cyclic group and M a C-module. Let N be the sub-C-module of M consisting of all elements of finite additive order. Assume that D is a subgroup of C such that $N^D = M^C$. Then the natural map*

$$M^D \longrightarrow (M/N)^D$$

is surjective.

Proof. Take $A = \mathbb{Z}[C]$. Let σ be a generator for C, and τ one for D. Put $a = \sigma - 1$ and $c = \tau - 1$. It is not difficult to see that $c \in Aa$. By assumption we have $N[c] = N^D = M^C = M[a]$. Now apply Theorem 3.1. □

Non-example. If we omit the assumption that C be cyclic, the result is false, as the following example shows. Let V be the Klein four-group and $a, b \in V$ distinct non-trivial elements. Let M be the abelian group $(\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}$, with V-action given by letting a act as the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and b as the matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. The first summand $\mathbb{Z}/2\mathbb{Z}$ of M is the subgroup N of elements of finite additive order.

Let $D = \langle a \rangle$ be the subgroup generated by a. We have $M^V \subset M^{\langle b \rangle} = N$ and $N^V = N$, so $N^D = N = M^V$. Furthermore, one checks that $M^D = (\mathbb{Z}/2\mathbb{Z}) \oplus 2\mathbb{Z}$ and $(M/N)^D = M/N$. It follows that the image of the natural map $M^D \to (M/N)^D$, given by projection onto the second coordinate, is a subgroup of index 2.

3.2 Pila systems

Let A be a ring. We will be interested in certain collections of elements in A indexed by a partially ordered set. We first fix some terminology and notation concerning partially ordered sets.

Let $P = (P, \preceq)$ be a partially ordered set. Given any two elements $p, q \in P$, an element $r \in P$ is called an *infimum* of p and q if for any $s \in P$ one has that $s \preceq p$ and $s \preceq q$ if and only if $s \preceq r$. The element r is clearly uniquely determined by p and q; it will be denoted $p \wedge q$. Dually we define a *supremum* of two elements p and q in P; again it is uniquely determined by p and q, and we denote it by $p \vee q$. A partially ordered set P is called a *lattice* if any two elements have a supremum and an infimum in P. A *lattice homomorphism* $\Psi : P \to Q$ between lattices $(P, \preceq)$ and $(Q, \sqsubseteq)$ is a map of sets such that for any two elements p and q in P one has

$$\Psi(p \vee q) = \Psi(p) \vee \Psi(q), \qquad \Psi(p \wedge q) = \Psi(p) \wedge \Psi(q).$$

Notice that a lattice homomorphism preserves the order, i.e., for any two elements p and q in P one has that $p \preceq q$ implies $\Psi(p) \sqsubseteq \Psi(q)$. A function $\Psi : P \to Q$ is called a *lattice anti-homomorphism* if it interchanges infima and suprema.

Examples 3.3. (1) Any totally ordered set P is a lattice.

(2) Let X be a set. The set of subsets of X is a lattice under the relation $\subset$ of inclusion. The infimum resp. supremum of two subsets S and T of X is given by

$$S \wedge T = S \cap T \text{ and } S \vee T = S \cup T.$$

(3) Let M be a module over a ring. The set of submodules of M is a lattice under $\subset$. Two submodules N and P of M have infimum resp. supremum

$$N \wedge P = N \cap P \text{ and } N \vee P = N + P.$$

The following specialization of example (2) will play an important role in the remainder of this section.

(4) A subset S of a partially ordered set $(P, \preceq)$ is called an *initial segment* if for all $p \in S$ and $q \in P$ with $q \preceq p$ one has $q \in S$. The set of finite initial segments of a partially ordered set is a lattice under $\subset$; infima and suprema are given by the formulae in example (2).

Definition 3.4. [Pil02, Prop 2.5] Let A be a ring. A *Pila system* in A is a pair (P, Z) consisting of a partially ordered set $P = (P, \preceq)$ and a system of elements $Z = (z_p)_{p \in P}$ in A indexed by P such that:

(1) for each $p \in P$, the set $\{q \in P : q \preceq p\}$ is finite;

(2) any two elements $p, q \in P$ have an infimum $p \wedge q$;

(3) for any two elements $p, q \in P$ we have that $Az_p + Az_q = Az_{p \wedge q}$.

Proposition 3.5. *Let (P, Z) be a Pila system in A. Then there is a family $\Sigma = (\sigma_p)_{p \in P}$ of elements of A with the property that*

$$z_p = \prod_{q \preceq p} \sigma_q$$

for all $p \in P$.

Proof. See [Pil02, Prop. 2.5]. □

Examples 3.6. (1) Let P be the set $\mathbb{Z}_{>0}$ together with the partial ordering $|$ of divisibility, and take $A = \mathbb{Z}$. Then a Pila system in A indexed by P is an integer sequence $(a_n)_{n \geq 1}$ such that for all integers $m, n \geq 1$,

$$\gcd(a_m, a_n) = a_{\gcd(m,n)}.$$

Such integer sequences are called *strong divisibility sequences*. Proposition 3.5 asserts that for each strong divisibility sequence (a_n) there exists a sequence of integers (b_n) such that $a_n = \prod_{d|n} b_d$ for each n.

(2) Let A be the polynomial ring $\mathbb{Z}[X]$, and let P be as in the previous example. We have shown that $(X^n - 1)_n$ is a Pila system in A in Lemma 2.5. The family of cyclotomic polynomials $(\Phi_n)_n$ is uniquely determined by the relations $X^n - 1 = \prod_{d|n} \Phi_d$ for $n \in \mathbb{Z}_{>0}$, hence is the unique family satisfying the conclusion of Proposition 3.5.

(3) Let $\phi : A \to B$ be a ring homomorphism. Let P be a partially ordered set. If $(z_p)_{p \in P}$ is a Pila system in A, then $(\phi(z_p))_{p \in P}$ is a Pila system in B. If the family $(\sigma_p)_{p \in P}$ satisfies the conclusion of Proposition 3.5 for the Pila system $(z_p)_{p \in P}$ in A, then the family $(\phi(\sigma_p))_{p \in P}$ does so for the Pila system $(\phi(z_p))_{p \in P}$ in B.

In general the collection Σ in Proposition 3.5 is not uniquely determined by the Pila system (P, Z). However, the following is true. For a finite subset S of P, define the element $\mathfrak{J}_\Sigma(S)$ by

$$\mathfrak{J}_\Sigma(S) = \prod_{p \in S} \sigma_p. \tag{9}$$

Pila showed [Pil02, Prop. 2.6] that if S is a finite initial segment of P, the ideal in A generated by $\mathfrak{J}_\Sigma(S)$ does not depend on the particularly chosen collection Σ satisfying the conclusion of Proposition 3.5. In fact, the element $\mathfrak{J}_\Sigma(S)$ itself is independent of the choice of Σ.

Lemma 3.7. *Let (P, Z) satisfy the hypotheses of Proposition 3.5, and let $\Sigma = (\sigma_p)_{p \in P}$ and $\Sigma' = (\sigma'_p)_{p \in P}$ be two collections satisfying the conclusion of Proposition 3.5. Then for each finite initial segment S of P we have that*

$$\mathfrak{J}_\Sigma(S) = \mathfrak{J}_{\Sigma'}(S). \tag{10}$$

Proof. We proceed by induction on the cardinality $n = \#S$ of S. If $n = 0$, then S is the empty set, and both sides in (10) are equal to the empty product $1 \in A$.

Let $n \geq 1$, and assume (10) proved for all finite initial segments S of P having less than n elements. Let T be a finite initial segment of P having precisely n elements. Let $p \in P$ be a maximal element of T. Then the subsets $T \setminus \{p\}$ and $\{q \in P : q \prec p\}$ are finite initial segments of P of cardinality less than n. By the inductive hypothesis, these two sets satisfy (10), so we may suppress the subscript for them indicating whether they were defined using Σ or Σ'.

Since Σ and Σ' satisfy the conclusion of Proposition 3.5, we have

$$\sigma_p \cdot \mathfrak{J}(\{q \in P : q \prec p) = z_p = \sigma'_p \cdot \mathfrak{J}(\{q \in P : q \prec p\}).$$

Since $\{q \in P : q \prec p\} \subset T \setminus \{p\}$, the element $\mathfrak{J}(\{q \in P : q \prec p\})$ divides $\mathfrak{J}(T \setminus \{p\})$, so

$$\mathfrak{J}_\Sigma(T) = \sigma_p \cdot \mathfrak{J}(T \setminus \{p\}) = \sigma'_p \cdot \mathfrak{J}(T \setminus \{p\}) = \mathfrak{J}_{\Sigma'}(T),$$

completing the inductive step.

The assertion follows by the inductive principle. □

As in the proof of Lemma 3.7, we will henceforth suppress the subscript in (9) in case S is an initial segment of P.

Lemma 3.8. *Let $S, T \subset P$ be finite initial segments. Then $A \cdot \mathfrak{J}(S) + A \cdot \mathfrak{J}(T) = A \cdot \mathfrak{J}(S \cap T)$.*

Proof. Let Σ be a collection satisfying the conclusion of Proposition 3.5. In view of the relations $\mathfrak{J}(S) = \mathfrak{J}_\Sigma(S \setminus T)\mathfrak{J}(S \cap T)$ and $\mathfrak{J}(T) = \mathfrak{J}_\Sigma(T \setminus S)\mathfrak{J}(S \cap T)$, we need only show that $\mathfrak{J}_\Sigma(S \setminus T)$ and $\mathfrak{J}_\Sigma(T \setminus S)$ generate the unit ideal modulo the annihilator ideal of $\mathfrak{J}(S \cap T)$. By definition (9), it suffices to prove the following contention: for each $p \in S \setminus T$ and $q \in T \setminus S$ the elements σ_p and σ_q generate the unit ideal modulo the annihilator ideal of $\mathfrak{J}(S \cap T)$.

Since $p \not\preceq p \wedge q$ and $q \not\preceq p \wedge q$, the defining property (3) of Pila systems $Az_p + Az_q = Az_{p \wedge q}$ yields that the elements σ_p and σ_q generate the unit ideal modulo the annihilator ideal of $z_{p \wedge q}$. Since $p \wedge q \in S \cap T$, the element $z_{p \wedge q}$ divides $\mathfrak{J}(S \cap T)$, whence the annihilator ideal of $z_{p \wedge q}$ is contained in that of $\mathfrak{J}(S \cap T)$. This proves our contention, and finishes the proof. □

3.3 Pila systems and abelian categories

In this section (and in this section only) we do not assume that all our rings are commutative, because we will be encountering some non-commutative endomorphism rings.

Let M be a module over a commutative ring A, and let (P, Z) be a Pila system in A. In Examples 3.3(3–4) we saw that the set of submodules of M, and the set of finite initial segments of P form lattices. The main aim of this section is to prove the following proposition, which relates these two lattices to each other.

For an element $a \in A$ we denote the image and kernel of the multiplication-by-a endomorphism of M by aM resp. $M[a]$.

Proposition 3.9. *Let A be a commutative ring, and let (P, Z) be a Pila system in A. For each finite initial segment S of P, define $\mathfrak{J}(S)$ by (9). Let M be an A-module. Then the function*

$$\begin{aligned} \{\textit{finite initial segments of } P\} &\to \{\textit{submodules of } M\} \\ S &\mapsto M[\mathfrak{J}(S)] \end{aligned}$$

is a lattice homomorphism and the function

$$\{\textit{finite initial segments of } P\} \to \{\textit{submodules of } M\}$$
$$S \mapsto \mathfrak{J}(S) \cdot M$$

is a lattice anti-homomorphism.

In fact, we will prove, as Theorem 3.12 and Corollary 3.14, a generalization of Proposition 3.9 formulated in the context of an action of a commutative ring on an object in an abelian category, and will deduce Proposition 3.9 from this. To state it, we will need to define the analogue of the lattice of submodules of a module, for an object in an abelian category, the so-called *lattice of subobjects*. We will ignore set-theoretical issues.

We conclude this section with a technical result, Proposition 3.15, on certain decompositions of modules that will be used in Section 3.4 to establish Proposition 1.7.

Let $\mathcal{A}$ be an arbitrary category and let X be an object in $\mathcal{A}$. We define the partially ordered set of subobjects of X.

Let $f : Y \to X$ and $g : Z \to X$ be two monomorphisms in $\mathcal{A}$. We say f is *smaller* than g and write $f \leq g$ if there exists a morphism $h : Y \to Z$ such that $f = gh$. It is easy to see that $\leq$ defines a reflexive and transitive relation on the set of monomorphisms into X.

We call two monomorphism f and g into X *equivalent* if both $f \leq g$ and $g \leq f$. An equivalence class of such morphisms is called a *subobject* of X. It is not difficult to see that equivalent monomorphisms have isomorphic domains. By abuse of language, we will often refer to a subobject simply by a monomorphism of its class, or even the domain thereof if the associated monomorphism is clear.

Now $\leq$ descends to a partial order on the set of subobjects of X, which we also denote by $\leq$.

Dually one defines a *quotient object* of X as an equivalence class of epimorphisms $f : X \to Y$ in $\mathcal{A}$. If $g : X \to Z$ is another epimorphism, then we say that f is *greater* than g if g factorises through f. Again this order descends to a partial order on the set of quotient objects of X.

Now assume that $\mathcal{A}$ is an *abelian category*, i.e.:

1. For each pair of objects X and Y, the morphism set $\mathrm{Mor}(X, Y)$ is endowed with the structure of an abelian group such that the composition of morphisms is bilinear with respect to the addition in these groups.
2. Finite products and finite coproducts exist.
3. Each morphism $f : X \to Y$ has a kernel $\ker f$ and a cokernel $\operatorname{cok} f$.
4. For each morphism $f : X \to Y$ the morphism $\operatorname{cok} \ker f \to \ker \operatorname{cok} f$ induced by f is an isomorphism.

Examples 3.10. (1) Let R be a (not necessarily commutative) ring. The category $\mathbf{Mod}_R$ of R-modules with R-linear maps is an abelian category, with addition of homomorphisms being defined pointwise [Par70, Par. 4.2, Example].

(2) By taking $R = \mathbb{Z}$ in the previous example, we see that the category $\mathbf{Ab}$ of abelian groups with homomorphisms of such is an abelian category.

(3) Let $\mathcal{A}$ be an abelian category. Then the opposite category $\mathcal{A}^{\mathrm{opp}}$ of $\mathcal{A}$ is naturally an abelian category, with for objects $A, B \in \mathcal{A}$ the addition in $\mathrm{Hom}_{\mathcal{A}^{\mathrm{opp}}}(B, A)$ corresponding to that in $\mathrm{Hom}_{\mathcal{A}}(A, B)$.

Let R be a ring, and let M be an object of $\mathbf{Mod}_R$, that is, an R-module. A monomorphism in $\mathbf{Mod}_R$ is the same as an injective R-linear map. One checks that two monomorphisms

$f_1 : N_1 \to M$ and $f_2 : N_2 \to M$ are equivalent if and only if they have the same image, i.e., $f_1[N_1] = f_2[N_2]$. Thus to give a subobject of M is to give a submodule of M. Therefore Examples 3.3(3) shows that the subobjects of M constitute a lattice. More generally, this is true for the subobjects (and quotient objects) of an object in an arbitrary abelian category.

Proposition 3.11. *Let X be an object in an abelian category $\mathcal{A}$. The partially ordered set of subobjects in X is a lattice. Dually, the partially ordered set of quotient objects of X is a lattice that is anti-isomorphic to the lattice of the subobjects, via the map that sends a quotient object of X to the equivalence class of the kernel of one of its representatives.*

Since we will proceed using only the universal property of the infimum of two subobjects and of the supremum of two subobjects – not any explicit construction of theirs – we content ourselves with providing a reference for the proof.

Proof of Proposition 3.11. See [Par70, Par. 4.3, Lemma 5]. □

To emphasise the analogy between the lattice of submodules of a module and the lattice of subobjects of an object in an abelian category, in the latter lattice we will by abuse of notation use the symbols $\subset$, $\cap$ and $+$ instead of $\leq$, $\wedge$ resp. $\vee$.

We can now state the main result of this section. By an action of a ring A on an object X in an abelian category $\mathcal{A}$, we mean a ring homomorphism $\phi : A \to \mathrm{End}_{\mathcal{A}}(X)$. This generalises the notion of module: an action of a ring A on an object M in the category **Ab** of abelian groups is just an A-module structure on the abelian group M.

Theorem 3.12. *Let $\mathcal{A}$ be an abelian category and X and object in $\mathcal{A}$. Let $\phi : A \to \mathrm{End}_{\mathcal{A}}(X)$ be an action of a commutative ring on X. Let (P, Z) be a Pila system in A. For each finite initial segment S of P, define $\mathfrak{J}(S)$ by* (9)*. Then the function*

$$\begin{aligned} \{\textit{finite initial segments of } P\} &\to \{\textit{subobjects of } X\} \\ S &\mapsto \ker(\phi[\mathfrak{J}(S)]) \end{aligned}$$

is a lattice homomorphism.

In the proof of Theorem 3.12 we will use the following two facts concerning kernels and images in abelian categories.

Proposition 3.13. *Let $\mathcal{A}$ be an abelian category.*

(1) *Let $f, g : X \to Y$ be two morphisms in $\mathcal{A}$. Then $\mathrm{im}(f+g) \subset \mathrm{im}(f) + \mathrm{im}(g)$ and $\ker(f) \cap \ker(g) \subset \ker(f+g)$.*

(2) *Let $f : X \to Y$ and $g : Y \to Z$ be composable morphisms in $\mathcal{A}$. Then $\ker(f) \subset \ker(gf)$ and $\mathrm{im}(gf) \subset \mathrm{im}(g)$.*

Proof. See [Par70, Par. 4.3, Lemma 6] for the statements about images. The statements for kernels are proved similarly. □

Proof of Theorem 3.12. Applying Examples 3.6(3) to the homomorphism $\phi : A \to \phi(A)$ of commutative rings shows that $\phi(Z)$ is a Pila system in $\phi(A)$. Thus by replacing Z by $\phi(Z)$ and A by $\phi(A)$, we may assume that A is a commutative subring of $\mathrm{End}_{\mathcal{A}}(X)$, and that ϕ is the inclusion map.

Let $S, T \subset P$ be finite initial segments. Write $a = \mathfrak{J}(S \cap T)$, $ab = \mathfrak{J}(S)$, $ac = \mathfrak{J}(T)$; then $abc = \mathfrak{J}(S \cup T)$. By Lemma 3.8 there exist $x, y \in A$ such that $xab + yac = a$. Note that since A

is commutative, the endomorphisms x, y, a, b, c all commute.

We first show that $\ker(\mathfrak{J}(S)) \cap \ker(\mathfrak{J}(T)) = \ker(\mathfrak{J}(S \cap T))$, that is, $\ker(ab) \cap \ker(ac) = \ker(a)$. By Proposition 3.13(2) the subobject $\ker(a)$ is smaller than $\ker(ab)$ and $\ker(ac)$, hence it is smaller than their infimum $\ker(ab) \cap \ker(ac)$. Conversely, since $a = xab + yac$ by Proposition 3.13(1–2) we have that $\ker(ab) \cap \ker(ac) \subset \ker(xab) \cap \ker(yac) \subset \ker(a)$, as desired.

We now show that $\ker(\mathfrak{J}(S)) + \ker(\mathfrak{J}(T)) = \ker(\mathfrak{J}(S \cup T))$, that is, $\ker(ab) + \ker(ac) = \ker(abc)$. By Proposition 3.13(2) the subobject $\ker(abc)$ is greater than $\ker(ab)$ and $\ker(ac)$, hence it is greater than their supremum $\ker(ab) + \ker(ac)$.

For the converse, write $K = \ker(abc)$. Since $xb, abc \in A$ commute, xb restricts to an endomorphism f of K. By Proposition 3.13(1) we have $K = \mathrm{im}(1) = \mathrm{im}(f) + \mathrm{im}(1 - f)$. Thus it suffices to show that $\mathrm{im}(f) \subset \ker(ac)$ and $\mathrm{im}(1 - f) \subset \ker(ab)$.

We first show that $\mathrm{im}(f) \subset \ker(ac)$. We have that $K \to \mathrm{im}(f) \to K \to A \xrightarrow{ac} A = K \xrightarrow{f} K \to A \xrightarrow{ac} A = K \to A \xrightarrow{xb} A \xrightarrow{ac} A = K \to A \xrightarrow{abc} A \xrightarrow{x} A = 0$ since $K = \ker(abc)$. Since $K \to \mathrm{im}(f)$ is an epimorphism, it follows that $\mathrm{im}(f) \to A \xrightarrow{ac} A = 0$. By the universal property of $\ker(ac)$, it follows that $\mathrm{im}(f) \subset \ker(ac)$.

The argument that $\mathrm{im}(1 - f) \subset \ker(ab)$ is similar, noting that

$$ab(1 - xb) = b(a - xab) = b(yac) = y(abc).$$

We conclude that $\ker(abc) = K = \mathrm{im}(f) + \mathrm{im}(1 - f) \subset \ker(ab) + \ker(ac)$, as remained to be shown. □

Corollary 3.14. *Let the notation be as in Theorem 3.12. Then the function*

$$\{\textit{finite initial segments of } P\} \to \{\textit{subobjects of } X\}$$
$$S \mapsto \mathrm{im}(\phi[\mathfrak{J}(S)])$$

is a lattice anti-homomorphism.

Proof. Consider X as object in the opposite category $\mathcal{A}^{\mathrm{opp}}$ of $\mathcal{A}$ (cf. Examples 3.10(3)). Since the ring A is commutative, we have an action $\phi^* : A \to \mathrm{End}_{\mathcal{A}}(X)^{\mathrm{opp}} = \mathrm{End}_{\mathcal{A}^{\mathrm{opp}}}(X)$ of A on the object X in $\mathcal{A}^{\mathrm{opp}}$. By Theorem 3.12 we find that the assignment $S \mapsto \ker(\phi^*[\mathfrak{J}(S)]) = \mathrm{cok}(\phi[\mathfrak{J}(S)])$ induces a lattice homomorphism. Composition with the lattice anti-isomorphism in Proposition 3.11 yields that $S \mapsto \ker \mathrm{cok}(\phi[\mathfrak{J}(S)]) = \mathrm{im}(\phi[\mathfrak{J}(S)])$ defines a lattice anti-homomorphism, as desired. □

We will now use Theorem 3.12 to prove Proposition 3.9, which was stated in the introduction of this section.

Proof of Proposition 3.9. In view of the remark preceding Theorem 3.12, the A-module structure on the abelian group M corresponds to an A-action $\phi : A \to \mathrm{End}_{\mathbf{Ab}}(M)$ on the object M of $\mathbf{Ab}$, which sends $a \in A$ to the endomorphism of M given by multiplication by a. Since $\ker(\phi(a)) = M[a]$ and $\mathrm{im}(\phi(a)) = aM$ for each $a \in A$, the proof is concluded by invoking Theorem 3.12 and Corollary 3.14. □

We conclude this section with the following result, which will be our main tool in proving Theorem 3.17.

Proposition 3.15. *Let the notation be as in Proposition 3.9. Suppose in addition that A is an algebra over a commutative ring K, and that for each $p \in P$ a sub-K-module M_p of M is given such that*

$$M[z_p] = M[\mathfrak{J}(\{q \in P : q \prec p\})] \oplus M_p. \tag{11}$$

Then for each finite initial segment S of P we have

$$M[\mathfrak{J}(S)] = \bigoplus_{p \in S} M_p. \tag{12}$$

Moreover, if K is a Dedekind domain and M is a projective K-module, such a collection $(M_p)_{p \in P}$ exists.

Proof. For the first assertion, let S be a finite initial segment of P, and put $n = \#S$. We show by induction on n that (12) holds. For $n = 0$ our claim is clear. Now let $n \geq 1$ and suppose we have proved that (12) holds for all finite initial segments of P having less than n elements. Let S be a finite initial segment of P having n elements. Let p be a maximal element of S. Let $T = \{q \in P : q \preceq p\}$ and $U = S \setminus \{p\}$. Then $T \cup U = S$ and $T \cap U = \{q \in P : q \prec p\}$. Hence we have by Proposition 3.9 that

$$\ker(\mathfrak{J}(T)) \cap \ker(\mathfrak{J}(U)) = \ker(\mathfrak{J}(T \cap U)), \quad \ker(\mathfrak{J}(T)) + \ker(\mathfrak{J}(U)) = \ker(\mathfrak{J}(S)).$$

Furthermore, by the inductive hypothesis we have

$$\ker(\mathfrak{J}(T)) = \bigoplus_{p \in T} M_p, \quad \ker(\mathfrak{J}(U)) = \bigoplus_{p \in U} M_p, \quad \ker(\mathfrak{J}(T \cap U)) = \bigoplus_{p \in T \cap U} M_p.$$

From this, it follows that

$$\ker(\mathfrak{J}(S)) = \bigoplus_{p \in T \cup U} M_p,$$

whence we have completed the inductive step. The assertion follows by the principle of induction.

Now suppose that M is a projective module over a Dedekind domain K, and let $p \in P$. Multiplication by $j := \mathfrak{J}(\{q \in P : q \prec p\})$ induces an exact sequence of K-modules

$$0 \to M[j] \to M[z_d] \to jM[z_d] \to 0$$

that is split because $jM[z_d]$ is projective as a submodule of the projective K-module M (here we use that K is a Dedekind domain). A splitting yields a submodule M_p of M satisfying (11), as desired. □

We remark that the existence of decompositions (12) in the module M conversely implies that the conclusion of the part of Proposition 3.9 pertaining to kernels holds for M.

3.4 Modules over finite cyclic groups

We specialize Proposition 3.9 and Proposition 3.15 to the context of a module over a finite cyclic group. As a corollary, we deduce the De Bruijn–Rédei theorem.

Let C be a finite cyclic group, n its order and σ a generator of C. Consider the set $P = \{d : d \mid n\}$ with the partial order $\mid$ of divisibility. Let $A = \mathbb{Z}[C]$; using Examples 3.6(2–3) we see that the collection $Z = (z_d)_{d|n} := (\sigma^d - 1)_{d|n}$ is a Pila system in A. The collection $(\Phi_d(\sigma))_{d|n}$ constitutes a family satisfying the conclusion of Lemma 3.7. Now the part of Proposition 3.9 pertaining to kernels reads as follows.

Corollary 3.16. *Let C be a finite cyclic group and M a C-module. Then the mapping*

$$\{\textit{finite initial segments of } P\} \to \{\textit{submodules of } M\}$$
$$S \mapsto M\left[\prod_{d\in S} \Phi_d(\sigma)\right]$$

is a lattice homomorphism.

We remark that if $d \mid n$ and $S = \{e : e \mid d\}$, then $M[\mathfrak{J}(S)] = M[\sigma^d - 1]$ is the set of elements invariant under the action of the subgroup of C of index d.

Non-example. The above corollary shows that for a module M over a finite cyclic group, the lattice generated by $\{M^D : D \text{ is a subgroup of } C\}$ is distributive. For non-cyclic groups, this need not be true. For example, let V be a Klein four-group and let M be the group algebra $(\mathbb{Z}/2\mathbb{Z})[V]$ of V over $\mathbb{Z}/2\mathbb{Z}$, viewed as a V-module. Let I_V be the augmentation ideal of M, that is, the submodule consisting of linear combinations $\sum_{v\in V} a_v v$ with $\sum_{v\in V} a_v = 0$, and let $\mathrm{Tr}_V = \sum_{v\in V} v \in M$.

Let H_1, H_2, H_3 be the three subgroups of order 2 of V. Then each of the modules M^{H_i} of invariants is a 2-dimensional vector space over $\mathbb{Z}/2\mathbb{Z}$ generated by $\sum_{v\in H_i} v$ and Tr_V, and thus included in I_V. Further, for $i \neq j$ one checks that $M^{H_i} + M^{H_j} = I_V$ is of dimension 3 and that $M^{H_i} \cap M^{H_j} = M^{H_iH_j} = M^V$. Thus, we have

$$(M^{H_3} + M^{H_1}) \cap (M^{H_3} + M^{H_2}) = I_V \neq M^{H_3} = M^{H_3} + M^V = M^{H_3} + (M^{H_1} \cap M^{H_2}),$$

whence the lattice is not distributive.

Theorem 3.17. *Let C be a finite cyclic group, n its order and σ a generator for C. Let the Pila system (P, Z) in $\mathbb{Z}[C]$ be defined as at the start of this section. Let M be a C-module whose additive group is free. Then there exists a collection $(M_d)_{d|n}$ of subgroups of M such that each M_d is elementwise invariant under the action of the subgroup of C of index d and the following holds. Let S be a finite initial segment of P. Then*

$$M[\mathfrak{J}(S)] = \bigoplus_{d\in S} M_d. \tag{13}$$

If D is a subgroup of C and d its index, then

$$M^D = \bigoplus_{e|d} M_e.$$

Proof. For the first assertion, we apply Proposition 3.15 with $K = \mathbb{Z}$ and $A = \mathbb{Z}[C]$ to our module M and the Pila system (P, Z) defined as above. Since $\mathbb{Z}$ is a principal ideal domain, and M is free as a $\mathbb{Z}$-module, condition (11) is satisfied. Hence there exists a collection $(M_d)_{d|n}$ of subgroups of M such that (13) is satisfied.

Now let D be a subgroup of C, and d its index. We have that

$$M^D = M[\sigma^d - 1] = M[\mathfrak{J}(\{e \mid d\})] = \bigoplus_{e|d} M_e. \tag{14}$$

Finally, this shows that $M_d \subset M^D$, i.e. the module M_d is elementwise invariant under the action of the subgroup of C of index d. □

We conclude this section by showing that Theorem 3.17 implies the De Bruijn–Rédei theorem.

Alternative proof of Theorem 2.10. The proof consists of applying Theorem 3.17 to $M = \mathbb{Z}[C]$ considered as module over itself. Let $\alpha_p = \sum_{\gamma \in C:\, \gamma^p = 1} \gamma = \sum_{i=0}^{p-1} \sigma^{in/p}$ be as before.

Since

$$(X^{n/p} - 1) \cdot \sum_{i=0}^{p-1} X^{in/p} = X^n - 1 = \Phi_n \cdot \prod_{d|n : d \neq n} \Phi_d \in \mathbb{Z}[X],$$

we have

$$\Phi_n(\sigma)\mathbb{Z}[C] = M \left[\prod_{d|n : d \neq n} \Phi_d(\sigma) \right] = M[\mathfrak{J}(\{d \mid n : d \neq n\})]$$

and

$$M \left[\mathfrak{J} \left(\left\{ d \mid \frac{n}{p} \right\} \right) \right] = M[\sigma^{n/p} - 1] = \alpha_p \mathbb{Z}[C].$$

As $\{d \mid n : d \neq n\} = \bigcup_{p|n \text{ prime}} \{d \mid \frac{n}{p}\}$. we find by 3.17 that

$$\Phi_n(\sigma)\mathbb{Z}[C] = M[\mathfrak{J}(\{d \mid n : d \neq n\})] = \sum_{p|n \text{ prime}} M \left[\mathfrak{J} \left(\left\{ d \mid \frac{n}{p} \right\} \right) \right] = \sum_{p|n \text{ prime}} \alpha_p \mathbb{Z}[C]. \qquad \square$$

3.5 Proof of main results

In this section we prove Theorem 1.4 as Theorem 3.22 and Theorem 1.5 as Theorem 3.21. We make use of the following lemma, due to the German mathematician Kronecker [Kro57, Theorem 2].

Lemma 3.18 (Kronecker)**.** *Let α be a nonzero algebraic integer such that all conjugates of α over $\mathbb{Q}$ in $\mathbb{C}$ lie in the closed unit disk. Then α is a root of unity.*

Proof. Let $f_{\mathbb{Q}}^{\alpha}$ be the minimal polynomial of α over $\mathbb{Q}$, and $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ its degree. Since α is integral over $\mathbb{Z}$, we have $f_{\mathbb{Q}}^{\alpha} \in \mathbb{Z}[X]$. The sum of the absolute values of the coefficients of

$$f_{\mathbb{Q}}^{\alpha} = \prod_{\sigma \in \mathrm{Hom}(\mathbb{Q}(\alpha), \mathbb{C})} (X - \sigma(\alpha))$$

is at most 2^n, since in the product all conjugates $\sigma(\alpha)$ of α have modulus at most 1. We conclude that $f_{\mathbb{Q}}^{\alpha}$ is a polynomial of degree at most n with integral coefficients and that the sum of the absolute values of the coefficients of $f_{\mathbb{Q}}^{\alpha}$ is at most 2^n.

Since for every $m \in \mathbb{Z}_{\geq 0}$ the element α^m also satisfies the hypothesis of this lemma and $[\mathbb{Q}(\alpha^m) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}] = n$, the same conclusion holds for the minimal polynomial $f_{\mathbb{Q}}^{\alpha^m}$ of α^m over $\mathbb{Q}$. There are only finitely many such polynomials, and they have only finitely many roots. Thus we must have $\alpha^m = \alpha^l$ for some integers $m < l$. It follows that $1 = \alpha^{l-m}$, where $l - m > 0$. We conclude that α is a root of unity. $\square$

We call an algebraic extension field K of $\mathbb{Q}$ a *CM-field* if it has a field automorphism ϱ such that for all $x \in K$ and embeddings $\sigma : K \to \mathbb{C}$ we have $\overline{\sigma x} = \sigma \varrho x$. Note that if such a ϱ exists, it is unique and its order equals 1 or 2. Furthermore, the fixed field of ϱ is the maximal totally real subfield K^+ of K. Some authors demand ϱ to have order 2, but we allow ϱ to be the identity, since it allows a more unified treatment of the proof of Theorem 1.4.

Lemma 3.19. [Ste17, Exercise 5.32] *Let K be a number field that is a CM-field, K^+ the maximal totally real subfield of K and ϱ as above. Then there is a group homomorphism $\psi : \mathcal{O}_K^* \to \mu_K$ mapping $u \in \mathcal{O}_K^*$ to $u/\varrho(u)$. It satisfies*

$$\ker \psi = \mathcal{O}_{K^+}^*, \qquad [\mu_K : \psi[\mathcal{O}_K^*]] \cdot [\mathcal{O}_K^* : \mu_K \mathcal{O}_{K^+}^*] = 2.$$

Proof. Let $u \in \mathcal{O}_K^*$. For every embedding $\sigma : K \to \mathbb{C}$ the complex number

$$\sigma\left(\frac{u}{\varrho u}\right) = \frac{\sigma(u)}{\sigma(\varrho(u))} = \frac{\sigma u}{\overline{\sigma u}}$$

has modulus 1. By Lemma 3.18 the element $u/\varrho u$ is a root of unity.

We have $u \in \ker(\psi)$ if and only if $u = \varrho(u)$, that is, $u \in \mathcal{O}_{K^+}^*$.

Since under the induced injection $\mathcal{O}_K^*/\mathcal{O}_{K^+}^* \to \mu_K$ the subgroup $\mu_K/\{\pm 1\} = \mu_K \mathcal{O}_{K^+}^*/\mathcal{O}_{K^+}^*$ has image μ_K^2, we obtain an injective homomorphism $\phi : \mathcal{O}_K^*/\mu_K \mathcal{O}_{K^+}^* \to \mu_K/\mu_K^2$. Since the group μ_K has even order, we find that

$$2 = \#(\mu_K/\mu_K^2) = \#\operatorname{coker}\phi \cdot \#\operatorname{im}\phi = [\mu_K : \psi[\mathcal{O}_K^*]] \cdot [\mathcal{O}_K^* : \mu_K \mathcal{O}_{K^+}^*]. \qquad \square$$

Lemma 3.20. *Let $K/\mathbb{Q}$ be an abelian extension of $\mathbb{Q}$. Then K is a CM-field.*

Proof. Assume that $K \subset \mathbb{C}$. Let ϱ be the restriction of complex conjugation to K and $\sigma : K \to \mathbb{C}$ an arbitrary embedding. Since $K/\mathbb{Q}$ is normal with abelian Galois group, the elements $\varrho, \sigma \in \mathrm{Gal}(K/\mathbb{Q})$ commute. Hence for every $x \in K$ we have that $\overline{\sigma x} = \varrho\sigma x = \sigma\varrho x$. $\square$

We now restate and prove Theorem 1.5.

Theorem 3.21. *Let $K/\mathbb{Q}$ be a finite cyclic extension, and C its Galois group. Let R be an order in K which is stable under the action of C. Then C acts naturally on R^* and R^*/μ_R. Moreover, for every subgroup $D \subset C$ the natural map*

$$(R^*)^D \to (R^*/\mu_R)^D$$

is surjective.

Proof. One verifies readily that the action of C on R fixes the unit group R^* and descends to an action on R^*/μ_R.

First assume that D contains the automorphism ϱ as in the definition of a CM-field. We apply Corollary 3.2 to the C-module $M = R^*$. Since the submodule N of M consisting of the elements of finite order is the group μ_R of roots of unity in R, we are left to show that the hypothesis $(\mu_R)^D = (R^*)^C$ is satisfied. Since we have $\varrho \in D$, the field K^D is totally real, whence its only roots of unity are ± 1. By the Galois correspondence and since R is an order, we have $R^C = \mathbb{Z}$. It follows that

$$(\mu_R)^D = \mu_{R^D} = \{\pm 1\} = \mathbb{Z}^* = (R^C)^* = (R^*)^C. \qquad \square$$

In case D is an arbitrary subgroup of C, we observe that Lemma 3.19 shows that R^*/μ_R is pointwise invariant under ρ. Therefore we can replace D in $(R^*/\mu_R)^D$ by the subgroup generated by $D \cup \{\varrho\}$, thus finishing the proof by the previous case.

Example. Let K be a CM-number field, and K^+ its maximal totally real subfield. By Lemma 3.19 we have $[\mathcal{O}_K^* : \mu_K \mathcal{O}_{K^+}^*] \in \{1, 2\}$. Applying Theorem 3.21 with $R = \mathcal{O}_K$ and $D = \mathrm{Gal}(K/K^+)$ shows that if the extension $K/\mathbb{Q}$ is cyclic, this index equals 1.

Suppose that $K = \mathbb{Q}(\zeta_n)$ with $n > 1$ and $n \not\equiv 2 \bmod 4$. Then $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the maximal totally real subfield of K, and it has ring of integers $\mathcal{O}_{K^+} = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$. We show that the index

$$[\mathcal{O}_K^* : \mu_K \mathcal{O}_{K^+}^*] = [\mathbb{Z}[\zeta_n]^* : \langle \zeta_n \rangle \mathbb{Z}[\zeta_n + \zeta_n^{-1}]^*]$$

equals 1 if n is a prime power, and 2 else.

Suppose $n = p^\alpha$ for some prime p and $\alpha \in \mathbb{Z}_{>0}$. If p is odd, the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*$ is cyclic, and the result follows from Theorem 3.21. To cover the case $p = 2$ as well, we proceed using Lemma 3.19 and show that $\psi[\mathcal{O}_K^*] \neq \mu_K$. Assume the contrary. Then there exists $u \in \mathcal{O}_K^*$ such that $\psi(u) = -\zeta_n$. The element $v = (1 - \zeta_n)u^{-1}$ is contained in K^+ by Lemma 3.19 since $\psi(v) = \psi(1 - \zeta_n)\psi(u)^{-1} = 1$. Since $n > 2$ the field K is quadratic over K^+, whence

$$N_{K^+/\mathbb{Q}}(v)^2 = N_{K/\mathbb{Q}}(v) = N_{K/\mathbb{Q}}(1 - \zeta_n) N_{K/\mathbb{Q}}(u)^{-1} = \Phi_n(1) \cdot \pm 1 = \pm p.$$

Since $\pm p$ is a non-square in $\mathbb{Q}^*$, this gives the desired contradiction.

If n is not a power of a prime, then $1 - \zeta_n \in \mathcal{O}_K*$ as $N_{K/\mathbb{Q}}(1 - \zeta_n) = \Phi_n(1) = 1$, and $\psi(1 - \zeta_n) = -\zeta_n$ generates μ_K. It follows that $\psi[\mathcal{O}_K^*] = \mu_K$, whence by Lemma 3.19 we have $[\mathcal{O}_K : \mu_K \mathcal{O}_{K^+}] = 2$.

We remark that this last example shows that the assumption in Theorem 3.21 that $K/\mathbb{Q}$ be cyclic is irredundant.

We now restate and prove Theorem 1.4. In fact, the result holds for any, not necessarily maximal, order in a cyclic number field that is stable under the action of the Galois group.

Theorem 3.22. *Let $K/\mathbb{Q}$ be a finite cyclic extension and C its Galois group. Let R be an order in K which is stable under the action of C. Then R has a fundamental system of units that contains for each subfield L of K a fundamental system of units for the order $R \cap L$ in L.*

Proof. Let $n = \#C = [K : \mathbb{Q}]$. For each $m \mid n$ write C_m for the subgroup of C having index m. We consider $M = R^*/\mu_R$ as a $\mathbb{Z}[C]$-module. Dirichlet's unit theorem tells us, inter alia, that M is free as an abelian group. By Theorem 3.17 we can take a collection $(M_d)_{d|n}$ of subgroups of M such that for each $m \mid n$

$$M^{C_m} = \bigoplus_{d|m} M_d. \tag{15}$$

Let $m \mid n$. By Galois theory $K_m = K^{C_m}$ is the unique subfield of K having degree m over $\mathbb{Q}$. Using Theorem 3.21 we may identify $(R^{C_m})^*/\mu_{R^{C_m}}$ with $(R^*/\mu_R)^{C_m} = M^{C_m}$. Since $M_m \subset M^{C_m}$ by (15), we can and do lift a $\mathbb{Z}$-basis of M_m to a set H_m of multiplicatively independent units of the ring $R^{C_m} = R \cap K_m$.

We contend that $\bigcup_{d|n} H_d$ is the required fundamental system of units for R. Since $K = K_n$ and $\{K_m : m \mid n\}$ is the set of subfields of K, we are done if we show for each $m \mid n$ that $\bigcup_{d|m} H_d$ is a fundamental system of units for $R \cap K_m$.

So let $m \mid n$. For each $d \mid m$ we have $H_d \subset K_d \subset K_m$, so the set $\bigcup_{d|m} H_d$ consists of units in K_m. Under the map $R^* \to R^*/\mu_R$ the set $\bigcup_{d|m} H_d$ is mapped injectively to a $\mathbb{Z}$-basis of $\bigoplus_{d|m} M_d = M^{C_m} = (R^{C_m})^*/\mu_{R^{C_m}}$. Thus $\bigcup_{d|m} H_d$ is indeed a fundamental system of units for $R^{C_m} = R \cap K_m$, as desired. □

Example. Let ζ_{13} be a root of unity of order 13, and consider the cyclotomic field $K = \mathbb{Q}(\zeta_{13})$ and its ring of integers $R = \mathcal{O}_K = \mathbb{Z}[\zeta_{13}]$. We construct a fundamental system of units for R as in Theorem 3.22, i.e., one that contains a fundamental system of units for the ring of integers of each subfield of K. We mirror the proof of Theorem 3.22.

The extension $K/\mathbb{Q}$ is cyclic of degree 12, with group $C := \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/13\mathbb{Z})^*$, with $a \in (\mathbb{Z}/13\mathbb{Z})^*$ corresponding to the automorphism $\sigma_a : \zeta_{13} \mapsto \zeta_{13}^a$. Since 2 is a primitive root modulo 13, the automorphism $\sigma := \sigma_2$ generates C.

We have that $\mu_R = \mu_K = \langle -\zeta_{13} \rangle$. Let M be the C-module $R^*/\mu_R = \mathbb{Z}[\zeta_{13}]^*/\langle -\zeta_{13} \rangle$. We first give an explicit description of the C-module structure of M.

The real cyclotomic field $K^+ = \mathbb{Q}(\zeta_{13} + \zeta_{13}^{-1})$ has trivial class group, since all its primes have norm $\equiv 0, \pm 1 \bmod 13$ and its Minkowski constant equals $\frac{6!}{6^6}\sqrt{13^5} = 9.40.. < 12$. It follows by [Was12, Lemma 8.1 and Theorem 8.2] that M is generated by the elements

$$\xi_a := \frac{1 - \zeta_{13}^a}{1 - \zeta_{13}} \cdot \mu_R \in M, \quad a \in (\mathbb{Z}/13\mathbb{Z})^*.$$

Theorem 3.21 shows that each ξ_a may be lifted to a totally real unit in K^+. Indeed, if we put $\zeta = \zeta_{13}^7$, then we have

$$\xi_a = \frac{\zeta^a - \zeta^{-a}}{\zeta - \zeta^{-1}} \cdot \mu_R.$$

One verifies that for $a, b \in (\mathbb{Z}/13\mathbb{Z})^*$ we have $\xi_{ab} = \sigma_b(\xi_a)\xi_b$. Since 2 is a primitive root modulo 13, it follows that M is a cyclic $\mathbb{Z}[C]$-module generated by the element

$$\xi_2 = \frac{\zeta^2 - \zeta^{-2}}{\zeta - \zeta^{-1}} \cdot \mu_R = (\zeta + \zeta^{-1})\mu_R.$$

Now let D be the quotient group of C of order 6; then the group ring $\mathbb{Z}[D]$ is naturally a C-module. Let I_D be the $\mathbb{Z}[D]$-ideal generated by $\sum_{\gamma \in D} \gamma$. We contend that there is an isomorphism of C-modules

$$\begin{aligned} \phi : \mathbb{Z}[D]/I_D &\xrightarrow{\sim} M \\ 1 &\mapsto (\zeta + \zeta^{-1})\mu_R. \end{aligned}$$

First, we show the map ϕ is well-defined. Since $\zeta + \zeta^{-1} \in K^+$ is a totally real unit, we have that $\sigma^6(\zeta + \zeta^{-1}) = \zeta + \zeta^{-1}$ and $\prod_{j=0}^5 \sigma^j(\zeta + \zeta^{-1}) = N_{K^+/\mathbb{Q}}(\zeta + \zeta^{-1}) \in \{\pm 1\}$. This shows that the C-homomorphism $\mathbb{Z}[C] \to M$ sending 1 to ξ_2 factorizes through $\mathbb{Z}[C]/(\sigma^6 - 1, \sum_{j=0}^5 \sigma^j) \cong \mathbb{Z}[D]/I_D$ to give a C-linear map $\phi : \mathbb{Z}[D]/I_D \to M$.

The map ϕ is surjective since $\xi_2 = (\zeta + \zeta^{-1})\mu_R$ generates M over $\mathbb{Z}[C]$.

It remains to be shown that ϕ is injective. The totally imaginary field $\mathbb{Q}(\zeta_{13})$ has 6 pairs of complex-conjugate embeddings, so by Dirichlet's unit theorem M has rank $6 - 1 = 5$. Also, it is not difficult to see that $\mathbb{Z}[D]/I_D$ has $\mathbb{Z}$-rank $\#D - 1 = 5$. Since ϕ is surjective and the abelian groups M and $\mathbb{Z}[D]/I_D$ are free of the same finite rank, by a well-known theorem ϕ is injective. This establishes our contention.

We return to the construction of the desired fundamental system of units for R.

Write τ for the image of σ in $\mathbb{Z}[D]/I_D$. Then a decomposition of the C-module $N = \mathbb{Z}[D]/I_D$ as in Theorem 3.17 is given by

$$N_2 = \mathbb{Z}(1 + \tau^2 + \tau^4), \quad N_3 = \mathbb{Z}(1 + \tau^3) \oplus \mathbb{Z}(\tau + \tau^4), \quad N_6 = \mathbb{Z} \cdot 1 \oplus \mathbb{Z}\tau, \quad N_d = 0 \text{ else.}$$

Via ϕ this corresponds to the following decomposition of M as in the proof of Theorem 3.22:

$$\begin{aligned}
M_2 &= \langle(\zeta+\zeta^{-1})(\zeta^4+\zeta^{-4})(\zeta^3+\zeta^{-3})\mu_R\rangle,\\
M_3 &= \langle(\zeta+\zeta^{-1})(\zeta^8+\zeta^{-8})\mu_R\rangle \times \langle(\zeta^2+\zeta^{-2})(\zeta^3+\zeta^{-3})\mu_R\rangle,\\
M_6 &= \langle(\zeta+\zeta^{-1})\mu_R\rangle \times \langle(\zeta^2+\zeta^{-2})\mu_R\rangle,\\
M_d &= 0 \text{ else.}
\end{aligned}$$

For each $m \mid 12$ write C_m for the subgroup of C of index m, and let $K_m = K^{C_m}$ be the subfield of K of degree m over $\mathbb{Q}$. We have $K_m = \mathbb{Q}(\eta_m)$, where $\eta_m = \sum_{k\in C_m} \zeta^k$ is the Gauss period of degree m. For each $m \mid 12$, we lift the above $\mathbb{Z}$-basis for M_m to a set H_m of units in K_m:

$$H_2 = \{1-\eta_2\}, \quad H_3 = \{\sigma^2(\eta_3), \eta_3\}, \quad H_6 = \{\eta_6, \sigma(\eta_6)\}.$$

We conclude that the ring of integers R of $\mathbb{Q}(\zeta_{13})$ has a fundamental system of units

$$R^* = \mu_R \times \langle 1-\eta_2\rangle \times \langle\sigma^2(\eta_3)\rangle \times \langle\eta_3\rangle \times \langle\eta_6\rangle \times \langle\sigma(\eta_6)\rangle$$

that contains a fundamental system of units for the ring of integers of each subfield of $\mathbb{Q}(\zeta_{13})$.

A Appendix on commutative algebra

In this appendix, we state, mostly without proof, several results on localization and on integral extensions that are used in this thesis.

Recall that all rings are assumed to be commutative with 1.

A.1 Integral extensions

Let $A \subset B$ be a ring extension. An element $x \in B$ is called *integral* over A if it is a root of a *monic* polynomial with coefficients in A, i.e., it satisfies an equation

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n = 0,$$

for some positive integer n and $a_1, \ldots, a_n \in A$. The elements of B which are integral over A form a sub-A-algebra C of B; see [AM69, Proposition 5.3]. We say that B is *integral* over A, and call the extension $A \subset B$ integral, if $C = B$.

Proposition A.1. *Let $A \subset B$ be a ring extension. Then B is finitely generated as an A-module if and only if B is finitely generated as an A-algebra and is integral over A.*

Proof. Stated and proved on the first 2 pages of [AM69, Chapter 5]. □

Furthermore, we will use the following lemma.

Lemma A.2. *Let A be a ring and n be a positive integer. For every $i = 1, 2, \ldots, n$ let $A \subset B_i$ be an integral ring extension. Then the diagonal embedding $A \subset \prod_{i=1}^n B_i$ is integral.*

Proof. Let $x = (x_i)_i \in \prod_{i=1}^n B_i$. For every i the ring B_i is integral over A, so there exists a monic polynomial f_i with coefficients in A such that $f_i(x_i) = 0$. Then $f = \prod_{i=1}^n f_i$ is monic as well, and satisfies $f(x_i) = 0$ for every i. It follows that $f(x) = (f(x_i))_i = 0$. This shows that x is integral over A. □

A.2 Localization

Let A be a ring and S a *multiplicatively closed* subset of A, that is to say, a subset of A such that $1 \in S$ and S is closed under multiplication.

Localization of an A-module M with respect to S yields an $S^{-1}A$-module, which we denote by $S^{-1}M$. Furthermore, to a homomorphism $f : M \to N$ of A-modules we assign an $S^{-1}A$-module homomorphism $S^{-1}f : S^{-1}M \to S^{-1}N$ defined by $(S^{-1}f)(m/s) = f(m)/s$ for all $m \in M$ and $s \in S$. It is clear this assignment is functorial, so that localization with respect to S gives rise to a functor from the category of A-modules to the category of $S^{-1}A$-modules. This functor is exact, i.e., transforms exact sequences into exact sequences.

Proposition A.3. *Let $M \xrightarrow{f} N \xrightarrow{g} P$ be an exact sequence of A-modules. Then the induced sequence $S^{-1}M \xrightarrow{S^{-1}f} S^{-1}N \xrightarrow{S^{-1}g} S^{-1}P$ is exact.*

Proof. See [AM69, Proposition 3.3]. □

A submodule N of M corresponds to an exact sequence $0 \to N \to M$. By Proposition A.3 the induced sequence $0 \to S^{-1}N \to S^{-1}M$ is exact as well. Thus we may, and will, identify $S^{-1}N$ with its image $\{n/s \colon n \in N, s \in S\}$ in $S^{-1}M$. In particular, if I is an A-ideal, then $S^{-1}I$ is the $S^{-1}A$-ideal $\{x/s \colon x \in I, s \in S\}$.

Lemma A.4. *Let N and P be submodules of an A-module M, and let I and J be A-ideals. Then*

(i) $S^{-1}(N + P) = S^{-1}N + S^{-1}P$;

(ii) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$;

(iii) $S^{-1}(IM) = (S^{-1}I)(S^{-1}M)$;

(iv) $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$.

Proof. Appling Proposition A.3 to an exact sequence $0 \to N \cap P \to N \oplus P \to N + P \to 0$ establishes (i) and (ii). The assertions (iii) and (iv) follow readily from the definitions. □

Frequently one takes $S = A \setminus \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of A. The ring $S^{-1}A$ is then denoted by $A_\mathfrak{p}$ and called the *localization* of A at $\mathfrak{p}$. The ring $A_\mathfrak{p}$ is local with maximal ideal $\mathfrak{p}A_\mathfrak{p}$. Similarly, we write $M_\mathfrak{p} = S^{-1}M$ and $f_\mathfrak{p} = S^{-1}f$ for the localization at $\mathfrak{p}$ of an A-module M or an A-linear map f.

Many properties of modules and their homomorphisms are local, i.e., they are satisfied if and only if they are 'locally' satisfied. For example, the injectivity and surjectivity of a module homomorphism is a local property.

Lemma A.5. *Let $f : M \to N$ be a homomorphism of A-modules. Then the following are equivalent:*

(i) *$f : M \to N$ is injective (surjective);*

(ii) *$f_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ is injective (surjective) for every prime ideal $\mathfrak{p}$ of A;*

(iii) *$f_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{m}$ is injective (surjective) for every maximal ideal $\mathfrak{m}$ of A.*

Proof. See [AM69, Lemma 3.9]. □

Moreover, equality of submodules is a local property.

Lemma A.6. *Let M be an A-module. Then for two submodules N and P of M the following are equivalent:*

(i) $N = P$;

(ii) $N_\mathfrak{p} = P_\mathfrak{p}$ *for every prime ideal* $\mathfrak{p}$ *of* A;

(iii) $N_\mathfrak{m} = P_\mathfrak{m}$ *for every maximal ideal* $\mathfrak{m}$ *of* A.

Proof. (i) $\implies$ (ii): Trivial.
(ii) $\implies$ (iii): A maximal ideal is prime.
(iii) $\implies$ (i): It suffices to show that $N \subset P$ if and only if $N_\mathfrak{m} \subset P_\mathfrak{m}$ for every maximal ideal $\mathfrak{m}$.

The inclusion $N \subset P$ is equivalent to the surjectivity of the natural map $P \to P + N$. By the equivalence (i) $\iff$ (iii) of Lemma A.5 and by Lemma A.4(i), this map is surjective if and only if the natural map $P_\mathfrak{m} \to (P+N)_\mathfrak{m} = P_\mathfrak{m} + N_\mathfrak{m}$ is surjective for every maximal ideal $\mathfrak{m}$, i.e., if and only if $N_\mathfrak{m} \subset P_\mathfrak{m}$ for every maximal ideal $\mathfrak{m}$. □

Furthermore, integrality of a ring extension is a local property. This is a corollary of the following lemma.

Lemma A.7. *Let $A \subset B$ be rings and C the integral closure of A in B. Let S be a multiplicative subset of A. Then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

Proof. See [AM69, Proposition 5.12]. □

Lemma A.8. *Let $A \subset B$ be rings. Then the following are equivalent:*

(i) B *is integral over* A;

(ii) $B_\mathfrak{p}$ *is integral over* $A_\mathfrak{p}$ *for every prime ideal* $\mathfrak{p}$ *of* A;

(iii) $B_\mathfrak{m}$ *is integral over* $A_\mathfrak{m}$ *for every maximal ideal* $\mathfrak{m}$ *of* A.

Proof. Left to the reader, using Lemma A.6 and Lemma A.7. □

References

[AM69] M. F. Atiyah and I.G. MacDonald. *Introduction to commutative algebra.* Addison–Wesley, 1969.

[DB53] N.G. de Bruijn. On the factorization of cyclic groups. *Nederl. Akad. Wetensch. Proc. Ser. A*, 61(4):370–377, 1953.

[KM85] N.M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves.* Princeton University Press, 1985.

[Kro57] L. Kronecker. Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten. *J. Reine Angew. Math.*, 1857(53):173–175, 1857.

[Lat34] C.G. Latimer. On the units in a cyclic field. *Amer. J. Math.*, 56(1/4):69–74, 1934.

[Len77] H.W. Lenstra. *Euclidische getallenlichamen.* PhD thesis, Universiteit van Amsterdam, 1977.

[Mol12] V. Moll. *Numbers and functions.* American Mathematical Society, 2012.

[Par70] B. Pareigis. *Categories and functors.* Academic Press, New York, 1970.

[Pil02] J. Pila. Concordant sequences and concordant entire functions. *Rend. Circ. Mat. Palermo*, 51(1):51–82, 2002.

[Ré50] L. Rédei. Ein Beitrag zum Problem der Faktorisation von endlichen Abelschen Gruppen. *Acta Math. Acad. Sci. Hungar.*, 1(2–4):197–207, 1950.

[Ste17] P. Stevenhagen. *Number rings.* Universiteit Leiden, 2017.

[Was12] L.C. Washington. *Introduction to cyclotomic fields.* Springer, 2012.