Intrinsic factorization of ideals in Dedekind domains

Mawunyo Kofi Darkey-Mensah
(Joint work with Przemysław Koprowski)

June 29, 2018

Institute of Mathematics
University of Silesia

ALaNT 5 — Joint Conferences on Algebra, Logic and Number Theory
Będlewo (Poland), June 24–29 2018

Table of contents

Introduction

Introduction I

Let R be a Dedekind domain. Every ideal $\mathfrak{a} \lhd R$ has a unique factorization into a product of powers of prime ideals.

There are cases where this factorization is algorithmically computable. For instance, if $R = \mathbb{Z}_K$, $K = \mathbb{Q}(\vartheta)$ in [1] or [2].


H. Cohen.
Advanced topics in computational number theory, volume 193 of *Graduate Texts in Mathematics*.


J. Guàrdia, J. Montes, and E. Nart.
A new computational approach to ideal theory in number fields.

Introduction I

Let R be a Dedekind domain. Every ideal $\mathfrak{a} \lhd R$ has a unique factorization into a product of powers of prime ideals.

There are cases where this factorization is algorithmically computable. For instance, if $R = \mathbb{Z}_K$, $K = \mathbb{Q}(\vartheta)$ in [1] or [2].


H. Cohen.
Advanced topics in computational number theory, volume 193 of *Graduate Texts in Mathematics*.


J. Guàrdia, J. Montes, and E. Nart.
A new computational approach to ideal theory in number fields.

The algorithms can be adapted also to global function fields. They depend however on knowing an embedding of the ring of integers (or polynomials) into R.

Introduction II

We discussed the problem of performing the computations intrinsically in the monoid of R-ideals without relaying on these embeddings.

Introduction II

We discussed the problem of performing the computations intrinsically in the monoid of R-ideals without relaying on these embeddings.

The ideal to be factored passes through a three-stage process:

- Radical decomposition
- Distinct degree factorization
- Equal degree factorization

Radical decomposition of ideals

Radical decomposition I

Let R be a Dedekind domain and $\mathfrak{a} \lhd R$. Assume

$$\mathfrak{a} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_s^{k_s}, \tag{1}$$

For any $j \leq m := \max\{k_1, \ldots, k_s\}$ denote

$$\mathfrak{g}_j := \bigcap_{\substack{1 \leq i \leq s \\ k_i = j}} \mathfrak{p}_i.$$

This way we may write $\mathfrak{a}$ as a product

$$\mathfrak{a} = \mathfrak{g}_1 \cdot \mathfrak{g}_2^2 \cdots \mathfrak{g}_m^m. \tag{2}$$

and call 2 the radical decomposition of the ideal $\mathfrak{a}$

Radical decomposition II

The following operations are the basic building blocks for our first algorithm. Given $\mathfrak{a}, \mathfrak{b} \lhd R$, compute

- radical $\operatorname{rad}(\mathfrak{a})$
- sum $(\mathfrak{a} + \mathfrak{b})$
- colon $(\mathfrak{a} : \mathfrak{b})$

If all three operations are computable in R, then R is said to be a ring with computable ideal arithmetic.

Radical decomposition III

Proposition 2

Let $\Bbbk$ be a perfect, computable field and $C := \{F = 0\}$ be a smooth, geometrically irreducible algebraic curve over $\Bbbk$, defined by a bivariate polynomial $F \in \Bbbk[X, Y]$. Then the coordinate ring $R = \Bbbk[C] = {}^{\Bbbk[X,Y]}/_{\langle F \rangle}$ admits computable ideal arithmetic.

Radical decomposition III

Proposition 2

Let $\Bbbk$ be a perfect, computable field and $C := \{F = 0\}$ be a smooth, geometrically irreducible algebraic curve over $\Bbbk$, defined by a bivariate polynomial $F \in \Bbbk[X, Y]$. Then the coordinate ring $R = \Bbbk[C] = \Bbbk[X, Y]/\langle F \rangle$ admits computable ideal arithmetic.

Lemma 3

Keep the assumptions of the proposition. If $\mathfrak{a}, \mathfrak{b} \lhd R$ are two ideals, then

$$\mathfrak{a}^{ce} = \mathfrak{a} \qquad \operatorname{rad}(\mathfrak{a}) = \left(\operatorname{rad}(\mathfrak{a}^c)\right)^e \qquad (\mathfrak{a} : \mathfrak{b}) = (\mathfrak{a}^c : \mathfrak{b}^c)^e$$

Algorithm 1 – Radical Decomposition of an ideal

Given $\mathfrak{a} \lhd R$. Define three sequences $(\mathfrak{a}_i)$, $(\mathfrak{b}_i)$, $(\mathfrak{g}_i)$ as follows:

1. Let $\mathfrak{a}_0 \leftarrow \mathfrak{a}$, $\mathfrak{b}_1 \leftarrow \mathrm{rad}(\mathfrak{a})$ and $\mathfrak{a}_1 = (\mathfrak{a} : \mathfrak{b})$
2. Compute $\mathfrak{b}_{i+1} \leftarrow \mathfrak{a}_i + \mathfrak{b}_i$. The ideal $\mathfrak{b}_i$ satisfy:

$$\mathfrak{b}_i = \mathfrak{g}_i \cdot \mathfrak{g}_{i+1} \cdots \mathfrak{g}_m$$

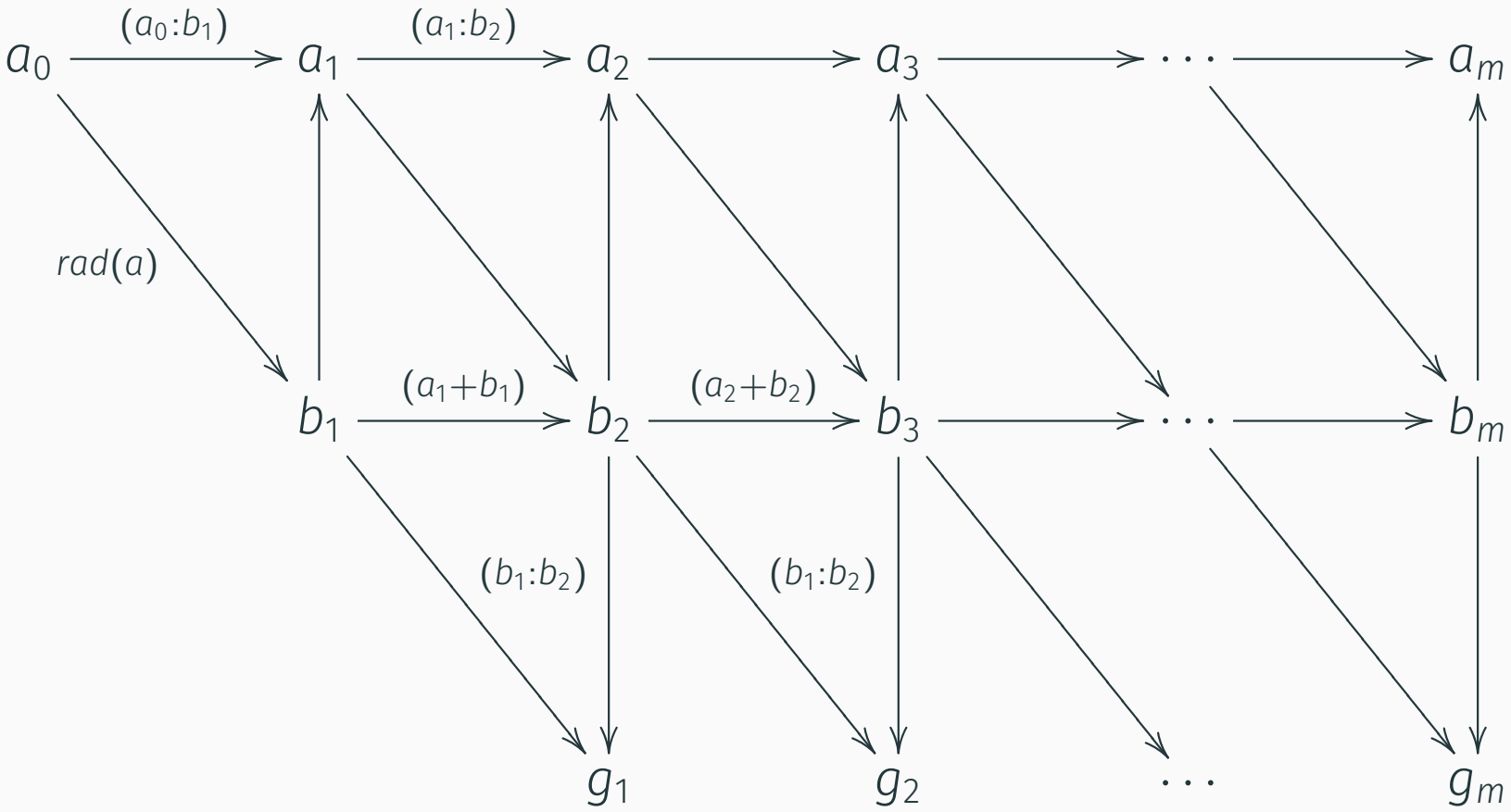
3. Compute $\mathfrak{a}_{i+1} \leftarrow (\mathfrak{a}_i : \mathfrak{b}_{i+1})$. The ideal $\mathfrak{a}_i$ satisfy:

$$\mathfrak{a}_i = \mathfrak{g}_{i+1} \cdot \mathfrak{g}_{i+2}^2 \cdots \mathfrak{g}_m^{m-i}$$

4. Finally we build the sequence $(\mathfrak{g}_1, \ldots, \mathfrak{g}_i)$ as

$$\mathfrak{g}_i = (\mathfrak{b}_i : \mathfrak{b}_{i+1})$$

Algorithm 1 – Diagram



Distinct degree factorization

Distinct degree factorization I

Let $\Bbbk$ be a fixed finite field and let $R = \Bbbk[C] = \Bbbk[X, Y]/\langle F \rangle$. Given a radical ideal $\mathfrak{a} \lhd R$, consider its factorization into primes

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_s.$$

Collate the primes with respect to their residual degrees setting

$$\mathfrak{h}_j := \prod_{\substack{\mathfrak{p} \mid \mathfrak{a} \\ \deg \mathfrak{p} = j}} \mathfrak{p}.$$

Consequently the ideal $\mathfrak{a}$ may be expressed as a product

$$\mathfrak{a} = \mathfrak{h}_1 \cdots \mathfrak{h}_m, \qquad \text{where} \quad m := \max\{\deg \mathfrak{p} \mid \mathfrak{p} \text{ divides } \mathfrak{a}\}. \tag{3}$$

We shall call (3) the distinct degree factorization of $\mathfrak{a}$.

Distinct degree factorization II

We will compute the distinct degree factorization of a given ideal $\mathfrak{a}$ by constructing successive greatest common divisors of $\mathfrak{a}$ and $\mathfrak{u}_k$,

$$\mathfrak{u}_k := \prod_{\substack{\mathfrak{p} \text{ prime} \\ \deg \mathfrak{p} | k}} \mathfrak{p}.$$

Distinct degree factorization II

We will compute the distinct degree factorization of a given ideal $\mathfrak{a}$ by constructing successive greatest common divisors of $\mathfrak{a}$ and $\mathfrak{u}_k$,

$$\mathfrak{u}_k := \prod_{\substack{\mathfrak{p} \text{ prime} \\ \deg \mathfrak{p} | k}} \mathfrak{p}.$$

Let $(x_\mathfrak{p}, y_\mathfrak{p})$ be the unique points associated with $\mathfrak{p}$ on the curve C, with coordinates in the algebraic closure of $\Bbbk = \mathbb{F}_q$, $q = p^l$.

The degree of $\mathfrak{p}$ divides k if and only if $x_\mathfrak{p}, y_\mathfrak{p}$ lie in $\mathbb{F}_{q^k}$ consists of elements satisfying $a^{q^k} - a = 0$.

Distinct degree factorization II

We will compute the distinct degree factorization of a given ideal $\mathfrak{a}$ by constructing successive greatest common divisors of $\mathfrak{a}$ and $\mathfrak{u}_k$,

$$\mathfrak{u}_k := \prod_{\substack{\mathfrak{p} \text{ prime} \\ \deg \mathfrak{p} | k}} \mathfrak{p}.$$

Let $(x_\mathfrak{p}, y_\mathfrak{p})$ be the unique points associated with $\mathfrak{p}$ on the curve C, with coordinates in the algebraic closure of $\Bbbk = \mathbb{F}_q$, $q = p^l$.

The degree of $\mathfrak{p}$ divides k if and only if $x_\mathfrak{p}, y_\mathfrak{p}$ lie in $\mathbb{F}_{q^k}$ consists of elements satisfying $a^{q^k} - a = 0$.

Lemma 4

For every $k \geq 1$, the ideal $\mathfrak{u}_k$ is generated by $x^{q^k} - x$ and $y^{q^k} - y$, where x, y are images of $X, Y \in \Bbbk[X, Y]$ in R .

Algorithm 1 – Radical Decomposition of an ideal

Given a radical $\mathfrak{a} \lhd R$ we compute the distinct degree factorization as follows.

1. Initialize $k \leftarrow 1$ and $\mathfrak{a}_1 \leftarrow \mathfrak{a}$
2. Compute $\mathfrak{u}_k \leftarrow \left\langle x^{q^k} - x, y^{q^k} - y \right\rangle$
3. Next compute $\mathfrak{h}_k \leftarrow \mathfrak{u}_k + \mathfrak{a}_k$
4. Compute $\mathfrak{a}_{k+1}$ from the colon $(\mathfrak{a}_k : \mathfrak{h}_k)$
5. Increase k by 1 and repeat until $\mathfrak{a}_k = R$.
6. Return $\mathfrak{h}_1, \ldots, \mathfrak{h}_k$

Equal degree factorization

Equal degree factorization I

- 👍 radical decomposition
- 👍 distinct degree factorization

we are left with a list of radical ideals

$$\mathfrak{h}_1, \ldots, \mathfrak{h}_k \quad \text{s.t.} \quad \mathfrak{h}_i := \prod_{\substack{\mathfrak{p} \text{ prime} \\ \deg \mathfrak{p} \mid k}} \mathfrak{p}$$

We can deal with such ideals using a generalization of a classical Cantor–Zassenhaus algorithm for factoring polynomials over finite fields.

Equal degree factorization II

Let $\mathfrak{a} \lhd R$ be a radical ideal with some unknown factorization

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_m$$

and the residual degrees of $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ are all the same and known. Denote this common degree by d.

Lemma 6

Let b be an element of R not in $\mathfrak{a}$. Denote $\overline{b} := b + \mathfrak{a}$ the class of b in $R/\mathfrak{a}$ and $e := q^d - 1$. The following conditions are equivalent:

1. the ideal $\mathfrak{b} := \langle b \rangle + \mathfrak{a}$ is a proper divisor of $\mathfrak{a}$;
2. the element $\overline{b}$ is a zero-divisor in $R/\mathfrak{a}$;
3. $\overline{b}^e \neq 1$.

Algorithm 3 – Equal degree factorization

Input: a radical ideal $\mathfrak{a} \lhd R$ and an integer d such that the residual degree of every prime factor of $\mathfrak{a}$ equals d.
Output: prime factors $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ of $\mathfrak{a}$.

1. Select a random element $b \in R \setminus \mathfrak{a}$.
2. Set $\overline{b} \leftarrow b + \mathfrak{a} \in {}^{R}/_{a}$ the class of b in ${}^{R}/_{a}$.
3. Compute $\overline{b}^{e}$ which is either 1 if $b \notin \mathfrak{p}_i$, or 0 if $b \in \mathfrak{p}_i$.
4. If $\overline{b}^{q^d-1} \neq 1$, set $\mathfrak{b} \leftarrow \langle b \rangle + \mathfrak{a}$ and $\mathfrak{c} \leftarrow (\mathfrak{a} : \mathfrak{b})$.
5. $r_1 \leftarrow$ Equal degree factorization of $\mathfrak{b}$
6. $r_2 \leftarrow$ Equal degree factorization of $\mathfrak{c}$
7. Repeat until $|{}^{R}/_{\mathfrak{a}}| = q^d$ and return $r_1 \cup r_2$

Algorithm 4 – Complete factorization

Input: an ideal $\mathfrak{a}$ in R.
Output: the list of pairs $(\mathfrak{p}_i, k_i)$ of prime divisors and multiplicities, see Eq. (1).

1. $Factors = []$.
2. $G \leftarrow$ radical decomposition of $\mathfrak{a}$ (Algorithm 1).
3. Set $\mathfrak{g}_j \leftarrow G[j]$.
4. $H \leftarrow$ distinct degree factorization of $\mathfrak{g}_j$ (Algorithm 2).
5. Set $\mathfrak{h}_d \leftarrow H[d]$.
6. $P \leftarrow$ equal degree factorization of $\mathfrak{h}_d$ (Algorithm 3).
7. $Factors \leftarrow Factors \cup \big[(\mathfrak{p}, j) : \mathfrak{p} \in P\big]$

Example

Example

- $K = \mathbb{F}_{13}(x, y)$
- $F = y^2 - (x^5 - x)(x^4 + 2)$
- $R := \mathbb{F}_{13}[x, y]/\langle F \rangle$.

Consider the ideal $\mathfrak{a} \lhd R$

$$\mathfrak{a} = \langle x^9 + 8x^7 + 5x^6 + 10x^5 + 6x^4 + 4x^3 + 9x^2 + 6x + 4,$$
$$11x^8 + 8x^7 + 2x^6 + 10x^5 + 6x^4 + x^3y + x^3 + 4x^2y + 7x^2 + 4xy + 9y + 7\rangle$$

1. Compute the radical decomposition $\mathfrak{a} = \mathfrak{g}_1 \cdot \mathfrak{g}_2^2$ using Algorithm 1

$$\mathfrak{g}_1 = \langle x^6 + 9x^5 + 7x^4 + 10x^3 + 4x^2 + 4x + 12,$$
$$y + 12x^5 + x^4 + 11x^3 + 10x^2 + 3x + 8\rangle$$
$$\mathfrak{g}_2 = \langle x^3 + 4x^2 + 4x + 9, y + 7x^2 + 9x + 12\rangle$$

Example

2. Next, using Algorithm 2, we compute the distinct degree factorization for each element of the radical decomposition.
   - For $\mathfrak{g}_1$ it returns $\mathfrak{h}_{11} = \mathfrak{h}_{12} = R$ and

$$\mathfrak{h}_{13} = \langle 8x^5y + 5x^4y + 9x^3y + xy + 5y + 1, \\ x^6y + 9x^5y + 7x^4y + 10x^3y + 4x^2y + 4xy + 12y \rangle.$$

   - For $\mathfrak{g}_2$ it returns $\mathfrak{h}_{21} = \mathfrak{h}_{22} = R$ and

$$\mathfrak{h}_{23} = \left\langle 5x^2y + 5xy + 6y + 1, x^3y + 4x^2y + 4xy + 9y \right\rangle.$$

Example

3. Finally we compute the equal degree factorization for each of the above factors using Algorithm 3.
   - For $\mathfrak{h}_{13}$ we obtain the following primes

$$\mathfrak{p}_1 = \left\langle x^3 + 4x^2 + 4x + 9, y + 6x^2 + 4x + 1 \right\rangle$$
$$\mathfrak{p}_2 = \left\langle x^3 + 5x^2 + 9x + 10, y + 3x^2 + 7x + 4 \right\rangle$$

   - and for $\mathfrak{h}_{23}$ we get

$$\mathfrak{p}_3 = \left\langle x^3 + 4x^2 + 4x + 9, y + 7x^2 + 9x + 12 \right\rangle$$

Hence the complete factorization of $\mathfrak{a}$ is $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3^2$.

Thank You!

Any Questions?