Universiteit
Leiden
The Netherlands

Decompositions in algebra

Gent, D.M.H. van

Citation
Gent, D. M. H. van. (2024, March 5). *Decompositions in algebra*. Retrieved from https://hdl.handle.net/1887/3720065

Version:	Publisher's Version
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/3720065

Note: To cite this publication please use the final published version (if applicable).

CHAPTER 6

Roots of ideals in number rings

6.1 Introduction

Let R be an order, not necessarily in a number field. A *fractional ideal* of R is a finitely generated R-submodule $\mathfrak{a} \subseteq \mathbb{Q}R$ such that $\mathbb{Q}\mathfrak{a} = \mathbb{Q}R$. For fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ of R we write $\mathfrak{a} + \mathfrak{b}$ and $\mathfrak{a} \cdot \mathfrak{b}$ for the R-submodule of $\mathbb{Q}R$ given by $\{a + b \mid a \in \mathfrak{a},\, b \in \mathfrak{b}\}$ and generated by $\{ab \mid a \in \mathfrak{a},\, b \in \mathfrak{b}\}$ respectively. We say a fractional ideal $\mathfrak{a}$ of R is *invertible* if there exists a fractional ideal $\mathfrak{a}^{-1}$ of R such that $\mathfrak{a}\mathfrak{a}^{-1} = R$, and we write $\mathcal{I}(R)$ for the group of invertible fractional ideals of R.

Any fractional ideal of R is a free abelian group of the same rank as R, and we will encode a fractional ideal of R by a $\mathbb{Z}$-basis in $\mathbb{Q}R$. Using standard techniques as in [5], it is possible to compute $\mathfrak{a} \cap \mathfrak{b}$, $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{a} \cdot \mathfrak{b}$ and $\mathfrak{a}^{-1}$ in polynomial time on input R, $\mathfrak{a}$ and $\mathfrak{b}$. This chapter we dedicate to the computation of another elementary operation, namely taking roots of fractional ideals.

A fractional R-ideal can have multiple n-th roots as $\mathcal{I}(R)$ can have non-trivial torsion, while if R is the maximal order the n-th root is unique if it exists. This makes it impossible to produce such a root functorially under isomorphisms; see Example 6.7.6. Instead we solve the following problem.

Theorem 6.7.3. *There exists a polynomial-time algorithm that, given an order R in a number field and fractional ideal $\mathfrak{a}$ of R, computes the maximal $n \in \mathbb{Z}_{\geq 0}$ with respect to divisibility for which there exist an order $R \subseteq S \subseteq \mathbb{Q}R$ and fractional ideal $\mathfrak{b}$ of S such that $\mathfrak{b}^n = S\mathfrak{a}$, where $\mathfrak{b}^0 := S$, and additionally computes such S and $\mathfrak{b}$. The output of this algorithm is functorial under isomorphisms of R.*

If a fractional R-ideal $\mathfrak{a}$ has an n-th root say $\mathfrak{b}$, then the S-ideal $S\mathfrak{a}$ also has an n-th root, namely $S\mathfrak{b}$, for any order $R \subseteq S \subseteq \mathbb{Q}R$. However, if $S\mathfrak{a}$ has an n-th root for some S, then $\mathfrak{a}$ does not need to have an n-th root; see Example 6.7.5.

A maximal order in a number field has unique prime factorization of ideals. However, we cannot expect to compute in polynomial time, given an ideal $\mathfrak{a}$ of a number ring R, the set of prime ideals $\mathfrak{a} \subseteq \mathfrak{p}$ of R, for the same reason that factorization of integers is considered hard. An often good enough substitute is a coprime factorization: For a set X of ideals of R, we compute a set C of pairwise coprime invertible proper ideals so that every ideal of X is a (necessarily unique) product of ideals of C, potentially enlarging the order R in the process as in Theorem 6.7.3. We say C is *reduced* if $\langle C \rangle$ is a direct summand of $\mathcal{I}(R)$. For finite C this is equivalent to the elements of C having no proper roots in $\mathcal{I}(R)$. For orders $R \subseteq S \subseteq \mathbb{Q}R$ and a set X of fractional ideals of R we write $S \cdot X = \{S\mathfrak{a} \mid \mathfrak{a} \in X\}$, and we say

C is *strongly reduced* if $S \cdot C$ is reduced for every order $R \subseteq S \subseteq \mathbb{Q}R$. Using the previous theorem we may compute strongly reduced coprime bases.

Theorem 6.8.5. *There exists a polynomial-time algorithm that, given a order R in a number field and a finite set X of fractional ideals contained in R, computes an order $R \subseteq S \subseteq \mathbb{Q}R$ such that $S \cdot X$ has a strongly reduced coprime basis and computes such a coprime basis. The output of this algorithm is functorial under isomorphisms of R.*

For both theorems we produce an order S functorially, so one can wonder whether this S has a compact definition other than it being the output of the algorithm, as will be the case in Theorem 6.2.5 and Theorem 6.4.8. However, we were unable to find such a description.

6.2 Fractional ideals

Let R be a commutative ring. We say $x \in R$ is *regular* if multiplication by x is injective and *invertible* if it is surjective. Let S be the set of regular elements of R. Then S is a multiplicatively closed set, and we write $\mathrm{Q}(R) = S^{-1}R$, the localization of R by S, for the *total ring of fractions* of R. The natural map $R \to \mathrm{Q}(R)$ is an injective ring homomorphism, and we treat it as an inclusion. If R is a reduced order, then $\mathrm{Q}(R) = \mathbb{Q}R$. If $R \subseteq S \subseteq \mathrm{Q}(R)$ are (sub)rings, then $\mathrm{Q}(S) = \mathrm{Q}(R)$.

For R-submodules $\mathfrak{a}, \mathfrak{b} \subseteq \mathrm{Q}(R)$ we write $\mathfrak{a} + \mathfrak{b} = \{a + b \,|\, a \in \mathfrak{a},\, b \in \mathfrak{b}\}$, write $\mathfrak{a} \cdot \mathfrak{b}$ or $\mathfrak{a}\mathfrak{b}$ for the additive group generated by $\{ab \,|\, a \in \mathfrak{a},\, b \in \mathfrak{b}\}$ and write $\mathfrak{a} : \mathfrak{b} = \{x \in \mathrm{Q}(R) \,|\, x\mathfrak{b} \subseteq \mathfrak{a}\}$. A *fractional ideal* of R, which is not necessarily an ideal of R, is a finitely generated R-submodule $\mathfrak{a} \subseteq \mathrm{Q}(R)$ such that $\mathrm{Q}(R) \cdot \mathfrak{a} = \mathrm{Q}(R)$. An *invertible ideal* of R is a fractional ideal $\mathfrak{a}$ of R for which there exists an R-submodule $\mathfrak{b} \subseteq \mathrm{Q}(R)$ such that $\mathfrak{a}\mathfrak{b} = R$.

Lemma 6.2.1. *Let R be a commutative ring with fractional ideal $\mathfrak{a}$. Then $\mathfrak{a}$ contains a regular element of R.*

Proof. Since $\mathrm{Q}(R)\mathfrak{a} = \mathrm{Q}(R)$ we may write $\sum_{k=1}^{n}(r_k/s_k) \cdot a_k = 1$ for some $n \in \mathbb{Z}_{\geq 0}$, $r_k, s_k \in R$ and $a_k \in \mathfrak{a}$ with s_k regular. Multiplying this equation by the regular element $s = \prod_{k=1}^{n} s_k$ we obtain $\mathfrak{a} \ni \sum_{k=1}^{n} r_k(s/s_k)a_k = s$. □

Lemma 6.2.2. *Let R be a commutative ring and suppose $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$ are fractional ideals of R. Then*

1. *R, $\mathfrak{a} + \mathfrak{b}$ and $\mathfrak{a}\mathfrak{b}$ are fractional ideals of R;*
2. *$(\mathfrak{a} + \mathfrak{b})\mathfrak{c} = \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}$ and $\mathfrak{a} : R = \mathfrak{a}$;*
3. *If $\mathfrak{b} \subseteq \mathfrak{c}$, then $\mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{a} + \mathfrak{c}$, $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{c}$, $\mathfrak{b} : \mathfrak{a} \subseteq \mathfrak{c} : \mathfrak{a}$ and $\mathfrak{a} : \mathfrak{b} \supseteq \mathfrak{a} : \mathfrak{c}$;*
4. *We have $\mathfrak{c}(R : \mathfrak{c}) = R$ if and only if $\mathfrak{c}$ is invertible;*

5. *If* $\mathfrak{c}$ *is invertible, then* $\mathfrak{ac} : \mathfrak{bc} = \mathfrak{a} : \mathfrak{b}$, $\mathfrak{a} : \mathfrak{c} = \mathfrak{a}(R : \mathfrak{c})$, *and* $\mathfrak{ac} \subseteq \mathfrak{bc}$ *implies* $\mathfrak{a} \subseteq \mathfrak{b}$*;*
6. *If* R *is Noetherian or* $\mathfrak{c}$ *is invertible, then* $\mathfrak{a} : \mathfrak{c}$ *is a fractional ideal;*
7. *If* $\mathfrak{a}$ *is of the form* Ra *for some unit* $a \in \mathrm{Q}(R)$*, then* $\mathfrak{a}$ *is invertible. If* R *is semi-local, then the converse also holds.* □

Proof. We will prove the non-trivial parts.

4. If $\mathfrak{cd} = R$ for some $\mathfrak{d}$, then $\mathfrak{d} \subseteq R : \mathfrak{c}$ and $R = \mathfrak{cd} \subseteq \mathfrak{c}(R : \mathfrak{c}) \subseteq R$, so we have equality throughout. Suppose $\mathfrak{c}(R : \mathfrak{c}) = R$. It suffices to show that $R : \mathfrak{c}$ is finitely generated. We have $1 = \sum_{i \in I} c_i d_i$ for some finite set I and $c_i \in \mathfrak{c}$ and $d_i \in R : \mathfrak{c}$. If $x \in R : \mathfrak{c}$, then $x = \sum_{i \in I}(c_i x)d_i \in \sum_{i \in I} Rd_i$, so the d_i generate $R : \mathfrak{c}$.

5. Write $\mathfrak{d} = R : \mathfrak{c}$. Note that $\mathfrak{a} : \mathfrak{b} \subseteq \mathfrak{ae} : \mathfrak{be}$ for all $\mathfrak{e}$. Hence $\mathfrak{a} : \mathfrak{b} \subseteq \mathfrak{ac} : \mathfrak{bc} \subseteq \mathfrak{acd} : \mathfrak{bcd} = \mathfrak{a} : \mathfrak{b}$, so we have equality throughout. Using this we have $\mathfrak{a} : \mathfrak{c} = \mathfrak{ad} : \mathfrak{cd} = \mathfrak{ad} : R = \mathfrak{ad}$. Note that $\mathfrak{e} \subseteq \mathfrak{f}$ is equivalent to $R \subseteq \mathfrak{f} : \mathfrak{e}$, from which one then deduces the last statement.

6. We have $cR \subseteq \mathfrak{c}$ for some $c \in \mathrm{Q}(R)^*$ by Lemma 6.2.1, so $\mathfrak{a} : \mathfrak{c} \subseteq \mathfrak{a} : cR = \frac{1}{c}\mathfrak{a}$. Assuming R is Noetherian, $\mathfrak{a} : \mathfrak{c}$ is Noetherian because $\frac{1}{c}\mathfrak{a} \cong \mathfrak{a}$ is Noetherian. If $\mathfrak{c}$ is invertible, then $\mathfrak{a} : \mathfrak{c} = \mathfrak{a}(R : \mathfrak{c})$ is fractional.

7. For all maximal ideals $\mathfrak{m}$ choose $a_\mathfrak{m} \in \mathfrak{a}$ and $b_\mathfrak{m} \in R : \mathfrak{a}$ so that $a_\mathfrak{m} b_\mathfrak{m} \in R \setminus \mathfrak{m}$, and choose $\lambda_\mathfrak{m} \in R \setminus \mathfrak{m}$ with $\lambda_\mathfrak{m} \in \mathfrak{n}$ for all maximal $\mathfrak{n} \neq \mathfrak{m}$. Then $a = \sum_\mathfrak{m} \lambda_\mathfrak{m} a_\mathfrak{m} \in \mathfrak{a}$ and $b = \sum_\mathfrak{m} \lambda_\mathfrak{m} b_\mathfrak{m} \in R : \mathfrak{a}$ satisfy $ab \equiv \lambda_\mathfrak{m}^2 a_\mathfrak{m} b_\mathfrak{m} \not\equiv 0 \pmod{\mathfrak{m}}$ for all $\mathfrak{m}$. Hence $ab \in R^*$ and $a \in \mathrm{Q}(R)^*$. Finally $\mathfrak{a} = ab\mathfrak{a} \subseteq a(R : \mathfrak{a})\mathfrak{a} = aR \subseteq \mathfrak{a}$ and we have equality throughout. □

If $\mathfrak{a}$ is an invertible ideal of R, we write $\mathfrak{a}^{-1} = R : \mathfrak{a}$ for the unique R-submodule of $\mathrm{Q}(R)$ such that $\mathfrak{a}\mathfrak{a}^{-1} = R$. We write $\mathcal{I}(R)$ for the set of invertible ideals of R, which by Lemma 6.2.2 is closed under taking inverses, and is thus a group under multiplication.

Example 6.2.3. The group $\mathcal{I}(R)$ can contain non-trivial torsion for an order R in a number field.

Consider $R = \mathbb{Z}[2\mathrm{i}]$. Then $\mathrm{i} \in \mathbb{Q}R \setminus R$ is a fourth root of unity, hence $\mathrm{i}R \in \mathcal{I}(R)$ is non-trivial torsion. More generally, for orders $R \subseteq S \subseteq \mathbb{Q}R$ the group S^*/R^* is torsion and the natural map to $\mathcal{I}(R)$ is injective.

Lemma 6.2.4. *Let* $R \subseteq S \subseteq \mathrm{Q}(R)$ *be commutative (sub)rings. There is a map from the set of fractional ideals of* R *to the set of fractional ideals of* S *that sends* $\mathfrak{a}$ *to* $S\mathfrak{a}$*, and it preserves inverses of invertible ideals and respects addition and multiplication.* □

Theorem 6.2.5. *There exists a polynomial-time algorithm that, given an order R in a number field and a fractional R-ideal $\mathfrak{a}$, computes the unique minimal order $R \subseteq S \subseteq \mathbb{Q}R$ such that $S\mathfrak{a}$ is invertible.*

Proof. In [8] it is shown that $S\mathfrak{a}$ is invertible for the order $S = \mathfrak{a}^n : \mathfrak{a}^n$ with $n = [K : \mathbb{Q}] - 1$. Any order $R \subseteq T \subseteq \mathbb{Q}R$ where $T\mathfrak{a}$ is invertible satisfies $S = \mathfrak{a}^n : \mathfrak{a}^n \subseteq T(\mathfrak{a}^n : \mathfrak{a}^n) \subseteq (T\mathfrak{a}^n) : (T\mathfrak{a}^n) = T$, so S is the unique minimum. □

Theorem 6.2.5 probably also holds when R is any order, with essentially the same proof. This generalization would be sufficient to prove generalizations to general orders for all algorithmic theorems in this chapter.

6.3 Lengths of modules

Let R be a commutative ring and M a R-module. A *chain* in M is a set of submodules of M that is totally ordered by inclusion. We define the *length* of M to be

$$\ell_R(M) = \sup\{\#C \mid C \text{ a chain in } M\} - 1 \in \mathbb{Z}_{\geq 0} \cup \{\infty\}.$$

Note that we do not distinguish between infinite cardinal numbers. Similarly we define the *Krull dimension* of R to be

$$\dim(R) = \sup\{\#C \mid C \text{ a chain in } R \text{ of prime ideals}\} - 1.$$

Note that $\ell_R(0) = 0$ and $\dim(0) = -1$. We say M has finite length if $\ell_R(M) < \infty$, which is equivalent to M being both Noetherian and Artinian. For a prime ideal $\mathfrak{p} \subseteq R$ write $R_\mathfrak{p}$ for the localization of R at $\mathfrak{p}$ and $M_\mathfrak{p} = R_\mathfrak{p} \otimes_R M$. If M has finite length we write

$$[M]_R = \left(\ell_{R_\mathfrak{m}}(M_\mathfrak{m})\right)_\mathfrak{m} \in \mathbb{Z}_{\geq 0}^{(\max \operatorname{spec} R)}.$$

where $\max \operatorname{spec} R$ is the set of maximal ideals of R.

Lemma 6.3.1 (Theorem 2.13 in [12])**.** *Let R be a commutative ring and $N \subseteq M$ be R-modules. Then $\ell_R(M) = \ell_R(N) + \ell_R(M/N)$ and*

$$\ell_R(M) = \sum_{\mathfrak{m} \subseteq R} \ell_{R_\mathfrak{m}}(M_\mathfrak{m}),$$

where the sum ranges over all maximal ideals $\mathfrak{m}$. □

Lemma 6.3.2. *Let R be a Noetherian commutative ring. If $\dim(R) \leq 1$, then for every fractional R-ideal $\mathfrak{a} \subseteq R$ the R-module $R/\mathfrak{a}$ has finite length.*

Proof. Write $\mathrm{chain}(R)$ for the set of chains of prime ideals of R. The primes of $R/\mathfrak{a}$ correspond to the primes of R containing $\mathfrak{a}$, so we get a surjective map $f\colon \mathrm{chain}(R) \to \mathrm{chain}(R/\mathfrak{a})$ that discards primes not containing $\mathfrak{a}$. Minimal prime ideals contain no regular elements (Theorem 3.1 in [12]), while $\mathfrak{a}$ does (Lemma 6.2.1). Maximal elements of $\mathrm{chain}(R)$ contain a minimal prime, which gets discarded by f. Hence $\dim(R/\mathfrak{a}) \leq \dim(R) - 1 \leq 0$. It then follows from Corollary 9.1 in [12] that $R/\mathfrak{a}$ has finite length. □

Examples of a Noetherian commutative ring with Krull dimension at most 1 include any order and its localizations.

Proposition 6.3.3. *Let $R \subseteq S \subseteq \mathrm{Q}(R)$ be commutative (sub)rings. If $\dim(R) \leq 1$ and $\ell_R(S/R) < \infty$, then for all invertible ideals $\mathfrak{a} \subseteq R$ we have $[S/S\mathfrak{a}]_R = [R/\mathfrak{a}]_R$.*

Proof. It suffices to prove for local R that $\ell(S/S\mathfrak{a}) = \ell(R/\mathfrak{a})$. In this case $\mathfrak{a} = \alpha R$ for some regular $\alpha \in R$. Note that the map $S/R \to S\mathfrak{a}/\mathfrak{a}$ given by $x \mapsto \alpha x$ is an isomorphism since α is regular in S. We conclude that $\ell(S\mathfrak{a}/\mathfrak{a}) = \ell(S/R) < \infty$. We have exact sequences of R-modules

$$0 \to R/\mathfrak{a} \to S/\mathfrak{a} \to S/R \to 0 \quad \text{and} \quad 0 \to S\mathfrak{a}/\mathfrak{a} \to S/\mathfrak{a} \to S/S\mathfrak{a} \to 0.$$

Hence $\ell(R/\mathfrak{a}) + \ell(S/R) = \ell(S\mathfrak{a}/\mathfrak{a}) + \ell(S/S\mathfrak{a})$ by Lemma 6.3.2. □

Example 6.3.4. With the notation as in Proposition 6.3.3, the R-modules $R/\mathfrak{a}$ and $S/S\mathfrak{a}$ need not be isomorphic. In fact, if R and S are orders, then the modules need not even be isomorphic over $\mathbb{Z}$.

Take $R = \mathbb{Z}[2\mathrm{i}]$ and $S = \mathbb{Z}[\mathrm{i}]$ with $\mathfrak{a} = 2\mathrm{i}R$, which is clearly invertible. Then $R/\mathfrak{a} \cong \mathbb{Z}/4\mathbb{Z}$ and $S/S\mathfrak{a} \cong (\mathbb{Z}/2\mathbb{Z})^2$ as $\mathbb{Z}$-modules, which are non-isomorphic.

Lemma 6.3.5. *Let R be a commutative ring with fractional ideals $\mathfrak{a} \subseteq \mathfrak{b}$. Then there exists some regular $r \in R$ such that $r\mathfrak{b} \subseteq \mathfrak{a}$. If R is Noetherian with $\dim(R) \leq 1$, then $\ell_R(\mathfrak{b}/\mathfrak{a}) < \infty$.*

Proof. We may choose generators $r_1/s_1, \ldots, r_n/s_n \in \mathrm{Q}(R)$ of $\mathfrak{b}$. Then $y = \prod_i s_i$ is regular and satisfies $y\mathfrak{b} \subseteq R$. By Lemma 6.2.1 there exists some regular $x \in R$ such that $xR \subseteq \mathfrak{a}$. Hence we may take $r = xy$. We have a surjection $\mathfrak{b}/xR \to \mathfrak{b}/\mathfrak{a}$, so it suffices to show $\ell_R(\mathfrak{b}/xR) < \infty$. The injection $\mathfrak{b}/xR \to \frac{1}{y}R/xR$ and the fact that $\frac{1}{y}R/xR \cong R/xyR$ has finite length by Lemma 6.3.2 finish the proof. □

As a consequence of Lemma 6.3.5, every fractional ideal $\mathfrak{a}$ of R can be written as $\mathfrak{b} : \mathfrak{c}$ for some ideals $\mathfrak{b}, \mathfrak{c} \subseteq R$ with $\mathfrak{c}$ invertible: As $r\mathfrak{a} \subseteq R$ for some regular r we may take $\mathfrak{b} = r\mathfrak{a}$ and $\mathfrak{c} = rR$. Under additional invertibility assumptions we may even take $\mathfrak{b}$ and $\mathfrak{c}$ coprime.

Lemma 6.3.6. *Let R be a commutative ring and let $\mathfrak{a}$ be a fractional R-ideal such that $\mathfrak{a}$ and $R + \mathfrak{a}$ are invertible. Then $R + \mathfrak{a}^{-1}$ is invertible and $\mathfrak{b} = (R + \mathfrak{a}^{-1})^{-1}$ and $\mathfrak{c} = (R + \mathfrak{a})^{-1}$ satisfy (1) $\mathfrak{b}, \mathfrak{c} \subseteq R$; (2) $\mathfrak{b} + \mathfrak{c} = R$ and (3) $\mathfrak{a} = \mathfrak{b} : \mathfrak{c}$.*

Proof. Note that $R + \mathfrak{a}^{-1} = \mathfrak{a}^{-1}(R + \mathfrak{a})$ is invertible. Rearranging gives $\mathfrak{a} = (R + \mathfrak{a}) : (R + \mathfrak{a}^{-1}) = \mathfrak{b} : \mathfrak{c}$. We have $\mathfrak{b} + \mathfrak{c} = \mathfrak{a}\mathfrak{c} + \mathfrak{c} = (\mathfrak{a} + R)\mathfrak{c} = R$. In particular, we have $\mathfrak{b}, \mathfrak{c} \subseteq R$. □

Proposition 6.3.7. *There exists a polynomial-time algorithm that, given an order R in a number field and an invertible ideal $\mathfrak{a}$ of R, decides whether $\mathfrak{a}$ is torsion, and if so computes the minimal order $R \subseteq S \subseteq \mathbb{Q}R$ such that $S\mathfrak{a} = S$.*

Proof. We compute using Theorem 6.2.5 the minimal order $R \subseteq S \subseteq \mathbb{Q}R$ where $R + \mathfrak{a}$ becomes invertible. We claim $\mathfrak{a}$ is torsion if and only if $S\mathfrak{a} = S$.

($\Rightarrow$) As $S\mathfrak{a}$ is the quotient of $\mathfrak{b} = (S + (S\mathfrak{a})^{-1})^{-1}$ and $\mathfrak{c} = (S + S\mathfrak{a})^{-1}$ as in Lemma 6.3.6 with $\mathfrak{b} + \mathfrak{c} = S$, the ideal $S\mathfrak{a}$ is torsion if and only if $\mathfrak{b}$ and $\mathfrak{c}$ are. However, since $\mathfrak{b}, \mathfrak{c} \subseteq S$, this is only possible if $\mathfrak{b} = \mathfrak{c} = S$. Hence $S\mathfrak{a} = S : S = S$.

($\Leftarrow$) Let $k \in \mathbb{Z}_{>0}$. For $x \in R : S$ we have $xS = xS\mathfrak{a}^k \subseteq R\mathfrak{a}^k = \mathfrak{a}^k$, so $x \in \mathfrak{a}^k$. Hence $R : S \subseteq \mathfrak{a}^k \subseteq S$. By Lemma 6.3.5 the R-module $S/(R : S)$ has finite length, so in particular it is a finite group. Thus $\mathfrak{a}^k$ can take only finitely many values, so by invertibility $\mathfrak{a}$ must be torsion.

Finally, suppose that $\mathfrak{a}$ is torsion and $R \subseteq T \subseteq \mathbb{Q}R$ is an order such that $T\mathfrak{a} = T$. Then $T(R + \mathfrak{a}) = T$ is invertible, so $S \subseteq T$. Hence S is the unique minimal order where $S\mathfrak{a} = S$. □

6.4 Coprime bases

It is easy to see that for a set C of pairwise coprime invertible proper ideals of a commutative ring R the natural map $\mathbb{Z}^{(C)} \to \mathcal{I}(R)$ is injective with image $\langle C \rangle$ and that $\langle C \rangle$ is closed under addition. In fact, $\mathbb{Z}^{(C)} \to \langle C \rangle$ is an isomorphism of partially ordered groups.

Lemma 6.4.1. *There exists a polynomial-time algorithm that, given a reduced order R and a finite set C of pairwise coprime invertible proper ideals*

of R and some invertible ideal $\mathfrak{a}$ of R, decides whether $\mathfrak{a}$ is in the image of the injection $\mathbb{Z}^{(C)} \to \mathcal{I}(R)$ and if so computes the preimage.

Proof. First verify whether $R+\mathfrak{a}$ is invertible, as it should be if $\mathfrak{a} \in \langle C \rangle$. If so, then by Lemma 6.3.6 we may write $\mathfrak{a} = \mathfrak{b} : \mathfrak{c}$ for invertible $\mathfrak{b}, \mathfrak{c} \subseteq R$. We then proceed using trial division. □

Definition 6.4.2. Given a commutative ring R and a set X of fractional ideals contained in R, we write $\langle\langle X \rangle\rangle$ for the multiplicative monoid generated by X with unit R, and we define the *closure of* X, written $\mathrm{cl}_R(X)$ or simply $\mathrm{cl}(X)$, to be the smallest set of fractional ideals in R such that $\langle\langle X \rangle\rangle \subseteq \mathrm{cl}(X)$ and for all $\mathfrak{a}, \mathfrak{b} \in \mathrm{cl}(X)$ we have $\mathfrak{ab}, \mathfrak{a}+\mathfrak{b} \in \mathrm{cl}(X)$, and if $\mathfrak{b}$ is invertible and $\mathfrak{a} : \mathfrak{b} \subseteq R$ also $\mathfrak{a} : \mathfrak{b} \in \mathrm{cl}(X)$.

From Lemma 6.2.4 we deduce the following.

Lemma 6.4.3. *Let $R \subseteq S \subseteq \mathrm{Q}(R)$ be commutative (sub)rings and let X be a set of fractional ideals contained in R. Writing $S \cdot X = \{S\mathfrak{a} \mid \mathfrak{a} \in X\}$, we have $S \cdot \mathrm{cl}_R(X) \subseteq \mathrm{cl}_S(S \cdot X)$.* □

Lemma 6.4.4. *Let R be a commutative ring R and C a set of invertible ideals contained in R which are pairwise coprime. Then* $\mathrm{cl}(C) = \langle\langle C \rangle\rangle$.

Proof. Clearly $\langle\langle C \rangle\rangle \subseteq \mathrm{cl}(C)$. For all $\mathfrak{a}, \mathfrak{b} \in \langle\langle C \rangle\rangle$ we may write $\mathfrak{a} = \prod_{\mathfrak{c} \in C} \mathfrak{c}^{a_\mathfrak{c}}$ and $\mathfrak{b} = \prod_{\mathfrak{c}} \mathfrak{c}^{b_\mathfrak{c}}$ with $a_\mathfrak{c}, b_\mathfrak{c} \in \mathbb{Z}_{\geq 0}$. Then

$$\mathfrak{a} + \mathfrak{b} = \prod_{\mathfrak{c} \in C} \mathfrak{c}^{\min\{a_\mathfrak{c}, b_\mathfrak{c}\}} \quad \text{and} \quad \mathfrak{a} : \mathfrak{b} = \prod_{\mathfrak{c} \in C} \mathfrak{c}^{a_\mathfrak{c} - b_\mathfrak{c}}.$$

Hence $\mathfrak{a}+\mathfrak{b} \in \langle\langle C \rangle\rangle$, and $\mathfrak{a} : \mathfrak{b} \in \langle\langle C \rangle\rangle$ if $\mathfrak{a} : \mathfrak{b} \subseteq R$. Thus $\langle\langle C \rangle\rangle = \mathrm{cl}(C)$. □

Definition 6.4.5. Let R be a commutative ring and X a set of fractional ideals contained in R. A *coprime basis* for X is a set C of invertible proper ideals of R, which are pairwise coprime and satisfy $X \subseteq \langle\langle C \rangle\rangle$.

Note that a coprime basis need not exist for every X. At the very least, the ideals in X should be invertible.

Lemma 6.4.6. *For a commutative ring R and a set X of fractional ideals contained in R we may equip the set of coprime bases of X with a partial order where $C \leq D$ if and only if $\langle\langle C \rangle\rangle \subseteq \langle\langle D \rangle\rangle$.*

Proof. It suffices to verify for coprime bases C and D that $\langle\langle C \rangle\rangle = \langle\langle D \rangle\rangle$ implies $C = D$. Let $m_{\mathfrak{cd}} \in \mathbb{Z}_{\geq 0}$ be such that $\mathfrak{c} = \prod_{\mathfrak{d} \in D} \mathfrak{d}^{m_{\mathfrak{cd}}}$. Since the elements of C are pairwise coprime, there is for every $\mathfrak{d} \in D$ at most one

$\mathfrak{c} \in C$ such that $m_{\mathfrak{c}\mathfrak{d}} > 0$. Because $\langle\langle D \rangle\rangle \subseteq \langle\langle C \rangle\rangle$, there is no $\mathfrak{d} \in D$ such that for all $\mathfrak{c} \in C$ we have $m_{\mathfrak{c}\mathfrak{d}} = 0$.

Let $\mathfrak{d} \in D$. Then there exist $\mathfrak{c} \in C$ and $m > 0$ such that $\mathfrak{c} = \mathfrak{d}^m$ and in turn by symmetry $\mathfrak{e} \in D$ and $n > 0$ such that $\mathfrak{e} = \mathfrak{c}^n$. Then $\mathfrak{e} = \mathfrak{d}^{mn}$, so $\mathfrak{e} = \mathfrak{d}$ and $m = n = 1$. Thus $\mathfrak{d} = \mathfrak{c} \in C$ and $D \subseteq C$. By symmetry we have $C = D$. □

Proposition 6.4.7. *Let R be a Noetherian commutative ring and X a set of fractional ideals contained in R. Then:*

1. *X has a coprime basis if and only if $\mathrm{cl}(X) \subseteq \mathcal{I}(R)$;*
2. *if X has a coprime basis, then it has a unique minimal one;*
3. *if C is a coprime basis of X, then C is minimal if and only if $C \subseteq \mathrm{cl}(X)$.*

Proof. (1) Suppose X has a coprime basis D. Then $X \subseteq \langle\langle D \rangle\rangle = \mathrm{cl}(D)$ by Lemma 6.4.4, so $\mathrm{cl}(X) \subseteq \mathrm{cl}(D) = \langle\langle D \rangle\rangle \subseteq \mathcal{I}(R)$. Suppose instead that $\mathrm{cl}(X) \subseteq \mathcal{I}(R)$. We will show that

$$C = \{\mathfrak{a} \in \mathrm{cl}(X) \mid \forall\, \mathfrak{b} \in \mathrm{cl}(X),\ \mathfrak{a} \subsetneq \mathfrak{b} \Leftrightarrow \mathfrak{b} = R\}$$

is a coprime basis of X.

First, note that the elements of C are pairwise coprime: For $\mathfrak{a}, \mathfrak{b} \in C$ we have $\mathfrak{a} + \mathfrak{b} \in \mathrm{cl}(X)$. If $\mathfrak{a} \subsetneq \mathfrak{a} + \mathfrak{b}$, then $\mathfrak{a} + \mathfrak{b} = R$ by definition of C, and similarly when $\mathfrak{b} \subsetneq \mathfrak{a} + \mathfrak{b}$. Otherwise $\mathfrak{a} = \mathfrak{a} + \mathfrak{b} = \mathfrak{b}$. Second, we show $\mathrm{cl}(X) \subseteq \langle\langle C \rangle\rangle$ using Noetherian induction: Certainly $R \in \langle\langle C \rangle\rangle$. Now let $\mathfrak{a} \in \mathrm{cl}(X) \setminus \{R\}$ and suppose $\mathfrak{c} \in \langle\langle C \rangle\rangle$ for all $\mathfrak{c} \in \mathrm{cl}(X)$ with $\mathfrak{a} \subsetneq \mathfrak{c}$. Either $\mathfrak{a} \in C$, or there is some $\mathfrak{b} \in \mathrm{cl}(X)$ such that $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq R$, in which case $\mathfrak{b}, (\mathfrak{a} : \mathfrak{b}) \in \langle\langle C \rangle\rangle$ by the induction hypothesis and hence $\mathfrak{a} \in \langle\langle C \rangle\rangle$. Thus C is a coprime basis for X, as was to be shown.

(2) Suppose now that X has a coprime basis. We will show that C as in (1) is the unique minimal coprime basis. Let D be any coprime basis of X. We have $C \subseteq \mathrm{cl}(X)$, so $\mathrm{cl}(C) \subseteq \mathrm{cl}(X)$. On the other hand, $X \subseteq \mathrm{cl}(C)$, so $\mathrm{cl}(C) = \mathrm{cl}(X)$. Similarly for D we have $\mathrm{cl}(X) \subseteq \mathrm{cl}(D)$. Hence $\langle\langle C \rangle\rangle = \mathrm{cl}(C) = \mathrm{cl}(X) \subseteq \mathrm{cl}(D) = \langle\langle D \rangle\rangle$ by Lemma 6.4.4. Thus $C \leq D$, as was to be shown.

(3) It is clear that the minimal coprime basis from (2) satisfies $C \subseteq \mathrm{cl}(X)$. Let D be any coprime basis of X such that $D \subseteq \mathrm{cl}(X)$. Then as before we obtain $\langle\langle D \rangle\rangle = \mathrm{cl}(D) = \mathrm{cl}(X)$. Hence $\langle\langle C \rangle\rangle = \mathrm{cl}(X) = \langle\langle D \rangle\rangle$ and $C = D$ by Lemma 6.4.6. Hence D is minimal. □

Theorem 6.4.8. *There exists a polynomial-time algorithm that, given a order R in a number field and a finite set X of fractional ideals contained*

in R, computes the unique minimal order S such that $R \subseteq S \subseteq \mathbb{Q}R$ and $\mathrm{cl}(S \cdot X) \subseteq \mathcal{I}(S)$, and then computes the minimal coprime basis of $S \cdot X$.

Note that the output of this algorithm is clearly functorial under isomorphisms of R.

Proof. Start with S equal to the minimal order $R \subseteq S \subseteq \mathrm{Q}(R)$ where the elements of X become invertible using Theorem 6.2.5, and let $C = X$.

Iteratively compute $\mathfrak{c} = S\mathfrak{a} + S\mathfrak{b}$ for distinct $\mathfrak{a}, \mathfrak{b} \in C$. If $\mathfrak{c} \neq S$, replace S by the unique minimal order $S \subseteq T \subseteq \mathrm{Q}(R)$ where $T\mathfrak{c}$ is invertible using Theorem 6.2.5, replace $\mathfrak{a}$ and $\mathfrak{b}$ in C by $T\mathfrak{a} : T\mathfrak{c}$ and $T\mathfrak{b} : T\mathfrak{c}$, and add $T\mathfrak{c}$ to C. Once $S\mathfrak{a} + S\mathfrak{b} = S$ for all distinct $\mathfrak{a}, \mathfrak{b} \in C$ we terminate and return the order S and coprime basis $S \cdot C$.

Polynomial run time follows from the fact that $\sum_{\mathfrak{a} \in C} \ell_R(S/\mathfrak{a}S)$, which is bounded by the length of the input, decreases by at least 1 after every iteration where $\mathfrak{c} \neq S$. For this, the fact that S changes throughout the algorithm is irrelevant by Proposition 6.3.3. This also gives a polynomial bound on $\#C$ and hence the number of pairs $\mathfrak{a}, \mathfrak{b} \in C$ to check for coprimality every iteration.

It remains to show correctness. With induction on the number of steps one shows that during the algorithm $S \cdot X \subseteq \langle\!\langle S \cdot C \rangle\!\rangle$, so that $S \cdot C$ is indeed a coprime basis for $S \cdot X$, and $S \cdot C \subseteq \mathrm{cl}(S \cdot X)$, so it is minimal by Proposition 6.4.7. Suppose $R \subseteq T \subseteq \mathrm{Q}(R)$ be such that $\mathrm{cl}(TX) \subseteq \mathcal{I}(T)$. Then at every point of the algorithm we could replace S by $S \cap T$ and preserve invertibility, so $S \subseteq T$ at every step by minimality of S guaranteed by Theorem 6.2.5. Hence S is minimal such that $\mathrm{cl}(SX) \subseteq \mathcal{I}(S)$, and the algorithm is correct. □

In the above algorithm, once $S\mathfrak{a} + S\mathfrak{b} = S$ for some S, we will also have $T\mathfrak{a} + T\mathfrak{b} = T$ for any $S \subseteq T \subseteq \mathrm{Q}(R)$. Keeping track of which pairs are coprime could speed up the iterative algorithm in practice. Moreover, once we compute $S\mathfrak{a}$ we may replace $\mathfrak{a}$ in C by $S\mathfrak{a}$ to potentially speed up later computations.

6.5 Fitting ideals

Let R be a commutative ring and M a finitely generated R-module. Then there exists an exact sequence

$$R^{(I)} \xrightarrow{f} R^n \to M \to 0$$

for some set I and $n \in \mathbb{Z}_{\geq 0}$, where we interpret f as a matrix. Note that I can be infinite, as M need not be finitely presentable. For $k \leq n$ we define the *k-th Fitting ideal of M*, written $\mathrm{Fit}_k(M)$, to be the R-ideal generated by the determinants of all $(n-k) \times (n-k)$ minors of the matrix f, which is 0 when no such minors exist. Note that $\mathrm{Fit}_k(M) = 0$ for $k < 0$, and vacuously $\mathrm{Fit}_n(M) = R$ as the determinant of a 0×0 matrix is 1. It is clear that $\mathrm{Fit}_i(M) \subseteq \mathrm{Fit}_j(M)$ for $i \leq j \leq n$. We extend the definition of $\mathrm{Fit}_k(M)$ to arbitrary $k \in \mathbb{Z}$ where $\mathrm{Fit}_k(M) = R$ for $k > n$. By a theorem of Fitting [14] the Fitting ideals do not depend on the choice of exact sequence.

Lemma 6.5.1. *Let R be a non-zero Artinian commutative ring, M a finitely generated R-module and $k \in \mathbb{Z}_{\geq 0}$. Then:*

1. *M can be generated by k elements if and only if $\mathrm{Fit}_k(M) = R$;*
2. *M is free of rank k if and only if $\mathrm{Fit}_{k-1}(M) = 0$ and $\mathrm{Fit}_k(M) = R$;*
3. *if M is free of rank k, then every set of generators of M of cardinality k is a basis.*

Proof. The first two follow from Propositions 20.6 and 20.8 in [12], while the third is elementary. □

Proposition 6.5.2. *There exists a polynomial time algorithm that, given a finite commutative ring R and a finitely generated R-module M, computes the minimal number of generators n for M, and $\mathrm{Fit}_{n-1}(M)$.*

Proof. Using Theorem 4.1.3 from [5] we may compute such minimal n and generators $m_1, \ldots, m_n$ of M. We may then compute an exact sequence $R^m \xrightarrow{f} R^n \to M \to 0$, so that $\mathrm{Fit}_{n-1}(M)$ is the ideal generated by the coefficients of f. □

It is very possible a more direct proof of Proposition 6.5.2 can be given.

6.6 Finite-étale algebras

Let R be a commutative ring and S an R-algebra. We write S^{o} for the opposite ring of S. Then $S^{\mathrm{e}} = S \otimes_R S^{\mathrm{o}}$ is a ring and S is an S^{e}-module where the module structure is given by $(s \otimes s') \cdot t = sts'$. We say S is *separable* if S is projective as S^{e}-module. We say S is *finite-étale* over R if S is commutative and S is projective and separable over R.

Lemma 6.6.1. *Let R be a commutative ring and S a finite-étale R-algebra. Then*

1. *for all ideals $\mathfrak{a} \subseteq R$ the $R/\mathfrak{a}$-algebra $S/\mathfrak{a}S$ is finite-étale;*
2. *for all maximal ideals $\mathfrak{m} \subseteq R$ the $R_{\mathfrak{m}}$-algebra $S_{\mathfrak{m}}$ is finite-étale;*

3. *if R is a field, then S is a product of fields.*

Proof. For 1 and 2 it suffices to verify separability. For 1 it is trivial that $R/\mathfrak{a}$ is separable over R, hence $S/\mathfrak{a}S$ is separable over $R/\mathfrak{a}$ by Proposition III.1.7 of [28]. For 2 we have Proposition III.2.5 of [28]. Finally, 3 is a consequence of Theorem III.3.1 of [28]. □

Proposition 6.6.2. *There exists a polynomial-time algorithm that, given a finite commutative ring R and a finite commutative R-algebra S, decides whether S is finite-étale over R and if not, computes either some ideal $0 \subsetneq \mathfrak{a} \subsetneq R$ or some ideal $0 \subsetneq \mathfrak{b} \subsetneq S$. The output of this algorithm is functorial under isomorphisms.*

Proof. Projectivity over finite rings can be tested using Theorem 5.4.1 from [5], hence the finite-étale property can be tested. Suppose S is not finite-étale. If S is not free over R, then the ideal $\mathfrak{a}$ we obtain from Proposition 6.5.2 satisfies $0 \subsetneq \mathfrak{a} \subsetneq R$ by Lemma 6.5.1. If S is not separable over $\mathbb{Z}$, we obtain a ideal $0 \subsetneq \mathfrak{b} \subsetneq S$ from Proposition 6.1.3 from [5] which is functorial under isomorphisms.

Suppose S is free over R and separable over $\mathbb{Z}$. Then certainly S is projective over R. Hence S is separable over R by Proposition 6.2.14.ii from [5], so S is finite-étale over R. □

6.7 Roots of ideals

In this section we will prove the main theorems on taking roots in orders.

Proposition 6.7.1. *Let $Z \subseteq R \subseteq S \subseteq \mathrm{Q}(R)$ be commutative (sub)rings such that Z is Dedekind and S is finitely generated as a Z-module. Let $\mathfrak{a} \subseteq R$ be an invertible ideal. Write $a = \mathfrak{a} \cap Z$ and suppose $R/\mathfrak{a}$ is finite-étale over Z/a. If $m \in \mathbb{Z}_{\geq 0}$ is such that there exists an ideal $\mathfrak{b} \subseteq S$ with $S\mathfrak{a} = \mathfrak{b}^m$, then there exists an ideal $b \subseteq Z$ with $a = b^m$.*

In this proposition one can think of Z as $\mathbb{Z}$ and S as the maximal order of a number field $\mathrm{Q}(R)$.

Proof. It suffices to prove the proposition for local Z: All conditions on the rings and ideals are preserved by localization at a prime of Z, which for the finite-étale property is Lemma 6.6.1.2, and the conclusion holds if it holds everywhere locally. If Z is a field, then $Z = R = S = \mathrm{Q}(R)$ and the proposition holds trivially. Thus we may assume Z is a discrete valuation ring with maximal ideal $p = \pi Z$. Note that Z is Noetherian, hence S and consequently R are Noetherian Z-modules and in particular Noetherian

rings. Hence because Z is semi-local and of dimension 1, so are both R and S.

Suppose $\mathfrak{b} \subseteq S$ is such that $S\mathfrak{a} = \mathfrak{b}^m$. Write $a = p^k$ for some $k \geq 0$. To show there exists an ideal b with $a = b^m$, it suffices to show that $m \mid k$. We may assume that $k > 0$, otherwise this is trivial. Because $\mathfrak{a}$ and $\mathfrak{b}$ are invertible ideals of a semi-local ring, we have $\mathfrak{a} = \alpha R$ and $\mathfrak{b} = \beta S$ for some regular $\alpha \in R$ and $\beta \in S$ by Lemma 6.2.2.7.

By Lemma 6.3.5 we have $\ell_R(S/R) < \infty$, so by Proposition 6.3.3 we have $[R/\alpha R]_R = [S/\alpha S]_R$. We have inclusions

$$S \supseteq \beta S \supseteq \cdots \supseteq \beta^m S = \alpha S.$$

For all i we have an isomorphism $S/\beta S \to \beta^i S/\beta^{i+1} S$ since β^i is regular, so

$$[R/\alpha R]_R = [S/\alpha S]_R = m \cdot [S/\beta S]_R.$$

Write $A_i = \pi^i \cdot (R/\alpha R)$. We have inclusions

$$A_0 \supseteq A_1 \supseteq \cdots \supseteq A_k = 0.$$

Because $R/\alpha R$ as $Z/\pi^k Z$-algebra is finite-étale by assumption, it is projective and hence free. Therefore multiplication by π^i for $0 \leq i < k$ is an isomorphism $A_0/A_1 \to A_i/A_{i+1}$ of Z-modules and hence of R-modules. We conclude that

$$k \cdot [A_0/A_1]_R = [R/\alpha R]_R = m \cdot [S/\beta S]_R.$$

Note that A_0/A_1 is finite-étale over $Z/\pi Z$ by Lemma 6.6.1, and that $Z/\pi Z$ is a field. Hence $A_0/A_1 = R/(\alpha R + \pi R)$ is a product of fields. In particular, if we choose any maximal $\mathfrak{m} \subset R$ containing $\alpha R + \pi R$ we obtain $[A_0/A_1]_R(\mathfrak{m}) = \ell_{R_\mathfrak{m}}((A_0/A_1)_\mathfrak{m}) = 1$. It follows that $k = m \cdot [S/\beta S]_R(\mathfrak{m})$, as was to be shown. □

Example 6.7.2. Under the assumptions of Proposition 6.7.1 it need not be the case that $\mathfrak{a}$ itself be an m-th power in $\mathcal{I}(R)$.

Let $R = \mathbb{Z}[2\sqrt{2}]$ and $\mathfrak{a} = (2 + 2\sqrt{2})R$. Then $R/\mathfrak{a} \cong \mathbb{Z}/a$ as $\mathbb{Z}/a$-algebra for $a = \mathfrak{a} \cap \mathbb{Z} = 4\mathbb{Z}$, so $R/\mathfrak{a}$ is certainly étale. Since $1 + \sqrt{2}$ is a unit in the maximal order $S = \mathbb{Z}[\sqrt{2}]$, we have that $S\mathfrak{a} = (S\sqrt{2})^2$. Suppose $\mathfrak{c} \in \mathcal{I}(R)$ satisfies $\mathfrak{c}^2 = \mathfrak{a}$. Square roots of ideals in S are unique, so $S\mathfrak{c} = S\sqrt{2}$ and $\mathfrak{c} \subseteq S\sqrt{2}$. On the other hand we have

$$\mathfrak{c} = \mathfrak{a} \cdot (R : \mathfrak{c}) \supseteq \mathfrak{a} \cdot (S2 : S\sqrt{2}) = 2\sqrt{2}S.$$

Thus $\mathfrak{c}$ corresponds to some R-submodule $\mathfrak{d}$ of $S/2S$ with square $(1+\sqrt{2})R+2S$. Clearly $\mathfrak{d} \neq S/2S$, so $\mathfrak{d} = dR + 2S$ for some $d \in S/2S$. As $d^2 \in \{0, 1\}$ we conclude that $\mathfrak{d}^2 \neq (1 + \sqrt{2})R + 2S$, so no such $\mathfrak{c}$ exists.

Theorem 6.7.3. *There exists a polynomial-time algorithm that, given an order R in a number field and fractional ideal $\mathfrak{a}$ of R, computes the maximal $n \in \mathbb{Z}_{\geq 0}$ with respect to divisibility for which there exist an order $R \subseteq S \subseteq \mathbb{Q}R$ and fractional ideal $\mathfrak{b}$ of S such that $\mathfrak{b}^n = S\mathfrak{a}$, where $\mathfrak{b}^0 := S$, and additionally computes such S and $\mathfrak{b}$. The output of this algorithm is functorial under isomorphisms of R.*

Note that $n = 0$ corresponds to the case where $\mathfrak{a}$ is torsion.

Proof. First compute some order $R \subseteq S \subseteq \mathrm{Q}(R)$ such that $S\mathfrak{a}$ and $S+S\mathfrak{a}$ are invertible using Theorem 6.2.5. Then write $S\mathfrak{a} = \mathfrak{a}_+ : \mathfrak{a}_-$ with $\mathfrak{a}_+, \mathfrak{a}_- \subseteq S$ invertible and coprime as in Lemma 6.3.6, and apply the algorithm recursively to $\mathfrak{a}_+$ and $\mathfrak{a}_-$ separately with S in the place of R. Since the ideals are coprime, we may obtain a solution $n = \gcd(n_+, n_-)$ from solutions n_+ and n_- for $\mathfrak{a}_+$ and $\mathfrak{a}_-$ respectively, and similarly we may construct S and $\mathfrak{b}$. Hence we may now assume that $\mathfrak{a} \subsetneq R$.

Suppose that at some point during the algorithm we obtain an ideal $\mathfrak{a} \subsetneq \mathfrak{d} \subsetneq R$. Then compute some extension T and a coprime basis C for $\{T\mathfrak{a}, T\mathfrak{d}\}$ using Theorem 6.4.8. Using Lemma 6.4.1 we may write $T\mathfrak{a} = \prod_{\mathfrak{c} \in C} (T\mathfrak{c})^{m_\mathfrak{c}}$ for some $m_\mathfrak{c} \in \mathbb{Z}_{\geq 0}$. As before we may solve the problem by applying the algorithm recursively to all $\mathfrak{c} \in C$. By the assumption on $\mathfrak{d}$ we have $\mathfrak{a} \subsetneq \mathfrak{c}$ for all $\mathfrak{c} \in C$, so the recursion is well-founded.

Now we proceed to the actual algorithm. Compute $a \in \mathbb{Z}_{>1}$ such that $\mathfrak{a} \cap \mathbb{Z} = a\mathbb{Z}$. By Proposition 6.6.2 we may assume that $R/\mathfrak{a}$ is finite-étale over $\mathbb{Z}/a\mathbb{Z}$, otherwise we can proceed recursively as above. Then write $a = b^m$ for some $b, m \in \mathbb{Z}_{>0}$ with m maximal. If $b \notin \mathfrak{a}$, then we may proceed recursively with $\mathfrak{d} = bR + \mathfrak{a}$. Otherwise $b \in a\mathbb{Z}$, so $a = b$ and $m = 1$, in which case the solution is $n = 1$ and $\mathfrak{b} = \mathfrak{a}$ by Proposition 6.7.1.

That the algorithm runs in polynomial time follows from all theorems applied. □

Corollary 6.7.4. *There exists a polynomial-time algorithm that, given an order R in a number field, a fractional ideal $\mathfrak{a}$ of R and a positive integer n, decides whether there exist an order $R \subseteq S \subseteq \mathbb{Q}R$ and fractional ideal $\mathfrak{b}$ of S such that $\mathfrak{b}^n = S\mathfrak{a}$ and if so computes such S and $\mathfrak{b}$. The output of this algorithm is functorial under isomorphisms of R.* □

Example 6.7.5. A fractional ideal of an order R can have a square root in an order $R \subseteq S \subseteq \mathbb{Q}R$, while not having such a square root in R, even when R is a domain.

Let $R = \mathbb{Z}[2\mathrm{i}]$ and $\mathfrak{a} = 2R$. For $S = \mathbb{Z}[\mathrm{i}]$ and $\mathfrak{c} = (1 + \mathrm{i})S$ we have $\mathfrak{c}^2 = 2\mathrm{i}S = \mathfrak{a}S$, so $\mathfrak{a}$ has a square root in a larger order. Since S is Dedekind, the group $\mathcal{I}(S)$ is torsion-free, so $\mathfrak{c}$ is even the unique square root of $\mathfrak{a}S$.

Suppose $\mathfrak{b}$ is some fractional ideal of R such that $\mathfrak{b}^2 = \mathfrak{a}$. Then $\mathfrak{b}S = \mathfrak{c}$ by uniqueness of $\mathfrak{c}$, so $\mathfrak{b} \subseteq \mathfrak{c} \subseteq S$. Let $x \in \mathfrak{b}$. Then $x = s + t\mathrm{i}$ for $s, t \in \mathbb{Z}$. As

$$2R = \mathfrak{b}^2 \ni x^2 = (s^2 - t^2) + 2st\mathrm{i},$$

we conclude that $s, t \in 2\mathbb{Z}$. Hence $\mathfrak{b} \subseteq 2S$. But then $2R = \mathfrak{b}^2 \subseteq 4S$, which is false. Hence $\mathfrak{b}$ does not exist.

Example 6.7.6. It is impossible to functorially take square roots of ideals in arbitrary number rings without passing to a larger order.

Consider $R = \mathbb{Z}[2\mathrm{i}]$ with invertible fractional ideals $\mathfrak{b} = 2(1 + \mathrm{i})R \subseteq R$ and $\mathfrak{c} = 2(1 - \mathrm{i})R \subseteq R$. We have $\mathfrak{b}^2 = 8\mathrm{i}R = \mathfrak{c}^2$. Note that $8\mathrm{i}R$ is invariant under the automorphism group of R, so likewise should a functorially chosen square root of it be invariant. Since $\mathfrak{b}$ and $\mathfrak{c}$ are distinct conjugates, there should be a third square root of $8\mathrm{i}R$. We will show that the 2-torsion subgroup $\mathcal{I}(R)[2]$ of $\mathcal{I}(R)$ has cardinality 2, giving a contradiction.

Suppose $\mathfrak{a} \in \mathcal{I}(R)$ satisfies $\mathfrak{a}^2 = R$. Write $S = \mathbb{Z}[\mathrm{i}]$ for the maximal order. Then $(S\mathfrak{a})^2 = S$, and because S is Dedekind also $S\mathfrak{a} = S$, so $\mathfrak{a} \subseteq S$. On the other hand we have $\mathfrak{a} \supseteq \mathfrak{a}^2(R : \mathfrak{a}) \supseteq R(R : S) = 2S$. Hence $\mathfrak{a}$ corresponds to some subgroup of $S/2S$. Clearly $\mathfrak{a}$ is neither S nor $2S$, leaving 3 possible subgroups. However, the order of $\mathcal{I}(R)[2]$ is a non-trivial power of 2, so this power must be 2, as was to be shown.

6.8 Reduced coprime bases

Now that we can take roots of ideals we will use this to give a variation on the coprime basis algorithm (Theorem 6.4.8).

Definition 6.8.1. Let G be a group. We say a subgroup $H \subseteq G$ is *pure* if for all $h \in H$ and $k \in \mathbb{Z}_{>0}$ for which there exists a $g \in G$ such that $g^k = h$, such a g exists in H.

Lemma 6.8.2. *Let R be a reduced order. Suppose $H \subseteq \mathcal{I}(R)$ is a finitely generated torsion-free subgroup, then H is a direct summand of $\mathcal{I}(R)$ if and only if it is a pure subgroup.*

Proof. We have a natural isomorphism $\mathcal{I}(R) \cong \bigoplus_{\mathfrak{p}} \mathcal{I}(R_{\mathfrak{p}})$ and H is a subgroup of some direct summand $G = \bigoplus_{\mathfrak{p} \in \mathcal{P}} \mathcal{I}(R_{\mathfrak{p}})$ for a finite set of maximal ideals $\mathcal{P}$. Note that H is pure in $\mathcal{I}(R)$ if and only if it is pure in G. Since G is finitely generated and H is torsion free, the equivalence follows. □

Definition 6.8.3. Let R be a commutative ring, X a set of fractional ideals contained in R and C a coprime basis of X. We say that C is *reduced* if $\langle C \rangle$ is

a pure subgroup of $\mathcal{I}(R)$. Let $\mathcal{O}$ be the integral closure of R in $\mathrm{Q}(R)$. We say that C is *strongly reduced* if $S \cdot C$ is reduced for every subring $R \subseteq S \subseteq \mathcal{O}$.

Equivalently, C is strongly reduced if $\mathcal{O} \cdot C$ is reduced.

Example 6.8.4. Not every X that admits a coprime basis also admits a reduced coprime basis.

Consider $R = \mathbb{Z}[\sqrt[2]{2}, \sqrt[3]{2}]$ and $X = \{2R\}$ and suppose C is a reduced coprime basis of X. As $(\sqrt[2]{2}R)^2 = 2R = (\sqrt[3]{2}R)^3$ the group $\langle C \rangle$ should include a second and third root of $2R$. If we uniquely express $2R = \prod_{\mathfrak{c} \in C} \mathfrak{c}^{k_\mathfrak{c}}$, then $6 \mid k_\mathfrak{c}$ for all $\mathfrak{c}$. In particular, $2R = \mathfrak{b}^6$ for some $\mathfrak{b} \subseteq R$. Since $R/2R \cong (\mathbb{Z}/2\mathbb{Z})^6$ as group, we must have that $\ell_{\mathbb{Z}/2\mathbb{Z}}(R/\mathfrak{b}) = 1$ and $R/\mathfrak{b} \cong \mathbb{Z}/2\mathbb{Z}$ as ring. Hence $\mathfrak{b}$ is a prime above 2, which must be $\mathfrak{b} = \sqrt[2]{2}R + \sqrt[3]{2}R$. As $\mathfrak{b}^5 \subseteq 2R$ we have that $\mathfrak{b}^6 \neq 2R$, so we arrive at a contradiction.

Theorem 6.8.5. *There exists a polynomial-time algorithm that, given a order R in a number field and a finite set X of fractional ideals contained in R, computes an order $R \subseteq S \subseteq \mathbb{Q}R$ such that $S \cdot X$ has a strongly reduced coprime basis and computes such a coprime basis. The output of this algorithm is functorial under isomorphisms of R.*

Proof. Compute an order $R \subseteq S \subseteq \mathbb{Q}R$ and a minimal coprime basis C for $S \cdot X$ using Theorem 6.4.8. Then compute an order $S \subseteq T \subseteq \mathbb{Q}R$ where every $T\mathfrak{c}$ for $\mathfrak{c} \in C$ has a maximal root $\mathfrak{b}_\mathfrak{c}$ and compute $B = \{\mathfrak{b}_\mathfrak{c} \mid \mathfrak{c} \in C\}$ using Theorem 6.7.3. From the fact that the elements of B are pairwise coprime we may deduce that $\langle B \rangle$ is pure, even for larger orders in $\mathbb{Q}R$. Hence B is strongly reduced. One easily verifies that B is minimal. □