Fundamenta Informaticae XXI (2001) 1001–1014
DOI 10.3233/FI-2016-0000
IOS Press

Intrinsic factorization of ideals in Dedekind domains

Mawunyo Kofi Darkey-Mensah
Institute of Mathematics
University of Silesia
ul. Bankowa 14, 40-007 Katowice, Poland
mdarkeymensah@gmail.com

Przemysaw Koprowski
Institute of Mathematics
University of Silesia
ul. Bankowa 14, 40-007 Katowice, Poland
przemyslaw.koprowski@us.edu.pl

Abstract. We present a generalization of a polynomial factorization algorithm that works with ideals in maximal orders of global function fields. The method presented in this paper is intrinsic in the sense that it does not depend on the embedding of the ring of polynomials into the Dedekind domain in question.

Keywords: Dedekind domain, ideal factorization, polynomial factorization, algorithm, square-free decomposition

1. Introduction

Let R be a Dedekind domain. A fundamental and well known property of Dedekind domains is that every ideal $\mathfrak{a} \lhd R$ has a unique factorization into a product of powers of prime ideals. There are cases when this factorization is algorithmically computable. For instance, if $R = \mathbb{Z}_K$ is the ring of algebraic integers (i.e. the integral closure of $\mathbb{Z}$) in some algebraic number field $K = \mathbb{Q}(\vartheta)$, then a suitable algorithm can be found e.g. in [1, Algorithm 2.3.22] or [2, §2.2]. 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. In this paper we discuss the problem of performing the computations intrinsically in the monoid of R-ideals without relaying on these embeddings. The procedure of factoring ideals, that we propose, resembles a method of factoring polynomials over finite fields. We show how to generalize known algorithms for polynomial factorization to make them work with ideals in maximal orders of global function fields. The ideal to be factored passes through a three-stage process: radical decomposition, distinct degree factorization and equal degree factorization.

The algorithms presented in [1, 2] are quite efficient, hence the aim of developing intrinsic methods is not so much to reduce the computation time but rather to construct algorithm that do not dependent on the particular structure of global fields and so have potential to be generalized to other rings. In particular the first step of the process, namely the radical decomposition, can be performed in *any* Dedekind domain in which three elementary operation on ideals are computable. This class of rings include coordinate rings of smooth, algebraically irreducible curves over a computable, perfect field (see Proposition 2.2). Some early experiments of the authors suggest that the algorithms presented here can be generalized to compute primary decomposition of ideals in affine algebras. This subject need further investigation, though.

The paper is organized as follows. In Section 2 we discuss the radical decomposition of ideals, which is an analog of a square-free factorization of polynomials. Given an ideal $\mathfrak{a} \lhd R$, this procedure produces a list of radical ideals $\mathfrak{g}_1, \ldots, \mathfrak{g}_m$ such that $\mathfrak{a}$ is a product of their respective powers. Next, in Section 3 we show how to factor a radical ideal (i.e. any of the ideals $\mathfrak{g}_1, \ldots, \mathfrak{g}_m$) into a product of (radical) ideals such that each one of these new ideals is a product of primes of the same residual degree. Finally in Section 4 we present a variant of Cantor–Zassenhaus algorithm (Algorithm 3) capable of factoring radical ideals with prime divisors of a fixed degree. The algorithms discussed in this paper were implemented by the authors in a computer algebra system Magma [3]. In the closing section we presented two examples obtained with our implementation.

In the whole paper the letter R always denotes a (fixed) Dedekind domain with a field of fractions K. For readers convenience our notation follows the one used in [4], in particular fraktur letters are used to denote ideals. All the ideals in this paper are integral ideals.

2. Radical decomposition of ideals

Let R be a Dedekind domain and $\mathfrak{a} \lhd R$ be an ideal in R. Assume that $\mathfrak{a}$ factors into primes as

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

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are distinct (and unknown) prime ideals and $k_1, \ldots, k_s > 0$ their multiplicities. Collate the factors of equal multiplicities. 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 analogous to a square-free factorization of a polynomial:

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

We shall call (2) the *radical decomposition* of the ideal $\mathfrak{a}$. The name is justified by the following observation.

Observation 2.1. Ideals $\mathfrak{g}_1, \ldots, \mathfrak{g}_m$ are radical.

Indeed, radicals are preserved by intersection (see e.g. [4, Ch. 1]), hence

$$\operatorname{rad}(\mathfrak{g}_j) = \operatorname{rad}\Big(\bigcap_{k_i=j} \mathfrak{p}_i\Big) = \bigcap_{k_i=j} \operatorname{rad}(\mathfrak{p}_i) = \bigcap_{k_i=j} \mathfrak{p}_i = \mathfrak{g}_j.$$

In our settings, the ideals $\mathfrak{g}_1, \ldots, \mathfrak{g}_m$ play roles analogous to square-free factors of a polynomial in case of the square-free factorization, so that we shall call them *radical factors* of $\mathfrak{a}$.

The following operations are the basic building blocks for our first algorithm:

- given an ideal $\mathfrak{a}$ compute its radical $\operatorname{rad}\mathfrak{a}$,
- given two ideals $\mathfrak{a}$ and $\mathfrak{b}$ compute their sum $\mathfrak{a}+\mathfrak{b}$ and the colon ideal $(\mathfrak{a}:\mathfrak{b}) = \{x \mid x\mathfrak{b} \subseteq \mathfrak{a}\}$.

We shall say that R is a ring with *computable ideal arithmetic* if all the three operations are computable for ideals of R.

Proposition 2.2. 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.

The proof of the proposition needs to be preceded by a lemma. Let $\kappa : \Bbbk[X,Y] \twoheadrightarrow R$ be the canonical epimorphism. By superscripts $\cdot^c$, $\cdot^e$ we shall denote respectively the ideal contraction and extension with respect to κ.

Lemma 2.3. Keep the assumptions of the proposition. If $\mathfrak{a}, \mathfrak{b} \lhd R$ are two ideals, then

$$\mathfrak{a}^{ce} = \mathfrak{a}, \qquad \operatorname{rad}(\mathfrak{a}) = \big(\operatorname{rad}(\mathfrak{a}^c)\big)^e, \qquad (\mathfrak{a}:\mathfrak{b}) = (\mathfrak{a}^c : \mathfrak{b}^c)^e.$$

Proof:
The inclusion $\mathfrak{a}^{ce} \subseteq \mathfrak{a}$ holds always (see e.g. [4, Proposition 1.17]). The other inclusion follows from the fact that κ is an epimorphism. Consequently we have

$$\operatorname{rad}(\mathfrak{a}) = \big(\operatorname{rad}(\mathfrak{a})\big)^{ce} = \big(\operatorname{rad}(\mathfrak{a}^c)\big)^e,$$

where the last equality follows from [4, Exercise 1.18]. Likewise we may write

$$(\mathfrak{a}^c : \mathfrak{b}^c)^e \subseteq (\mathfrak{a}^{ce} : \mathfrak{b}^{ce}) = (\mathfrak{a} : \mathfrak{b}) = (\mathfrak{a} : \mathfrak{b})^{ce} \subseteq (\mathfrak{a}^c : \mathfrak{b}^c)^e.$$

This concludes the proof. □

Proof of Proposition 2.2
If we do not insist on obtaining the 2-generators representation of the result, the computation of the sum $\mathfrak{a} + \mathfrak{b}$ of two ideals can be as simple as a concatenation of their lists of generators. Next, an algorithm for computing a quotient of two ideal in a multivariate polynomial ring is well known and so it follows from the above lemma that one may compute the quotient of ideals in R. Finally, being a Dedekind domain, the ring R has dimension one. Consequently every nontrivial ideal $\mathfrak{a} \lhd R$ lifts to a zero-dimensional ideal $A \lhd \Bbbk[X, Y]$. The radical of a zero-dimensional ideal in a multivariate polynomial ring over a perfect field is computable using Seidenberg's formula (see [5]). Thus, the radical of $\mathfrak{a}$ is computable, as well by the previous lemma. □

We are now ready to present an algorithm for the radical decomposition. The reader may wish to observe that it is a generalization of Musser's algorithm [6] for the square-free factorization of polynomials over a field of characteristic zero.

Algorithm 1: Radical decomposition of an ideal

Input: An ideal $\mathfrak{a}$ in a Dedekind domain R with computable ideal arithmetic.
Output: Radical factors $\mathfrak{g}_1, \ldots, \mathfrak{g}_m$ of $\mathfrak{a}$.
// Initialization
$\mathfrak{a}_0 \leftarrow \mathfrak{a}$;
$i \leftarrow 1$;
$\mathfrak{b}_1 \leftarrow \mathrm{rad}(\mathfrak{a})$;
$\mathfrak{a}_1 \leftarrow (\mathfrak{a}_0 : \mathfrak{b}_1)$;
// Main loop
while $\mathfrak{b}_i \neq R$ **do**
  $\mathfrak{b}_{i+1} \leftarrow \mathfrak{a}_i + \mathfrak{b}_i$;
  $\mathfrak{a}_{i+1} \leftarrow (\mathfrak{a}_i : \mathfrak{b}_{i+1})$;
  $\mathfrak{g}_i \leftarrow (\mathfrak{b}_i : \mathfrak{b}_{i+1})$;
  $i \leftarrow i + 1$;
end
return $\mathfrak{g}_1, \ldots, \mathfrak{g}_i$;

Before we show the correctness of the algorithm, we present a slightly technical lemma that gives an explicit description of ideals $\mathfrak{a}_i$ and $\mathfrak{b}_i$ constructed during the execution of the algorithm.

Lemma 2.4. Keep the notation as in Algorithm 1. The ideals $\mathfrak{a}_i$ and $\mathfrak{b}_i$ satisfy:

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

Proof:
We proceed by induction. The assertion is trivially true for $\mathfrak{a}_0$ and $\mathfrak{b}_1$. Assume that the two formulas hold for ideals $\mathfrak{a}_{i-1}$ and $\mathfrak{b}_i$. Take any $x \in \mathfrak{g}_{i+1} \cdot \mathfrak{g}_{i+2}^2 \cdots \mathfrak{g}_m^{m-i}$ and $y \in \mathfrak{b}_i = \mathfrak{g}_i \cdot \mathfrak{g}_{i+1} \cdots \mathfrak{g}_m$. Then their product xy lies in $\mathfrak{g}_i \cdot \mathfrak{g}_{i+1}^2 \cdots \mathfrak{g}_m^{m-i+1} = \mathfrak{a}_{i-1}$. Hence $x \in (\mathfrak{a}_{i-1} : \mathfrak{b}_i) = \mathfrak{a}_i$ proving an inclusion $\mathfrak{a}_i \supseteq \mathfrak{g}_{i+1} \cdot \mathfrak{g}_{i+2}^2 \cdots \mathfrak{g}_m^{m-i}$.

Conversely, take $x \in \mathfrak{a}_i = (\mathfrak{a}_{i-1} : \mathfrak{b}_i)$. Fix any prime ideal $\mathfrak{p}$ dividing $\mathfrak{a}_{i-1}$ and let $k := \operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})$ be the multiplicity of $\mathfrak{p}$ in the factorization (1) of $\mathfrak{a}$. By the inductive hypothesis, the ideal $\mathfrak{p}$ divides $\mathfrak{b}_i$ and $k-i+1$ is the multiplicity of $\mathfrak{p}$ in the factorization of $\mathfrak{a}_{i-1}$. By the strong approximation theorem (see e.g. [7, Corollary 10.5.11]) there exists an element $y \in R$ such that

$$\operatorname{ord}_{\mathfrak{p}} y = 1 \qquad \text{and} \qquad \operatorname{ord}_{\mathfrak{q}} y \geq 1 \quad \text{for all } \mathfrak{q} \mid \mathfrak{b}_i.$$

In particular, y is an element of $\mathfrak{b}_i$ and $y \notin \mathfrak{p}^2$. By the definition of the colon ideal, $xy \in x \cdot \mathfrak{b}_i \subseteq \mathfrak{a}_{i-1} \subseteq \mathfrak{p}^{k-i+1}$. It follows that the $\mathfrak{p}$-adic valuation of the product xy is at least $k-i+1$. Therefore, we have

$$k - i + 1 \leq \operatorname{ord}_{\mathfrak{p}}(xy) = \operatorname{ord}_{\mathfrak{p}} x + 1.$$

Consequently $\operatorname{ord}_{\mathfrak{p}} x \geq k - i$, which means that $x \in \mathfrak{p}^{k-i}$. As this holds for every prime $\mathfrak{p}$ dividing $\mathfrak{a}_{i-1}$, we see that

$$x \in \bigcap_{\substack{\mathfrak{p} \mid \mathfrak{a} \\ \operatorname{ord}_{\mathfrak{p}}(\mathfrak{a}) \geq i}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})-i} = \prod_{\substack{\mathfrak{p} \mid \mathfrak{a} \\ \operatorname{ord}_{\mathfrak{p}}(\mathfrak{a}) \geq i}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})-i} = \prod_{k \geq i} \Bigg(\prod_{\substack{\mathfrak{p} \mid \mathfrak{a} \\ \operatorname{ord}_{\mathfrak{p}}(\mathfrak{a}) = k}} \mathfrak{p} \Bigg)^{k-i} = R \cdot \mathfrak{g}_{i+1} \cdot \mathfrak{g}_{i+2}^2 \cdots \mathfrak{g}_m^{m-i}.$$

This shows that $\mathfrak{a}_i \subseteq \mathfrak{g}_{i+1} \cdot \mathfrak{g}_{i+2}^2 \cdots \mathfrak{g}_m^{m-i}$.

We now prove the equality $\mathfrak{b}_{i+1} = \mathfrak{g}_{i+1} \cdots \mathfrak{g}_m$. One inclusion is immediate.

$$\mathfrak{b}_{i+1} = \mathfrak{a}_i + \mathfrak{b}_i = \left\langle \mathfrak{g}_{i+1} \cdot \mathfrak{g}_{i+1}^2 \cdots \mathfrak{g}_m^{m-i} \cup \mathfrak{g}_i \cdot \mathfrak{g}_{i+1} \cdots \mathfrak{g}_m \right\rangle$$

The radical ideals $\mathfrak{g}_i$ are pairwise coprime, hence

$$\begin{aligned}
&= \left\langle \bigcap_{j \geq i+1} \mathfrak{g}_j^{j-i} \cup \Big(\mathfrak{g}_i \cap \bigcap_{j \geq i+1} \mathfrak{g}_j \Big) \right\rangle \\
&= \left\langle \Big(\bigcap_{j \geq i+1} \mathfrak{g}_j^{j-i} \cup \mathfrak{g}_i \Big) \cap \Big(\bigcap_{j \geq i+1} \mathfrak{g}_j^{j-i} \cup \bigcap_{j \geq i+1} \mathfrak{g}_j \Big) \right\rangle \\
&\subseteq \left\langle \Big(\bigcap_{j \geq i+1} \mathfrak{g}_j \cup \mathfrak{g}_i \Big) \cap \bigcap_{j \geq i+1} \mathfrak{g}_j \right\rangle \\
&= \left\langle \bigcap_{j \geq i+1} \mathfrak{g}_j \right\rangle = \mathfrak{g}_{i+1} \cdot \mathfrak{g}_{i+1} \cdots \mathfrak{g}_m.
\end{aligned}$$

In order to show the other inclusion fix an element $x \in \mathfrak{g}_{i+1} \cdots \mathfrak{g}_m$. Ideals $\mathfrak{g}_i$ and $\mathfrak{g}_{i+1}\mathfrak{g}_{i+2}^2 \cdots \mathfrak{g}_m^{m-i} = \mathfrak{a}_i$ are relatively prime, hence there exist elements $y \in \mathfrak{g}_i$ and $z \in \mathfrak{a}_i$ such that $x = y + z$. Therefore, for any $j \geq i+1$ we have

$$y = x - z \in \mathfrak{g}_j + \mathfrak{a}_i \subseteq \mathfrak{g}_j + \mathfrak{g}_j = \mathfrak{g}_j.$$

It follows that $y \in \mathfrak{g}_{i+1} \cap \ldots \cap \mathfrak{g}_m = \mathfrak{b}_i$. Consequently, $x = y + z \in \mathfrak{b}_i + \mathfrak{a}_i = \mathfrak{b}_{i+1}$. □

We are now ready to show the correctness of the algorithm.

Proof of correctness of Algorithm 1:
It follows immediately from the preceding lemma that the algorithm terminates. All we need to show is that for every index i the colon ideal $(\mathfrak{b}_i : \mathfrak{b}_{i+1})$ equals the sought radical ideal $\mathfrak{g}_i$. One inclusion is immediate. By the lemma we have

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

and so $\mathfrak{g}_i \subseteq (\mathfrak{b}_i : \mathfrak{b}_{i+1})$. We need to prove the other inclusion. To this end take any $x \in (\mathfrak{b}_i : \mathfrak{b}_{i+1})$ and fix a prime divisor $\mathfrak{p}$ of $\mathfrak{g}_i$. The multiplicity of $\mathfrak{p}$ in the factorization of $\mathfrak{a}$ is thus $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a}) = i$. By the strong approximation theorem there is an element $y \in R$ such that $y \in \mathfrak{b}_{i+1} \setminus \mathfrak{p}$. Now, $xy \in x \cdot \mathfrak{b}_{i+1} \subseteq \mathfrak{b}_i \subseteq \mathfrak{p}$ but $y \notin \mathfrak{p}$, it follows that $x \in \mathfrak{p}$. This shows that x belongs to every prime divisor $\mathfrak{p}$ of $\mathfrak{a}$ of multiplicity $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a}) = i$. Therefore

$$x \in \bigcap_{\substack{\mathfrak{p}|a \\ \operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})=i}} \mathfrak{p} = \mathfrak{g}_i.$$

This proves the correctness of the algorithm. □

3. Distinct degree factorization

In this and the next section we restrict our attention to maximal orders in global function fields. Thus, let $\Bbbk$ be a fixed finite field and let $R = \Bbbk[C] = \Bbbk[X,Y]/\langle F \rangle$ be a Dedekind domain which is a coordinate ring of a smooth and geometrically irreducible curve C. In particular R is a maximal order in a field $\Bbbk(C)$ of rational functions on C (i.e. in a global function field). 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

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

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

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

By analogy to the polynomial case, we shall call (3) the *distinct degree factorization* of $\mathfrak{a}$.

We will compute the distinct degree factorization of a given ideal $\mathfrak{a}$ by constructing successive greatest common divisors (in the lattice of R-ideals) of $\mathfrak{a}$ and $\mathfrak{u}_k$, where $\mathfrak{u}_k$ is the intersection of all primes of residual degrees dividing k:

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

Before we continue, recall that with every prime ideal $\mathfrak{p}$ one can associate a unique point $(x_\mathfrak{p}, y_\mathfrak{p})$ on the curve C, with coordinates in the algebraic closure $\overline{\Bbbk}$ of $\Bbbk$. To this end treat elements of $R = \Bbbk[C]$ as polynomial functions on C and set $(x_\mathfrak{p}, y_\mathfrak{p})$ to be a unique point where all elements of $\mathfrak{p}$ vanish simultaneously. In this section $\Bbbk$ is a finite field, say $\Bbbk = \mathbb{F}_q$ for some prime power $q = p^l$. The degree of $\mathfrak{p}$ divides k if and only if $x_\mathfrak{p}, y_\mathfrak{p}$ lie in $\mathbb{F}_{q^k}$. It is well known that $\mathbb{F}_{q^k}$ consists of elements satisfying $a^{q^k} - a = 0$. Apply this fact to both coordinates.

Lemma 3.1. 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 in R of $X, Y \in \Bbbk[X, Y]$.

Proof:
Fix $k \geq 1$ and denote $\mathfrak{v}_k := \langle x^{q^k} - x, y^{q^k} - y \rangle \lhd R$. We shall prove first that the ideal $\mathfrak{v}_k$ is contained in $\mathfrak{u}_k$. It suffices to show that both its generators belong to every prime ideal $\mathfrak{p}$ of R whose residual degree divides k. Take any such prime $\mathfrak{p}$. The coordinates $x_\mathfrak{p}, y_\mathfrak{p}$ of the associated point belong to $\mathbb{F}_{q^k}$, hence $x_\mathfrak{p}^{q^k} - x_\mathfrak{p} = 0 = y_\mathfrak{p}^{q^k} - y_\mathfrak{p}$. Thus the generators of $\mathfrak{v}_k$ vanish on $(x_\mathfrak{p}, y_\mathfrak{p})$ and so $\mathfrak{v}_k \subseteq \mathfrak{p}$.

Next, we show that $\mathfrak{v}_k$ is not contained in any prime ideal $\mathfrak{p}$ whose degree does not divide k. Suppose that $\mathfrak{v}_k \subset \mathfrak{p}$ for some prime ideal $\mathfrak{p}$. In particular the generators $x^{q^k} - x, y^{q^k} - y$ belong to $\mathfrak{p}$. Therefore, they vanish on the associated point $(x_\mathfrak{p}, y_\mathfrak{p})$, which means that $x_\mathfrak{p}, y_\mathfrak{p} \in \mathbb{F}_{q^k}$ and so $\deg \mathfrak{p}$ divides k.

From what we have proved so far it follows that $\mathfrak{u}_k$ is the radical of $\mathfrak{v}_k$. In order to conclude the proof, it suffices to show that $\mathfrak{v}_k$ is a radical ideal itself. To this end we show that for every prime ideal $\mathfrak{p}$, $\deg \mathfrak{p} \mid k$ the valuation of at least one of the generators of $\mathfrak{v}_k$ equals 1. Consider two (reducible) algebraic curves $C_1 := \{x^{q^k} = x\}$ and $C_2 := \{y^{q^k} = y\}$. They both consist of parallel lines but they are not parallel to each other. Suppose that $\operatorname{ord}_\mathfrak{p}(x^{q^k} - x) > 1$ for some $\mathfrak{p}$. This means that $\mathfrak{p}$ is a ramified extension of an ideal $p \cdot \mathbb{F}_q[x]$ for some irreducible polynomial p in x. We may identify the valuation $\operatorname{ord}_\mathfrak{p}(x^{q^k} - x)$ with the intersection index $I\big((x_\mathfrak{p}, y_\mathfrak{p}), C \cap C_1\big)$. If

$$\operatorname{ord}_\mathfrak{p}\big(x^{q^k} - x\big) = I\big((x_\mathfrak{p}, y_\mathfrak{p}), C \cap C_1\big) > 1,$$

then C is tangent to C_1 at $(x_\mathfrak{p}, y_\mathfrak{p})$. Consequently it cannot be tangent to C_2 at $(x_\mathfrak{p}, y_\mathfrak{p})$ as C is non-singular. Therefore

$$\operatorname{ord}_\mathfrak{p}\big(y^{q^k} - y\big) = I\big((x_\mathfrak{p}, y_\mathfrak{p}), C \cap C_2\big) = 1.$$

This shows that for every prime ideal $\mathfrak{p}$, whose residual degree divides k, either $x^{q^k} - x \in \mathfrak{p} \setminus \mathfrak{p}^2$ or $y^{q^k} - y \in \mathfrak{p} \setminus \mathfrak{p}^2$. This implies that $\mathfrak{v}_k$ is radical. □

We may now present an algorithm for distinct degree factorization.

Algorithm 2: Distinct degree factorization

Input: A radical ideal $\mathfrak{a} \lhd R$.
Output: Distinct degree factors $\mathfrak{h}_1, \ldots, \mathfrak{h}_m$ of $\mathfrak{a}$.
// Initialization
$k \leftarrow 1$;
$\mathfrak{a}_1 \leftarrow \mathfrak{a}$;
// Main loop
while $\mathfrak{a}_k \neq R$ **do**
  $\mathfrak{u}_k \leftarrow \left\langle x^{q^k} - x, y^{q^k} - y \right\rangle$;
  $\mathfrak{h}_k \leftarrow \mathfrak{u}_k + \mathfrak{a}_k$;
  $\mathfrak{a}_{k+1} \leftarrow (\mathfrak{a}_k : \mathfrak{h}_k)$;
  $k \leftarrow k + 1$;
end
return $\mathfrak{h}_1, \ldots, \mathfrak{h}_k$;

Proof of correctness:
We proceed by an induction on k. Assume that $\mathfrak{h}_{k-1}$ is the $(k-1)$-th distinct degree factor of $\mathfrak{a}$ and $\mathfrak{a}_k$ is the product of the prime divisors of $\mathfrak{a}$ with residual degrees at least k. This is trivially true for $\mathfrak{a}_1 = \mathfrak{a}$ and $\mathfrak{h}_0 := R$. Lemma 3.1 asserts that $\left\langle x^{q^k} - x, y^{q^k} - y \right\rangle = \mathfrak{u}_k$. Compute

$$\mathfrak{u}_k + \mathfrak{a}_k = \langle \mathfrak{u}_k \cup \mathfrak{a}_k \rangle = \left\langle \bigcap_{\deg \mathfrak{p} | k} \mathfrak{p} \cup \bigcap_{\substack{\mathfrak{q} | \mathfrak{a} \\ \deg \mathfrak{q} \geq k}} \mathfrak{q} \right\rangle = \left\langle \bigcap_{\substack{\deg \mathfrak{p} | k \\ \mathfrak{q} | \mathfrak{a} \\ \deg \mathfrak{q} \geq k}} (\mathfrak{p} \cup \mathfrak{q}) \right\rangle = \left\langle \bigcap_{\substack{\deg \mathfrak{p} | k \\ \mathfrak{q} | \mathfrak{a} \\ \deg \mathfrak{q} \geq k}} (\mathfrak{p} + \mathfrak{q}) \right\rangle.$$

Now prime ideals $\mathfrak{p}, \mathfrak{q}$ are either equal or relatively prime. Hence $\mathfrak{p} + \mathfrak{q} = \mathfrak{p}$ when $\mathfrak{p} = \mathfrak{q}$ and $\mathfrak{p} + \mathfrak{q} = R$ if $\mathfrak{p} \neq \mathfrak{q}$. Consequently the above formula simplifies to

$$\mathfrak{u}_k + \mathfrak{a}_k = \bigcap_{\substack{\mathfrak{p} | \mathfrak{a} \\ \deg \mathfrak{p} = k}} \mathfrak{p} = \mathfrak{h}_k.$$

It follows that $\mathfrak{a}_{k+1} = (\mathfrak{a}_k : \mathfrak{h}_k)$ is the product off all those prime divisors of $\mathfrak{a}$ that have degrees strictly greater than k. □

4. Equal-degree factorization

After performing a radical decomposition and distinct degree factorization, we are left with a list of radical ideals such that each one is a product of primes all having the same (known) residual degree. We can deal with such ideals using a generalization of a classical Cantor–Zassenhaus algorithm. We shall first note the following fact.

Lemma 4.1. If $\mathfrak{a} \lhd R$ is a nonzero radical ideal, then the number of elements of the residue ring ${}^{R}\!/_{\mathfrak{a}}$ is algorithmically computable.

Proof:
As in the proof of Proposition 2.2 we use the ideal contraction with respect to the canonical epimorphism $\kappa : \Bbbk[X,Y] \twoheadrightarrow R$. The ring R is a Dedekind domain and $\mathfrak{a} \neq \{0\}$, hence ${}^{R}\!/_{\mathfrak{a}}$ is a finite ring isomorphic to ${}^{\Bbbk[X,Y]}\!/_{\mathfrak{a}^c}$. The number of elements of the latter ring is computable using a well known trick of counting monomials not in $\mathrm{lm}(\mathfrak{a}^c)$, where $\mathrm{lm}(\mathfrak{a}^c)$ is an ideal spanned by leading monomials of $\mathfrak{a}^c$ with respect any monomial order in $\Bbbk[X,Y]$. □

From now on we assume that $\mathfrak{a} \lhd R$ is 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 a priori known. Denote this common degree by d.

Lemma 4.2. 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. $\overline{b}^e \neq 1$.

Proof:
Assume that $\mathfrak{b}$ is a proper divisor of $\mathfrak{a}$. This means that $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq R$. In particular b cannot lie in $\mathfrak{a}$ and so $\overline{b} \neq 0$. The ring ${}^{R}\!/_{\mathfrak{a}}$ is finite, hence it suffices to show that $\overline{b}$ is not invertible. Suppose a contrario that there is an element $c \in R$ such that $\overline{c} \cdot \overline{b} = 1$. But then $1 \in \mathfrak{b}$ and this contradicts the assumption that $\mathfrak{b} \neq R$.

The implication (2) $\Longrightarrow$ (3) is trivial. In order to prove the remaining implication (3) $\Longrightarrow$ (1), assume that $\overline{b}^e \neq 1$. By the Chinese reminder theorem there is an isomorphism

$$\varphi : {}^{R}\!/_{\mathfrak{a}} \xrightarrow{\sim} {}^{R}\!/_{\mathfrak{p}_1} \times \cdots \times {}^{R}\!/_{\mathfrak{p}_m},$$

where each quotient ring ${}^{R}\!/_{\mathfrak{p}_i}$ is in turn isomorphic to $\mathbb{F}_{q^d}$. Let $\pi_i : {}^{R}\!/_{\mathfrak{p}_1} \times \cdots \times {}^{R}\!/_{\mathfrak{p}_m} \twoheadrightarrow {}^{R}\!/_{\mathfrak{p}_i}$ be the projection onto the i-th coordinate. For every $i \leq m$, the image $(\pi_i \circ \varphi)(\overline{b}^e)$ is either 1 if $b \notin \mathfrak{p}_i$, or 0 if $b \in \mathfrak{p}_i$. Not all coordinates can be equal 1, because $\overline{b}^e \neq 1$. Neither all the coordinates are equal zero, since $b \notin \mathfrak{a}$. Denote

$$I := \big\{ i \leq m : (\pi \circ \varphi)(b^e) = 0 \big\} = \big\{ i \leq m : b \in \mathfrak{p}_i \big\},$$

we then have

$$\mathfrak{b} = \prod_{i \in I} \mathfrak{p}_i$$

and it is clear that $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq R$. □

We may now present a randomized recursive algorithm, in a spirit of Cantor–Zassenhaus, for factoring radical ideals of constant residual degree.

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 $\mathfrak{a}$.
// Recursion termination
if $|\frac{R}{\mathfrak{a}}| = q^d$ **then**
  return $\mathfrak{a}$;
end
// Main loop
while True **do**
  $b \leftarrow$ random element of $R \setminus \mathfrak{a}$;
  $\overline{b} \leftarrow b + \mathfrak{a} \in {}^{R}\!/_{a}$;
  if $\overline{b}^{q^d-1} \neq 1$ **then**
    $\mathfrak{b} \leftarrow \langle b \rangle + \mathfrak{a}$;
    $\mathfrak{c} \leftarrow (\mathfrak{a} : \mathfrak{b})$;
      // Recursion;
    $r_1 \leftarrow$ Equal degree factorization of $\mathfrak{b}$;
    $r_2 \leftarrow$ Equal degree factorization of $\mathfrak{c}$;
    return $r_1 \cup r_2$;
  end
end

The correctness of the algorithm follows immediately from the lemma preceding it. For the sake of completeness we present an algorithm for the complete factorization of an ideal, that summarizes the whole discussion.

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).
$Factors \leftarrow []$;
$G \leftarrow$ radical decomposition of $\mathfrak{a}$;
(Algorithm 1);
for $j \leq |G|$ **do**
  $\mathfrak{g}_j \leftarrow G[j]$;
  $H \leftarrow$ distinct degree factorization of $\mathfrak{g}_j$;
  (Algorithm 2);
  for $d \leq |H|$ **do**
    $\mathfrak{h}_d \leftarrow H[d]$;
    $P \leftarrow$ equal degree factorization of $\mathfrak{h}_d$;
    (Algorithm 3);
    $Factors \leftarrow Factors \cup \big[(\mathfrak{p}, j) : \mathfrak{p} \in P\big]$;
  end
end
return $Factors$;

5. Examples

The authors implemented algorithms described in this paper in a computer algebra system Magma [3]. Below we preset two examples computed using our implementation.

Example

Let $K = \mathbb{F}_{13}(x, y)$ be a hyperelliptic function field given by a generating polynomial

$$F = y^2 - (x^5 - x)(x^4 + 2)$$

and let $R := {}^{\mathbb{F}_{13}[x,y]}\big/_{\langle F \rangle}$. Consider the ideal $\mathfrak{a} \lhd R$

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

Use Algorithm 1 to compute the radical decomposition $\mathfrak{a} = \mathfrak{g}_1 \cdot \mathfrak{g}_2^2$, where

$$\begin{aligned}\mathfrak{g}_1 &= \langle x^6 + 9x^5 + 7x^4 + 10x^3 + 4x^2 + 4x + 12, \\ &\qquad y + 12x^5 + x^4 + 11x^3 + 10x^2 + 3x + 8\rangle, \\ \mathfrak{g}_2 &= \left\langle x^3 + 4x^2 + 4x + 9, y + 7x^2 + 9x + 12\right\rangle.\end{aligned}$$

Next, using Algorithm 2, we compute the distinct degree factorization for each element of the radical decomposition. For $\mathfrak{g}_1$ it returns two trivial factors $\mathfrak{h}_{11} = \mathfrak{h}_{12} = R$ and one nontrivial, degree 3 factor

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

For $\mathfrak{g}_2$ the situation is fully analogous: $\mathfrak{h}_{21} = \mathfrak{h}_{22} = R$ and

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

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 $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3^2$.

Example

In this example, we consider an elliptic function field $K = \mathbb{F}_{19}(x, y)$ with full constant field $\mathbb{F}_{19}$, where

$$y^2 + y = x^3 - 2x^2 + 1$$

Take a and ideal

$$\mathfrak{a} = \langle x^{21} + 14x^{20} + 9x^{19} + 4x^{18} + 5x^{17} + 12x^{16} + 9x^{15} + 7x^{14} + 12x^{13} + 8x^{12} \\ + 3x^{11} + 8x^{10} + 14x^9 + 7x^8 + 12x^7 + x^6 + 9x^5 + 13x^4 + 9x^3 + 4x^2 + 18x + 4, \\ x^3y + 6x^2y + 3xy + 17y + 7x^{18} + 7x^{17} + 11x^{16} + x^{15} + 18x^{13} + 8x^{12} + 9x^{11} \\ + 15x^{10} + 13x^9 + 18x^8 + 12x^7 + x^6 + 14x^5 + 10x^4 + 7x^3 + 15x^2 + 9x + 5\rangle.$$

We again use Algorithm 1 to factor I into a product of radical ideals. It returns one trivial factor $\mathfrak{g}_3 = R$ and three nontrivial factors $\mathfrak{g}_1, \mathfrak{g}_2$ and $\mathfrak{g}_4$ where

$$\mathfrak{g}_1 = \langle x^3 + 6x^2 + 3x + 17, x^3y + 6x^2y + 3xy + 17y\rangle, \\ \mathfrak{g}_2 = \left\langle x^3 + 4x + 17, y + 8x^2 + 2x + 9 \right\rangle, \\ \mathfrak{g}_4 = \left\langle x^3 + 2x^2 + 10x + 4, y + 8x^2 + 3x \right\rangle.$$

Now we compute the distinct degree factors of the above ideals. For $\mathfrak{g}_1$ we have two trivial factors $\mathfrak{h}_{11} = \mathfrak{h}_{13} = R$ and two nontrivial one, degrees 2 and 4, respectively:

$$\mathfrak{h}_{12} = \langle x + 1 \rangle .$$
$$\mathfrak{h}_{14} = \langle x^2 + 5x + 17 \rangle$$

For $\mathfrak{g}_2$ it returns two trivial factors $\mathfrak{h}_{21} = \mathfrak{h}_{22} = R$ and one nontrivial, degree 3 factor

$$\mathfrak{h}_{23} = \langle x^3 + 4x + 17, y + 8x^2 + 2 * x + 9 \rangle .$$

Similarly for $\mathfrak{g}_4$ we have $\mathfrak{h}_{41} = \mathfrak{h}_{42} = R$ and

$$\mathfrak{h}_{43} = \langle x^3 + 2x^2 + 10x + 4, y + 8x^2 + 3x \rangle .$$

Finally we use Algorithm 3 to compute the equal degree factorization. It turns out that all four ideals $\mathfrak{h}_{12}, \mathfrak{h}_{14}, \mathfrak{h}_{23}$ and $\mathfrak{h}_{43}$ are in fact prime. Denoting

$$\mathfrak{p}_1 := \mathfrak{h}_{12}, \quad \mathfrak{p}_2 := \mathfrak{h}_{14}, \quad \mathfrak{p}_3 := \mathfrak{h}_{23}, \quad \mathfrak{p}_4 := \mathfrak{h}_{43},$$

we obtain the complete factorization of $\mathfrak{a}$, namely $\mathfrak{a} = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3^2 \cdot \mathfrak{p}_4^3$.

References

[1] Cohen H. Advanced topics in computational number theory, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. ISBN 0-387-98727-4. doi:10.1007/978-1-4419-8489-0. URL http://dx.doi.org/10.1007/978-1-4419-8489-0.

[2] Guàrdia J, Montes J, Nart E. A new computational approach to ideal theory in number fields. *Found. Comput. Math.*, 2013. **13**(5):729–762. URL https://doi.org/10.1007/s10208-012-9137-5.

[3] Bosma W, Cannon J, Playoust C. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 1997. **24**(3-4):235–265. doi:10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993), URL http://dx.doi.org/10.1006/jsco.1996.0125.

[4] Atiyah MF, Macdonald IG. Introduction to commutative algebra. Addison-Wesley Series in Mathematics. Westview Press, Boulder, CO, economy edition, 2016. ISBN 978-0-8133-5018-9; 0-201-00361-9; 0-201-40751-5. For the 1969 original see [MR0242802].

[5] Seidenberg A. Constructions in algebra. *Trans. Amer. Math. Soc.*, 1974. **197**:273–313. doi:10.2307/1996938. URL https://doi.org/10.2307/1996938.

[6] Musser DR. Algorithms for polynomial factorization. Ph.D. thesis, University of Wisconsin, 1971.

[7] Cohn PM. Basic algebra. Springer-Verlag London, Ltd., London, 2003. ISBN 1-85233-587-4. Groups, rings and fields, URL https://doi.org/10.1007/978-0-85729-428-9.

[8] Gerhard J. Fast modular algorithms for squarefree factorization and Hermite integration. *Appl. Algebra Engrg. Comm. Comput.*, 2001. **11**(3):203–226. doi:10.1007/PL00004222. URL http://dx.doi.org/10.1007/PL00004222.

[9] Guersenzvaig NH, Szechtman F. Roots multiplicity and square-free factorization of polynomials using companion matrices. *Linear Algebra Appl.*, 2012. **436**(9):3160–3164. doi:10.1016/j.laa.2011.10.018. URL http://dx.doi.org/10.1016/j.laa.2011.10.018.

[10] Horowitz E. Algorithms for symbolic integration of rational functions. Ph.D. thesis, University of Wisconsin, 1969.

[11] Koprowski Pa. Roots multiplicity without companion matrices. *Fund. Inform.*, 2017. **153**(3):265–270. URL https://doi.org/10.3233/FI-2017-1540.

[12] Lorenzini D. An invitation to arithmetic geometry, volume 9 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1996. ISBN 0-8218-0267-4.

[13] Stichtenoth H. Algebraic function fields and codes. Universitext. Springer-Verlag, Berlin, 1993. ISBN 3-540-56489-6.

[14] Tobey RG. Algorithms for antidifferentiation of rational functions. Ph.D. thesis, Harvard, 1967.

[15] Yun DY. On Square-free Decomposition Algorithms. In: Proceedings of the Third ACM Symposium on Symbolic and Algebraic Computation, SYMSAC '76. ACM, New York, NY, USA, 1976 pp. 26–35. doi:10.1145/800205.806320. URL http://doi.acm.org/10.1145/800205.806320.

[16] RSFDGrC. International Conference on Rough Sets, Fuzzy Sets, Data Mining, and Granular-Soft Computing. http://dblp.uni-trier.de/db/conf/rsfdgrc/index.html. Accessed: 2015-08-29.

[17] Baker G, Hacker P. Wittgenstein: Understanding and Meaning, Volume 1 of an Analytical Commentary on the Philosophical Investigations, Part II: Exegesis 1-184. Wiley-Blackwell Publishing, 2004. ISBN 9780470753101. doi:10.1002/9780470753101. 2nd Edition.

[18] Szczuka MS, Sosnowski L, Krasuski A, Krenski K. Using Domain Knowledge in Initial Stages of KDD: Optimization of Compound Object Processing. *Fundamenta Informaticae*, 2014. **129**(4):341–364. doi:10.3233/FI-2014-975.

[19] Krasuski A, Jankowski A, Skowron A, Ślęzak D. From Sensory Data to Decision Making: A Perspective on Supporting a Fire Commander. In: 2013 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology, Atlanta, Georgia, USA, 17-20 November 2013, Workshop Proceedings [20], 2013 pp. 229–236. doi:10.1109/WI-IAT.2013.188. URL http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=6690661.

[20] 2013 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology, Atlanta, Georgia, USA, 17-20 November 2013, Workshop Proceedings. IEEE Computer Society, 2013. ISBN 978-1-4799-2902-3. URL http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=6690661.