Journal of Number Theory 165 (2016) 382–407

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Computation of integral bases ☆

Jens-Dietrich Bauch

Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven, The Netherlands

A R T I C L E   I N F O

Article history:
Received 31 July 2015
Received in revised form 3 January 2016
Accepted 11 January 2016
Available online 3 March 2016
Communicated by M. Pohst

Keywords:
p-Integral bases
Maximal order
Montes algorithm
Dedekind domain

A B S T R A C T

Let A be a Dedekind domain, K the fraction field of A, and $f \in A[x]$ a monic irreducible separable polynomial. For a given non-zero prime ideal $\mathfrak{p}$ of A we present in this paper a new characterization of a $\mathfrak{p}$-integral basis of the extension of K determined by f. This characterization yields in an algorithm to compute $\mathfrak{p}$-integral bases, which is based on the use of simple multipliers that can be constructed with the data that occurs along the flow of the Montes Algorithm. Our construction of a $\mathfrak{p}$-integral basis is significantly faster than the similar approach from [8] and provides in many cases a priori a triangular basis.

0. Introduction

Let A be a Dedekind domain, K the fraction field of A, and $\mathfrak{p}$ a non-zero prime ideal of A. By $A_{\mathfrak{p}}$ we denote the localization of A at $\mathfrak{p}$. Let $\pi \in \mathfrak{p}$ be a prime element of $\mathfrak{p}$.

Denote by $\theta \in K^{\text{sep}}$ a root of a monic irreducible separable polynomial $f \in A[x]$ of degree n and let $L = K(\theta)$ be the finite separable extension of K generated by θ. We

☆ This research was supported by MTM2012-34611 and MTM2013-40680 from the Spanish MEC and by the Netherlands Organisation for Scientific Research (NWO) under grant 613.001.011.

E-mail address: j.bauch@tue.nl.

http://dx.doi.org/10.1016/j.jnt.2016.01.011
0022-314X/© 2016 Published by Elsevier Inc.

denote by $\mathcal{O}$ the integral closure of A in L and by $\mathcal{O}_\mathfrak{p}$ the integral closure of $A_\mathfrak{p}$ in L. A $\mathfrak{p}$-integral basis of $\mathcal{O}$ is an $A_\mathfrak{p}$-basis of $\mathcal{O}_\mathfrak{p}$ (cf. Definition 3.1).

If A is a PID, then $\mathcal{O}$ is a free A-module of rank n, and its easy to construct an A-basis of $\mathcal{O}$ from the different $\mathfrak{p}$-integral bases, for prime ideals $\mathfrak{p}$ of A that divide the discriminant of f.

In this work we follow the approach from [8] to apply the notion of reduceness in the context of integral bases. By weakening the concept of reduceness we deduce a new characterization of $\mathfrak{p}$-integral bases (Theorem 3.2). This yields in an algorithm to compute a $\mathfrak{p}$-integral basis: We construct for any prime ideal $\mathfrak{P}$ of $\mathcal{O}$ lying over $\mathfrak{p}$ a local set $\mathcal{B}^*_\mathfrak{P} \subset \mathcal{O}$ and a multiplier $z_\mathfrak{P} \in L$ such that $\cup_{\mathfrak{P}|\mathfrak{p}} z_\mathfrak{P}\mathcal{B}^*_\mathfrak{P}$ is a $\mathfrak{p}$-integral basis of $\mathcal{O}$, where $z_\mathfrak{P}\mathcal{B}^*_\mathfrak{P}$ denotes the set we obtain by multiplying all elements in $\mathcal{B}^*_\mathfrak{P}$ by $z_\mathfrak{P}$. The construction of these local sets and the multipliers is based on the *Okutsu–Montes (OM) representations* of the prime ideals of $\mathcal{O}$ lying over $\mathfrak{p}$, provided by the Montes algorithm. In comparison with the existing methods from [7] and [8] our construction of the multipliers is much simpler (and faster) and results in many cases directly in a triangular $\mathfrak{p}$-integral basis $\mathcal{B}$ of $\mathcal{O}$, that is, $\mathcal{B} = \{b_0, \dots, b_{n-1}\}$, where $b_i = g_i(\theta)/\pi^{m_i}$ with $g_i \in A[x]$, monic of degree i and $m_i \in \mathbb{Z}$. Hence the transformation into a basis in HNF becomes especially efficient.

The article is divided into the following sections. In section 1 we summarize the Montes algorithm briefly and introduce the basic ingredients of our algorithm for the computation of a $\mathfrak{p}$-integral basis. That is, we define types, Okutsu invariants, and a local set $\mathcal{B}_\mathfrak{P} \subset A[x]$ (cf. Definition 1.7) for a prime ideal $\mathfrak{P}$ of $\mathcal{O}$ lying over $\mathfrak{p}$. In section 2 we introduce the notion of (semi-)reduced bases, which provides a new characterization of $\mathfrak{p}$-integral bases (Theorem 3.2) and a new method of constructing multipliers $z_\mathfrak{P}$, for any prime ideal $\mathfrak{P}$ of $\mathcal{O}$ over $\mathfrak{p}$, such that the union of the sets $\{z_\mathfrak{P} \cdot b(\theta)/\pi^{m_b} \mid b \in \mathcal{B}_\mathfrak{P}\}$, for $\mathfrak{P}|\mathfrak{p}$ and certain integers m_b, is a $\mathfrak{p}$-integral basis. If we assume that $A/\mathfrak{p}$ is finite with q elements and $\mathcal{R}$ is a set of representatives of $A/\mathfrak{p}$ then we will see that the complexity of the method is dominated by $O\left(n^{1+\epsilon}\delta \log q + n^{1+\epsilon}\delta^{2+\epsilon} + n^{2+\epsilon}\delta^{1+\epsilon}\right)$ operations in $\mathcal{R}$ (Lemma 3.10), where $\delta := v_\mathfrak{p}(\mathrm{Disc} f)$. In section 4 we consider the practical performance of our method in the context of algebraic function fields. We have implemented the method for the case $A = k[t]$, where k is a finite field or $k = \mathbb{Q}$. The package can be downloaded from `https://github.com/JensBauch/Integral_Basis`.

1. Montes algorithm

We consider the monic separable and irreducible polynomial $f \in A[x]$. For a non-zero prime ideal $\mathfrak{p}$ of A we denote the induced discrete valuation by $v_\mathfrak{p} : A \to \mathbb{Z} \cup \{\infty\}$ and the completion of K at $\mathfrak{p}$ by $K_\mathfrak{p}$. The valuation $v_\mathfrak{p}$ extends in an obvious way to $K_\mathfrak{p}$. Denote by $\hat{A}_\mathfrak{p}$ the valuation ring of $v_\mathfrak{p}$ and by $\mathfrak{m}_\mathfrak{p} = \mathfrak{p}\hat{A}_\mathfrak{p}$ its maximal ideal.

By the classical theorem of Hensel [11] the prime ideals of $\mathcal{O}$ lying over $\mathfrak{p}$ are in one-to-one correspondence with the monic irreducible factors of f in $\hat{A}_\mathfrak{p}[x]$.