UNIVERSITEIT•STELLENBOSCH•UNIVERSITY

jou kennisvennoot • your knowledge partner

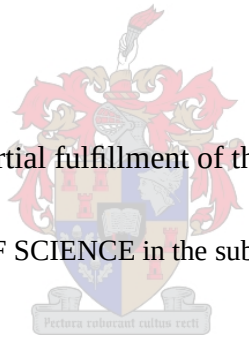
Studies on Factoring Polynomials over Global Fields

Author: ILHEM BENZAOUI

Supervisor : Prof Barry GREEN

Studies on Factoring Polynomials over Global Fields

By: ILHEM BENZAOUI



Thesis submitted in partial fulfillment of the requirements for the degree of

MASTERS OF SCIENCE in the subject of MATHEMATICS

at the

UNIVERSITY OF STELLENBOSCH

SUPERVISED BY: **Prof**. **Barry GREEN**

Department of Mathematics

Stellenbosch University

December 2007

Declaration

I, the undersigned, hereby declare that the work contained in this thesis is my own work and has not previously, in its entirety or in part, been submitted at any other university for a degree.

Signature: .....

Date: .....

Abstract

In this thesis, we surveyed the most important methods for factorization of polynomials over a global field, focusing on their strengths and showing their most striking disadvantages. The algorithms we have selected are all modular algorithms. They rely on the Hensel factorization technique, which can be applied to all global fields giving an output in a local field that can be computed to a large enough precision. The crucial phase of the reconstruction of the irreducible global factors from the local ones, determines the difference between these algorithms. For different fields and cases, different techniques have been used such as residue class computations, ideal calculus, lattice techniques.

The tendency to combine ideas from different methods has been of interest as it improves the running time. This appears for instance in the latest method due to van Hoeij, concerning the factorization over a number field. The ideas here can be used over a global function field in the form given by Belabas et al. using the logarithmic derivative instead of Newton sums.

Complexity analysis was not our objective, nevertheless it was important to mention certain results as part of the properties of these algorithms.

Opsomming

In hierdie proefskrif het ons die belangrikste metodes vir die faktorisering van polinome oor globale liggame bespreek en het op die vernaamste voordele en nadele klem gelê. Hierdie algoritmes is almal modulêr van aard en maak staat op die faktoriseringstegniek van Hensel, wat van toepassing is op enige globale liggaam wat oor ’n geskikte lokale liggaam tot die verlangde akkuraatheid uitgevoer kan word. Die kritieke punt by die herkonstruering van die onherleibare globale faktore vanuit die lokale faktore is die vernaamste verskil in die algoritmes.

Vir verskillende liggame en gevalle word verskillende tegnieke aangewend, soos byvoorbeeld residuklasberekeninge, ideal calculus en tralie tegnieke. Die tendens om idees van verskillende metodes saam te vat is van belang omdat die looptyd van die algoritmes hierdeur verbeter word. ’n Voorbeeld hiervan word gegee in die nuutste metode van van Hoeij, met betrekking tot faktorisering oor ’n getalleliggaam. Hierdie idees kan oor ’n globale liggaam toegepas word soos onlangs deur Belabas et al, waar die logaritmiese afgeleide in plaas van Newton somme gebruik word.

Die kompliksiteit van die metodes het nie deel van hierdie ondersoek uitgemaak nie, maar nogtans was dit belangrik om sekere resultate te noem toe die eienskappe van hierdie algoritmes bespreek word.

Acknowledgements

Words would not be sufficient to express my gratitude to my supervisor Prof Barry Green for providing me support and advice and for considering me not as a student but as a colleague and a friend. I have been overwhelmed by his kindness and patience with me. For that I wish to extend to him my sincere appreciation and consideration.

I would like to acknowledge the number theory team and their guests for the convivial discussions during the regular seminars and colloquia I had the chance to attend. I cite particularly: Dr Florian Breuer, Dr Arnold Keet, Prof Carl Maxson, Prof Georg Rück and Prof Ernst Gekeler.

Dr Claus Fieker, Dr Tadashi Tokieda, Dr Clemens Heuberger, and Prof Helmut Prodinger are gratefully acknowledged for answering my questions; and Dr Liz Moyer is acknowledged for providing me an important paper.

I would like to express my thanks to each and every one I have known in the University of Stellenbosch for the friendly atmosphere that surrounded me here. Many thanks go particularly to the wonderful people I met in the International Office, in the Library -especially the Interlending section-, in the binding service, and in the Mathematics department. Many thanks to all of them for being very helpful and very efficient in their work. I was really amazed! The Abrahams family as well, should receive hereby my heartiest thanks for their hospitality and kindness. *Baie baie dankie vir almal*!

I am also grateful to the University of Stellenbosch itself and to my former Institute AIMS, for contributing together in supporting me financially during my Msc studies. This achievement would not be possible without their support.

Lastly, I wish to thank every one from whom I learnt some Mathematics and/or I learnt to love Mathematics. I cite particularly Mr Lahcene Chebab who taught me the basics of logic and algebraic reasoning. Realising how fortunate I have been having him as the Mathematics' teacher during the three years of High-school, I deem it my duty to say:

قُمْ لِلمُعَلِّـمِ وَفِّـهِ التَّبجِـيلَ كَادَ المُعَلِّمُ أَن يَكُونَ رَسُولَا

I should not conclude without thanking my family for their support and encouragements.

And finally, I wish to gratefully thank my examiners for a generous feedback about this thesis.

Dedication

This work is dedicated to the memory of my dear Grandfather Ahmed. His soul and values enlightned my way during my journey far from my homeland.

Quotation

C’est faire qui est important
et non pas ce qui a été fait.

Contents

Notations and Abbreviations

$\mathbb{N}$, $\mathbb{Z}$	rings of natural numbers and rational integers
$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	fields of rational, real, complex numbers
$\mathbb{F}_q$	Finite Field of q elements
$\overline{\mathbb{Q}}$, $\bar{\mathbb{K}}$, $\bar{\mathbb{F}}_q$	the algebraic closure of these fields
$\mathbb{K}$, $\mathcal{O}_{\mathbb{K}}$	a global field and its ring of integers
$m_\alpha(\mathtt{Y})$	the minimal polynomial of an algebraic element α
$\mathcal{O}_{\mathfrak{p}}$	the valuation ring with maximal ideal $\mathfrak{p}$
$\mathbb{K}_{\mathfrak{p}}$ $\mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$	a local field and its ring of integers
$W_{\mathtt{k}}(\mathbb{F}_q)$	a ring of $q^{\mathtt{k}}$ element (ring of Witt vectors)
$deg(f)$	degree of the polynomial f
$lc(f)$	leading coefficient of the polynomial f
$discr(f)$	discriminant of the polynomial f
$discr(\mathbb{K})$	discriminant of the field $\mathbb{K}$
CRT	Chinese Remainder Theorem
CRA	Chinese Remainder Algorithm
UFD	Unique Factorization Domain
PID	Principal Ideal Domain
GCD	Greatest Common Divisor
LLL	standing for A.K. Lenstra, H. W. Lenstra Jr, and L. Lovász
$cont(f)$	The content of a polynomial f
$pp(f)$	The primitive part of the polynomial f
$d(\Lambda)$	the determinant of a lattice Λ
$\Pi(\Lambda)$	the fundamental domain of a lattice Λ
O_d	the orthogonality defect of a lattice basis in $\mathbb{R}^n$
$\lvert\ \rvert$	the absolute value in $\mathbb{C}$
$\lvert\ \rvert_\infty$	the ordinary norm Sup in $\mathbb{R}^n$
$\lVert\ \rVert$	the Euclidean norm on $\mathbb{R}^n$, also generalised to polynomial rings

$\lfloor z \rceil := \lfloor z + \frac{1}{2} \rfloor$	the operator rounding to the nearest integer
r_{max}	The radius of the largest ball inscribed in the fundamental domain of a lattice Λ
$W^{\perp}$	the orthogonal complement of a vector space $W \subset \mathbb{R}^n$
$b_1^*, \cdots, b_k^*$	the Gram-Schmidt orthogonal basis obtained from a basis $b_1, \cdots, b_k$ of a lattice or a vector space.
b^{tr}	the transpose of the vector b
$\mathcal{H}(f)$	The height of a polynomial f
$\mathcal{M}(f)$	The Mahler measure of f
$\mathcal{L}(f)$	The length of f
$defect(\alpha)$	the defect of the integral basis $1, \alpha, \cdots, \alpha^{m-1}$
σ_i	the distinct embeddings of $\mathbb{K}$ in an algebraic closure $\bar{K}$ of K
$N(a)$	the (absolute) norm of an element in an algebraic extension of K
$Res_{\mathtt{Y}}(u(\mathtt{Y}), v(\mathtt{Y}))$	the resultant of the two polynomials u and v
$\binom{d}{j}$	binomial coefficient
$\Re e(z)$, $\Im m(z)$, $\bar{z}$	real and imaginary parts, and the conjugate of the complex number z
T_2	the T_2-norm
$\mathcal{S}_i(h)$	the i^{th} *Newton sum* of h
$\langle a \rangle$	the ideal genarated by a
$\mathbb{L}_{\infty}$	field of Puiseux series at the place at infinity

Introduction

In this thesis, we intend to study polynomial factorization. Our work is motivated by the very recent publications due to Pohst and Omaña (in [Om-P] and [POH 2]), and to Belabas, van Hoeij, Klüners, and Steel (in [B-H-K-S]). Their results, together with Lenstra's, Trager's and Weinberger & Rothschild's, will form the core of this thesis, which will be mainly a survey of the most important results up-to-date. A deeper theoretical investigation including implementations and trial of some variants for the algorithms given here, might be the subject of later research since it is beyond the scope of this thesis. An important goal here, from a number theoretical point of view, consists in a better understanding of the algebraic structure of global fields and their rings of integers, in addition to an entrance into, and an appreciation of, the area of Algorithmic Algebraic Number Theory.

The importance of the problem of factorization of univariate/multivariate polynomials over finite/infinite local/global fields, made it a favorite topic for PhD theses of many mathematicians since early in the 70's. Those we are aware of are the PhD's of: D.R. Musser (Wisconsin, 1971), E. Kaltofen (New York, 1982), A.K. Lenstra (Amsterdam, 1984), P. Guan (Ohio, 1985), J.A. Abbott (Bath, 1988), M.J. Encarnación (Linz, 1995), L. Zhi (Beijing, 1996), X-F Roblot (Bordeaux, 1997), J-F Ragot (Limoges, 1997), F. Abu-Salem (Oxford, 2004). And surprisingly, B.M. Trager, whose thesis was on the integration of algebraic funtions (MIT, 1985) and M.H.F. van Hoeij, whose thesis was on the factorization of linear differential operators (Nijmegen, 1996), added such an important contribution to the theory of polynomial factorization that their names have became as well-known for this theory as Berlekamp's, Zassenhaus', and Lenstra's.

The factorization of polynomials, in general, is an important operation needed in many problems of computational algebra, some of them coming from: symbolic computation, cryptography, coding theory, number theory.... For example, it is a crucial step in computing an explicit basis of Newforms for a space of Modular forms.

This wide need for factorization of polynomials makes it an important subject of investigation for math-

ematicians and computer scientists, and already in 1707, Isaac Newton, in his "Arithmetica Universalis", gave a method for finding linear and quadratic factors of polynomials with integer coefficients. This method was extended by Nicolas Bernoulli in 1708, and in 1793 the astronomer Friedrich von Schubert extended this method more explicitely and gave a finite-step algorithm for computing all factors of degree d of a univariate polynomial with integer coefficients.

About 90 years later, Leopold Kronecker rediscovered Schubert's method and also gave algorithms for factoring univariate and multivariate polynomials with integer coefficients. The key idea in these algorithms is that a polynomial of degree n is completely determined by its values at $(n+1)$ different points, by means of the Lagrange interpolation method for instance. Hence one can reduce the factorization of a polynomial to the factorization of its values at these different points, and then collect information about the polynomial factors sought.

Kronecker is then considered as the first inventor of a general algorithm for factorization of polynomials with integer coefficients, which can be applied also to the factorization of polynomials over algebraic extension fields. The idea was to reduce this factorization to one over the ground field, which can be either the field of the rational numbers, in the case of an algebraic number field, or the field of rational functions, in the case of an algebraic function field. This was one of the first attempts to study simultaneously: the theory of algebraic numbers and the one of algebraic functions in one variable, which we will investigate simultaneously in this thesis.

Dedekind and Weber have observed that many of the results obtained by Dedekind while studying and generalising the properties of the rings of integers in number fields, also apply to the rings of integers in funtion fields. This invites one to unify the study of certain problems in number and function fields. However, such a general theory had to wait until more abstract concepts in algebra have been set up.

For our work, we not only need deep results and concepts from algebra, but also some tools from the geometry of numbers for both number and function fields. Those for the latter fields became available only quite recently with the work by M. Schörnig in his PhD thesis (Berlin, 1996).

We recall that a *global field* $\mathbb{K}$ is either an *algebraic number field*, that is, a finite extension of the rational number field $\mathbb{Q}$, or else an *algebraic function field*, that is, a finite extension of a field $\mathbb{F}_q(t)$ of rational functions in an indeterminate t over a finite field $\mathbb{F}_q$.

The arithmetic in a global field relies on the properties of its *ring of integers*. For a rational global field ($\mathbb{Q}$ or $\mathbb{F}_q(t)$), the ring of integers is $\mathbb{Z}$ or $\mathbb{F}_q[t]$, respectively, and it is well knwon that these two rings

have many properties in common. Both rings are *Euclidean domains*, and hence PIDs (Principal Ideal Domains) and UFDs (Unique Factorization Domains); both have the property that the *residue class ring* of any non-zero ideal is *finite*, both rings have infinitely many *prime elements*, and both rings have finitely many *units*. (cf [ROS] for a proof of these statements).

Consequently, we also find common or similar properties for the rings of integers of a general number field and a general function field. These rings are the *integral closure* of $\mathbb{Z}$ (respectively $\mathbb{F}_q[t]$) in the extension field. One of the main properties they share is the fact that they are both *Dedekind Domains* (cf [Fr-T] and [ART]). This will play an important role in our work because Dedekind Domains retain desirable properties of $\mathbb{Z}$, in particular, the possibility and unicity of decomposition of ideals into a product of prime ideals (cf [EIC]).

We will be considering polynomial rings over such Dedekind domains and over their quotient fields, exploring different results related to the factorization of primitive univariate polynomials in the above polynomial rings. Most of our discussions will be around some algorithm that, in a specific context, gives the complete factorization of our polynomial. A factorization is said to be *complete* when all the irreducible factors are produced.

We recall that in our context, rings will always mean commutative rings with unit, even if it is not specified, and we use gothic letters to denote ideals, following Hilbert who introduced this notation in his Zahlbericht (1897).

We have divided our thesis into four chapters preceded by this introduction which gives a survey and brief introduction to the subject. The four chapters are organized as follows.

In the first chapter, we give some important tools that will be used throughout all the thesis, starting by introducing the principle for *modular algorithms*, then giving some important theorems needed, mainly the Chinese Remainder Theorem and Hensel's and Gauss' lemmata. We will also introduce the quite recent notion of lattice-basis reduction, and for the case of a number field, we give the LLL algorithm for basis reduction and all the properties of an LLL reduced basis. We end the chapter by some assumptions to be made throughout the thesis, namely we have chosen to consider a monic squarefree polynomial with integral coefficients.
For the case of a number field, we have also chosen to study extensively the problem of factorization of polynomials over an extension field (with $[\mathbb{K} : \mathbb{Q}] \geq 2$), the factorization of polynomials over the rationals being considered known. We have recalled the important results concerning the factorization of polynomials over the rationals in the first chapter as we aim to show how they extend to a general

number field. And for lack of space, we will assume the factorization techniques over finite fields known refering to the bibliography.

Trager's method of factorization over algebraic extension fields will be the subject of the second chapter. It has the advantage of being applicable simultaneously to number and function fields, relying on the algebraic properties of the extention fields and using the norm as a tool. The norm map, which is a homomorphism that sends elements of an extension field to elements in the ground field, will enable reducing the problem of factoring a polynomial with coefficients in the extention field, to the problem of factoring another polynomial over the ground field, assuming we have enough tools to solve the latter problem. Usually, the ground field is the rational number field for which a whole bunch of efficient factorization algorithms are known, but Trager's method can also be applied to towers of algebraic extention fields as well. Encarnación's quite recent improvement of this method will also be given.

Other techniques, which we will call *direct factorization methods* by contrast to Trager's indirect one, will be presented in the latter chapters.
We dedicated the third chapter to the direct factorization methods over a general number field, and the fourth chapter to the direct factorization methods over a function field. This is done separately as not all the algorithms presented work equally for number and function fields.
Weinberger and Rothschild's algorithm, the LLL factorization algorithm, and van Hoeij's algorithm, are applicable only to number fields. They will be described and analysed in the third chapter.
We dedicated the last chapter to Pohst and Omaña's results for the case of a global function field.

CHAPTER ONE

PREREQUISITES

1.1 Homomorphism methods and modular algorithms

An important class of problems in number theory including the theory of function fields, can be dealt with using homomorphisms, transporting the problem to a simpler domain where one can see how to solve it more easily. The original problem will then be solved by means of some tools that allow one to return to the original domain.

The first well known tool, which we are interested in, is the *Chinese Remainder Theorem* (CRT).

Theorem 1.1

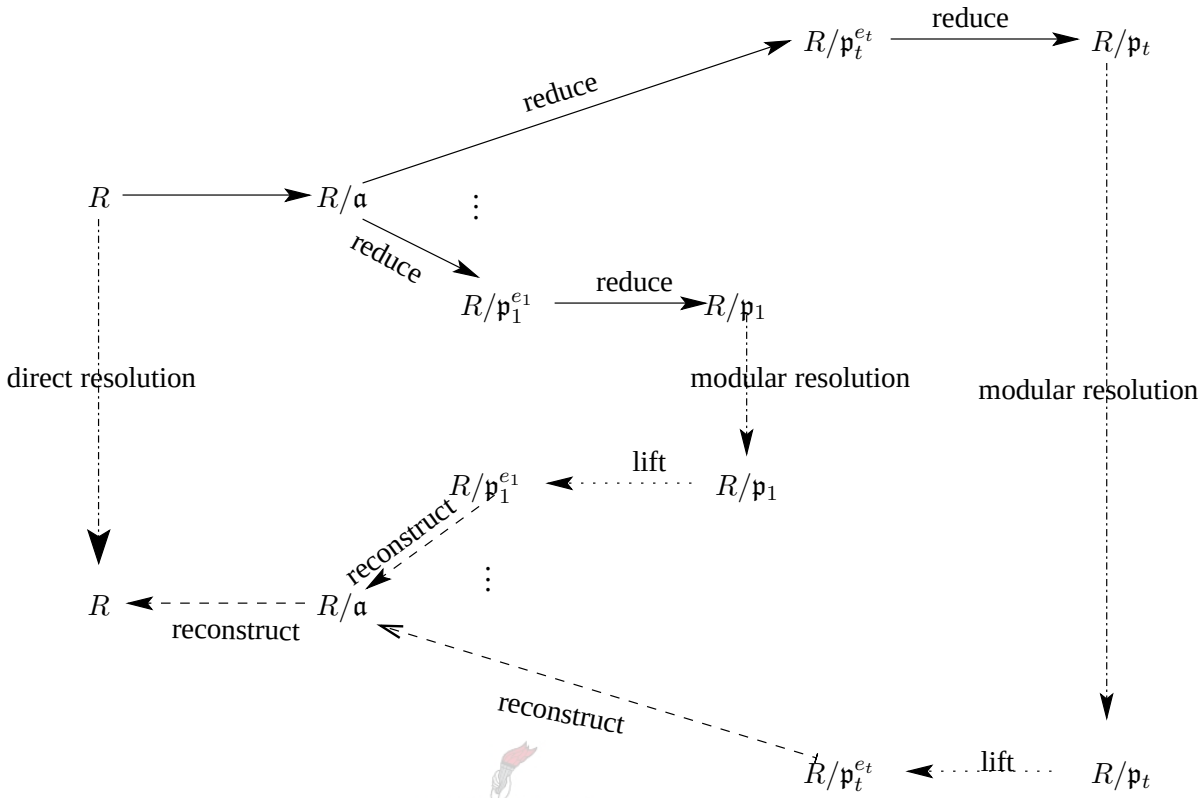
Let R be an integral domain, and let $\{\mathfrak{a}_1, \cdots, \mathfrak{a}_t\}$ be a set of relatively prime ideals of R (i.e $\mathfrak{a}_i + \mathfrak{a}_j = R$ for $i \neq j$). Then the map: $R \longrightarrow \prod_{i=1}^{t} R/\mathfrak{a}_i$, is surjective. It's kernel is $\prod_{i=1}^{t} \mathfrak{a}_i = \bigcap_{i=1}^{t} \mathfrak{a}_i$. And hence, there is a ring isomorphism:

$$R/\mathfrak{a}_1 \cdots \mathfrak{a}_t \cong \prod_{i=1}^{t} R/\mathfrak{a}_i$$

This theorem gave rise to the so called *modular algorithms* where instead of solving an algebraic computational problem over an integral domain R directly, one solves it modulo one or several ideals of this domain and uses these modular solutions together to find the solution in R.

An important gain in efficiency can be realized when the computation in $R/\mathfrak{a}$ is easy. This is the case when $\mathfrak{a}$ is a maximal ideal of R and $R/\mathfrak{a}$ is finite (e.g $R = \mathbb{Z}$, $\mathfrak{a} = p\mathbb{Z}$), thus, the residue class ring $R/\mathfrak{a}$ is actually a finite field.

Again, if we assume $R = \mathcal{D}$ a Dedekind domain, then every non-zero prime ideal of R is maximal. And since every ideal of R is uniquely expressible as a product of nonzero prime ideals of R, up to order of factors, we can always solve any algebraic computational problem over R using the following general scheme, where we note that the dotted arrows show procedures while the plain ones show homomorphisms,



and where we assume the ideal $\mathfrak{a}$ of R to be expressible as:

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}$$

with the $\mathfrak{p}_i$ distinct prime ideals of R and the e_i positive integers.

The Chinese Remainder Theorem will be then used for the first reconstruction stage, but some more work is needed for the second stage, which we will clarify later for our context.

The passage from $R/\mathfrak{p}_i$ to $R/\mathfrak{p}_i^{e_i}$ is ensured by the Hensel lifting which will be discussed in the next section and which will turn out to be more useful in practice since it deals with only one prime ideal.

For a general ideal $\mathfrak{a}$, we may be faced with the serious drawback of the general scheme above, namely the possibility that a huge number of the image problems need to be solved. It turns out that this number grows exponentially with the size of the solution, which interferes with the efficiency of our method. This should then be taken into consideration while choosing the moduli.

In addition, our choice of the moduli should enable us to recover the solution in the original domain R which requires finding a bound on the solution in R at first.

1.2 Hensel lifting

Early in the 1900's, K. Hensel gave a new theorem which was one of his motivations for introducing p-adic numbers. He published it in 1918 under the title "A new theorem of algebraic numbers". This theorem is well known since then as *Hensel's lemma*.

There are many different formulations of this lemma, all of them give equivalent conditions for a valued field to be Henselian.

Without entering into details, and without giving the exact definition of a Henselian field, we just mention briefly the important result that a complete field for a rank-1 valuation is Henselian (cf [Pr-D]). This result applies to the fields we are interested in. In addition, we refer to A. M. Robert [1] for some applications of the Hensel's lemma in contexts other than ours.

Here, we will give two forms of Hensel's lemma that we think are most relevant to our work.

Theorem 1.2 Hensel's Lemma

Let R be a local ring with maximal ideal $\mathfrak{M}$ and residue field $\mathbf{k} = R/\mathfrak{M}$.

Assume that R is $\mathfrak{M}$-adically complete.

For any polynomial $f(\mathtt{X}) \in R[\mathtt{X}]$, let $\bar{f}(\mathtt{X}) \in \mathbf{k}[\mathtt{X}]$ denote its residue $mod\,\mathfrak{M}$.

Let $f(\mathtt{X}) \in R[\mathtt{X}]$ be monic and such that there is a factorization:

$$\bar{f}(\mathtt{X}) = u(\mathtt{X})v(\mathtt{X}) \;\; in\; \mathbf{k}[\mathtt{X}]$$

where $u(\mathtt{X})$ and $v(\mathtt{X})$ are monic and relatively prime.

Then there exists a factorization:

$$f(\mathtt{X}) = h(\mathtt{X})k(\mathtt{X}) \;\; in\; R[\mathtt{X}]$$

with $h(\mathtt{X})\,,\; k(\mathtt{X})$ monic, such that:

$$\bar{h}(\mathtt{X}) = u(\mathtt{X})\,,\; \bar{k}(\mathtt{X}) = v(\mathtt{X})$$

For practical applications we actually prefer a constructive form of Hensel's lemma that yields an algorithm for lifting factorizations.

We give here the one given by Pohst and Zassenhaus in [P-Z].

[1] "A course in p-adic analysis", Springer-Verlag 2000

Theorem 1.3 Hensel's Lemma: Constructive form

Let R be a commutative ring, $\mathfrak{b}$ an ideal of R and $f\,,\ f_{1,0}\,,\ f_{2,0} \in R[\mathtt{X}]$ be monic non-constant polynomials such that there is a factorization:

$$f \equiv f_{1,0} f_{2,0}\ mod\, \mathfrak{b}[\mathtt{X}]$$

with $f_{1,0}\,,\ f_{2,0}$ relatively prime $mod\, \mathfrak{b}[\mathtt{X}]$, that is:

$$a_{1,0} f_{1,0} + a_{2,0} f_{2,0} = 1 + a_{0,0} \quad \big(\textit{for some } a_{i,0} \in R[\mathtt{X}],\ 0 \leq i \leq 2, a_{0,0} \in \mathfrak{b}[\mathtt{X}]\big)$$

Then for every $\mathtt{k} \in \mathbb{N}$ there holds a congruence factorization

$$f \equiv f_{1,\mathtt{k}} f_{2,\mathtt{k}}\ mod\, \mathfrak{b}^{2^{\mathtt{k}}}[\mathtt{X}]$$

with $f_{1,\mathtt{k}} f_{2,\mathtt{k}} \in R[\mathtt{X}]$ monic non-constant polynomials, satisfying the coherence condition

$$f_{i,\mathtt{k}} \equiv f_{i,0}\ mod\, \mathfrak{b}[\mathtt{X}] \quad (i = 1, 2)$$

and an equation

$$a_{1,\mathtt{k}} f_{1,\mathtt{k}} + a_{2,\mathtt{k}} f_{2,\mathtt{k}} = 1 + a_{0,\mathtt{k}}$$
$$\Big(a_{i,\mathtt{k}} \in R[\mathtt{X}], deg(a_{i,\mathtt{k}}) < deg(f_{3-i,\mathtt{k}})\, 0 \leq i \leq 2, a_{0,\mathtt{k}} \in \mathfrak{b}^{2^{\mathtt{k}}}[\mathtt{X}]\Big)$$

The key idea in the proof of this theorem was the construction of a solution of a congruence equation:

$$a_1(\mathtt{X}) f_1(\mathtt{X}) + a_2(\mathtt{X}) f_2(\mathtt{X}) \equiv b(\mathtt{X})\ \ mod\, \mathfrak{b}[\mathtt{X}] \tag{1.1}$$

given that f_1 and f_2 are relatively prime modulo that ideal or a power of it, and using the fact that it is possible to satisfy the degree condition by reducing modulo suitable polynomials. This follows since both *remainder* and *quotient* obtained by a long division of any element of an ideal $\mathfrak{b}[\mathtt{X}]$, by any polynomial in $R[\mathtt{X}]$, actually belong to $\mathfrak{b}[\mathtt{X}]$, (the ideal $\mathfrak{b}$ of R being stable for the operations involved by the long division algorithm).

The above congruence equation (1.1) is not obvious, and already in the case $R = \mathbb{Z}\,,\ \mathfrak{b} = p\mathbb{Z},\ p$ prime, we know that the factor ring $\mathbb{Z}/p^{\mathtt{k}}\mathbb{Z}[\mathtt{X}]$ need not be a UFD, nor need there always be a GCD for two given elements. In [ZAS 2], Zassenhaus gave the conditions for the existence of GCD's in such factor rings, and explains, in greater detail, the algorithm he suggested earlier in his seminal paper [ZAS 1]. His second paper came in response to a remark of D. Yun who studied extensively the Hensel lemma in his MIT PhD thesis entitled " *The Hensel Lemma in Algebraic Manipulations*" (1974).

The method given in the theorem above is called a quadratic Hensel lifting. The original Hensel construction, which is linear, lifts a factorization from $mod\, \mathfrak{b}^{\mathtt{k}}[\mathtt{X}]$ to $mod\, \mathfrak{b}^{\mathtt{k}+1}[\mathtt{X}]$ at the $\mathtt{k}^{\text{th}}$ step, while the

quadratic one lifts a factorization from $mod\, \mathfrak{b}^{2^k}[\mathtt{X}]$ to $mod\, \mathfrak{b}^{2^{k+1}}[\mathtt{X}]$.
Lots of work has been done to implement and compare varieties of the two approaches (see e.g [ABB] or [G-G]), the quadratic lift seems to converge faster. Nevertheless, the linear one requiring less computation at each step, may be the best choice in different circumstances.

Here, following Pohst and Zassenhaus, we choose the quadratic Hensel Construction, giving the algorithm below which provides a subroutine that can be iterated up to the accuracy needed.

Algorithm 1.4 "Hensel Lifting" (cf [Om-P])

Input. *An integral domain R with a proper ideal $\mathfrak{b}$ and monic non-constant polynomials*
$f(\mathtt{X})\,,\ h(\mathtt{X})\,,\ k(\mathtt{X}) \in R[\mathtt{X}]$ *such that:*

$$\begin{aligned} f(\mathtt{X}) &\equiv h(\mathtt{X})k(\mathtt{X}) && mod\, \mathfrak{b}[\mathtt{X}] \\ u(\mathtt{X})h(\mathtt{X}) + v(\mathtt{X})k(\mathtt{X}) &\equiv 1 && mod\, \mathfrak{b}[\mathtt{X}] \end{aligned}$$

for suitable $u(\mathtt{X})\,,\ v(\mathtt{X}) \in R[\mathtt{X}]$

Output. *Monic polynomials* $\tilde{h}(\mathtt{X})\,,\ \tilde{k}(\mathtt{X}) \in R[\mathtt{X}]$ *satisfying:*

$$\begin{aligned} f(\mathtt{X}) &\equiv \tilde{h}(\mathtt{X})\tilde{k}(\mathtt{X}) && mod\, \mathfrak{b}^2[\mathtt{X}] \\ h(\mathtt{X}) &\equiv \tilde{h}(\mathtt{X}) && mod\, \mathfrak{b}[\mathtt{X}] \\ k(\mathtt{X}) &\equiv \tilde{k}(\mathtt{X}) && mod\, \mathfrak{b}[\mathtt{X}] \\ \tilde{u}(\mathtt{X})\tilde{h}(\mathtt{X}) + \tilde{v}(\mathtt{X})\tilde{k}(\mathtt{X}) &\equiv 1 && mod\, \mathfrak{b}^2[\mathtt{X}] \end{aligned}$$

with $\tilde{u}(\mathtt{X})\,,\ \tilde{v}(\mathtt{X}) \in R[\mathtt{X}]$ *and* $deg(\tilde{u}) < deg(\tilde{k})\,,\ deg(\tilde{v}) < deg(\tilde{h})$

Step 1. *Set* $a(\mathtt{X}) := f(\mathtt{X}) - h(\mathtt{X})k(\mathtt{X})$, *and* $b(\mathtt{X}) := u(\mathtt{X})h(\mathtt{X}) + v(\mathtt{X})k(\mathtt{X}) - 1$

Step 2. *Set*

$$\begin{aligned} c(\mathtt{X}) &:= Rem\,(v(\mathtt{X})a(\mathtt{X}), h(\mathtt{X})), \quad \tilde{h}(\mathtt{X}) := h(\mathtt{X}) + c(\mathtt{X}), \\ d(\mathtt{X}) &:= Rem\,(u(\mathtt{X})a(\mathtt{X}), k(\mathtt{X})), \quad \tilde{k}(\mathtt{X}) := k(\mathtt{X}) + d(\mathtt{X}), \end{aligned}$$

Step 3. *Set* $e(\mathtt{X}) := b(\mathtt{X}) + u(\mathtt{X})c(\mathtt{X}) + v(\mathtt{X})d(\mathtt{X})$, *and*

$$\tilde{u}(\mathtt{X}) := Rem\left(u(\mathtt{X})(1 - e(\mathtt{X})), \tilde{k}(\mathtt{X})\right),\ \ \tilde{v}(\mathtt{X}) := Rem\left(v(\mathtt{X})(1 - e(\mathtt{X}), \tilde{h}(\mathtt{X})\right)$$

Where $Rem(\alpha, \beta)$ *denotes the remainder of the division of* α *over* β.

The following example will illustrate this algorithm.

Example: Let $R = \mathbb{Z}$, $\mathfrak{b} = 3\mathbb{Z}$ and $f(\mathtt{X}) = \mathtt{X}^4 - 394\mathtt{X}^3 - 4193\mathtt{X}^2 + 126\mathtt{X} + 596 \in \mathbb{Z}[\mathtt{X}]$. Then

$$\begin{aligned} f(\mathtt{X}) &\equiv \mathtt{X}^4 - \mathtt{X}^3 + \mathtt{X}^2 - 1 \ \ mod\, 3 \\ &\equiv (\mathtt{X}^2 + \mathtt{X} + 1)(\mathtt{X}^2 + \mathtt{X} - 1) \ \ mod\, 3 \end{aligned}$$

Let [2]: $h(\mathtt{X}) = \mathtt{X}^2 + \mathtt{X} + 1$ and $k(\mathtt{X}) = \mathtt{X}^2 + \mathtt{X} - 1$

So $f(\mathtt{X}) \equiv h(\mathtt{X})k(\mathtt{X}) \ \ mod\, 3$, with $h(\mathtt{X})$ and $k(\mathtt{X})$ relatively prime since they don't have common roots.

Let's apply **Algorithm 1.4** to lift this factorization to one $mod\, 3^2$.

Step 0. By means of the Extended Euclidean Algorithm, we can always compute $u(\mathtt{X}),\ v(\mathtt{X}) \in \mathbb{Z}[\mathtt{X}]$ such that $u(\mathtt{X})h(\mathtt{X}) + v(\mathtt{X})k(\mathtt{X}) \equiv 1 \ \ mod\, 3$ with $deg(v) < deg(h) = 2$ and $deg(u) < deg(k) = 2$, but we notice here that it suffices to take $u(\mathtt{X}) = -1$ and $v(\mathtt{X}) = +1$.

Step 1. $a(\mathtt{X}) = f(\mathtt{X}) - h(\mathtt{X})k(\mathtt{X}) = -396\mathtt{X}^3 - 4194\mathtt{X}^2 + 126\mathtt{X} + 597$

$b(\mathtt{X}) = u(\mathtt{X})h(\mathtt{X}) + v(\mathtt{X})k(\mathtt{X}) - 1 = -3$

Note that $a(\mathtt{X}) \in 3\mathbb{Z}[\mathtt{X}]$, idem for $b(\mathtt{X})$.

Step 2. Let $c^*(\mathtt{X}) = v(\mathtt{X})a(\mathtt{X})$

$d^*(\mathtt{X}) = u(\mathtt{X})a(\mathtt{X})$

By two long divisions we get:

$$\begin{aligned} c^*(\mathtt{X}) &= (-396\mathtt{X} - 3798)h(\mathtt{X}) + (4320\mathtt{X} + 4395) \\ d^*(\mathtt{X}) &= (396\mathtt{X} + 3798)k(\mathtt{X}) + (-3528\mathtt{X} + 3201) \end{aligned}$$

Hence: $c^*(\mathtt{X}) = Rem(c^*, h) = 4320\mathtt{X} + 4395$ and $d^*(\mathtt{X}) = Rem(d^*, k) = -3528\mathtt{X} + 3201$

$$\begin{aligned} \text{Define} \quad \tilde{h}(\mathtt{X}) &= h(\mathtt{X}) + c(\mathtt{X}) \\ &= \mathtt{X}^2 + 4321\mathtt{X} + 4396 \\ &= \mathtt{X}^2 + (9 \times 480 + 1)\mathtt{X} + (9 \times 488 + 4) \\ \tilde{k}(\mathtt{X}) &= k(\mathtt{X}) + d(\mathtt{X}) \\ \text{Hence:} \quad \tilde{h}(\mathtt{X})\tilde{k}(\mathtt{X}) &\equiv \mathtt{X}^4 + 2\mathtt{X}^3 + \mathtt{X}^2 + 2 \ \ mod\, 9 \\ &\equiv f(\mathtt{X}) \qquad\qquad mod\, 9 \end{aligned}$$

Step 3. $e(\mathtt{X}) := b(\mathtt{X}) + uc + vd = -(9 \times 872\mathtt{X} + 9 \times 133)$

Since $deg(u) = deg(v) = 0$, we don't need to reduce $u(\mathtt{X})(1 - e(\mathtt{X}))$ and $v(\mathtt{X})(1 - e(\mathtt{X}))$.

We take:

$\tilde{u}(\mathtt{X}) = u(\mathtt{X})(1 - e(\mathtt{X})) = -\left((9 \times 872)\mathtt{X} + (9 \times 133 + 1)\right)$

$\tilde{v}(\mathtt{X}) = v(\mathtt{X})(1 - e(\mathtt{X})) = (9 \times 872)\mathtt{X} + (9 \times 133 + 1)$

which satisfy $\tilde{u}\tilde{h} + \tilde{v}\tilde{k} \equiv 1 \ \ mod\, 9$.

We refer to Geddes et al. in [G-C-L] for many more examples illustrating the linear Hensel Lifting and other forms of it.

[2] For this example of illustration, we do not care whether $f(\mathtt{X})$ preserves squarefreeness $mod\, 3$, for it is not a requirement for Hensel's Lemma.

1.3 Gauss lemma

1.3.1 Algebraic properties of univariate polynomial rings

Let R be a ring.

The following theorem summarises most of the algebraic properties of the ring $R[\mathtt{X}]$.

Theorem 1.5

1. *If R is an integral domain, so is $R[\mathtt{X}]$. The units of $R[\mathtt{X}]$ being exactly those of R, i.e $(R[\mathtt{X}])^* = R^*$.*
2. *If R is a UFD, so is $R[\mathtt{X}]$. Its primes are either the primes of R or the polynomials of $R[\mathtt{X}]$, that cannot be factored, apart from units and associates.*
3. *If R is a Euclidean domain, then $R[\mathtt{X}]$ is a UFD.*
4. *R is a field, then $R[\mathtt{X}]$ is a Euclidean domain with valuation $v(f(\mathtt{X})) = deg(f(\mathtt{X}))$.*
5. *If R is a Dedekind domain that is not a UFD, with quotient field K, then at least property (1.) applies to $R[\mathtt{X}]$ and (4.) applies to $K[\mathtt{X}]$.*

We recall that in a UFD:

- GCD's exist and are unique up to units.
- Primes and irreducibles coincide.
- The factorization of elements into primes is unique.

Property (2.) is actually an important theorem due to Gauss, the proof of which relies on another important result known as Gauss' Lemma, which we will introduce after some necessary definitions.

1.3.2 Content and primitive part of a polynomial

Let R be a UFD with quotient field K, and consider a nonzero polynomial $f \in R[\mathtt{X}]$. A first step in the factorization of $f(\mathtt{X})$ is to extract the units and the constants.

Example: $R = \mathbb{Z}$

$$\begin{aligned} f(\mathtt{X}) &= -4\mathtt{X}^3 - 8\mathtt{X}^2 + 6\mathtt{X} - 18 \\ &= (-1)(2)(2\mathtt{X}^3 + 4\mathtt{X}^2 - 3\mathtt{X} + 9) \end{aligned}$$

This is always possible over a UFD, it suffices to consider the GCD of the coefficients of $f(\mathtt{X})$.

Definition 1.6

The content *of a nonzero polynomial $f(\mathtt{X}) \in R[\mathtt{X}]$, where R is a UFD, denoted $cont(f(\mathtt{X}))$, is the GCD of its coefficients, up to associates. The polynomial $f(\mathtt{X})/cont(f(\mathtt{X}))$ will then have content 1. It is called the* primitive part *of $f(\mathtt{X})$, and denoted $pp(f(\mathtt{X}))$*

Remark:

The definition of content and primitive parts can be extended to polynomials $f(\mathtt{X}) \in K[\mathtt{X}]$, where K is the quotient field of the UFD R, as follows:

Write: $f(\mathtt{X}) = \sum b_i \mathtt{X}^i / d$, where $b_i \in R$ and $d \in R \setminus \{0\}$ is a common denominator of the coefficients of f. Then:

$$cont(f(\mathtt{X})) := \frac{1}{d} cont\left(\sum b_i \mathtt{X}^i\right) \quad \text{and} \quad pp(f(\mathtt{X})) = f(\mathtt{X})/cont(f(\mathtt{X})) \text{ as usual.}$$

This yields a unique representation of $f(\mathtt{X})$ in the form:

$$f(\mathtt{X}) = cont(f(\mathtt{X})) \cdot pp(f(\mathtt{X}))$$

By convention, we define: $cont(0) = 0\ ,\ pp(0) = 1$.

Definition 1.7

A non zero polynomial $f(\mathtt{X}) \in R[\mathtt{X}]$, where R is a UFD, is said to be primitive *if it has content 1, i.e it is a normalised polynomial with relatively prime coefficients.*

In particular, a non zero monomial is primitive if it is monic.

Example:

$$R = \mathbb{Z}, \quad f(\mathtt{X}) = 3\mathtt{X}^2 - 2\mathtt{X} + 25$$
$$R = \mathbb{Q}, \quad f(\mathtt{X}) = \mathtt{X}^2 + \frac{2}{3}\mathtt{X} - 9$$

Note that, over a field, primitive polynomials are the monic ones.

Remark:

If $f(\mathtt{X})$ is a polynomial over a UFD R, then the coefficients of its primitive part lie in R.

Lemma 1.8

Let $f(\mathtt{X}) \in R[\mathtt{X}]$, where R is a UFD with quotient field K. Then for every $c \in K, c \neq 0$

$$cont\left(c \cdot f(\mathtt{X})\right) = c \cdot cont(f(\mathtt{X})) \quad \text{and} \quad pp\left(c \cdot f(\mathtt{X})\right) = pp\left(f(\mathtt{X})\right)$$

Note that our definition of the content and primitive part of a polynomial yields:

$$cont(c) = c\ ,\ pp(c) = 1$$

Hence the above equalities can be written:

$$cont\left(c \cdot f(\mathtt{X})\right) = cont(c) \cdot cont(f(\mathtt{X})) \quad \text{and} \quad pp\left(c \cdot f(\mathtt{X})\right) = pp(c) \cdot pp\left(f(\mathtt{X})\right)$$

1.3.3 Gauss lemma over UFD's and Dedekind domains

Theorem 1.9 Gauss Lemma

Let R be a UFD. Then, the product of two primitive polynomials in $R[\mathtt{X}]$ is primitive.

Proof:

Let $f(\mathtt{X})\,,\ g(\mathtt{X}) \in R[\mathtt{X}]$ be two primitive polynomials, and let $p \in R$ be a prime.

The ring $\mathcal{D} = R/\langle p\rangle$ is an integral domain, and hence $\mathcal{D}[\mathtt{X}]$ is also an integral domain.

Since $f(\mathtt{X})$ and $g(\mathtt{X})$ have content 1 by assumption, $f \,mod\, p$ and $g \,mod\, p$ are both nonzero in $\mathcal{D}[\mathtt{X}]$, and hence their product in $\mathcal{D}[\mathtt{X}]$, $fg \,mod\, p$ is nonzero as well.

i.e $p \nmid cont(fg)$. And this is true for any p prime.

Hence $cont(fg) = 1$ and fg is primitive.

□

Corollary 1.10

Let R be a UFD and $f(\mathtt{X})\,,\ g(\mathtt{X}) \in R[\mathtt{X}]$. Then

$$cont(fg) = cont(f) \cdot cont(g) \quad \text{and} \quad pp(fg) = pp(f) \cdot pp(g)$$

Proof:

$$\begin{aligned} fg &= (cont(f)pp(f)) \cdot (cont(g)pp(g)) \\ &= \underbrace{(cont(f)cont(g))}_{c} \cdot \underbrace{pp(f)pp(g)}_{h} \end{aligned}$$

where $c \in R \setminus \{0\}$ and h is primitive by Gauss Lemma above.

Hence: $cont(fg) = c \cdot cont(h) = c = cont(f)cont(g)$,

and thus: $pp(fg) = fg/cont(f)cont(g) = pp(f) \cdot pp(g)$.

□

To generalise Gauss lemma for polynomials over Dedekind domains, we need to extend first the notions of content, primitive part, and/or primitive polynomials in this context.

Definition 1.11 (cf [Fr-T])

Let $R = \mathcal{D}$ be a Dedekind domain with quotient field K, and consider $f(\mathtt{X}) \in K[\mathtt{X}]$.

We define the content *of f, denoted $\mathcal{C}_f$, to be the fractional $\mathcal{D}$-ideal generated by the coefficients of f.*

Then f is said to be primitive *if*

$$\mathcal{C}_f = \mathcal{D}.$$

Here $\mathcal{D}$, the Dedekind domain itself, is no more than the identity of the abelian group of fractional $\mathcal{D}$-ideals in K.

A primitive polynomial can also be characterised by the *valuation* of it's content as follows.

For every prime ideal $\mathfrak{p}$ of $\mathcal{D}$, we denote by

$$\nu_{\mathfrak{p}}(f) := \nu_{\mathfrak{p}}(\mathcal{C}_f)$$

where $\nu_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic valuation defined on the group of fractional $\mathcal{D}$-ideals of K.

Then f is *primitive* if and only if

$$\text{For each prime ideal } \mathfrak{p} \text{ of } \mathcal{D}, \quad \nu_{\mathfrak{p}}(f) = 0.$$

The map thus defined for a prime ideal $\mathfrak{p}$ of $\mathcal{D}$

$$\begin{aligned} K[\mathtt{X}] &\longrightarrow \mathbb{Z} \\ f &\longmapsto \nu_{\mathfrak{p}}(f) \end{aligned}$$

retains a nice property of the $\mathfrak{p}$-adic valuation which yields the following form of Gauss lemma:

Theorem 1.12

For any nonzero polynomials $f\,,\ g \in K[\mathtt{X}]$, and for each prime ideal $\mathfrak{p}$ of $\mathcal{D}$

$$\nu_{\mathfrak{p}}(fg) = \nu_{\mathfrak{p}}(f) + \nu_{\mathfrak{p}}(g)$$

Proof: See [Fr-T].

Theorem 1.13

Let $\mathcal{D}$ be Dedekind domain. Then the product of two primitive polynomials in $\mathcal{D}[\mathtt{X}]$ is primitive.

Proof:

Let $f\,,\ g \in \mathcal{D}[\mathtt{X}]$. Assume that for all $\mathfrak{p}$ prime in $\mathcal{D}$, $\nu_{\mathfrak{p}}(f) = \nu_{\mathfrak{p}}(g) = 0$. Then

$$\nu_{\mathfrak{p}}(fg) = \nu_{\mathfrak{p}}(f) + \nu_{\mathfrak{p}}(g) = 0$$

□

As a consequence, we have the following important theorem.

Theorem 1.14

Let $\mathcal{D}$ be a Dedekind domain with quotient field K.

If $f(\mathtt{X})\,,\ g(\mathtt{X})\,,\ h(\mathtt{X})$ are monic polynomials in $K[\mathtt{X}]$ such that:

$$f(\mathtt{X}) = g(\mathtt{X})h(\mathtt{X})$$

and $f(\mathtt{X}) \in \mathcal{D}[\mathtt{X}]$, then

$$g(\mathtt{X}),\ h(\mathtt{X}) \in \mathcal{D}[\mathtt{X}]$$

i.e The monic factors of a monic polynomial of $\mathcal{D}[\mathtt{X}]$, lie in $\mathcal{D}[\mathtt{X}]$.

Proof:

Note that an ideal $\mathfrak{a}$ of $\mathcal{D}$ is characterised by:

$$\nu_{\mathfrak{p}}(\mathfrak{p}) \geq 0.$$

Now, since $f(\mathtt{X})$ has coefficients in $\mathcal{D}[\mathtt{X}]$, $\mathcal{C}_f$ is an ideal of $\mathcal{D}$.

The monicity of f implies then $\nu_{\mathfrak{p}}(\mathfrak{p}) = 0$ for all prime ideals $\mathfrak{p}$ of $\mathcal{D}$.

On the other hand, since $g(\mathtt{X})$ and $h(\mathtt{X})$ are both monic polynomials in $K[\mathtt{X}]$, for all prime ideals $\mathfrak{p}$ of $\mathcal{D}$,

$$\nu_{\mathfrak{p}}(g) \leq 0 \quad \text{and} \quad \nu_{\mathfrak{p}}(h) \leq 0.$$

By Gauss lemma (1.12)

$$0 = \nu_{\mathfrak{p}}(f) = \nu_{\mathfrak{p}}(g) + \nu_{\mathfrak{p}}(h)$$

Hence: $\nu_{\mathfrak{p}}(g) = \nu_{\mathfrak{p}}(h) = 0$ for all $\mathfrak{p}$.

Thus, $\mathcal{C}_g\,,\ \mathcal{C}_h \subset \mathcal{D}$.

And so, $g(\mathtt{X})\,,\ h(\mathtt{X}) \in \mathcal{D}[\mathtt{X}]$.

□

1.4 Squarefreeness

Definition 1.15

Let $f(\mathtt{X}) \in R[\mathtt{X}]$, where R is a UFD (Unique Factorization Domain).

$f(\mathtt{X})$ *is said to be* squarefree *if it has no repeated factors, that is, if there is no polynomial $g(\mathtt{X})$ such that: $deg(g(\mathtt{X})) \geq 1$ and $g(\mathtt{X})^2 | f(\mathtt{X})$*

Theorem 1.16

In characteristic zero, we have:

$$f(\mathtt{X}) \text{ is square-free } \iff GCD(f, f') = 1$$

Indeed, if there exits a non-constant polynomial $g(\mathtt{X})$ such that $g(\mathtt{X})^2 \mid f(\mathtt{X})$. Then $g(\mathtt{X}) \mid f'(\mathtt{X})$ and is a common factor to f and f'.

If $f'(\mathtt{X}) \neq 0$, the Euclidean algorithm yields non trivial factors, that are, $GCD(f, f')$ and $f/GCD(f, f')$, whence $GCD(f, f') \neq 1$.

Now, if $GCD(f, f') = 1$, by the Extended Euclidean Algorithm, there exist polynomials $U(\mathtt{X}), V(\mathtt{X}) \in R[\mathtt{X}]$ such that:

$$U(\mathtt{X})f(\mathtt{X}) + V(\mathtt{X})f'(\mathtt{X}) = 1 \tag{1.2}$$

It suffices to observe that f is squarefree if and only if, the roots of f in an algebraic closure of the field of fractions of R, are all simple, that is, f is separable.

By (1.2), one concludes that f and f' have no common roots, hence f has only simple roots and is squarefree.

□

In the case $f'(\mathtt{X}) = 0$, with the existence of a non-constant common factor to f and f', the field of fractions of R is necessarily of finite characteristic, which is then a prime number.

Let p be this prime number. Then every power of $\mathtt{X}$ in f, that corresponds to a non-zero coefficient, is necessarily a p-th power, whence so is $f(\mathtt{X})$, i.e $f(\mathtt{X}) = h(\mathtt{X})^p$, for some polynomial $h(\mathtt{X})$.

This is due to the fact that

$$h(\mathtt{X}^{p^r}) = h(\mathtt{X})^{p^r} \ , \quad \forall h(\mathtt{X}) \in \mathbb{F}_{p^r}[\mathtt{X}].$$

Hence, over any UFD, a GCD between a polynomial f and its derivative extracts all the repeated factors of f. This observation allows us to compute the squarefree part of $f \in R[\mathtt{X}]$, which is $f/GCD(f, f')$, and in which each irreducible factor of f appears exactly once. The remaining part, that is $GCD(f, f')$, forms the non-squarefree part of f and will not play a role in the factorization process, which consists in finding all irreducible factors. Their multiplicity will then be found by direct division.

Remark:

Applying the reduction map of section (1.1), we notice that:

Squarefreeness is preserved by all but a finite number of primes, namely those primes that ramify!

1.5 Lattices and reduction

1.5.1 Basic facts on lattices

Let $\Lambda \subset \mathbb{R}^n$ be a *lattice* of dimension k, that is, a free-$\mathbb{Z}$-module of finite rank $k := dim(\mathbb{R} \otimes_{\mathbb{Z}} \Lambda)$. then Λ contains k $\mathbb{R}$-linearly independent vectors $b_1, \cdots, b_k$ such that:

$$\Lambda = \sum_{i=1}^{k} \mathbb{Z} b_i$$

We denote by $d(\Lambda)$, the determinant of the lattice Λ, that is, the number:

$$d(\Lambda) := |det(b_1, \cdots, b_k)| = \left| \left(b_i^{tr} b_j \right)_{1 \leq i,j \leq k} \right|^{1/2}$$

where b_i^{tr} denotes the transpose of the vector b_i, and $b_1, \cdots, b_k$ is any *basis* for Λ.

We recall that $d(\Lambda)$ is an invariant of the lattice that does not depend on the choice of the basis. Moreover: $d(\Lambda) > 0$ (since the b_i are $\mathbb{R}$-linearly independent).

Note that the determinant of a lattice Λ is also the volume of its fundamental domain:

$$\Pi(\Lambda) := \{x \in \mathbb{R}^n |\ x = \sum_{i=1}^{k} x_i b_i\ ,\ 0 \leq x_i < 1\ ,\ 1 \leq i \leq k\}$$

The fundamental domain of a lattice Λ has the property that every point of the Euclidean space $\mathbb{R}^n$, is congruent, modulo Λ, to at most one *interior point* of $\Pi(\Lambda)$, points congruent to a boundary point may be repeated. And we have

$$\Pi(\Lambda) \cong \mathbb{R}^n/\Lambda$$

Lemma 1.17 (cf [BEL 1] or [LEN 2])

Let $r_{max} := Sup\{r \in \mathbb{R}^+ |\ B(0,r) \subset \Pi(\Lambda)\}$ be the radius of the largest ball inscribed in the fundamental domain $\Pi(\Lambda)$, where $B(0,r)$ is the open ball of $\mathbb{R}^n$, centered at 0, and having radius r.
For $x \in \mathbb{R}^n$, there exists at most one $y \in \mathbb{R}^n$ such that

$$x \equiv y\ (mod\ \Lambda)\ \ and\ \ \|y\| < r_{max}$$

where $\|\ \|$ denotes the Euclidean norm on $\mathbb{R}^n$.
If it exists, y is the unique element of $\Pi(\Lambda)$ congruent to x modulo Λ.
Let M be the matrix giving the basis vectors b_i, then y is given by

$$y \equiv x\, mod\, M := x - M\lfloor M^{-1}x \rceil$$

where $\lfloor z \rceil := \lfloor z + \frac{1}{2} \rfloor$ is the operator rounding to the nearest integer and is to be applied coordinatewise.

We will give later a formula for computing r_{max} explicitely for any lattice, but a best way to maximize it is to use a LLL-reduced basis. Before that we need to define the concept of *basis reduction*.

An important question in the Geometry of Numbers is the *Existence and Construction* of lattice basis vectors with special properties; and that's the general scope of *reduction* as we define it here. The aim is to exhibit lattice vectors that are of computational interest, such as the shortest vectors in a lattice.

1.5.2 The LLL lattice-basis reduction for number fields

An interesting definition of "reduced basis" was given by the three mathematicians A.K. Lenstra, H. W. Lenstra Jr, and L. Lovász in 1982, who gave a very efficient polynomial time algorithm for finding such a basis. These bases are then easy to compute, and in addition they have so many properties that make them very important for computational purposes.

Definition 1.18

A basis $b_1, \cdots, b_k$ of a lattice Λ is said to be LLL-reduced [3] *if $b_1, \cdots, b_k$ and the vectors $b_1^*, \cdots, b_k^*$ of the corresponding orthogonal basis together with their corresponding constants (see below), satisfy:*

$$\begin{aligned} &(1) \quad |\mu_{ij}| \leq \tfrac{1}{2} && (1 \leq j < i \leq k) \\ &(2) \quad \|b_i^* + \mu_{i,i-1} b_{i-1}^*\|^2 \geq \tfrac{3}{4}\|b_{i-1}^*\|^2 && (1 < i \leq k) \end{aligned}$$

The second condition is due to Laszlo Lovász and known as Lovász condition .

The constant $\frac{3}{4}$ is arbitrarily chosen, and may be replaced by any fixed real number α, such that $\frac{1}{4} < \alpha < 1$. In such a case, the powers of 2 appearing in the inequalities of lemma (1.20) below should be replaced by the same powers of the number $\frac{4}{4\alpha-1}$ called the LLL-constant.

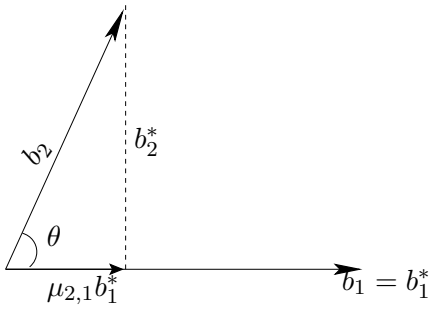
The number α, called the LLL-parameter, is used to check the Lovász condition and determine the frequency of swaps in the LLL algoritm.

Examples:

For $k = 2$, the basis (b_1, b_2) is LLL-reduced if:

(1) $|\mu_{2,1}| \leq \frac{1}{2}$, thus $\|\mu_{2,1} b_1^*\| \leq \frac{1}{2}\|b_1\|$

(This happens when the angle between the vectors b_1 and b_2, $\theta = (b_1, b_2)$, is relatively large (θ is at least $\frac{\pi}{3}$).)



(2) $\|b_2\|^2 = \|b_2^* + \mu_{2,1} b_1^*\|^2 \geq \frac{3}{4}\|b_1\|^2$ (This means that $\|b_2\|$ is not too small compared to $\|b_1\|$.)

In the above definition, we use the orthogonal basis corresponding to $b_1, \cdots, b_k$, which is obtained by applying the Gram-Schmidt orthogonalization process as follows:

$$\begin{aligned} b_1^* &= b_1 \\ &\vdots \\ b_i^* &= b_i - \textstyle\sum_{j=1}^{i-1} \mu_{ij} b_j^* \qquad \text{where} \quad \mu_{ij} = \dfrac{b_i^{tr}\, b_j^*}{b_j^{*\,tr}\, b_j^*}, \quad (1 \leq j < i \leq k) \end{aligned}$$

This can be represented in matrix form as follows.

[3] LLL standing for A.K. Lenstra, H. W. Lenstra Jr, and L. Lovász

Let $M = (b_1, \cdots, b_k)$ be the matrix whose columns are the b_i,
and $M^* = (b_1^*, \cdots, b_k^*)$ be the matrix whose columns are the b_i^*, Then:

$$M = M^*G, \quad \text{where } G = \begin{pmatrix} 1 & \mu_{2,1} & \mu_{3,1} & \cdots & \mu_{k,1} \\ 0 & 1 & \mu_{3,2} & \cdots & \mu_{k,2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \mu_{k,k-1} \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

Hence:

$$(b_1^*, \cdots, b_k^*) = (b_1, \cdots, b_k)G^{-1} = (b_1, \cdots, b_k) \begin{pmatrix} 1 & -\mu_{2,1} & -\mu_{3,1} & \cdots & -\mu_{k,1} \\ 0 & 1 & -\mu_{3,2} & \cdots & -\mu_{k,2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -\mu_{k,k-1} \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

Recall that, the Gram-Schmidt orthogonalization process is a polynomial time algorithm and needs only $O(n^3)$ arithmetic operations.

Note that, the $b_i^* \notin \Lambda$ in general, and consequently we only get a vector space basis! Nevertheless, the Gram-Schmidt orthogonal basis has the following nice properties:

- $b_1^*, \cdots, b_k^*$ are pairwise orthogonal and $\mathbb{R}$-linearly independent.
- $W_i := \sum_{1 \leq j \leq i} \mathbb{R} b_j^* = \sum_{1 \leq j \leq i} \mathbb{R} b_j$ for all i, $1 \leq i \leq k$
- b_i^* is the projection of b_i onto $W_i^{\perp}$ the orthogonal complement of W_{i-1}, and hence in particular $\|b_i^*\| \leq \|b_i\|$.
- $det(b_1, \cdots, b_k) = det(b_1^*, \cdots, b_k^*)$

As a consequence, we obtain the following famous inequality:

Theorem 1.19 *"Hadamard's Inequality"*

Let $(b_1, \cdots, b_k)$ be a basis of a lattice Λ. Then: $d(\Lambda) \leq \prod_{i=1}^{k} \|b_i\|$

from which, we conlude that $\frac{\prod_{i=1}^{k}\|b_i\|}{d(\Lambda)} \geq 1$

This quantity is actually a measure of orthogonality for the basis $(b_1, \cdots, b_k)$, and is called the "Orthogonality Defect". By Hadamard's Inequality one can see that, for a basis, to be "reduced" means also that it "is not too far" from being orthogonal.

Properties of a LLL-reduced basis

Lemma 1.20

Let $(b_1, \cdots, b_k)$ be a LLL-reduced basis of a lattice $\Lambda \subset \mathbb{R}^n$ with the corresponding orthogonal basis $(b_1^*, \cdots, b_k^*)$. Then the following estimates hold:

1. $\|b_{i-1}^*\|^2 \leq 2\|b_i^*\|^2 \qquad (1 \leq i \leq k)$
2. $\|b_j\|^2 \leq 2^{i-1}\|b_i^*\|^2 \qquad (1 \leq j \leq i \leq k)$
3. $d(\Lambda) \leq \prod_{i=1}^{k}\|b_i\| \leq 2^{\frac{k(k-1)}{4}} d(\Lambda)$
4. $\|b_1\| \leq 2^{\frac{k-1}{4}} d(\Lambda)^{1/k}$
5. $\|b_1\|^2 \leq 2^{k-1}\|x\|^2$ *for all* $x \in \Lambda, \quad x \neq 0$
6. $\|b_j\|^2 \leq 2^{k-1} max\{\|x_1\|^2, \cdots, \|x_t\|^2\}$, $(1 \leq j \leq t)$
   for any linearly independent vectors $x_1, \cdots, x_t$ of Λ.

For a proof of this lemma, we refer to [L-L-L].

We also cite the following results from [BEL 1] concerning the fundamental domain of a lattice.

Lemma 1.21

The radius of the largest ball inscribed in the fundamental domain of a lattice Λ of basis $(b_1, \cdots, b_k)$ is given by

$$r_{max} = \min_i \frac{1}{2T_i}, \qquad \textit{such that} \qquad T_i := (\sum_j t_{i,j}^2 / \|b_j^*\|^2)^{\frac{1}{2}}$$

where the $t_{i,j}$ are the coefficients of the inverse of the Gram matrix $G = (b_i^*)$.

Lemma 1.22

If the lattice Λ is given by a LLL-reduced basis $(b_1, \cdots, b_k)$ then

$$r_{max} \geq \frac{1}{2}\min_i \|b_i\| \times \left(\frac{\prod_{i=1}^{k}\|b_i\|}{d(\Lambda)}\right)^{-1}$$

Combining these two results with the properties of a LLL-reduced basis we get

Lemma 1.23 (cf [BEL 1])

If the basis of the lattice $\Lambda \subset \mathbb{R}^n$ is LLL-reduced then

$$r_{max} \geq \frac{\|b_1\|}{2\left(3\sqrt{2}/2\right)^{n-1}}$$

Algorithm for LLL-basis reduction

Algorithm 1.24 "LLL-reduction" (cf [P-Z])

Input. Basis vectors $b_1, \cdots, b_k$ of a lattice $\Lambda \subset \mathbb{R}^n$.

Output. A basis $b_1, \cdots, b_k$ of Λ that is LLL-reduced.

Step 1. [initialize] For $i = 1, 2, \cdots, k$

$$\text{Set } \mu_{ij} \longleftarrow \frac{b_i^{tr} b_j^*}{B_j}$$

$$b_i^* \longleftarrow b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^* \ , \quad B_i \longleftarrow b_i^{*\,tr} b_i^*$$

Then set $m \longleftarrow 2$

Step 2. [Set l]

Set $\quad l \longleftarrow m - 1$

Step 3. [Reduce μ_{ml} in case $|\mu_{ml}| > \frac{1}{2}$]

If $|\mu_{ml}| > \frac{1}{2}$ set $r \longleftarrow \lfloor \mu_{ml} \rceil$ and

$$\begin{aligned} b_m &\longleftarrow b_m - r b_l \\ \mu_{mj} &\longleftarrow \mu_{mj} - r\mu_{lj} \quad (1 \leq j \leq l-1), \\ \mu_{ml} &\longleftarrow \mu_{ml} - r \end{aligned}$$

For $l = m - 1$ go to [Step 4.] else to [Step 5.]

Step 4. [Inequality (2) violated on level m ?]

For $B_m < (\frac{3}{4} - \mu_{m,m-1}^2) B_{m-1}$ go to [Step 6.]

Step 5. [Decrease l]

Set $\quad l \longleftarrow l - 1$. For $l > 0$ go to [Step 3.]

For $m = k$ terminate; else set $\ m \longleftarrow m + 1$ and go to [Step 2.]

Step 6. [Interchange $b_{m-1},\ b_m$]

Set $\mu \longleftarrow \mu_{m,m-1},\ B \longleftarrow B_m + \mu^2 B_{m-1},\ \mu_{m,m-1} \longleftarrow \mu B_{m-1}/B,$

$B_m \longleftarrow B_{m-1}B_m/B,\ \ B_{m-1} \longleftarrow B;$

then set for $1 \leq j \leq m-2$ and $m+1 \leq i \leq k$

$$\begin{pmatrix} b_{m-1} \\ b_m \end{pmatrix} \longleftarrow \begin{pmatrix} b_m \\ b_{m-1} \end{pmatrix}, \quad \begin{pmatrix} \mu_{m-1,j} \\ \mu_{mj} \end{pmatrix} \longleftarrow \begin{pmatrix} \mu_{mj} \\ \mu_{m-1,j} \end{pmatrix},$$

$$\begin{pmatrix} \mu_{i,m-1} \\ \mu_{i,m} \end{pmatrix} \longleftarrow \begin{pmatrix} 1 & \mu_{m,m-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -\mu \end{pmatrix} \begin{pmatrix} \mu_{i,m-1} \\ \mu_{im} \end{pmatrix}.$$

For $m > 2$ decrease m by 1. Then go to [Step 2.]

This is a *deterministic* and *polynomial* time algorithm, which is very efficient not only for the application that Lenstra et al. gave in their landmark paper [L-L-L], but also for so many problems that deal with lattices.

In [L-L-L], Lenstra et al. proved the following proposition and gave a detailed complexity analysis for the LLL lattice-basis reduction algorithm when applied to integral lattices.

Proposition 1.25

If the real number $B \geq 2$ is such that $\|b_i\|^2 \leq B$, for each i, then the number of arithmetic operations needed for the LLL algorithm is $O(n^4 log B)$ and the integers on which these operations are performed each have length $O(n log B)$.

Remark:

For the sake of simplicity, we have chosen to present the LLL reduction as was given in the original paper [L-L-L] knowing that Zassenhaus, using his theory of idempotents, has shown that the LLL algorithm is applicable to the quadratic form T_2 for number fields using floating points instead of integer programming (see [ZAS 2]). And in fact, we can define an LLL-reduced basis with any norm corresponding to a chosen positive definite quadratic form (see [COH] or [BEL 1]).

1.6 Factorization over the rationals

Let $f(\mathtt{X}) \in \mathbb{Q}[\mathtt{X}]$ be a polynomial of degree $deg(f) \geq 2$.

Without loss of generality, we assume f squarefree, monic, and having coefficients in $\mathbb{Z}$ (see section (1.7) below), and hence our task is reduced to a factorization in $\mathbb{Z}[\mathtt{X}]$.

Now, in order to factorize $f(\mathtt{X})$ in $\mathbb{Z}[\mathtt{X}]$, Zassenhaus, in [ZAS 1], proposed a procedure that is in use since then. This procedure, based on the Hensel lemma, is a special case of the general Henselian technique which consists of the following:

Algorithm 1.26 "Henselian factorization technique" (cf [W-R])

Input. $f(\mathtt{X}) \in R[\mathtt{X}]$, a squarefree polynomial, where R is an integral domain.

Output. The complete factorization of $f(\mathtt{X})$ in $R[\mathtt{X}]$.

Step H1. Embed R in a ring R' so that Hensel's lemma holds in $R'[\mathtt{X}]$,
usually by taking R' to be the ring of integers of a local field corresponding to a suitable modulus; e.g for $R = \mathbb{Z}$, choose p a suitable prime, and take $R' = \mathbb{Z}_p$.

Step H2. Find a suitable approximation of $f(\mathtt{X})$ in $R'[\mathtt{X}]$. (For the above case, a polynomial $\phi_f(\mathtt{X}) \in \mathbb{Z}_p[\mathtt{X}]$ with $(\phi_f \bmod p) = (f \bmod p)$ in $\mathbb{F}_p[\mathtt{X}]$, would be the right candidate).

Step H3. Factor $f(\mathtt{X})$ in $R'[\mathtt{X}]$ using the constructive procedure from the proof of Hensel's lemma, i.e starting with a modular factorization that should be lifted up to a sufficiently good accuracy determined by a bound, that needs to be calculated, on the coefficients of the factors of f in $R[\mathtt{X}]$ allowing the reconstruction of these factors from those in $R'[\mathtt{X}]$.

Step H4. Recover the factors of f in $R[\mathtt{X}]$ by combining those obtained in $R'[\mathtt{X}]$. Each combination is tested by trial-division, and whenever a factor $g \in R[\mathtt{X}]$ is found, replace f by f/g and start again at (Step H3.) using what is left from the modular factorization of the old f after deleting those factors corresponding to g.

For our case, $f(\mathtt{X})$ in $\mathbb{Z}[\mathtt{X}]$, the first step consists in choosing a prime p not dividing the resultant of f and f', which is, up to sign, equal to the product of the leading coefficient of f and its discriminant. This choice of p allows $(f \bmod p)$ to have the same degree as f and to preserve the squarefreeness. Having chosen earlier f to be monic, it would be the same to work with the discriminant of f or its resultant.

The polynomial $\phi_f(\mathtt{X}) \in \mathbb{Z}_p[\mathtt{X}]$ satisfying $(\phi_f \bmod p) = (f \bmod p)$ in $\mathbb{F}_p[\mathtt{X}]$, provides the required approximation of $f(\mathtt{X})$ in $\mathbb{Q}_p[\mathtt{X}]$, we then can proceed to Step H3, i.e the factorization of $f(\mathtt{X})$ in $\mathbb{Q}_p[\mathtt{X}]$, seeking the p-adic monic irreducible factors of f. For that, we start by factoring $(f \bmod p)$, which is a factorization in a finite field, thus can be achieved using Berlekamp Algorithm, (cf [BER]). If $(f \bmod p)$ is irreducible, then f is also irreducible. Otherwise, we continue by computing a bound B on the coefficients of any non-trivial factor of $f(\mathtt{X})$, for instance Mignotte's bound (cf [MIG] & page 63 below).

Then, applying Hensel's lemma will enable us to lift the factorization found modulo p to one modulo p^e for some e satisfying $p^e > 2B$, so that the coefficients of any factor of $f(\mathtt{X})$ in $\mathbb{Z}[\mathtt{X}]$ are actually in the interval $]-\frac{p^e}{2}, \frac{p^e}{2}[$, and hence these factors are already reduced modulo p^e. In this case, the modular factors (i.e factors modulo p^e) represent accurate approximates of the p-adic factors.

Now, every monic factor $g \in \mathbb{Z}[\mathtt{X}]$ of $f(\mathtt{X})$ is actually a product of some of the p-adic factors, and conversely, every combination of some of the p-adic factors of f may correspond to a rational true factor of f. Therefore, we can recover all rational factors of f from the factors modulo p^e by forming all possible products of them, each taken at most once, then reducing the resulting polynomials modulo p^e and testing them by trial division.

The method just sketched for factorization over $\mathbb{Q}$, known as the Berlekamp-Zassenhaus algorithm, recovers the rational factors of f by essentially trying all combinations of the p-adic factors (2^s combinations, where s is the number of p-adic factors). Hence, this algorithm has an exponential worst case complexity.

However, in practice, this algorithm seems to work well, because the complexity is not exponential in the degree of f. It is only exponential in the number of p-adic factors, which is precisely the number of modular factors, and which is *usually* much smaller than $deg(f)$. The worst case may occur if all factors of f have very low degrees. An example is given by the Swinnerton-Dyer polynomials that are known to cause the standard Berlekamp-Zassenhaus algorithm to take an exponential running time. They have been generalised by Kaltofen et al. (cf [K-M-S]) who gave a larger class of polynomials having the same feature.

The r-th Swinnerton-Dyer polynomial is defined as:

$$f(\mathtt{X}) := \prod \left(\mathtt{X} \pm \sqrt{2} \pm \sqrt{3} \pm \cdots \pm \sqrt{p_r}\right)$$

where p_r is the r-th prime and where the product is taken over all 2^r possible choices of + or - signs. This polynomial lies in $\mathbb{Z}[\mathtt{X}]$, has degree $n = 2^r$, and is irreducible over $\mathbb{Z}$, being in fact the minimal polynomial over $\mathbb{Q}$ of the primitive element $\alpha = \sqrt{2} + \sqrt{3} + \cdots + \sqrt{p_r}$ of the extension of $\mathbb{Q}$ by the square roots of the first r primes, $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \cdots, \sqrt{p_r})$.

Knowing that for any prime p, $\mathbb{F}_{p^2}$ contains all the square roots of $2 \bmod p, 3 \bmod p, \cdots, p_r \bmod p$, because for any prime $\hat{p} \neq p$, the polynomial $\mathtt{X}^2 - \hat{p} \in \mathbb{F}_p[\mathtt{X}]$ is irreducible and defines the unique Galois Field $\mathbb{F}_{p^2}$, thus we conclude that $(f \bmod p)$ factorizes into linear factors over $\mathbb{F}_{p^2}$. Hence, the irreducible factors of $(f \bmod p)$ over $\mathbb{F}_p$ are either *linear* or *quadratic*, which yields $n/2 \leq s \leq n$, and may lead to a combinatoric explosion.

In order to reduce somehow the effect of the long combinatoric search, it is worthwhile trying the following tricks.

1. D. R Musser [4] suggested that several modular factorization s should be determined and different primes should be used to minimise the number of modular factors and to restrict their possible degrees. Comparing the different patterns of factorizations so obtained enables the elimination of some of them. Incompatibility of these patterns means irreducibility of the polynomial to be factored. For example, if f is the product of a linear and a cubic irreducible polynomials modulo one prime, and the product of two quadratic irreducible factors modulo another prime, then f is itself irreducible.

   Musser showed that the mean number of primes needed to establish the irreducibility of a random polynomial grows very slowly with the degree. For polynomials of degree less than or equal 200, five modular factorizations are enough.

2. The trial divisions needed to verify whether a product of some modular factors is a true rational factor of f or not, will not all be successful. The exponential behaviour corresponds exactly to the case where all the trial divisions must fail. So it is important to develop strategies to detect unsuccessful trial divisions as quickly as possible.

   Trying the constant coefficient of the polynomial first can eliminate some of the cases. And an *early abort trial division* strategy pointed out by Abbott (cf [ABB]) can eliminate other cases. It consists in checking the size of the coefficients during the division declaring the latter unsuccessful as soon as any coefficient becomes too big (exceeding the bound above), (cf also [COH]).

Another way of overcoming the combinatoric long search and yet discovering true factors of f, was given by Lenstra et al. in [L-L-L]. Their idea was to built certain lattices in $\mathbb{R}^{n+1}$ by means of which the rational factors of f will be determined. They use their LLL lattice-basis reduction algorithm to find the shortest vectors in these lattices as it turns out that the seeked irreducible factors of f do correspond to these shortest vectors.

An advantage of this method is that with one modular factor of f, we *definitely* discover an irreducible rational factor of f, while the combinatoric search doesn't ensure a right choice of combinations for the first few trials. In addition, the eventual irreducibility of f, becomes easy to decide since in this case, the first irreducible factor discovered will be f itself.

But the more important feature of this method is its polynomial-time complexity! The factorization of polynomials over the rationals entered then a new era: This problem is no longer difficult since we know

[4] in his paper: *On the efficiency of a polynomial irreducibility test, Journal ACM 25 pp 271-282, April 1978.*

a *good* algorithm that solves it. An algorithm being *good* when its running time is polynomial in the size of the input data.
Surprisingly, in practice the LLL factorization algorithm seems to be slower than the Berlekamp Zassenhaus algorithm, and could not replace it as a standard factorization method. The lattice-basis reduction part of the former algorithm, consumes a lot of time because of the large dimension of the lattice so obtained and the large size of the coefficients of the vectors so involved. This leads to a poor performance and motivates more research again.

A nice algorithm was suggested quite recently by van Hoeij [HOE 2] which efficiently solves the combinatoric problem by reducing it to a type of a Knapsack problem that can be solved using the LLL lattice-basis reduction algorithm. Although the Knapsack problem is an NP-hard problem, the use of the LLL lattice-basis reduction algorithm should give this new algorithm a polynomial-time complexity.
Van Hoeij's new algorithm is much more efficient in practice than the original LLL factorization algorithm proposed by Lenstra et al. because the lattice constructed in van Hoeij's algorithm has dimension equal to the number of modular factors, which is usually much smaller than the degree of f; in addition the vectors of the lattice have much smaller entries.

1.7 Some assumptions

In this work, we study the problem of factoring a univariate polynomial $f(\mathtt{X})$ whose coefficients are in a global field $\mathbb{K}$ of the ring of integers $\mathcal{O}_{\mathbb{K}}$.
Since $\mathbb{K}$ is a field, we are certain of the existence and unicity, up to units, of the solution for our problem. So our task would be to identify the most efficient available methods that explicitly determines the irreducible factors of $f(\mathtt{X})$.
Writing $f(\mathtt{X}) = cont(f) \cdot pp(f)$, when possible, we notice that to completely factor $f(\mathtt{X})$ means to factor its content as well, which is an integer factorization problem and involves other approaches, that will not be subject of our study. In addition, factoring large random integers is much harder than factoring integral polynomials. So, we will only be concerned with factoring primitive polynomials.
Besides this remark, we know that GCD's exist in $\mathbb{K}[\mathtt{X}]$, so we can compute $GCD(f, f')$ and determine the squarefree part of $f(\mathtt{X})$ as in section (1.4). Therefore, from now on, we make the following assumption:

The polynomial to be factored is *squarefree.* **(Sqf)**

If not, a reduction to a squarefree polynomial will be performed as first step of our factorization algorithm.

In addition, since $\mathbb{K}$ is a field, we can assume without loss of generality that $f(\mathtt{X})$ is monic. For, if it is not the case, $\frac{1}{lc(f)}f(\mathtt{X})$ is a monic polynomial in $\mathbb{K}[\mathtt{X}]$.

But since it would be very handy to perform computations in $\mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ instead, we will then need to assume not only *monicity* of f, but also *integrality* of its coefficients; in such a case, Gauss lemma simplifies our task.

We recall that the long division with remainder in a polynomial ring $R[\mathtt{X}]$ is not always possible when R is not a field. Nevertheless, long division by a monic polynomial always works.

So it would be advantageous to ensure both conditions, which can be achieved by a change of variables as follows. If $f(\mathtt{X}) = \tilde{f}(\mathtt{X})/d$, where $d \in \mathcal{O}_{\mathbb{K}},\ d \neq 0$ and $\tilde{f}(\mathtt{X}) = \sum_{i=0}^{n} a_i \mathtt{X}_i \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}],\ a_n \neq 0$.

Set: $\mathtt{X}_1 = a_n\mathtt{X}$, then,

$$\begin{aligned}\tilde{f}(\mathtt{X}) &= a_n\left(\frac{\mathtt{X}_1}{a_n}\right)^n + a_{n-1}\left(\frac{\mathtt{X}_1}{a_n}\right)^{n-1} + \cdots + a_1\left(\frac{\mathtt{X}_1}{a_n}\right) + a_0 \\ &= \frac{1}{a_n^{n-1}}\left[\mathtt{X}_1^n + a_{n-1}\mathtt{X}_1^{n-1} + a_n a_{n-2}\mathtt{X}_1^{n-2} + \quad \cdots \quad + a_n^{n-2}a_1\mathtt{X}_1 + a_n^{n-1}a_0\right]\end{aligned}$$

Hence: $da_n^{n-1}f(\mathtt{X})$ is a monic polynomial with integral coefficients in the indeterminate $\mathtt{X}_1$.

Therefore, we can assume from now onwards that, unless otherwise stated:

The polynomial to be factored is *monic* and has *integral coefficients*. **(Mon)**

By Gauss lemma, we know that the factorization in $\mathbb{K}[\mathtt{X}]$ and the factorization in $\mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ *coincide* for *monic* polynomials. While it doesn't always have a meaning to talk about unique factorization in $\mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ since the latter need not be a UFD. Since $\mathcal{O}_{\mathbb{K}}$ is a Dedekind domain, by Gauss lemma, the monic irreducible factors of f we are seeking in $\mathbb{K}[\mathtt{X}]$, do belong to $\mathcal{O}_{\mathbb{K}}[\mathtt{X}]$, which enables us to save a lot of energy by working directly with algebraic integers.

CHAPTER TWO

TRAGER'S METHOD FOR FACTORIZATION OVER AN ALGEBRAIC EXTENSION FIELD

2.1 Introduction and fundamental results

A field extension $\mathbb{K}/K$ is said to be *separable* if the separable degree[1] of $\mathbb{K}$ over K is maximum, that is, is equal to the degree of the extension $[\mathbb{K} : K]$. If $\mathbb{K} = K(\alpha)$, for some element α that is algebraic over K, then $\mathbb{K}$ is separable over K if and only if the minimal polynomial of α is separable, that is, has no repeated roots. By the Primitive Element Theorem, for every finite separable field extension $\mathbb{K}/K$, there exists an element $\alpha \in \mathbb{K}$ such that $\mathbb{K} = K(\alpha)$.

Let $\mathbb{K}$ be a finite separable extension of degree m of the field K $(= \mathbb{Q}$ or $\mathbb{F}_q(t))$ [2] and assume $\mathbb{K} = K(\alpha)$, where the algebraic element α has the minimal polynomial $m_\alpha(\mathtt{Y}) \in R[\mathtt{Y}]$, where $R = \mathbb{Z}$ or $\mathbb{F}_q[t]$.

Let $f(\mathtt{X}) \in \mathbb{K}[\mathtt{X}]$ be a polynomial that we assume squarefree, monic, and having coefficients in $\mathbb{Z}[\alpha]$, for the number field case, or in $\mathbb{F}_q[t][\alpha]$, for the function field case. And consider the problem of finding the complete factorization of $f(\mathtt{X})$ over $\mathbb{K}[\mathtt{X}]$ using Trager's method.

Trager's method for factorization over an algebraic extension field has its origin in Kronecker's work. It has been improved quite recently by Encarnación [ENC].

Assuming that efficient factorization algorithms for polynomials over the rational number and function fields are known, the main idea of Trager's factorization method is to reduce the problem of factoring $f(\mathtt{X})$ in $\mathbb{K}[\mathtt{X}]$, to a factorization of an other polynomial in $K[\mathtt{X}]$, ($K = \mathbb{Q}$ or $\mathbb{F}_q(t)$).
This can be done via the norm map that sends elements of an extension field back to the ground field.

[1] cf [LAN] page 177

[2] Note that for $K = \mathbb{Q}$ the separability condition is superfluous, since $\mathbb{Q}$ is a perfect field.

Denote by $\sigma_1, \cdots, \sigma_m$ the distinct embeddings of $\mathbb{K}$ in an algebraic closure $\bar{K}$ of K. There are exactly m of them, since we assumed the extension separable.

For an element $a \in \mathbb{K}$, the norm is the element of K defined as:

$$N(a) := \prod_{i=1}^{m} \sigma_i(a)$$

Applying the norm coefficient-wise to a polynomial $g(\mathtt{X}) \in \mathbb{K}[\mathtt{X}]$, we can extend the definition of the norm to elements of $\mathbb{K}[\mathtt{X}]$. In particular, we have:

$$N\left(g(\mathtt{X})\right) = \prod_{i=1}^{m} \sigma_i\left(g(\mathtt{X})\right)$$

where the isomorphisms σ_i are applied to $g(\mathtt{X})$ coefficient-wise.

From Galois theory, we know that $N(a) \in K$ because it is fixed by all elements of the Galois group $Gal(\mathbb{K}|K)$, and hence $N\left(g(\mathtt{X})\right) \in K[\mathtt{X}]$.

In addition, since the σ_i are field homomorphisms, the norm is a multiplicative map from $\mathbb{K}[\mathtt{X}]$ to $K[\mathtt{X}]$ as well. i.e

$$N\left(g_1(\mathtt{X})g_2(\mathtt{X})\right) = N\left(g_1(\mathtt{X})\right) N\left(g_2(\mathtt{X})\right) \quad \text{for all } g_1(\mathtt{X}), g_2(\mathtt{X}) \in \mathbb{K}[\mathtt{X}]$$

There are several formulae for the norm. For an element $a \in \mathbb{K}$, the norm can be calculated as the constant term, up to sign, of its minimal polynomial. This term can be formulated as a determinant, and it turns out that it is directly related to the notion of the resultant.

The resultant is a computationally efficient tool for computing the norm, and one can show that the resultant is multiplicative and satisfies:

$$Res_{\mathtt{Y}}(u(\mathtt{Y}), v(\mathtt{Y})) = lc(u)^{deg(v)} \prod_{\rho_j} v(\rho_j)$$

where the ρ_j's run through all roots of the polynomial $u(\mathtt{Y})$, and $lc(u)$ denotes the leading coefficient of the polynomial u.

Hence for a polynomial $g(\mathtt{X}) \in \mathbb{K}[\mathtt{X}]$, as it is defined over $\mathbb{K} = \mathbb{Q}(\alpha)$, it can be considered as a polynomial in two variables defined over $\mathbb{Q}$, that is $g(\mathtt{X}) = g(\mathtt{X}, \mathtt{Y})_{|\mathtt{Y}=\alpha}$. So, we get:

$$\begin{aligned} Res_{\mathtt{Y}}\left(\boldsymbol{m}_\alpha(\mathtt{Y}), g(\mathtt{X}, \mathtt{Y})\right) &= \prod_{i=1}^{m} g(\mathtt{X}, \sigma_i(\alpha)) \\ &= \prod_{i=1}^{m} \sigma_i(g(\mathtt{X})) = N(g(\mathtt{X})) \end{aligned} \tag{2.1}$$

The norm can then be given by the formula:

$$N(g(\mathtt{X})) = Res_{\mathtt{Y}}\left(\boldsymbol{m}_\alpha(\mathtt{Y}), g(\mathtt{X}, \mathtt{Y})\right)$$

Note that from (2.1) we deduce that:

$$deg\,(N(g(\mathtt{X}))) = m\,deg\,(g(\mathtt{X})) = deg\,(\boldsymbol{m}_\alpha)\,deg\,(g) \tag{2.2}$$

And we have the following results about this map.

Lemma 2.1

If $g(\mathtt{X}) \in \mathbb{K}[\mathtt{X}]$ is irreducible, then $N\,(g(\mathtt{X}))$ is the power of an irreducible polynomial of $K[\mathtt{X}]$.

Proof:

Let $N\,(g(\mathtt{X})) = \prod_j N_j^{e_j}(\mathtt{X})$ be a factorization of $N\,(g(\mathtt{X}))$ into irreducible factors in $K[\mathtt{X}]$. By considering $\sigma = id$, we know that $g(\mathtt{X}) \mid N\,(g(\mathtt{X}))$ in $\mathbb{K}[\mathtt{X}]$.

Since $g(\mathtt{X})$ is irreducible in $\mathbb{K}[\mathtt{X}]$, $g(\mathtt{X})$ divides $N_j(\mathtt{X})$ in $\mathbb{K}[\mathtt{X}]$ for some j.

Hence $\sigma_i(g(\mathtt{X})) \mid N_j(\mathtt{X})$ in $\sigma_i(\mathbb{K}[\mathtt{X}])$ for all i and so $N\,(g(\mathtt{X})) \mid N_j^m(\mathtt{X})$ in $\mathbb{K}[\mathtt{X}]$. But $N_j(\mathtt{X}) \in K[\mathtt{X}]$, therefore $N\,(g(\mathtt{X})) \mid N_j^m(\mathtt{X})$ in $K[\mathtt{X}]$ and hence

$N\,(g(\mathtt{X})) = N_j^{m'}(\mathtt{X})$, for some $m' \leq m$, where $m = [\mathbb{K} : K]$.

□

Lemma 2.2

Suppose that both $g(\mathtt{X}) \in \mathbb{K}[\mathtt{X}]$ and $N\,(g(\mathtt{X})) \in K[\mathtt{X}]$ are squarefree.

Let $N\,(g(\mathtt{X})) = \prod_{j=1}^{t} N_j(\mathtt{X})$ be a factorization of $N\,(g(\mathtt{X}))$ into distinct irreducible factors in $K[\mathtt{X}]$. Then $\prod_{j=1}^{t} GCD\,(g(\mathtt{X}), N_j(\mathtt{X}))$ is a factorization of $g(\mathtt{X})$ into irreducible factors in $\mathbb{K}[\mathtt{X}]$.

Proof:

Let $g_1(\mathtt{X}), \cdots, g_r(\mathtt{X})$ be the irreducible factors of $g(\mathtt{X})$ in $\mathbb{K}[\mathtt{X}]$.

On the one hand, since the norm map is multiplicative, we have:

$$N\,(g(\mathtt{X})) = \prod_i N\,(g_i(\mathtt{X}))$$

On the other hand $N\,(g(\mathtt{X})) = \prod_j N_j(\mathtt{X})$ with the N_j all distinct, since $N\,(g(\mathtt{X}))$ is supposed squarefree.

As N_j is irreducible, we get $N_j \mid N\,(g_i(\mathtt{X}))$ for some $i = i(j)$.

But $g_i(\mathtt{X})$ is irreducible, hence, by the preceding lemma, $N\,(g_i(\mathtt{X}))$ is a power of its irreducible factor in $K[\mathtt{X}]$, N_j. This power would then divide the squarefree polynomial $N\,(g(\mathtt{X}))$. Whence

$$N\,(g_i(\mathtt{X})) = N_j \tag{2.3}$$

Reordering the factors of $N\,(g(\mathtt{X}))$, if necessary, we obtain: $r = t$ and

$$N\,(g_i(\mathtt{X})) = N_i\,, \quad \forall i = 1, \cdots, r$$

Hence g_i is a common divisor for N_i and the polynomial $g(\mathtt{X})$ which is squarefree, and so $GCD(g(\mathtt{X}), N_i(\mathtt{X}))$ is a factor of $g(\mathtt{X})$ which appears exactly once since in addition $GCD(g_j(\mathtt{X}), N(g_i(\mathtt{X}))) = 1$ for $i \neq j$.

□

Lemma 2.3

Let $g(\mathtt{X}) \in \mathbb{K}[\mathtt{X}]$ be a squarefree polynomial of degree n, where $\mathbb{K} = K(\alpha)$ is a separable extension, with $[\mathbb{K} : K] = m$.

Then there exists only finitely many λ such that $N\left(g(\mathtt{X} - \lambda\alpha)\right)$ is not squarefree.

Proof:

Let $\{\beta_{i,j}\}_{1 \leq i \leq n}$ be the roots of $\sigma_j(g(\mathtt{X}))$ in an algebraic closure of $\mathbb{K}$.

Then the zeros of $N\left(g(\mathtt{X} - \lambda\alpha)\right)$ are the $\{\beta_{i,j} + \lambda\sigma_j(\alpha)\}$ and hence, $N\left(g(\mathtt{X} - \lambda\alpha)\right)$ has repeated roots if and only if

$$\beta_{i,j} + \lambda\sigma_j(\alpha) = \beta_{k,l} + \lambda\sigma_l(\alpha)$$

for some $i \neq k$, $j \neq l$.

This would imply that: $\lambda = \dfrac{\beta_{i,j} - \beta_{k,l}}{\sigma_l(\alpha) - \sigma_j(\alpha)}$,

the division being possible since the extension is separable ($\sigma_j(\alpha) \neq \sigma_l(\alpha)$).

Obviously, there are only finitely many possibilities for λ such that $N\left(g(\mathtt{X} - \lambda\alpha)\right)$ is not squarefree.

Observe that there are at most $n(n-1)m(m-1)/2$ of them.

□

2.2 Trager's algorithm

Algorithm 2.4 *"Trager's Algorithm"* (cf [ENC])

Input. *A monic squarefree polynomial $f(\mathtt{X}) \in \mathbb{K}[\mathtt{X}]$ where $\mathbb{K} = K(\alpha)$ with α a root of its minimal polynomial $\boldsymbol{m}_\alpha(\mathtt{Y}) \in K[\mathtt{Y}]$. Assume that f has coefficients in $\mathbb{Z}[\alpha]$, for the number field case, or in $\mathbb{F}_q[t][\alpha]$, for the function field case.*

Output. *Complete factorization of f over $\mathbb{K}[\mathtt{X}]$.*

Step 1. *Compute λ such that the norm*

$$N_\lambda(f(\mathtt{X} - \lambda\mathtt{Y})) := res_{\mathtt{Y}}\left(\boldsymbol{m}_\alpha(\mathtt{Y}), f(\mathtt{X} - \lambda\mathtt{Y})\right)$$

is squarefree.

Step 2. *Completely factor the norm* $N_\lambda(f(\mathtt{X}-\lambda\mathtt{Y}))$ *into irreducible factors* $N_1,\cdots,N_t$ *over* K.

Step 3. *Compute the* $GCD's$ $G_i(\mathtt{X}) = GCD\,(N_i(\mathtt{X}), f(\mathtt{X}-\lambda\alpha))$ *over* $\mathbb{K}$.

Step 4. *Return* $\prod_{i=1}^{t} G_i(\mathtt{X}+\lambda\alpha)$ *the complete factorization of* f.

In practice, a few trials suffice to obtain the squarefree norm of step 1.

In [LAD], Landau showed that, for number fields, Trager's algorithm runs in polynomial time, provided we use a polynomial time algorithm to factor the norm.

2.3 Some improvements on Trager's algorithm

More recently, for the case $K=\mathbb{Q}$, Encarnación in [ENC] presented a device for reducing the number of combinations of modular factors of the norm, in case a combinatorial search is performed to recover true factors of the norm from the lifted ones modulo a higher power of a suitably chosen prime that has been used for the factorization modulo p step.

Theorem 2 in [ENC], characterises the modular factors of a *true combination* by some easy-to-check conditions. Any combination that does not satisfy these conditions, is then known to be *extraneous* and will be ignored during the trial division phase, which will help speeding up this phase of the algorithm.

We will give a general version of this theorem that applies to the Function Field case as well.

Theorem 2.5

Let $f(\mathtt{X}) = f(\mathtt{X},\alpha) \in \mathbb{Z}[\alpha][\mathtt{X}]$ *(or* $\mathbb{F}_q[t,\alpha][\mathtt{X}]$ *depending on whether* $\mathbb{K}$ *is a number field or a function field).*

Assume $f(\mathtt{X})$ *is a squarefree polynomial whose norm is also squarefree.*

Let's denote by p *a rational prime*[3] *that does not divide the leading coefficients* $lc(\boldsymbol{m}_\alpha)$ *and* $lc(N(f(\mathtt{X})))$ *nor the discriminants* $discr(\boldsymbol{m}_\alpha)$ *and* $discr(N(f(\mathtt{X})))$.

Let $\boldsymbol{m}_\alpha \equiv \boldsymbol{m}_{\alpha,1}\,\boldsymbol{m}_{\alpha,2}\cdots\boldsymbol{m}_{\alpha,s}\ (\bmod\ p)$ *be a complete factorization of* $\boldsymbol{m}_\alpha\ \ mod\, p$.

Let $N_i = Res_{\mathtt{Y}}\,(\boldsymbol{m}_{\alpha,i}(\mathtt{Y}), f(\mathtt{X},\mathtt{Y}))$, *the resultant being computed modulo* p.

If

$$N_i = \prod_{j=1}^{r_i} N_{i,j}$$

[3] $p\in\mathbb{Z}$ or $p\in\mathbb{F}_q[t]$ depending on the case.

is a complete factorization of N_i, for $i = 1, \cdots, s$, then a complete factorization of $N(f)$ modulo p is given by

$$N(f) \equiv \prod_{i=1}^{s} \left(\prod_{j=1}^{r_i} N_{i,j} \right) \pmod{p}$$

Furthermore, $deg(\boldsymbol{m}_{\alpha,i})$ divides $deg(N_{i,j})$, and $deg(N_i) = deg\,(\boldsymbol{m}_{\alpha,i})\, deg\,(f)$

Proof:

Since the resultant is multiplicative, we have

$$\begin{aligned} N = \quad & Res_{\mathtt{Y}}\,(\boldsymbol{m}_{\alpha}(\mathtt{Y}), f(\mathtt{X},\mathtt{Y})) && (\bmod\ p) \\ = \quad & Res_{\mathtt{Y}} \left(\prod_{i=1}^{s} \boldsymbol{m}_{\alpha,i}(\mathtt{Y}), f(\mathtt{X},\mathtt{Y}) \right) && (\bmod\ p) \\ = \quad & \prod_{i=1}^{s} Res_{\mathtt{Y}}\,(\boldsymbol{m}_{\alpha,i}(\mathtt{Y}), f(\mathtt{X},\mathtt{Y})) && (\bmod\ p) \\ = \quad & \prod_{i=1}^{s} N_i && (\bmod\ p) \end{aligned}$$

Hence the factorization of N_i into irreducible factors, yields a complete factorization of $N \pmod{p}$, all computations being done modulo p.

Moreover, the definition of the N_i and (2.2) above, yield

$$deg(N_i) = deg\,(\boldsymbol{m}_{\alpha,i})\, deg\,(f)$$

To show that $deg\,(\boldsymbol{m}_{\alpha,i})$ divides also the degrees of the irreducible factors $N_{i,j}$, we will first show that in fact $N_{i,j}$ is a norm of some polynomial over a finite field obtained by adjoining a root of $\boldsymbol{m}_{\alpha,i}$. And hence, by rewriting this norm as a resultant involving $\boldsymbol{m}_{\alpha,i}$ we deduce the divisibility property of the degrees again from (2.2) above.

For that, note that N_i is the norm of the polynomial $\tilde{f}(\mathtt{X},\mathtt{Y})|_{\mathtt{Y}=\alpha_p}$ where α_p is a root of $\boldsymbol{m}_{\alpha,i}$ and

$$f(\mathtt{X},\mathtt{Y}) \equiv \tilde{f}(\mathtt{X},\mathtt{Y}) \pmod{p}.$$

Since N is squarefree, and p was chosen to preserve the squarefreeness modulo p, N_i is squarefree for all i. But N_i is the norm of the squarefree polynomial $\tilde{f}(\mathtt{X}, \alpha_p)$. So we can use the result (2.3) in the proof of Lemma (2.2) and deduce that $N_{i,j}$ is the norm of an irreducible factor of $\tilde{f}(\mathtt{X}, \alpha_p)$, and therefore, $deg(N_{i,j})$ is a multiple of $deg(\boldsymbol{m}_{\alpha,i})$.

□

For an example of the implementation of this result, we refer to [ENC]. We just briefly mention here how can this theorem be applied, as proposed by Encarnación.

Instead of factoring the norm N modulo p, we first factor the *minimal polynomial* $\boldsymbol{m}_\alpha$ modulo p into irreducibles factors $\boldsymbol{m}_{\alpha,1}, \cdots, \boldsymbol{m}_{\alpha,s}$, then for $i = 1, \cdots, s$ we compute the resultants

$$N_i = Res_{\mathtt{Y}}\left(\boldsymbol{m}_{\alpha,i}(\mathtt{Y}), f(\mathtt{X}, \mathtt{Y})\right)$$

modulo p, and factor each N_i into irreducible factors $N_{i,1}, \cdots, N_{i,r_i}$. Then we lift the factorization

$$N = \prod_{i=1}^{s} \prod_{j=1}^{r_i} N_{i,j} \qquad (\mod p)$$

which is a complete factorization of the norm N modulo p, to a sufficiently high power of p. Let's for simplicity, denote the lifted factors also by $N_{i,j}$.

Let C_i denote the set of all the $N_{i,j}$, $(1 \leq j \leq r_i)$, occuring in a chosen combination of the lifted factors. Then if $C = C_1 \cup \cdots \cup C_s$ is the corresponding combination, by Theorem (3.10), we know that

$$C_i \neq \emptyset, \qquad i = 1, \cdots, s$$

So any combination that leaves one of the C_i empty, will be discarded because it can not correspond to a true factor.

In addition, we can check the following condition that should be satisfied by the degree of any potential factor g of f,

$$deg(g) = \frac{1}{deg\left(\boldsymbol{m}_{\alpha,i}\right)} \sum_{N_{i,j} \in C_i} deg(N_{i,j}) \qquad i = 1, \cdots, s$$

This condition actually implies the first one, i.e the condition on the C_i, but Encarnación suggests to retain both of them for clarity.

CHAPTER THREE

DIRECT FACTORIZATION METHODS OVER A GENERAL NUMBER FIELD

In this chapter, we will present various algorithms for factorization of polynomials having coefficients in a number field. These algorithms differ from Trager's algorithm, which avoids computations in the number field by sending the polynomial down to the ground field $\mathbb{Q}$, with the cost of a higher degree polynomial that needs to be factored over $\mathbb{Q}$. We will call them *direct factorization algorithms*, because they are applied to the polynomial as it is over the number field.

The first one did appear almost in the same time as Trager's algorithm and is a natural generalisation of the Berlekamp-Zassenhaus factorization algorithm over the rationals; while the last one is built on the most recent Knapsack factorization method.

Recall that in the whole chapter, $\mathbb{K}$ will denote a number field given by specifying a primitive element α whose minimal polynomial $\boldsymbol{m}_\alpha(\mathtt{Y}) \in \mathbb{Z}[\mathtt{Y}]$ is monic and has degree m, which may be assumed to be greater than 2.

3.1 Weinberger and Rothschild approach

The two powerful advantages that enable Weinberger and Rothschild in [W-R] to succeed in the generalisation of the usual Henselian technique for factoring polynomials in $\mathbb{Z}[\mathtt{X}]$, are:

1. A perfect choice of the representation of numbers in the number field $\mathbb{K}$, allowing a denominator that can be taken the same throughout all the steps of the algorithm.

2. An ability to handle finite fields and modular computations exaclty as needed for this purpose.

We start by explaining these points before giving the algorithm itself.

3.1.1 Representation of elements in $\mathbb{K}$

Since the primitive element α defines a $\mathbb{Q}$-basis for $\mathbb{K}$, elements of $\mathbb{K}$ can be represented as polynomials in α of degree less than m with coefficients in $\mathbb{Q}$, that may be chosen in $\frac{1}{d}\mathbb{Z}$ with d any denominator common to the former coefficients. Thus, given a polynomial $g(\mathtt{X})$ in $\mathbb{K}[\mathtt{X}]$, one can easily exhibit a denominator d, so that the coefficients of $g(\mathtt{X})$ can be represented as polynomials in α of degree $< m$ with coefficients in $\frac{1}{d}\mathbb{Z}$ and so $g(\mathtt{X})$ itself is in $\frac{1}{d}\mathbb{Z}[\alpha][\mathtt{X}]$.
On the other hand, elements of $\mathcal{O}_{\mathbb{K}}$ can also be viewed as elements of a certain $\frac{1}{d}\mathbb{Z}[\alpha]$, take for instance d to be the discriminant of $\mathbb{K}$ (cf e.g [NAR]). So $\left\{ d > 0 \,\middle|\, \mathcal{O}_{\mathbb{K}} \subset \frac{1}{d}\mathbb{Z}[\alpha] \right\} \neq \emptyset$ and the well order of $\mathbb{N}$ provides a smaller element for it. Actually, a more general statement is also true and we have the following.

Definition 3.1

We define the defect*of an* integral basis[1] $\{\omega_1, \cdots, \omega_m\}$ *to be the integer:*

$$\min \left\{ d > 0 \,\middle|\, \mathcal{O}_{\mathbb{K}} \subset \frac{1}{d}\mathbb{Z}[\omega_1, \cdots, \omega_m] \right\}$$

For the special case where $\omega_i = \alpha^{i-1}$, we denote the defect by $defect(\alpha)$. This is actually the largest denominator appearing in the reduced representation of the elements of $\mathcal{O}_{\mathbb{K}}$, i.e representations of the form $\frac{P(\alpha)}{d}$ with $P(\mathtt{Y}) \in \mathbb{Z}[\mathtt{Y}],\ deg(P) < m$ where d is coprime with $cont(P)$.

This number may not be easy to determine and one would be content with the following.

Lemma 3.2

Let D_0 be the largest positive integer whose square divides the discriminant of $\boldsymbol{m}_\alpha(\mathtt{Y})$.
Then $defect(\alpha) | D_0$ so that $\mathcal{O}_{\mathbb{K}} \subset \frac{1}{D_0}\mathbb{Z}[\alpha]$.

Proof: see [NAR].

Factoring polynomials in $\mathbb{K}[\mathtt{X}]$ introduces the problem of choosing an appropriate denominator for the polynomials involved. Weinberger and Rothschild pointed out that when factoring a polynomial $f(\mathtt{X}) \in \frac{1}{d}\mathbb{Z}[\alpha][\mathtt{X}]$, new denominators can occur, and the irreducible factors of f over $\mathbb{K}$ may have a denominator other than d. For example, over $\mathbb{K} = \mathbb{Q}(\alpha)$, where $\alpha = i\sqrt{3}$, the polynomial $\mathtt{X}^2 + \mathtt{X} + 1$, which is in $\frac{1}{d}\mathbb{Z}[\alpha][\mathtt{X}]$ with $d = 1$, factorises as $\mathtt{X}^2 + \mathtt{X} + 1 = \left(\mathtt{X} + \frac{1}{2}(1+\alpha)\right)\left(\mathtt{X} + \frac{1}{2}(1-\alpha)\right)$, with factors having coefficients in $\frac{1}{2}\mathbb{Z}[\alpha][\mathtt{X}]$.
This is however controllable by the following lemma that generalises the Gauss lemma.

[1] An integral basis of $\mathbb{K}$ is a system $\{\omega_1, \cdots, \omega_m\}$ of integers of $\mathbb{K}$ which is linearly independant over $\mathbb{Q}$ and generates $\mathcal{O}_{\mathbb{K}}$ as $\mathbb{Z}$-module.

Lemma 3.3 *(Weinberger & Rothschild)*

Let $f(\mathtt{X}) \in \frac{1}{d}\mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ *be a monic polynomial and suppose* $f(\mathtt{X}) = g(\mathtt{X})h(\mathtt{X}) \in \mathbb{K}[\mathtt{X}]$, *where* $g(\mathtt{X})\,,\ h(\mathtt{X})$ *are monic. Then* $g(\mathtt{X})\,,\ h(\mathtt{X}) \in \frac{1}{d}\mathcal{O}_{\mathbb{K}}[\mathtt{X}]$.

Proof: see [W-R].

Hence if the monic polynomial $f(\mathtt{X}) \in \frac{1}{d}\mathbb{Z}[\alpha][\mathtt{X}]$, certainly $f(\mathtt{X}) \in \frac{1}{d}\mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ since α is an algebraic integer, and thus by lemma (3.3) above, any monic factor $g(\mathtt{X})$ of $f(\mathtt{X})$ satisfies:

$$g(\mathtt{X}) \in \frac{1}{d}\mathcal{O}_{\mathbb{K}}[\mathtt{X}] \subset \frac{1}{d}\cdot\frac{1}{D_{_0}}\mathbb{Z}[\alpha][\mathtt{X}]$$

where $D_{_0}$ is the denominator of lemma (3.2) or even the absolute value of $discr\,(\boldsymbol{m}_{\alpha}(\mathtt{Y}))$.
Hence we can choose an integer $D = d \cdot D_{_0}$ such that:

$$f \text{ and all its monic factors over } \mathbb{K}[\mathtt{X}] \text{ lie in } \tfrac{1}{D}\mathbb{Z}[\alpha][\mathtt{X}].$$

3.1.2 Structure of the finite fields and rings involved

In order to generalise the factorization method for $\mathbb{Z}[\mathtt{X}]$ described in section (1.6), one needs to understand what happens when reducing modulo a prime or a power of a prime.
By describing $\mathbb{K}$ and $\mathbb{Z}[\alpha]$ as:

$$\mathbb{Q}(\alpha) \cong \mathbb{Q}[\mathtt{Y}]/\left\langle \boldsymbol{m}_{\alpha}(\mathtt{Y})\right\rangle = \left\{ \sum_{j=0}^{m-1} a_j\alpha^j \;\middle|\; a_j \in \mathbb{Q} \right\}$$

$$\mathbb{Z}[\alpha] \cong \mathbb{Z}[\mathtt{Y}]/\left\langle \boldsymbol{m}_{\alpha}(\mathtt{Y})\right\rangle = \left\{ \sum_{j=0}^{m-1} a_j\alpha^j \;\middle|\; a_j \in \mathbb{Z} \right\}$$

we can see that the behaviour of $\mathbb{K}$ and $\mathcal{O}_{\mathbb{K}}$ under the aforementioned reduction will be dominated and determined by the behaviour of $\boldsymbol{m}_{\alpha}(\mathtt{Y})$ under this reduction.

- If $\boldsymbol{m}_{\alpha}$ remains irreducible, the reduction $\bmod p$ affects only the coefficients of the polynomials in α, elements of $\mathbb{Z}[\alpha]$ or $\mathbb{Q}[\alpha]$. Thus $\mathbb{Z}[\alpha]$ maps onto $(\mathbb{Z}/p\mathbb{Z})\,[\alpha]$ which is a field of p^m elements, and so do the elements of $\mathbb{Q}[\alpha]$ with denomintors not divisible by p.
  In this case, the factorization algorithm of Weinberger and Rothschild will be very similar to the Berlekamp-Zassenhaus algorithm.

- If on the contrary, $\boldsymbol{m}_{\alpha} \bmod p$ is no longer irreducible, then $\mathbb{Z}[\alpha]/\langle p\rangle$ splits into different factors and Weinberger and Rothschild propose to use the Chinese Remainder Theorem (CRT) to combine the resulting algebraic numbers.

Assuming $p \nmid discr(\boldsymbol{m}_\alpha)$, so that $\boldsymbol{m}_\alpha \bmod p$ remains squarefree, let

$$\boldsymbol{m}_\alpha \mod p = \overline{\boldsymbol{m}}_{\alpha,1}\,\overline{\boldsymbol{m}}_{\alpha,2}\cdots\overline{\boldsymbol{m}}_{\alpha,s}$$

be a complete factorization of $\boldsymbol{m}_\alpha \bmod p$, where the $\overline{\boldsymbol{m}}_{\alpha,i}$ are monic irreducible polynomials in $(\mathbb{Z}/p\mathbb{Z})\,[\mathtt{Y}]$, and we assume knowing monic polynomials $\boldsymbol{m}_{\alpha,i}$ in $\mathbb{Z}[\mathtt{Y}]$ which reduces to $\overline{\boldsymbol{m}}_{\alpha,i}$, i.e such that $\boldsymbol{m}_{\alpha,i} \bmod p = \overline{\boldsymbol{m}}_{\alpha,i}$. In addition, the degrees $deg(\boldsymbol{m}_{\alpha,i}) = m_i$, satisfy $\sum_{i=1}^{s} m_i = m$ and we may assume the coefficients of $\boldsymbol{m}_{\alpha,i}$ to be reduced modulo p.

Then to each factor $\overline{\boldsymbol{m}}_{\alpha,i}$ of $\boldsymbol{m}_\alpha \bmod p$ corresponds a finite field of $q_i = p^{m_i}$ elements

$$\mathbb{F}_{q_i} = \mathbb{F}_{p^{m_i}} \cong (\mathbb{Z}/p\mathbb{Z})\,[\mathtt{Y}]/\,\langle\overline{\boldsymbol{m}}_{\alpha,i}(\mathtt{Y})\rangle$$

and we have the isomorphism:

$$\mathbb{Z}[\alpha]/\langle p\rangle \cong \mathbb{F}_{p^{m_1}} \times\cdots\times \mathbb{F}_{p^{m_s}}$$

Similarly, to each lifting of the $\boldsymbol{m}_{\alpha,i}$, $\boldsymbol{m}_{\alpha,i}^{(\mathtt{k})} \in \mathbb{Z}[\mathtt{Y}]$, corresponds a ring, denoted $W_{\mathtt{k}}(\mathbb{F}_{q_i})$, defined as:

$$W_{\mathtt{k}}(\mathbb{F}_{q_i}) := \mathbb{Z}[\mathtt{Y}]/\langle p^{\mathtt{k}},\ \boldsymbol{m}_{\alpha,i}^{(\mathtt{k})}(\mathtt{Y})\rangle \cong \left(\mathbb{Z}/p^{\mathtt{k}}\mathbb{Z}\right)[\mathtt{Y}]/\langle\overline{\boldsymbol{m}}_{\alpha,i}^{(\mathtt{k})}(\mathtt{Y})\rangle$$

This ring consisting of $q_i^{\mathtt{k}}$ elements, can be written as:

$$W_{\mathtt{k}}(\mathbb{F}_{q_i}) = \left\{ \sum_{j=0}^{m_i-1} a_j \alpha_{i,\mathtt{k}}^{j} \,\middle|\, a_j \in \mathbb{Z}/p^{\mathtt{k}}\mathbb{Z} \right\}$$

where $\alpha_{i,\mathtt{k}}$ is a root of $\overline{\boldsymbol{m}}_{\alpha,i}^{(\mathtt{k})}$. It can be mapped onto $\mathbb{F}_{q_i}$ by reducing the coefficients of the polynomials in $\alpha_{i,\mathtt{k}}$ modulo p. This ring will play the role of $\mathbb{Z}/p^{\mathtt{k}}\mathbb{Z}$ for the Berlekamp-Zassenhaus algorithm, during the necessary lifting process. The complete field playing the role of $\mathbb{Q}_p$, is here $\mathbb{K}\otimes\mathbb{Q}_p$.

The arithmetic in these residue class rings and fields is done *modulo the residue classes*. This is called *modular arithmetic*.

A way to approach modular computations, as given by Weinberger and Rothschild, is to consider " $\bmod$ " as a *binary operation*, which then will have the lowest precedence of all other binary operations defined over $\mathbb{K}$ or $\mathbb{K}[\mathtt{X}]$, and is allowed to have as its right operand, a list of operands defining $a \bmod (b,\, c)$ as:

$$a \mod (b,\, c) := (a \mod b) \mod (c \mod b)$$

Example

In $\mathbb{Q}[\mathtt{X}]$ take $a(\mathtt{X}) = 4\mathtt{X}^6 - 3\mathtt{X}^5 + \mathtt{X}^4 + \mathtt{X}^3 + 7\mathtt{X}^2 + 1$, $b = 3$, and $c(\mathtt{X}) = \mathtt{X}^2 - \mathtt{X} + 4$.

$$\begin{aligned} a(\mathtt{X}) \mod (3,\, c) &= \mathtt{X}^6 + \mathtt{X}^4 + \mathtt{X}^3 + \mathtt{X}^2 + 1 \mod (\mathtt{X}^2 - \mathtt{X} + 1) \\ &= 1 - \mathtt{X} - 1 + \mathtt{X} = 0 \mod (\mathtt{X}^2 - \mathtt{X} + 1) \end{aligned}$$

Recall that the modular inversion of non-zero elements, when possible, is done by means of the Extended Euclidean Algorithm.

In order to apply the CRT in this case, we need to build a ring homomorphism between $\mathbb{Z}[\alpha]$ and the above rings $W_{\mathtt{k}}(\mathbb{F}_{q_i})$. This is done by means of a reduction $\mod \left(p^{\mathtt{k}}, \boldsymbol{m}_{\alpha,i}^{(\mathtt{k})}\right)$ which works by first reducing the coefficients of the polynomials in α modulo $p^{\mathtt{k}}$, then taking the remainder of the division by $\boldsymbol{m}_{\alpha,i}^{(\mathtt{k})}$ of the polynomial so obtained and replacing α by $\alpha_{i,\mathtt{k}}$.
This map can be extended to $\mathbb{Z}[\alpha][\mathtt{X}]$ coefficient-wise, in addition, if D is such that: f and all its monic factors over $\mathbb{K}[\mathtt{X}]$ lie in $\frac{1}{D}\mathbb{Z}[\alpha][\mathtt{X}]$, then we can extend the above map to $\frac{1}{D}\mathbb{Z}[\alpha][\mathtt{X}]$ provided $p \nmid D$ so that $\left(D^{-1} \bmod p^{\mathtt{k}}\right)$ exists. This results in the following maps:

$$\begin{array}{rcl} \frac{1}{D}\mathbb{Z}[\alpha][\mathtt{X}] & \longrightarrow & W_{\mathtt{k}}(\mathbb{F}_{q_i})[\mathtt{X}] \\ g(\mathtt{X}) = \frac{1}{D}\sum_t b_t \mathtt{X}^t & \longmapsto & \sum_t \left(\left((D^{-1} \bmod p^{\mathtt{k}})b_t\right) \mod (p^{\mathtt{k}}, \boldsymbol{m}_{\alpha,i}^{(\mathtt{k})})\right)\mathtt{X}^t \end{array}$$

Note that the reductions of $g(\mathtt{X})$ in the rings $W_{\mathtt{k}}(\mathbb{F}_{q_i})[\mathtt{X}]$ all have the same degree, because a coefficient of $g(\mathtt{X})$ reduces to zero in one of the $W_{\mathtt{k}}(\mathbb{F}_{q_i})$ only when it is divisible by p. Hence we can apply the CRT only to s-tuples of equal-degree polynomials from $W_{\mathtt{k}}(\mathbb{F}_{q_1})[\mathtt{X}] \times \cdots \times W_{\mathtt{k}}(\mathbb{F}_{q_s})[\mathtt{X}]$, in such a case the CRT, applied coefficient-wise, guaranties the existence of $g(\mathtt{X}) \in \frac{1}{D}\mathbb{Z}[\alpha][\mathtt{X}]$ which reduces exactly to the chosen polynomials in the $W_{\mathtt{k}}(\mathbb{F}_{q_i})$.

3.1.3 The algorithm of Weinberger and Rothschild

We will give the algorithm of Weinberger and Rothschild slightly modified by applying it to a monic polynomial $f(\mathtt{X}) \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$, hence $d = 1$, and by not being explicit on the intermediate steps of the Hensel lifting.
Their algorithm completely factors a monic polynomial in $\mathbb{K}[\mathtt{X}]$, and is also applicable to nonmonic polynomials after some simple transformations of the polynomial and a good choice of the denominator.

Algorithm 3.4 "Weinberger & Rothschild " (cf [W-R])

Input. *A monic squarefree polynomial* $f(\mathtt{X}) \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$.

Output. *Complete factorization of* $f(\mathtt{X})$ *in* $\mathbb{K}[\mathtt{X}]$.

Step 1. *Determine* D *such that:*

f *and all its monic factors over* $\mathbb{K}[\mathtt{X}]$ *lie in* $\frac{1}{D}\mathbb{Z}[\alpha][\mathtt{X}]$.

Step 2. *Choose a prime* p *not dividing* D*, and if one takes* $D = defect(\alpha)$ *then make sure that* $p \nmid discr(\boldsymbol{m}_\alpha)$ *so that* $\boldsymbol{m}_\alpha$ *remains squarefree* $\mod p$.

Step 3. *Factor* $\boldsymbol{m}_\alpha(\mathtt{Y}) \bmod p$ *obtaining:*

$\boldsymbol{m}_\alpha \equiv \boldsymbol{m}_{\alpha,1}\,\boldsymbol{m}_{\alpha,2}\cdots\boldsymbol{m}_{\alpha,s} \pmod p$ *with* $deg(\boldsymbol{m}_{\alpha,i}) = m_i$ *and* $\sum_{i=1}^{s} m_i = m$.

May try different primes p *in order to minimise the number of factors* s *of* $\boldsymbol{m}_\alpha \bmod p$.

Step 4. *Compute several factorizations of* $f(\mathtt{X}) \bmod p$*, one for each factor* $\boldsymbol{m}_{\alpha,i}$ *of* $\boldsymbol{m}_\alpha \bmod p$ *thus obtaining:*

$$(D^{-1} \mod p)\cdot Df(\mathtt{X}) \equiv \prod_l f_{l,i}(\mathtt{X}) \mod (p, \boldsymbol{m}_{\alpha,i}),\ \ 1 \le i \le s$$

where $f_{l,i}(\mathtt{X}) \in \mathbb{F}_{q_i}[\mathtt{X}]$. *If for some* i, $f(\mathtt{X}) \bmod (p, \boldsymbol{m}_{\alpha,i})$ *is not squarefree, choose a new prime* p *starting again at (Step 2).*

Step 5. *Compute a bound* B *on the absolute values of the coefficients of any factor of* $f(\mathtt{X})$ *in* $\mathbb{K}[\mathtt{X}]$ *(cf [W-R]), and determine* $\mathtt{k}$ *such that* $p^{\mathtt{k}} > 2B$.

Step 6. *Lift the factorization of* $\boldsymbol{m}_\alpha \bmod p$ *up to accuracy* $p^{\mathtt{k}}$ *using the quadratic Hensel's algorithm (1.4) obtaining a factorization :*

$$\boldsymbol{m}_\alpha(\mathtt{Y}) \equiv \prod_{i=1}^{s} \boldsymbol{m}_{\alpha,i}^{(\mathtt{k})}(\mathtt{Y}) \mod p^{\mathtt{k}}$$
$$\text{where } \boldsymbol{m}_{\alpha,i}^{(\mathtt{k})} \equiv \boldsymbol{m}_{\alpha,i} \mod p$$

Step 7. *Lift the factorization of* $f(\mathtt{X}) \mod (p, \boldsymbol{m}_{\alpha,i})$ *up to accuracy* $p^{\mathtt{k}}$ *obtaining* s *factorizations in* $W_{\mathtt{k}}(\mathbb{F}_{q_i})$*, for* $1 \le i \le s$*:*

$$(D^{-1} \mod p^{\mathtt{k}})\cdot Df(\mathtt{X}) \equiv \prod_l f_{l,i}^{(\mathtt{k})}(\mathtt{X}) \mod \left(p^{\mathtt{k}}, \boldsymbol{m}_{\alpha,i}^{(\mathtt{k})}\right) \tag{3.1}$$
$$\text{such that } f_{l,i}^{(\mathtt{k})}(\mathtt{X}) \equiv f_{l,i}(\mathtt{X}) \mod p$$

Step 8. *Combine the combinatoric search with the Chinese Remainder Algorithm (CRA) applied to each possible* s*-tuple of equal-degree factors modulo* $\left(p^{\mathtt{k}}, \boldsymbol{m}_{\alpha,i}^{(\mathtt{k})}\right)$ *to find factors of* f *in* $\frac{1}{D}\mathbb{Z}[\alpha][\mathtt{X}]$.
If $s = 1$ *no CRT is needed.*

The time complexity of this algorithm is clearly much like the complexity of Berlekamp-Zassenhaus algorithm, although all constants are larger. The reason is that even though the CRA is polynomial time, lots of time is consumed by the combinatoric search as in the original algorithm for a factorization over the rationals. The number of trial divisions can become exponential in $n \times s$, which makes this algorithm not practically applicable if the number s of factors of $\boldsymbol{m}_\alpha \bmod p$ is not reasonably small, or if the degree of the polynomial to be factored is very high.

Another disadvantage of this algorithm occurs if there are several factors of the same degree in each of the modular factorizations of f. This increases the number of possible s-tuple of equal-degree factors on which the CRA is applied, and the only way to find the possible tuples that lead to true factors, is to try them all. We cite the following example from [ABB] that shows two exponential large searches, one on top of the other, due to the fact that both f and $\boldsymbol{m}_\alpha$ are actually Swinnerton-Dyer polynomials using different primes.

Let $f(\mathtt{X}) = \mathtt{X}^4 - 10\mathtt{X}^2 + 1 = \prod(\mathtt{X} \pm \sqrt{2} \pm \sqrt{3})$ (2^{nd} Swinnerton-Dyer polynomial),

$\boldsymbol{m}_\alpha = \mathtt{Y}^4 - 24\mathtt{Y}^2 + 4 = \prod(\mathtt{X} \pm \sqrt{5} \pm \sqrt{7})$ (a generalised Swinnerton-Dyer polynomial).

With $p = 1201$, $\boldsymbol{m}_\alpha(\mathtt{Y}) \equiv (\mathtt{Y} + 51)(\mathtt{Y} + 259)(\mathtt{Y} + 942)(\mathtt{Y} + 1150) \mod p$.

The factors of $\boldsymbol{m}_\alpha \mod p$ being all linear, the four fields $\mathbb{F}_{q_i}$ coincide with $\mathbb{F}_p$. This means that the four modular factorization of f will also be equal. But applying the algorithm, we need to consider them all. And it turns out that $f(\mathtt{X}) \mod p$ has also only linear factors:

$$f(\mathtt{X}) \equiv (\mathtt{X} + 202)(\mathtt{X} + 327)(\mathtt{X} + 874)(\mathtt{X} + 999) \mod p$$

which, after lifting, will produce a factorization with only linear factors.

Hence to test whether f has a linear factor over $\mathbb{K}$, we must apply the CRA to all $4 \times 4 \times 4 \times 4 = 256$ possible ways of picking a factor of f in every one of the four fields $\mathbb{F}_{q_i}$. Since there is no linear factor, we check the quadratic one. For that we need to try all $6 \times 6 \times 6 \times 6 = 1296$ possible ways of picking pairs of factors of f from the four modular factorizations $\cdots$. But the degree-4 polynomial f has no quadratic factors, and hence is irreducible.

3.2 The LLL factorization method

3.2.1 First use of lattices for factorization of polynomials over algebraic number fields

In this section we present a direct generalisation of the LLL method for factoring polynomials with rational coefficients sketched earlier (cf section(1.6)), focusing here on the factorization of polynomials with coefficients in a number field. This generalisation was given by A. Lenstra in [LEN 3].

By doing so, we start from Weinberger and Rothschild's work, as it is itself a generalisation of the Henselian technique on which the LLL factorization algorithm is also based. We will then use the same notations unless otherwise stated.

The important novelty that the LLL factorization algorithm brings is the use of lattices to overcome the combinatoric search, which evolves in a polynomial-time algorithm, but there are other advantages as well, not of less importance.

From Weinberger and Rothschild's work, we know that by reduction $\bmod p$, the minimal polynomial of α may split. Its complete factorization determines a number of finite fields over which f is factorised. Each of the modular factorizations of f, thus produced, is then lifted and a number of combinatoric searches followed by an application of the CRT, enable the reconstruction of the factorization seeked.

Besides the exponential-time combinatoric search, difficulties may arise at (**Step 4**) of Weinberger and Rothschild's algorithm:

> If for some i, $f(\mathtt{X}) \bmod (p, \boldsymbol{m}_{\alpha,i})$ is not squarefree,
> choose a new prime p and start again at (Step 2).

The LLL factorization algorithm is a remedy to this, because it needs only *one* finite field over which f is factorised, and it uses only *one suitable* modular factor of f to obtain a true irreducible factor of f over $\mathbb{K}$. This makes the Hensel lifting less cumbersome, having to deal only with two polynomials at a time.

The fact that one modular factor of f enables us to reach a true irreducible factor of f over $\mathbb{K}$ is due to the following two ingenious facts observed and exploited by Lenstra et al. first in [L-L-L],

(1) Due to the squarefreeness of f over the finite field, each modular factor corresponds to a *unique* true irreducible factor which may eventually be f itself, but there is also a certain *divisibility property* that can be preserved during the Hensel lifting which is of a high importance as well (see Proposition (3.5) below).

(2) A geometric view of the arithmetic problem allowing the use of *lattices* for which a polynomial-time algorithm is known to reduce their bases to ones with shortest vectors. But the more important fact is that a certain lattice can be built in such a way that whenever one of its vectors is short enough, it corresponds to a polynomial that has a non trivial co-divisor with f (see Proposition (3.6) below). In addition, among the shortest vectors of this lattice, a vector corresponding to an irreducible factor of f can be found.

Let $f, \boldsymbol{m}_\alpha, \boldsymbol{m}_{\alpha,i}$ and n, m, m_i be as in the last section.
Recall that even if f has coefficients in $\mathbb{Z}[\alpha]$ itself, not just integers as we assumed in (1.7), a new denominator may arise and need to be considered. So we choose D as in (3.1.3), i.e such that:

$$f \text{ and all its monic factors over } \mathbb{K}[\mathtt{X}] \text{ lie in } \tfrac{1}{D}\mathbb{Z}[\alpha][\mathtt{X}].$$

Choose a prime p such that: $p \nmid D \cdot discr(\boldsymbol{m}_\alpha) \cdot discr(f)$.

Then D is invertible modulo p, $(\boldsymbol{m}_\alpha \bmod p)$ remains squarefree, and we get an isomorphism:

$$\frac{1}{D}\mathbb{Z}[\alpha]/\langle p\rangle \cong \mathbb{F}_{q_1} \times \cdots \times \mathbb{F}_{q_s}$$

(See subsection (3.1.2)).

On the other hand, since $discr(f) \in \frac{1}{D}\mathbb{Z}[\alpha]$ and $p \nmid discr(f)$, the image of $discr(f)$ in $\mathbb{F}_{q_1} \times \cdots \times \mathbb{F}_{q_s}$ is not the zero vector and hence:

$$\exists i_0 \mid \ discr(f) \mod (p, \boldsymbol{m}_{\alpha,i_0}) \neq 0$$

Set $H = \boldsymbol{m}_{\alpha,i_0}$.

Hence, (cf page 40), $H(\mathtt{Y})$ is a monic polynomial in $\mathbb{Z}[\mathtt{Y}]$ of degree $m' := deg(H) = m_{i_0}$, such that $H \mod p = \overline{\boldsymbol{m}}_{\alpha,i_0}$. Such H determines the finite field on which a factorization of f is required, that is, $\mathbb{F}_q$ where $q = q_0 = p^{m_{i_0}}$. (Note that during the lifting process, the polynomial $H_{\mathtt{k}}(\mathtt{Y}) \in \mathbb{Z}[\mathtt{Y}]$ such that $H \equiv H_{\mathtt{k}} \mod p^{\mathtt{k}}$, is not necessarily equal to $\boldsymbol{m}^{(\mathtt{k})}_{\alpha,i_0}$.)

Assume we are given a polynomial $h \in \mathbb{Z}[\alpha][\mathtt{X}]$ satisfying the following conditions:

(C.1) h monic,

(C.2) $\big(h \mod (p^{\mathtt{k}}, H_{\mathtt{k}})\big)$ divides $\big(f \mod (p^{\mathtt{k}}, H_{\mathtt{k}})\big)$ in $W_{\mathtt{k}}(\mathbb{F}_q)[\mathtt{X}]$,

(C.3) $(h \mod (p, H_1))$ is irreducible in $\mathbb{F}_q[\mathtt{X}]$,

(C.4) $(h \mod (p, H_1))^2$ does not divide $(f \mod (p, H_1))$ in $\mathbb{F}_q[\mathtt{X}]$.

where $\mathtt{k}$ is a positive integer.

Note that, since h is monic, it has the same degree as $(h \mod (p, H_1))$ and $\big(h \mod (p^{\mathtt{k}}, H_{\mathtt{k}})\big)$. Hence by **(C.2)** $deg(h) \leq n$, and by **(C.3)** $deg(h) > 0$.

Let $l = \deg(h(\mathtt{X}))$. Hence $0 < l \leq n$

Proposition 3.5

The polynomial f has a monic irreducible factor $h_0 \in \frac{1}{D}\mathbb{Z}[\alpha][\mathtt{X}]$ of degree: $l \leq deg(h_0) \leq n$, uniquely determined up to sign, such that $(h \mod (p, H_1))$ divides $(h_0 \mod (p, H_1))$ in $\mathbb{F}_q[\mathtt{X}]$. Further, if $g(\mathtt{X})$ is a monic divisor of $f(\mathtt{X})$ in $\frac{1}{D}\mathbb{Z}[\alpha][\mathtt{X}]$, then the following assertions are equivalent:

(i) $(h \mod (p, H_1))$ *divides* $(g \mod (p, H_1))$ *in* $\mathbb{F}_q[\mathtt{X}]$,

(ii) $\big(h \mod (p^{\mathtt{k}}, H_{\mathtt{k}})\big)$ *divides* $\big(g \mod (p^{\mathtt{k}}, H_{\mathtt{k}})\big)$ *in* $W_{\mathtt{k}}(\mathbb{F}_q)[\mathtt{X}]$,

(iii) $h_0(\mathtt{X})$ *divides* $g(\mathtt{X})$ *in* $\frac{1}{D}\mathbb{Z}[\alpha][\mathtt{X}]$.

In particular $\left(h \mod (p^{\mathtt{k}}, H_{\mathtt{k}})\right)$ *divides* $\left(h_0 \mod (p^{\mathtt{k}}, H_{\mathtt{k}})\right)$ *in* $W_{\mathtt{k}}(\mathbb{F}_q)[\mathtt{X}]$.

Proof: See [2] [LEN 3] and section (4.7) below.

Now let's fix an integer r, $l \leq r < n$, and consider the set of polynomials in $\frac{1}{D}\mathbb{Z}[\alpha][\mathtt{X}]$ of degree $\leq r$, that when reduced $\mod p^{\mathtt{k}}$, are divisible by $\left(h \mod (p^{\mathtt{k}}, H_{\mathtt{k}})\right)$.

By Proposition (3.5) above, h_0 belongs to this set provided $deg(h_0) \leq r$.
Since h_0 is monic, we can as well, restrict ourselves to the subset L of such polynomials that, in addition, when they have the highest degree r, have their leading coefficient in $\mathbb{Z}$. So let's consider the latter set instead.

The aim now is to find simple conditions that ensure that h_0 effectively belongs to L, and enable to determine h_0 in this case.

By identifying an element $g = \sum_{i=0}^{r-1}\sum_{j=0}^{m-1} a_{ij}\,\alpha^j\,\mathtt{X}^i + a_{r_0}\mathtt{X}^r$ of L with the vector $\boldsymbol{g} = (a_{00}, a_{01}, \cdots, a_{r_0})^{tr}$ $\in \left(\frac{1}{D}\mathbb{Z}\right)^{rm+1} \subset \mathbb{R}^{rm+1}$, the set L can be viewed as a lattice in $\mathbb{R}^{rm+1}$ having an upper triangular basis given by:

$$\left\{\frac{1}{D}p^{\mathtt{k}}\,\alpha^j\,\mathtt{X}^i \quad \Big| \quad 0 \leq j < m',\ 0 \leq i < l\right\} \ \cup$$
$$\left\{\frac{1}{D}\alpha^{j-m'}H(\alpha)\mathtt{X}^i \Big| \ m' \leq j < m,\ 0 \leq i < l\right\} \ \cup$$
$$\left\{\frac{1}{D}\,\alpha^j\,h\mathtt{X}^{i-l} \quad \Big| \quad 0 \leq j < m,\ l \leq i < r\right\} \ \cup \ \left\{h\mathtt{X}^{r-l}\right\}$$

For the rational case the two sets introduced above coincide and correspond to a lattice with a basis given by:

$$\left\{p^{\mathtt{k}}\mathtt{X}^i \mid 0 \leq i < l\right\} \cup \left\{h\mathtt{X}^i \mid 0 \leq i \leq r-l\right\}$$

This lattice has determinant $d(L) = p^{\mathtt{k}l}$ and in general $d(L) = p^{\mathtt{k}lm'}$

We can measure the size of a polynomial $g \in L$ by:
The norm of g: $\|g\| = \|\boldsymbol{g}\|$ where $\|\boldsymbol{g}\| = (\sum_{i,j}|a_{ij}|^2)^{1/2}$ is the ordinary Euclidean norm in $\mathbb{R}^{rm+1}$.
The height of g: $\mathcal{H}(g) = |\boldsymbol{g}|_\infty$ where $|\boldsymbol{g}|_\infty = \max_{i,j}\{|a_{ij}|\}$ is the ordinary norm Sup in $\mathbb{R}^{rm+1}$.

[2] The proof of this proposition is very similar to the one for the rational case, we defer it to the next Chapter, section (4.7), where we will give proofs of this proposition, and the next one, in a more general context.

Proposition 3.6

Let a non-zero polynomial b of L satisfy:

$$p^{\mathtt{k}lm'} > \left(D\mathcal{H}(f)((n+1)m(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{m-1})^{1/2}\right)^{rm} \left(D\mathcal{H}(b)((r+1)m(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{m-1})^{1/2}\right)^{nm} \tag{3.2}$$

Then b is divisible by h_0 in $\mathbb{K}[\mathtt{X}]$, and in particular $GCD(f,b) \neq 1$.

Proof:

Let $g = GCD(f,b)$.

By Proposition (3.5), it suffices to show that $(h \mod (p,H))$ divides $(g \mod (p,H))$ in $\mathbb{F}_q[\mathtt{X}]$.

Assuming this is not true, we show that amongst the multiples of g built out of f and b, i.e elements of the form $\lambda f + \mu b$ with $\lambda, \mu \in \frac{1}{D}\mathbb{Z}[\alpha][\mathtt{X}]$, those that have a degree $< deg(g) + deg(h)$ will all reduce to zero modulo $\mod (p^{\mathtt{k}}, H_{\mathtt{k}})$, causing a certain lattice $\tilde{L}$, that we will precise later, to have a determinant bigger than $p^{\mathtt{k}lm'}/D^{(n+r)m}$, while by Inequality (3.2) this determinant should be strictly smaller than $p^{\mathtt{k}lm'}/D^{(n+r)m}$, which will give a contradiction that confirms that actually $(h \mod (p,H))$ divides $(g \mod (p,H))$ in $\mathbb{F}_q[\mathtt{X}]$.

The details of the proof will be given in section (4.7) (cf also [LEN 3]). Here we will just define $\tilde{L}$ and show how can the terms in Inequality (3.2) be derived.

For that, as we did earlier, we identify the polynomials

$$\left\{\alpha^j \mathtt{X}^i f \;\middle|\; 0 \leq j < m\,,\ 0 \leq i < deg(b) - deg(g)\right\} \cup \left\{\alpha^j \mathtt{X}^i b \;\middle|\; 0 \leq j < m\,,\ 0 \leq i < n - deg(g)\right\}$$

with the $m(n + deg(b) - 2deg(g))$-dimensional vectors of their coefficients.

Let $\tilde{L}$ be the lattice generated by the projections of the vectors above on

$$\frac{1}{D}\mathbb{Z}\mathtt{X}^{deg(g)} + \frac{1}{D}\mathbb{Z}\alpha\mathtt{X}^{deg(g)} + \cdots + \frac{1}{D}\mathbb{Z}\alpha^{m-1}\mathtt{X}^{n+deg(b)-deg(g)-1}$$

By Hadamard's inequality, we have:

$$d(\tilde{L}) \leq \prod_{i,j} \|\alpha^j \mathtt{X}^i f\| \prod_{i,j} \|\alpha^j \mathtt{X}^i b\| \tag{3.3}$$

So, to get the right contradiction, it suffices to bound this product from above strictly by $p^{\mathtt{k}lm'}/D^{(n+r)m}$ which is possible by Inequality (3.2) as we can show that for all i,j

$$\begin{aligned} \|\alpha^j \mathtt{X}^i f\| &\leq \left(\mathcal{H}(f)((n+1)m(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{m-1})^{1/2}\right)^{rm} \\ \text{and} \quad \|\alpha^j \mathtt{X}^i b\| &\leq \left(\mathcal{H}(b)((r+1)m(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{m-1})^{1/2}\right)^{nm} \end{aligned}$$

Indeed, by an induction on the positive integer t, we can prove that for all $\tilde{g} \in \frac{1}{D}\mathbb{Z}[\alpha][\mathtt{X}]$, and for all t, u,

$$\mathcal{H}(\alpha^t\, \mathtt{X}^u \tilde{g}) = \mathcal{H}(\alpha^t\, \tilde{g}) \leq \mathcal{H}(\tilde{g})(1 + \mathcal{H}(\boldsymbol{m}_\alpha))^t$$

and

$$\|\alpha^t\, \mathtt{X}^u \tilde{g}\| = \|\alpha^t\, \tilde{g}\| \leq \mathcal{H}(\tilde{g})\, (m(deg(\tilde{g}) + 1))^{1/2}\ (1 + \mathcal{H}(\boldsymbol{m}_\alpha))^t.$$

For that write $\tilde{g} = \sum_{i=0}^{deg(\tilde{g})} \sum_{j=0}^{m-1} a_{ij}\, \alpha^j\, \mathtt{X}^i$ and $\boldsymbol{m}_\alpha(\mathtt{Y}) = \mathtt{Y}^m + b_{m-1}\mathtt{Y}^{m-1} + \cdots + b_1\mathtt{Y} + b_0$,
so that $\alpha^m = -(b_{m-1}\alpha^{m-1} + \cdots + b_1\alpha + b_0)$.

Note that, by definition of the norm and height of polynomials:

$$\mathcal{H}(\alpha^t\, \mathtt{X}^u \tilde{g}) = \mathcal{H}(\alpha^t\, \tilde{g})\ , \quad \forall u$$

idem for the norm, the coefficients being globally not affected by the multiplication by powers of $\mathtt{X}$.

The case $t = 0$ is trivial.

Let $t = 1$. Then:

$$\begin{aligned}
\alpha\, \tilde{g} &= \sum_{i=0}^{deg(\tilde{g})} \sum_{j=0}^{m-1} a_{ij}\, \alpha^{j+1}\, \mathtt{X}^i \\
&= \sum_{i=0}^{deg(\tilde{g})} \left[-a_{i,m-1}b_0 + \sum_{j=1}^{m-1} (a_{i,j-1} - a_{i\,m-1}b_j)\alpha^j \right] \mathtt{X}^i \\
&= \sum_{i=0}^{deg(\tilde{g})} \sum_{j=0}^{m-1} (a_{i,j-1} - a_{i\,m-1}b_j)\, \alpha^j \mathtt{X}^i \\
&\qquad \text{where } a_{i,-1} = 0, \forall i.
\end{aligned}$$

Since, for all i, j,

$$\begin{aligned}
|a_{i,j-1} - a_{i,\,m-1}b_j| &\leq |a_{i,j-1}| + |a_{i,\,m-1}||b_j| \\
&\leq \mathcal{H}(\tilde{g}) + \mathcal{H}(\tilde{g})\mathcal{H}(\boldsymbol{m}_\alpha) \\
&\leq \mathcal{H}(\tilde{g})(1 + \mathcal{H}(\boldsymbol{m}_\alpha))
\end{aligned}$$

we deduce the following:

$$\mathcal{H}(\alpha\, \tilde{g}) = \max_{i,j} |a_{i,j-1} - a_{i,\,m-1}b_j| \leq \mathcal{H}(\tilde{g})(1 + \mathcal{H}(\boldsymbol{m}_\alpha))$$

and

$$\begin{aligned}
\|\alpha\, \tilde{g}\|^2 &= \sum_{i=0}^{deg(\tilde{g})} \sum_{j=0}^{m-1} |a_{i,j-1} - a_{i,\,m-1}b_j|^2 \\
&\leq \sum_{i=0}^{deg(\tilde{g})} \sum_{j=0}^{m-1} [\mathcal{H}(\tilde{g})(1 + \mathcal{H}(\boldsymbol{m}_\alpha)]^2 \\
&\leq [\mathcal{H}(\tilde{g})(1 + \mathcal{H}(\boldsymbol{m}_\alpha))]^2\, [m(deg(\tilde{g}) + 1)]
\end{aligned}$$

and so, our assertions are true for $t = 1$.

Now assuming the results true for t, we get:

$$\begin{aligned}\mathcal{H}(\alpha^{t+1}\,\tilde{g}) = \mathcal{H}(\alpha\cdot\alpha^{t}\,\tilde{g}) &\leq \mathcal{H}(\alpha^{t}\,\tilde{g})(1+\mathcal{H}(\boldsymbol{m}_\alpha))\\ &\leq \mathcal{H}(\tilde{g})(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{t}(1+\mathcal{H}(\boldsymbol{m}_\alpha)) = \mathcal{H}(\tilde{g})(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{t+1}\end{aligned}$$

Then, using this result we obtain:

$$\begin{aligned}\|\alpha^{t+1}\mathtt{X}^{u}\,\tilde{g}\|^2 = \|\alpha\,\cdot\alpha^{t}\tilde{g}\|^2 &\leq \left[\mathcal{H}(\alpha^{t}\tilde{g})(1+\mathcal{H}(\boldsymbol{m}_\alpha))\right]^2\left[m(deg(\alpha^{t}\tilde{g})+1)\right]\\ &\leq \left[\left(\mathcal{H}(\tilde{g})(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{t}\right)(1+\mathcal{H}(\boldsymbol{m}_\alpha))\right]^2\left[m(deg(\tilde{g})+1)\right]\\ &= \mathcal{H}(\tilde{g})^2(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{2(t+1)}\left[m(deg(\tilde{g})+1)\right]\end{aligned}$$

This finishes our induction.

Whence:

$$\begin{aligned}d(\tilde{L}) &\leq \prod_{i,j}\|\alpha^{j}\,\mathtt{X}^{i}f\|\prod_{i,j}\|\alpha^{j}\,\mathtt{X}^{i}b\|\\ &\leq \prod_{i,j}\mathcal{H}(f)(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{j+1}\left[m(deg(f)+1)\right]^{1/2}\prod_{i,j}\mathcal{H}(b)(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{j+1}\left[m(deg(b)+1)\right]^{1/2}\\ &\leq \left(\mathcal{H}(f)(m(n+1))^{1/2}\right)^{m(deg(b)-deg(g))}\left(\prod_{j=0}^{m-1}(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{j}\right)^{(deg(b)-deg(g))}\\ &\quad\times\left(\mathcal{H}(b)(m(deg(b)+1))^{1/2}\right)^{mn}\left(\prod_{j=0}^{m-1}(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{j}\right)^{n}\end{aligned}$$

And from $\prod_{j=0}^{m-1}(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{j} = (1+\mathcal{H}(\boldsymbol{m}_\alpha))^{\sum_{j=0}^{m-1}j} = (1+\mathcal{H}(\boldsymbol{m}_\alpha))^{m(m-1)/2}$, with $\mathcal{H}(\boldsymbol{m}_\alpha)\in\mathbb{N}^*$ and $deg(b)-deg(g)\leq deg(b)\leq r$ we deduce the inequalities:

$$\begin{aligned}d(\tilde{L}) &\leq \left(\mathcal{H}(f)((n+1)m(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{m-1})^{1/2}\right)^{rm}\left(\mathcal{H}(b)((r+1)m(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{m-1})^{1/2}\right)^{nm}\\ &< \frac{p^{\mathtt{k}lm'}}{D^{m(r+n)}}\end{aligned}$$

by (3.2).

□

For the rational case, inequality (3.3) reads:

$$d(\tilde{L}) \leq \prod_{i}\|\mathtt{X}^{i}f\|\prod_{i}\|\mathtt{X}^{i}b\| \leq \|f\|^{deg(b)}\,\|b\|^{n} \leq \|f\|^{r}\,\|b\|^{n}$$

So it suffices to have $p^{\mathtt{k}l} > \|f\|^{r}\,\|b\|^{n}$ or equivalently:

$$\|b\| < \left(p^{\mathtt{k}l}/\|f\|^{r}\right)^{1/n} \tag{3.4}$$

It becomes clear, then, that Proposition (3.6) above gives an upper bound for the norm of polynomials in L sharing a non-trivial divisor with f.

Theorem 3.7

Let $b_1, \cdots, b_{rm+1}$ be a LLL reduced basis for the lattice L defined in page 46.

Suppose that:

$$p^{\mathtt{k}lm'/m} > \left(2^{n(rm+1)}(n+1)^{n+r}(r+1)^n\binom{2r}{r}^n m^{4n+r}(m-1)^{n(m-1)} (1+\mathcal{H}(\boldsymbol{m}_\alpha))^{(n+r)(m-1)}|discr(\boldsymbol{m}_\alpha)|^{-n}\right)^{1/2} (D\mathcal{H}(f))^{n+r}\|\boldsymbol{m}_\alpha\|^{2n(m-1)} \quad (3.5)$$

Then: $deg(h_0) \leq r$ (i.e $h_0 \in L$), if and only if b_1 satisfies inequality (3.2).

Proof:

If b_1 satisfies inequality (3.2), then by Proposition (3.6), h_0 divides b_1 in $\mathbb{K}[\mathtt{X}]$.

Hence, $deg(h_0) \leq deg(b_1)$. But $deg(b_1) \leq r$ since b_1 is in L. Thus: $deg(h_0) \leq r$.

Now assume $deg(h_0) \leq r$. Then by combining the results of Mignotte and Weinberger and Rothschild, we get an upper bound for the norm of any monic factor of f of degree $\leq r$, (cf [LEN 3]).

Applied to h_0, this bound gives:

$$\|h_0\| \leq \mathcal{H}(f)\left(2(n+1)m^3(m-1)^{m-1}\binom{2r}{r}\right)^{1/2}\|\boldsymbol{m}_\alpha\|^{2(m-1)}\,|discr(\boldsymbol{m}_\alpha)|^{-1/2}$$

On the other hand, the basis $b_1, \cdots, b_{rm+1}$ is LLL reduced, and thus by Property 5 in Lemma (1.20), b_1 satisfies:

$$\|b_1\|^2 \leq 2^{dim(L)-1}\|x\|^2 \quad \text{for all } x \in \Lambda,\ \ x \neq 0.$$

In particular this is true for h_0 since $h_0 \in L$. So: $\|b_1\| \leq 2^{rm/2}\|h_0\|$.

Therefore,

$$\begin{aligned}\mathcal{H}(b_1)^n \leq \|b_1\|^n &\leq 2^{rmn/2}\|h_0\|^n \\ &\leq 2^{\frac{rmn}{2}}\mathcal{H}(f)^n\left(2(n+1)m^3(m-1)^{m-1}\binom{2r}{r}\right)^{n/2}\|\boldsymbol{m}_\alpha\|^{2n(m-1)}|discr(\boldsymbol{m}_\alpha)|^{-n/2}\end{aligned}$$

Hence:

$$\mathcal{H}(b_1)^n \leq 2^{n(rm+1)/2}(n+1)^{n/2}\binom{2r}{r}^{n/2} m^{3n/2}(m-1)^{n(m-1)/2} |discr(\boldsymbol{m}_\alpha)|^{-n/2}\mathcal{H}(f)^n\|\boldsymbol{m}_\alpha\|^{2n(m-1)}$$

Multiplying both sides of this inequality by

$$\left[D^n\left(m(r+1)(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{m-1}\right)^{n/2} \times D^r\mathcal{H}(f)^r\left(m(n+1)(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{m-1}\right)^{r/2}\right],$$

and grouping the terms together we obtain:

$$\begin{aligned} D^n\mathcal{H}(b_1)^n \left(m(r+1)(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{m-1}\right)^{n/2} \times D^r\mathcal{H}(f)^r \left(m(n+1)(1+\mathcal{H}(\boldsymbol{m}_\alpha))^{m-1}\right)^{r/2} \\ \leq 2^{n(rm+1)/2}(n+1)^{(n+r)/2}(r+1)^{n/2}\binom{2r}{r}^{n/2} m^{(4n+r)/2}(m-1)^{n(m-1)/2} \\ (1+\mathcal{H}(\boldsymbol{m}_\alpha))^{(m-1)(n+r)/2}|discr(\boldsymbol{m}_\alpha)|^{-n/2}\left(D\mathcal{H}(f)\right)^{n+r}\|\boldsymbol{m}_\alpha\|^{2n(m-1)} \\ < p^{\mathtt{k}lm'/m} \end{aligned}$$

by inequality (3.5), so we get the desired inequality.

□

Theorem (3.7) provides a simple way to check whether h_0 belongs to L or not. Having this tool in hand, we will show that we actually can achieve $h_0 = \pm b_1$.

Indeed, assume $deg(h_0) \leq r$ and consider the process of reducing the basis of L.
Assume that by applying Algorithm (1.24), at a certain step, we obtain the first t vectors of the LLL reduced basis of L, $b_1, \cdots, b_t$, with $1 \leq t \leq rm+1$. Then, we know that these vectors already satisfy properties (1) and (2) of Definition (1.18).
Thus, they actually form a reduced basis for the lattice of rank t spanned by the first t vectors of the initially given basis of L.
If $deg(h_0) \leq t$, it will be possible to find h_0 in the latter lattice.

Therefore, we fix at once $\mathtt{k}$ such that inequality (3.5) is satisfied for the value of $r = n-1$, which implies that inequality (3.5) also holds for any smaller value of r, and so Theorem (3.7) can be used for any such r. This choice of $\mathtt{k}$ will also determine $H_{\mathtt{k}}$ and $W_{\mathtt{k}}(\mathbb{F}_q)$.

Then, we consider the sequence of lattices L_r defined as in page (46), for the values of $r = l, l+1, \cdots, n-1$ in succession, reducing their bases, then applying Theorem (3.7) and checking whether $h_0 \in L_r$ or not, but we stop as soon as we find h_0 belonging to one of these lattices.
At this moment, since we are considering the values of $r = l, l+1, \cdots, n-1$ in succession, we know that $h_0 \notin L_{r-1}$. Thus, $r-1 < deg(h_0) \leq r$, and so $deg(h_0) = r$.
But, by Proposition (3.6), h_0 divides the first vector b_1 of the LLL reduced basis L_r, as b_1 satisfies inequality (3.2).
Hence, $r = deg(h_0) \leq deg(b_1) \leq r$. So the monic polynomial h_0 divides b_1 in $\mathbb{K}[\mathtt{X}]$ and have same degree as b_1. Therefore, $h_0 = c \cdot b_1$ with $c \in \mathbb{K}$. But $b_1 \in L_r$ and have degree r, so $lc(b_1) \in \mathbb{Z}$, and hence $c \in \mathbb{Z}$. This implies the equality $c \cdot lc(b_1) = lc(h_0) = 1$ in $\mathbb{Z}$, hence $c = \pm 1$, and $h_0 = \pm b_1$.

Now we are ready to give the LLL factorization algorithm.

Algorithm 3.8 "LLL factorization algorithm for Number Fields-1" (cf [LEN 3])

Input. *A monic squarefree polynomial* $f(\mathtt{X}) \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$.

Output. *Complete factorization of* $f(\mathtt{X})$ *in* $\mathbb{K}[\mathtt{X}]$.

Step 1. *Determine* D *such that:*

f *and all its monic factors over* $\mathbb{K}[\mathtt{X}]$ *lie in* $\frac{1}{D}\mathbb{Z}[\alpha][\mathtt{X}]$.

Step 2. *Choose a prime* p *such that:* $p \nmid D \cdot discr(\boldsymbol{m}_\alpha) \cdot discr(f)$.

Step 3. *Factor* $\boldsymbol{m}_\alpha(\mathtt{Y}) \bmod p$ *obtaining:*

$\boldsymbol{m}_\alpha \equiv \boldsymbol{m}_{\alpha,1}\, \boldsymbol{m}_{\alpha,2} \cdots \boldsymbol{m}_{\alpha,s} \pmod p$ *with* $deg(\boldsymbol{m}_{\alpha,i}) = m_i$ *and* $\sum_{i=1}^{s} m_i = m$.

Set $H = \boldsymbol{m}_{\alpha,i_0}$ *where* i_0 *is such that* $discr(f) \bmod (p, \boldsymbol{m}_{\alpha,i_0}) \neq 0$.

Step 4. *Factor* $f(\mathtt{X}) \bmod (p, H)$*, thus obtaining:*

$$(D^{-1} \bmod p) \cdot Df(\mathtt{X}) \equiv \prod_j f_j(\mathtt{X}) \mod (p, H)$$

If $f(\mathtt{X}) \bmod (p, H)$ *is irreducible, then* $f(\mathtt{X})$ *is irreducible. Set* $h_0 = f(\mathtt{X})$ *and stop.*

Step 5. *Pick an irreducible factor of* $f \bmod (p, H)$*, and choose* $h \in \mathbb{Z}[\alpha][\mathtt{X}]$ *so that* $h \bmod (p, H)$ *is the irreducible factor just chosen. We may assume the coefficients of* h *reduced* $\bmod p$.

Step 6. *Determine the least positive integer* $\mathtt{k}$ *satisfying (3.5) with* r *replaced by* $n-1$*, i.e such that:*

$$p^{\mathtt{k}lm'/m} > \left(2^{n((n-1)m+1)}(n+1)^{2n-1}(n)^n \binom{2(n-1)}{n-1}^n m^{5n-1}(m-1)^{n(m-1)} (1+\mathcal{H}(\boldsymbol{m}_\alpha))^{(2n-1)(m-1)} |discr(\boldsymbol{m}_\alpha)|^{-n}\right)^{1/2} (D\mathcal{H}(f))^{2n-1} \|\boldsymbol{m}_\alpha\|^{2n(m-1)}$$

Step 7. *Using the quadratic Hensel's algorithm (1.4), lift the factorization* $\boldsymbol{m}_\alpha \equiv H \times \prod_{i \neq i_0} \boldsymbol{m}_{\alpha,i} \bmod p$ *up to accuracy* $p^{\mathtt{k}}$ *for the value of* $\mathtt{k}$ *just calculated, thus obtaining a polynomial* $H_{\mathtt{k}}(\mathtt{Y}) \in \mathbb{Z}[\mathtt{Y}]$ *such that* $H \equiv H_{\mathtt{k}} \bmod p^{\mathtt{k}}$

Step 8. *Modify* h *without changing* $(h \bmod (p, H))$*, by lifting the factorization of* $(f \bmod (p, H))$ *up to accuracy* $p^{\mathtt{k}}$ *for the value of* $\mathtt{k}$ *calculated in (Step 6).*

We may assume the coefficients of h *reduced* $\bmod p^{\mathtt{k}}$ *so that* $\|h\| \leq (1 + lp^{2\mathtt{k}})$*, where* $l = deg(h)$.

Step 9. *Set* $r \longleftarrow l$.

Step 10. *Find a LLL reduced basis $b_1, \cdots, b_{rm+1}$ for the lattice L defined in (3.2.1).*

If b_1 does not satisfy inequality (3.2), then $deg(h_0) > r$, go to (Step 11), otherwise go to (Step 12).

Step 11. *While $r < n-2$, set $r \longleftarrow r+1$ and go back to (Step 10), otherwise $deg(h_0) > n-1$, so $h_0 = f$ and f is irreducible. Stop.*

Step 12. *Set $h_0 = \pm b_1$. Replace f by f/h_0 and from the list of irreducible factors of $f(\mathtt{X}) \bmod (p, H)$ of (Step 4), delete those that divide $h_0 \bmod (p, H)$. If it remains only one factor stop. Otherwise go back to Step 5.*

Remarks:

- By this algorithm, irreducibility becomes easy to decide as the first h_0 produced is f itself.
- Since $(h \bmod (p, H))$ is monic irreducible, the polynomials $(h \bmod (p^{\mathtt{k}}, H_{\mathtt{k}}))$ will all be monic irreducible and so, up to a very high accuracy $p^{\mathtt{k}}$, we actually construct a good approximation of the minimal polynomial of a p-adic root of f.

A complexity analysis of the above algorithm was given by A. Lenstra (cf Proposition (4.3) and Theorem (4.5) of [LEN 3]). It shows the polynomial-time character of this algorithm.

Theorem 3.9

The algorithm sketched above, computes the irreducible factorization of any monic squarefree polynomial $f(\mathtt{X}) \in \frac{1}{D}\mathbb{Z}[\alpha][\mathtt{X}]$ of degree $n > 0$. The number of arithmetic operations needed by the algorithm is $O\left(n^6m^6 + n^5m^6log(m\|\boldsymbol{m}_\alpha\|) + n^5m^5log(D\mathcal{H}(f))\right)$, the integers on which these operations are performed each have binary length $O\left(n^3m^3 + n^2m^3log(m\|\boldsymbol{m}_\alpha\|) + n^2m^2log(D\mathcal{H}(f))\right)$.

Proof: See [LEN 3].

Although the above algorithm is polynomial-time, it seems it is still slow, and for practical reasons, A. Lenstra recommend his second algorithm (3.10) below instead.

3.2.2 A 2^{nd} LLL factorization algorithm for polynomials over algebraic number fields

We present now another factorization algorithm for polynomials over algebraic number fields suggested also by A. Lenstra who actually recommend it as a more practical algorithm than the previous one even though its complexity may not be polynomial. This second algorithm, published in [LEN 2], relies also on Weinberger and Rothschild's work, so we will continue to use the same notations as in the last section and subsection unless otherwise needed.

Most of the necessary material for this new algorithm has already been introduced, so we will only recall the results and refer to where they appeared.

The first observation we need to make, concerns the application of Proposition (3.6) to an irreducible polynomial F with coefficients over $\mathbb{Z}$ (using then the rational version of Proposition (3.6)).
Defining a lattice L as in page 46 with $r < n$, (on which we will be more explicit later on), we see that Inequality (3.4) should not hold, as the only irreducible factor possible is F itself and any b divisible by F can not be in L as its degree exceeds r.
This means that for all non-zero polynomials $b \in L$:

$$\|b\| \geq \left(p^{\mathtt{k}l}/\|F\|^r\right)^{1/n}$$

Take $F(\mathtt{Y}) = \boldsymbol{m}_\alpha(\mathtt{Y})$ and $r = deg(\boldsymbol{m}_\alpha) - 1 = m - 1$, and define L to be the set of polynomials in $\mathbb{Z}[\mathtt{Y}]$ of degree $\leq m-1$, that when reduced modulo $p^{\mathtt{k}}$, are divisible by the irreducible factor $(H_{\mathtt{k}} \mod p^{\mathtt{k}})$ of $(\boldsymbol{m}_\alpha \mod p^{\mathtt{k}})$. That is, L is the lattice obtained as in page 46 and given by the following basis:

$$\left\{p^{\mathtt{k}}\mathtt{Y}^i \mid 0 \leq i < l\right\} \cup \left\{H_{\mathtt{k}}\mathtt{Y}^i \mid 0 \leq i < m-l\right\} \tag{3.6}$$

We recall that the monic polynomial $H_{\mathtt{k}} \in \mathbb{Z}[\mathtt{Y}]$ is the one defined in page 45, and l is here $l = deg(H_{\mathtt{k}})$.
Thus, for all non-zero polynomials $b \in L$:

$$\|b\| \geq \left(p^{\mathtt{k}l}/\|\boldsymbol{m}_\alpha\|^{m-1}\right)^{1/m}$$

This means that the non-zero polynomials of L have norms bounded from below by a monotone increasing function of $\mathtt{k}$.
When $\mathtt{k}$ is fixed sufficiently high to allow computations with acceptable accuracy, the inequality above always gives a lower bound for the norm of any non-zero element of L. In particular, this lower bound applies also to the elements of a LLL-reduced basis of L, say $b_1, b_2, \cdots, b_m$ ($dim(L) = m$), so we have:

$$\min_i \|b_i\| \geq \left(p^{\mathtt{k}l}/\|\boldsymbol{m}_\alpha\|^{m-1}\right)^{1/m}$$

On the other hand, from lemma (1.22) (cf page 22), we know that the radius of the largest ball inscribed in the fundamental domain, $\Pi(\Lambda)$, of a lattice Λ given by a LLL-reduced basis $b_1, b_2, \cdots, b_m$, satisfies:

$$r_{max} \geq \frac{1}{2}\min_i \|b_i\| \times \frac{1}{O_d}$$

where $O_d = \frac{\prod_{i=1}^{k}\|b_i\|}{d(\Lambda)}$ is the orthogonality defect of the basis $b_1, b_2, \cdots, b_m$.
In particular, for the lattice L defined above, assuming it given by a LLL-reduced basis $b_1, b_2, \cdots, b_m$, we get

$$r_{max} \geq \frac{1}{2 \cdot O_d} \times \left(p^{\mathtt{k}l}/\|\boldsymbol{m}_\alpha\|^{m-1}\right)^{1/m}$$

So

$$r_{max} \geq \frac{1}{2 \cdot \mathsf{C}} \times \left(p^{\mathtt{k}l} / \|\boldsymbol{m}_\alpha\|^{m-1} \right)^{1/m} \qquad \text{for any } \mathsf{C} \geq O_d.$$

As a consequence, any closed ball centered at the origin and having radius $r < \frac{1}{2 \cdot \mathsf{C}} \left(p^{\mathtt{k}l} / \|\boldsymbol{m}_\alpha\|^{m-1} \right)^{1/m}$, would be entirely contained in $\Pi(L)$.

In addition, by definition of the fundamental domain of a lattice Λ, every element of $\mathbb{R}^m$ has modulo Λ a representative in $\Pi(\Lambda)$. And an element that is not congruent to a boundary point, is then congruent to a *unique* interior point of the fundamental domain $\Pi(\Lambda)$.
Moreover, by Lemma (1.17) (cf page 19), for any vector $\boldsymbol{w} \in \mathbb{R}^m$, there is at most one $\tilde{\boldsymbol{w}} \in \Pi(\Lambda)$ such that: $\boldsymbol{w} \equiv \tilde{\boldsymbol{w}} \mod (\Lambda)$, and this element, when it exits is obtained by:

$$\tilde{\boldsymbol{w}} = \boldsymbol{w} - M \lfloor M^{-1} \boldsymbol{w} \rceil \tag{3.7}$$

where M is the matrix of the LLL-reduced basis of Λ.
For $\Lambda = L$, we would like to be able to reach $\tilde{\boldsymbol{w}}$ in the closed ball $B(0, r]$ when $\tilde{\boldsymbol{w}}$ is there. This enables the reconstruction of the algebraic numbers dealt with in the algorithm of Weinberger and Rothschild, avoiding then the CRT.

Indeed, by choosing $r = B$, a bound on the absolute values of the coefficients of any monic factor of f over $\mathbb{K}$, we are ensured that the fundamental domain of a lattice L contains all these coefficients, multiplied by D. A care need to be given to the denominator D as the lattice L is integral so it enables the representation of any element of $\mathbb{Z}[\alpha]$ but not the elements of $\frac{1}{D}\mathbb{Z}[\alpha]$ as they are.

As elements of $\mathbb{Z}[\alpha]$, the coefficients of the monic factors of f, multiplied by D, will be identified with the $m-$dimensional vectors of their coefficients (as polynomials of α). For simplicity, we will not make any distinction between the polynomial representation of the elements of $\mathbb{Z}[\alpha]$ and their corresponding vectors.

The lattice L just constructed, is defined in such a way that these coefficients of monic factors of f over $\mathbb{K}$, are congruent to the coefficients of the factors of $f \mod (p^{\mathtt{k}}, H_{\mathtt{k}})$, or equivalently factors of f over $W_{\mathtt{k}}(\mathbb{F}_q)$, which are easily found by lifting the factorization of $f \mod (p,\, H)$, and then forming the putative divisors of f by multiplying the irreducible factors of $f \mod (p^{\mathtt{k}}, H_{\mathtt{k}})$, as for Weinberger and Rothschild's algorithm.

The coefficients of the factors of f over $\mathbb{K}$, are the vectors of shortest norm in their residue classes $\mod L$ if $\mathtt{k}$ is chosen such that these coefficients are bounded by the radius $r = B$ chosen as above.

Therefore, they can be uniquely determined from their residues $\mod (p^{\mathtt{k}}, H_{\mathtt{k}})$ by means of Equation (3.7).

The same matrix M is valid for all the coefficients, so we only have to compute M and its inverse once.

Algorithm 3.10 "LLL factorization algorithm for Number Fields-2" (cf [LEN 2])

Input. *A monic squarefree polynomial* $f(\mathtt{X}) \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$.

Output. *Complete factorization of* $f(\mathtt{X})$ *in* $\mathbb{K}[\mathtt{X}]$.

Step 1. *Determine* D *such that:*

f *and all its monic factors over* $\mathbb{K}[\mathtt{X}]$ *lie in* $\frac{1}{D}\mathbb{Z}[\alpha][\mathtt{X}]$.

Step 2. *Choose a prime* p *such that:* $p \nmid D \cdot discr(\boldsymbol{m}_\alpha) \cdot discr(f)$.

Step 3. *Factor* $\boldsymbol{m}_\alpha(\mathtt{Y}) \mod p$ *obtaining:*

$\boldsymbol{m}_\alpha \equiv \boldsymbol{m}_{\alpha,1}\, \boldsymbol{m}_{\alpha,2} \cdots \boldsymbol{m}_{\alpha,s} \pmod p$ *with* $deg(\boldsymbol{m}_{\alpha,i}) = m_i$ *and* $\sum_{i=1}^{s} m_i = m$.

Set $H = \boldsymbol{m}_{\alpha,i_0}$ *where* i_0 *is such that* $discr(f) \mod (p, \boldsymbol{m}_{\alpha,i_0}) \neq 0$, *and set* $l = deg(H)$.

Step 4. *Factor* $f(\mathtt{X}) \mod (p, H)$, *thus obtaining:*

$$(D^{-1} \mod p) \cdot Df(\mathtt{X}) \equiv \prod_j f_j(\mathtt{X}) \mod (p, H)$$

If $f(\mathtt{X}) \mod (p, H)$ *is irreducible, then* $f(\mathtt{X})$ *is irreducible. Stop.*

Step 5. *Compute a bound* B/D *on the absolute values of the coefficients of any monic factor of* $f(\mathtt{X})$ *in* $\mathbb{K}[\mathtt{X}]$ *(cf [W-R]).*

Step 6. *Determine the least positive integer* $\mathtt{k}$ *satisfying:*

$$p^{\mathtt{k}l} > (2 \cdot \mathsf{C} \cdot B)^m \cdot \|\boldsymbol{m}_\alpha\|^{m-1}$$

where C *is any bound on the orthogonal defect of a reduced basis of the lattice* L *defined by (3.6).*

Step 7. *Determine the polynomial* $H_{\mathtt{k}}(\mathtt{Y}) \in \mathbb{Z}[\mathtt{Y}]$ *of degree* l *such that* $H \equiv H_{\mathtt{k}} \mod p^{\mathtt{k}}$, *for the value of* $\mathtt{k}$ *just calculated.*

Step 8. *Lift the factorization of* $f(\mathtt{X}) \mod (p, \boldsymbol{m}_{\alpha,i})$ *up to accuracy* $p^{\mathtt{k}}$ *thus obtaining:*

$$(D^{-1} \mod p^{\mathtt{k}}) \cdot Df(\mathtt{X}) \equiv \prod_j f_j^{(\mathtt{k})}(\mathtt{X}) \mod (p^{\mathtt{k}}, H_{\mathtt{k}})$$

Step 9. *Compute the matrix* M *of the LLL-reduced basis of the lattice* L *defined by (3.6).*

Step 10. *Proceed to a combinatorial search by computing all possible combinations:*

$$\tilde{h} = D \cdot \prod_{j_s} f_{j_s}^{(\mathtt{k})} \mod (p^{\mathtt{k}}, H_{\mathtt{k}}) = \sum_{i=0}^{deg(\tilde{h})} \boldsymbol{w}_i \, \mathtt{X}^i \,, \qquad \textit{with } deg(\tilde{h}) \leq \lfloor n/2 \rfloor$$

and checking, by trial division, whether the polynomial

$$h := \frac{1}{D} \cdot \left(\sum_{i=0}^{deg(\tilde{h})} (\boldsymbol{w}_i - M \lfloor M^{-1} \boldsymbol{w}_i \rceil) \, \mathtt{X}^i \right) \in \frac{1}{D} \mathbb{Z}[\alpha][\mathtt{X}]$$

is a factor of f over $\mathbb{K}$.

As one can see, this algorithm uses the lattice technique in a completely different way than the previous LLL-factorization algorithm.

The combinatoric search prevent it from being polynomial-time, but implementations, by A. Lenstra himself, show that show that it is much faster than Weinberger and Rothschild's algorithm. Actually, this should not be surprising as Lenstra's algorithm-2 uses only *one* ring $W_{\mathtt{k}}(\mathbb{F}_q)$ to reconstruct the factors of f over $\mathbb{K}$, while Weinberger and Rothschild's algorithm needs all the rings $W_{\mathtt{k}}(\mathbb{F}_{q_i})$ which makes the combinatoric search even longer, besides the CRA applied to each coefficient, which consumes time even though a polynomial-time, whereas, in the same time Lenstra's algorithm-2 uses the same matrix M for all the coefficients, and that's what makes it very practical.

3.3 Modular factorization : ideal approach

3.3.1 A generic algorithm

So far we have applied the Henselian technique for factorization of polynomials using a prime number $p \in \mathbb{Z}$, and residue class computations modulo this prime and some power of it. This was motivated by the successful efforts to generalise the Berlekamp-Zassenhaus algorithm to the case of number fields. Nevertheless, with more powerful computer algebra systems in hand, it becomes easy to apply Algorithm (1.26) with ideal calculus instead of rational integer calculus.

This ideal approach was already used by Zassenhaus himself in his paper[3] "On Hensel factorization II", which shows that, from a theoretical point of view, the method given in his earlier paper ([ZAS 1]), was already generalized at that time to polynomials over Dedekind domains using prime ideals rather than prime numbers. However, from an algorithmic point of view, this ideal approach had to wait until the mid 90's when it appeared independently in the work by Roblot ([ROB 1] and [ROB 2]) for number fields, and by Pohst (POH 2]) for a general global field.

[3] Symposia mathematica, Vol XV, (1973), pp 499-513

In this section, we want to consider several algorithms that rely on this ideal approach, and to start with, we will give an algorithm that we call a *generic algorithm* borrowing this expression from Pohst as it suits very well our context.

We first recall that $\mathbb{K},\ \mathcal{O}_{\mathbb{K}},\ \alpha,\ \boldsymbol{m}_{\alpha}, f,\ m,\ n$ are as defined earlier in this Chapter. We recall also that $\mathcal{O}_{\mathbb{K}}$ being a Dedekind domain, its prime ideals define discrete valuations on $\mathbb{K}$, and these are exactly all the non-archimedean valuations of $\mathbb{K}$ up to isomorphism. Therefore, for any choice of a prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$, it is possible to embed $\mathbb{K}$ in a non-archimedean complete field, that is, its completion at $\mathfrak{p}$. This field and its ring of integers $\mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}$, provide us with the possibility to apply Algorithm (1.26) taking $\mathfrak{p}$ as a modulus.

So let's fix henceforth, $\mathfrak{p}$ a prime ideal of $\mathcal{O}_{\mathbb{K}}$.
As for our choice of a prime number p, some conditions on $\mathfrak{p}$, imposed by our context, need to be satisfied. We choose the prime ideal $\mathfrak{p}$ such that $(f \mod \mathfrak{p})$ remains squarefree, so $\mathfrak{p}$ should not divide $discr(f)$, that is $discr(f) \notin \mathfrak{p}$. Similarly $\mathfrak{p}$ should not divide $discr(\boldsymbol{m}_{\alpha})$ so that the $\mathfrak{p}-$adic completion $\mathbb{K}_{\mathfrak{p}}$ of $\mathbb{K}$ is unramified. And without loss of generality, we can assume $2 \notin \mathfrak{p}$. We will not care about a denominator here, since we will be working in $\mathcal{O}_{\mathbb{K}}$ as it is. Nevertheless, we still need to impose another condition on $\mathfrak{p}$, that is, we choose $\mathfrak{p}$ of lowest residual degree and if possible of degree one, in such a case $\mathcal{N}(\mathfrak{p})$ would be some prime number p, otherwise it is a small power of p. This restriction on the degree of $\mathfrak{p}$ helps improving the factorization modulo $\mathfrak{p}$ and the Hensel lifting, while a larger residual degree yields a larger ring $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}^{\mathtt{k}}$ and so easier reconstruction of algebraic numbers from $\mathfrak{p}-$adic approximations of the coefficients of the factors.

Since it might be faster to work over a small finite field and then lift to obtain a higher accuracy, Pohst in [POH 2] insists on taking $\mathfrak{p}$ of degree 1. In practice, it seems easy to find such a prime, but there is no certainty that its norm p is small. Assuming GRH, the first prime number p for which there is $\mathfrak{p}$ above it of degree 1, is of order $O(Log^2|discr(\mathbb{K})|)$. If $\mathbb{K}/\mathbb{Q}$ is a Galois extension, it is not difficult to find even totally split primes, by the Chebotarev density theorem, they appear with probability $1/m$, while for a general number field, this probability is only known to be larger than $1/m$!. In all cases, we know it is positive .

After choosing $\mathfrak{p}$, the factorization of f follows the usual scheme, which yields the following algorithm.

Algorithm 3.11 "Generic factorization algorithm " (cf [POH 2])

Input. *A monic squarefree polynomial* $f(\mathtt{X}) \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$.

Output. *Complete factorization of* $f(\mathtt{X})$ *in* $\mathbb{K}[\mathtt{X}]$.

Step G1. *Choose an unramified prime ideal* $\mathfrak{p}$ *of lowest possible degree, not dividing* $2discr(f)discr(\boldsymbol{m}_\alpha)$.

Compute a bound on the coefficients of the factors of f *in* $\mathcal{O}_\mathbb{K}[\mathtt{X}]$ *with respect to a suitable norm, and determine a sufficiently large exponent* $\mathtt{k}$ *for the Hensel lifting.*

Step G2. *Factor* $(f \mod \mathfrak{p})$ *in the finite field* $\mathcal{O}_\mathbb{K}/\mathfrak{p}\ [\mathtt{X}]$.

May try several prime ideals $\mathfrak{p}$ *to get* $(f \mod \mathfrak{p})$ *with fewer factors in* $\mathcal{O}_\mathbb{K}/\mathfrak{p}\ [\mathtt{X}]$.

If $(f \mod \mathfrak{p})$ *is irreducible, then* f *is irreducible in* $\mathbb{K}[\mathtt{X}]$. *Otherwise go to (Step G3)*

Step G3. *Lift the factorization of* $(f \mod \mathfrak{p})$ *to a factorization in* $\mathcal{O}_\mathbb{K}/\mathfrak{p}^{\mathtt{k}}\ [\mathtt{X}]$ *for the value of* $\mathtt{k}$ *calculated in (Step G1).*

Step G4. *Recover a factorization of* f *in* $\mathbb{K}[\mathtt{X}]$.

All the algorithms we want to present in this section, will follow the four steps G1, $\cdots$, G4, however they will differ in their ways of recovering the true factors of f. This, as well, imposes specific choices of the bound and the exponent of Step G2.

Besides being based on the above generic algorithm, an important feature shared by the following algorithms is their use of a LLL-basis reduction at some stage of the recovering process. They are all, as to say, *lattice-based* techniques.

Remark:

Comparing the above generic algorithm with the algorithms presented earlier in this chapter, we notice that the modular factorization of $\boldsymbol{m}_\alpha$ is missing. Actually, from Dedekind's and Kummer's results on the decomposition of ideals in a number field, we know that any prime ideal $\mathfrak{p}$ of $\mathcal{O}_\mathbb{K}$ lies above the rational prime ideal generated by the prime number dividing $\mathcal{N}(\mathfrak{p})$, and if p doesn't divide the index $[\mathcal{O}_\mathbb{K} : \mathbb{Z}[\alpha]\ ]$, which is the case when $\mathfrak{p} \nmid discr(\boldsymbol{m}_\alpha)$, and if the generating polynomial $\boldsymbol{m}_\alpha$ factorizes modulo p as $\prod_i \boldsymbol{m}_{\alpha,i}^{e_i} \pmod p$, then: $p\mathcal{O}_\mathbb{K} = \prod_i \mathfrak{p}_i^{e_i}$ where the $\mathfrak{p}_i$ are exactly those prime ideals lying above p. Furthermore the $\mathfrak{p}_i$ have a two-elements representation:

$$\mathfrak{p}_i = p\mathcal{O}_\mathbb{K} + \boldsymbol{m}_{\alpha,i}(\alpha)\mathcal{O}_\mathbb{K}$$

and their residual degrees f_i satisfy: $f_i := [\mathcal{O}_\mathbb{K}/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}\ ] = deg(\boldsymbol{m}_{\alpha,i})$.

This means that, by choosing $\mathfrak{p}$, we implicitely have chosen an index i_0 and taken $\mathfrak{p} = p\mathcal{O}_\mathbb{K} + H(\alpha)\mathcal{O}_\mathbb{K}$, where $H = \boldsymbol{m}_{\alpha,i_0}$.

The lattice generated by p and H we used earlier, is then a sub-group of the ideal $\mathfrak{p}$.

3.3.2 Bounds on the coefficients of the factors

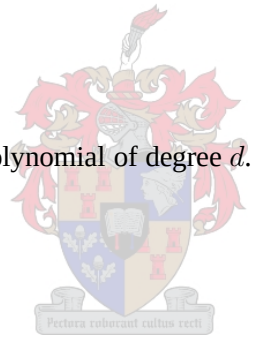
As for any modular algorithm, the concept of *Bounds* is crucial. In our case of polynomial factorization, the necessary bounds are those that enable us to determine the true factors of f, that is the factors in $\mathbb{K}[\mathtt{X}]$. A factor is known when its coefficients are known. So we actually need bounds on the ceofficients of any true factor of f. These coefficients, forming a finite set, are definitely bounded. However, for efficiency of computations, we need an a-priori bound to be available.

This brings to mind the idea of *height of a polynomial*, the height of a polynomial over $\mathbb{K}$ being the maximum of the absolute values of its coefficients considered as complex numbers. So we need an upper bound for the height of any factor of f. The height is then measuring how big is this factor. It is a measure of the size of a polynomial dividing f.

For the sake of completeness, we introduce different functions known to measure the size of a polynomial in $\mathbb{C}[\mathtt{X}]$. From their properties, we will derive some bounds that are useful for our purpose.

Size of a polynomial in $\mathbb{C}[\mathtt{X}]$

Let $h(\mathtt{X}) = \sum_{i=0}^{d} a_i \mathtt{X}^i \in \mathbb{C}[\mathtt{X}]$ be a polynomial of degree d.



Definition 3.12

We define

⋆ *the* height *of the polynomial* $h(\mathtt{X})$ *by:* $\mathcal{H}(h) := \max_{0\le i\le d} |a_i|$,

⋆ *the* length *of the polynomial* $h(\mathtt{X})$ *by:* $\mathcal{L}(h) := \sum_{i=0}^{d} |a_i|$,

⋆ *the* norm *of the polynomial* $h(\mathtt{X})$ *by:* $\|h\| := \left(\sum_{i=0}^{d} |a_i|^2\right)^{1/2}$.

⋆ *And if* $h(\mathtt{X}) = a_d \prod_{j=1}^{d} (\mathtt{X} - \rho_j)$, *where the* ρ_j *are the complex roots of* h, *counted with their multiplicities, then we define the* Mahler measure *of the polynomial* $h(\mathtt{X})$ *by:*

$$\mathcal{M}(h) := |a_d| \prod_{j=1}^{d} \max\{1,\ |\rho_j|\} = |a_d| \prod_{\substack{j=1 \\ |\rho_j|\ge 1}}^{d} |\rho_j| \tag{3.8}$$

Note that we have already used the notions of height and norm in page (46) where the polynomial g was actually considered as a bivariate polynomial in α and $\mathtt{X}$.

We will give a series of inequalities that help estimating the sizes of our polynomials.

Proposition 3.13

Let $h(\mathtt{X}) \in \mathbb{C}[\mathtt{X}]$ be a polynomial of degree d. Then:

$$\mathcal{H}(h) \leq \|h\| \leq \mathcal{L}(h) \leq \sqrt{d+1}\,\|h\| \leq (d+1)\mathcal{H}(h)$$

Proof: See [M-S].

Proposition 3.14

If the polynomial $h(\mathtt{X}) \in \mathbb{C}[\mathtt{X}]$ is not a monomial, then: $\mathcal{M}(h) < \|h\|$.

Proof: See [MIG] or [M-S].

Proposition 3.15

If $h(\mathtt{X}) = \sum_{i=0}^{d} a_i \mathtt{X}^i$ is a non constant polynomial ovec $\mathbb{C}$, then:

$$|a_i| \leq \binom{d}{i}\mathcal{M}(h)$$

and hence $\mathcal{H}(h) \leq \binom{d}{\lfloor d/2 \rfloor}\mathcal{M}(h) \leq 2^{d-1}\mathcal{M}(h)$ *and* $\mathcal{L}(h) \leq 2^d\mathcal{M}(h)$.

Proof:

Write $h(\mathtt{X}) = a_d \prod_{j=1}^{d}(\mathtt{X} - \rho_j)$, where the ρ_j are the complex roots of h.

Using the elementary functions of the roots, the coefficients of h can be obtained as follows:

$$a_{d-i} = (-1)^{d-i} a_d \sum_{j_1 < \cdots < j_i} \rho_{j_1} \cdots \rho_{j_i}$$

Therefore, for any i, $0 \leq i \leq d$, we have

$$\begin{aligned}
|a_{d-i}| &\leq |a_d| \sum_{j_1<\cdots<j_i} |\rho_{j_1} \cdots \rho_{j_i}| = |a_d| \sum_{j_1<\cdots<j_i} |\rho_{j_1}| \cdots |\rho_{j_i}| \\
&\leq |a_d| \sum_{j_1<\cdots<j_i} \prod_{\mathtt{k}=1}^{i} max\{1, |\rho_{j_\mathtt{k}}|\} \leq |a_d| \sum_{j_1<\cdots<j_i} \prod_{j=1}^{d} max\{1, |\rho_j|\} \\
&\leq \left(|a_d| \prod_{j=1}^{d} max\{1, |\rho_j|\}\right) \sum_{j_1<\cdots<j_i} 1 = \mathcal{M}(h) \times \binom{d}{i} = \mathcal{M}(h) \times \binom{d}{d-i}
\end{aligned}$$

Therefore, $\mathcal{H}(h) = \max_i |a_i| \leq \mathcal{M}(h) \times \max_i \binom{d}{i} = \mathcal{M}(h) \times \binom{d}{\lfloor d/2 \rfloor} \leq 2^{d-1}\mathcal{M}(h)$,
(the last statement can be proven by induction on d).

In addition we have, $\mathcal{L}(h) = \sum_i |a_i| \leq \mathcal{M}(h) \sum_i \binom{d}{i} = 2^d\mathcal{M}(h)$. □

Proposition 3.16

For any non constant polynomial $h(\mathtt{X}) \in \mathbb{C}[\mathtt{X}]$, we have: $\mathcal{M}(h) \leq (\sqrt{d+1})\mathcal{H}(h)$.

Proof: See [PRA].

This means that with the Mahler measure we can estimate all the other size functions, and in particular since the Mahler measure is clearly a multiplicative function, that is $\mathcal{M}(hg) = \mathcal{M}(h)\mathcal{M}(g)$ which can be easily shown using Definition (3.12), we can use this property to estimate the size of a factor in terms of the size of the polynomial to be factored.

Bounds on the roots of a polynomial

We shall give different bounds on the roots of a given monic polynomial over $\mathbb{C}$.

Theorem 3.17

Let $h(\mathtt{X}) = \mathtt{X}^d + a_{d-1}\mathtt{X}^{d-1} + \cdots + a_1\mathtt{X} + a_0$ with $a_i \in \mathbb{C}$.

Then inside the disk $|z| \leq 1 + \max_i |a_i|$, there are exactly d roots of h, counting multiplicities.

Proof: The proof relies on Rouché Theorem, see [PRA].

Theorem 3.18 *(Cauchy)*

Let $h(\mathtt{X}) = \mathtt{X}^d - b_{d-1}\mathtt{X}^{d-1} - \cdots - b_1\mathtt{X} - b_0$, where the b_i are nonnegative and at least one of them is nonzero, so that h is not reduced to a monomial. Then, the polynomial h has a unique positive root ρ, and the absolute value of the other roots do not exceed ρ.

Proof: See [PRA].

Theorem 3.19 *(Cauchy)*

Let $h(\mathtt{X}) = \mathtt{X}^d + a_{d-1}\mathtt{X}^{d-1} + \cdots + a_1\mathtt{X} + a_0 \in \mathbb{C}[\mathtt{X}]$.

Then, all the roots of h are inside the disk $|z| \leq \rho$ where ρ is the unique positive root of the polynomial:

$$\mathtt{X}^d - |a_{d-1}|\mathtt{X}^{d-1} - \cdots - |a_1|\mathtt{X} - |a_0|.$$

Proof: See [M-S].

Other bounds on the roots of a polynomial can be found in Stoer & Bulirsch[4], Theorem 5.5.8.

[4]Introduction to Numerical Analysis, 2^{nd} ed. Springer (1993).

Bounds on the factors and their coefficients

The following is a generalisation of Proposition 2.1.13 of [M-S] for monic polynomials over $\mathcal{O}_{\mathbb{K}}$, the ring of algebraic integers of our number field $\mathbb{K}$.

Proposition 3.20

Let $f(\mathtt{X}) \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ be a monic polynomial. Then, for any monic factor $g(\mathtt{X})$ of $f(\mathtt{X})$, we have:

(i) $\mathcal{M}(g) \leq \mathcal{M}(f)$,

(ii) $\mathcal{L}(g) \leq 2^{deg(g)}\mathcal{M}(f) \leq 2^{deg(g)}\|f\|$,

(iii) $\mathcal{H}(g) \leq 2^{deg(g)-1}\mathcal{M}(f) \leq 2^{deg(g)-1}\|f\|$.

Proof:

Since all the roots of g are roots of f, we obviously have $\mathcal{M}(g) \leq \mathcal{M}(f)$. We get the other inequalities by applying Proposition (3.15). □

Note that any bound on the height of g bounds all its coefficients.

Proposition 3.21

Let $g(\mathtt{X}) \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ be a monic divisor of degree d of the polynomial $f(\mathtt{X}) \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$, and let B be a bound on the roots of $f(\mathtt{X})$. Then, the coefficients b_j of $\mathtt{X}^j$ in $g(\mathtt{X})$ satisfies:

$$|b_j| \leq \binom{d}{j} B^{d-j}$$

Proof:

Immediate by expressing the coefficients b_j in terms of the roots of $g(\mathtt{X})$ which are all bounded by B since they are also roots of f. □

Theorem 3.22 *(Mignotte)*

Let $f(\mathtt{X}) \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ be a non constant monic polynomial, and let $g(\mathtt{X}) = \sum_{j=0}^{d} b_j \mathtt{X}^j$ be a monic divisor of $f(\mathtt{X})$. Then,

$$|b_j| \leq \binom{d}{j}\|f\|$$

Proof:

We first prove that $|b_j| \leq \binom{d}{j}\mathcal{M}(g)$ by applying Proposition (3.15). The remaining is due to the fact that $\mathcal{M}(g) \leq \mathcal{M}(f) \leq \|f\|$, since $lc(f) = lc(g) = 1$. □

Theorem 3.23 *(Mignotte)*

Let $f(\mathtt{X}) \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ *be a non constant monic polynomial, and let* $g(\mathtt{X}) = \sum_{j=0}^{d} b_j \mathtt{X}^j$ *be a monic divisor of* $f(\mathtt{X})$*. Then,*

$$|b_j| \leq \binom{d-1}{j} \|f\| + \binom{d-1}{j-1}$$

Proof: See [PRA] and [COH].

The proof of the first bound of Mignotte as given here might look easy, but in fact it relies on deep transcendental results such as Jensen's and Parseval's formulae, which were dissimulated in the non given proofs of earlier propositions.

We did refer to Mignotte's bounds many times in this thesis. They are well known and sharp enough to be widely used. For different situations, such as in Lenstra's or Roblot's cases, Mignotte's bounds were applied to get a refined bound that suits the need. Weinberger and Rothschild, in their original paper, used the bound in Proposition (3.21) to derive a bound on the rational integers that are coefficients of f considered as a bivariate polynomial in α and $\mathtt{X}$. They might not have been aware of the sharper bound by Mignotte. Recently, other bounds are known such as Beauzamy's bound (1992), but they don't seem to give an important improvement on the running time of the factorization algorithm.

3.3.3 Roblot's method of factorization over a number field

In Chapter (2), we have used the embeddings $\sigma_1, \cdots, \sigma_m$ of $\mathbb{K}$ in an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ to define the norm of an algebraic number of $\mathbb{K}$, a definition that can be extended to the polynomial ring $\mathbb{K}[\mathtt{X}]$. Here we will use these m distinct embeddings to define another norm, a norm in the topological sense now, choosing $\mathbb{C}$ as the algebraic closure $\bar{\mathbb{Q}}$.

Let (r_1, r_2) be the *signature* of $\mathbb{K}$, that is, we assume $\mathbb{K}$ having r_1-real embeddings and $2r_2$-non real complex embeddings, so that $m = r_1 + 2r_2$. Following the usual convention, we also assume that: $\sigma_1, \cdots, \sigma_{r_1}$ are the real embeddings of $\mathbb{K}$ in $\mathbb{C}$ and $\sigma_{r_1+1}, \cdots, \sigma_m$ are the complex embeddings satisfying: $\bar{\sigma}_{r_1+j} = \sigma_{r_1+r_2+j}$ for all j such that $1 \leq j \leq r_2$.

The conjugates by the σ_i of an element $a = \sum_{l=0}^{m-1} a_l \alpha^l \in \mathbb{K}$, can then be obtained as:

$\sigma_i(a) = \sum_{l=0}^{m-1} a_l \sigma_i(\alpha)^l$ where the conjugates $\sigma_i(\alpha)$ of α are all the distinct complex roots of $\boldsymbol{m}_\alpha$ and can be calculated, if necessary, to any desired accuracy.

The field $\mathbb{K}$ can then be embedded in $\mathbb{R}^m$ using the map ψ defined as follows:

$$a \longmapsto \left(\sigma_1(a), \cdots, \sigma_{r_1}(a), \Re e(\sigma_{r_1+1}(a)) + \Im m(\sigma_{r_1+1}(a)), \Re e(\sigma_{r_1+1}(a)) - \Im m(\sigma_{r_1+1}(a)), \cdots\right)^{tr}$$

This map induces on $\mathcal{O}_{\mathbb{K}}$ a map similar to the Minkowski map. The image of $\mathcal{O}_{\mathbb{K}}$ is then a lattice in $\mathbb{R}^m$. This is also true for any fractional ideal of $\mathbb{K}$.

Considering $\mathbb{K}$ as a $\mathbb{Q}$-vector space, we can define a scalar product by:

$$\begin{aligned} <,>: \quad \mathbb{K}\times\mathbb{K} &\longrightarrow \mathbb{R} \\ (a,b) &\longmapsto \sum_{i=1}^{m} \sigma_i(a)\overline{\sigma_i(b)} \end{aligned}$$

We can then measure the size of an algebraic number $a \in \mathbb{K}$ in terms of the so called T_2*-norm* defined by:

$$\begin{aligned} T_2 : \quad \mathbb{K} &\longrightarrow \mathbb{R}^+ \\ a &\longmapsto T_2(a) := < a, a > = \sum_{i=1}^{m} |\sigma_i(a)|^2 = \|\psi(a)\|^2 \end{aligned}$$

When the elements of $\mathbb{K}$ are represented using a basis $\omega_1, \cdots, \omega_m$ then, for $a = \sum_{l=1}^{m} a_l\omega_l$,

$$T_2(a) = \boldsymbol{a}^{tr} A\, \boldsymbol{a}$$

where $\boldsymbol{a} = (a_1, \cdots, a_m)^{tr}$ and $A = (< \omega_i, \omega_j >)_{1\le i,j\le m}$ is the Gram matrix of the positive definite quadratic form T_2. In particular when $\omega_1, \cdots, \omega_m$ is an integral basis (cf page 38), A becomes the Gram matrix of the basis of the lattice $\mathcal{O}_{\mathbb{K}}$. Note that, endowed with the quadratic form T_2, the lattice $\mathcal{O}_{\mathbb{K}}$ has determinant equal to $|discr(\mathbb{K})|^{1/2}$.

Weinberger and Rothschild, Abbott, and Lenstra, all used the norm $|a|_\infty := \max_{1\le i\le m} |\sigma_i(a)|$. This norm was enough for their needs but it won't be enough from now onwards because it doesn't come from a quadratic form, and so can not be used for the LLL-basis reduction algorithm on which the algorithms presented here are based.

Let's give now a generalisation of Mignotte's bound of Theorem (3.23).

Theorem 3.24

Let $f(\mathtt{X}) = \sum_{j=0}^{n} a_j \mathtt{X}^j \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ *be a non constant monic polynomial, and let* $g(\mathtt{X}) = \sum_{j=0}^{d} b_j \mathtt{X}^j$ *be a monic divisor of* $f(\mathtt{X})$. *Define* $T_2(f) := \sum_{j=0}^{n} T_2(a_j)$. *Then,*

$$T_2(b_j) \le \binom{d-1}{j} T_2(f) \left[\binom{d-1}{j} + 2\binom{d-1}{j-1}\right] + m\binom{d-1}{j-1}^2$$

Proof:

As field homomorphisms, the embeddings σ_i of $\mathbb{K}$ in $\mathbb{C}$, applied coefficient-wise to the elements of $\mathbb{K}[\mathtt{X}]$, preserve divisibility, in a sense that when g divides f, $\sigma_i(g)$ divides $\sigma_i(f)$, for all i.

Now applying Mignotte's bound of Theorem (3.23) to the coefficients $\sigma_i(b_j)$ of $\sigma_i(g)$, we obtain:

$$|\sigma_i(b_j)| \leq \binom{d-1}{j}\|\sigma_i(f)\| + \binom{d-1}{j-1}$$

where $\|\sigma_i(f)\|^2 = \sum_{k=0}^{n} |\sigma_i(a_k)|^2$. Hence,

$$|\sigma_i(b_j)|^2 \leq \binom{d-1}{j}^2 \|\sigma_i(f)\|^2 + \binom{d-1}{j-1}^2 + 2\binom{d-1}{j}\binom{d-1}{j-1}\|\sigma_i(f)\|$$

Since f is monic, $\|\sigma_i(f)\| \geq 1$, and thus $\|\sigma_i(f)\| \leq \|\sigma_i(f)\|^2$. Hence,

$$|\sigma_i(b_j)|^2 \leq \left[\binom{d-1}{j}^2 + 2\binom{d-1}{j}\binom{d-1}{j-1}\right]\|\sigma_i(f)\|^2 + \binom{d-1}{j-1}^2$$

Summing up, we obtain:

$$T_2(b_j) \leq \left[\binom{d-1}{j}^2 + 2\binom{d-1}{j}\binom{d-1}{j-1}\right]\sum_{i=1}^{m}\|\sigma_i(f)\|^2 + m\binom{d-1}{j-1}^2$$

On the other hand,

$$\sum_{i=1}^{m}\|\sigma_i(f)\|^2 = \sum_{i=1}^{m}\sum_{k=0}^{n}|\sigma_i(a_k)|^2 = \sum_{k=0}^{n}\sum_{i=1}^{m}|\sigma_i(a_k)|^2 = \sum_{k=0}^{n} T_2(a_k) = T_2(f)$$

which finally gives,

$$T_2(b_j) \leq \binom{d-1}{j}\left[\binom{d-1}{j} + 2\binom{d-1}{j-1}\right]T_2(f) + m\binom{d-1}{j-1}^2.$$

□

For the purpose of applying the generic algorithm, let $\mathfrak{p}$ be a prime ideal of $\mathbb{K}$, and consider the lattice $L = \mathfrak{p}^{\mathtt{k}}$. We will show that there is a lower bound for the T_2-norm of any nonzero element of L. This will then be used to reconstruct the algebraic numbers dealt with in the factorization algorithm, and so recover the true factors of f, in the same way as for Lenstra's algorithm-2.

Proposition 3.25

Let γ be a nonzero element of $\mathfrak{p}^{\mathtt{k}}$, where $\mathtt{k} \geq 1$. Then, $T_2(\gamma) \geq m\mathcal{N}(\mathfrak{p})^{2\mathtt{k}/m}$.

Proof:

The inequality between the arithmetic and geometric means gives:

$$\frac{1}{m}\sum_{i=1}^{m}|\sigma_i(\gamma)|^2 \geq \left(\prod_{i=1}^{m}|\sigma_i(\gamma)|^2\right)^{1/m}$$

But $\left(\prod_{i=1}^{m}|\sigma_i(\gamma)|^2\right)^{1/m} = |\prod_{i=1}^{m}\sigma_i(\gamma)|^{2/m} = |N(\gamma)|^{2/m}$, where $N(\gamma) = N_{\mathbb{K}/\mathbb{Q}}(\gamma)$ is the norm defined in Chapter (2). This norm is divisible by the norm of the ideal $\mathfrak{p}^{\mathtt{k}}$ since $\gamma \neq 0$, because it is equal to the norm of the principal ideal $<\gamma>$, which is contained in $\mathfrak{p}^{\mathtt{k}}$. So $|N(\gamma)| \geq \mathcal{N}(\mathfrak{p}^{\mathtt{k}}) = \mathcal{N}(\mathfrak{p})^{\mathtt{k}}$, and hence,

$$\frac{1}{m}T_2(\gamma) \geq |N(\gamma)|^{2/m} \geq \mathcal{N}(\mathfrak{p})^{2\mathtt{k}/m}$$

□

The existence of this lower bound will imply that the minimum of the T_2-norm of the elements of a basis of $\mathfrak{p}^{\mathtt{k}}$, will be larger than this lower bound $m\mathcal{N}(\mathfrak{p})^{2\mathtt{k}/m}$. In paticular, if the basis is LLL-reduced for the T_2-norm, the radius of the largest ball inscribed in the fundamental domain of the lattice $\mathfrak{p}^{\mathtt{k}}$, will satisfy:

$$r_{max} \geq \frac{1}{2\cdot \mathsf{C}} \times\ m\mathcal{N}(\mathfrak{p})^{2\mathtt{k}/m}$$

where $\mathsf{C} \geq O_d$, and the orthogonality defect O_d is calculated for the T_2-norm, (see page 55).

As a consequence, choosing $\mathtt{k}$ such that

$$r = B < \frac{1}{2\cdot \mathsf{C}} \times m\mathcal{N}(\mathfrak{p})^{2\mathtt{k}/m}\,, \tag{3.9}$$

allows the reconstruction of the coefficients of the factors of f over $\mathbb{K}$ from their approximations modulo $\mathfrak{p}^{\mathtt{k}}$, as they correspond to the elements of shortest T_2-norm in their residue classes modulo $\mathfrak{p}^{\mathtt{k}}$, since they belong to the fundamental domain. If B is any real number exceeding the bound given by Theorem (3.24) and satisfy Inequality (3.9), we are done. Indeed, Roblot's algorithm for factorization of polynomials over an algebraic number field, is then an application of the generic algorithm, where $\mathtt{k}$ is chosen such that:

$$\mathtt{k} > \frac{m}{2}\frac{Log(2\mathsf{C}\cdot B/m)}{Log(\mathcal{N}(\mathfrak{p}))}$$

and B is as just mentioned.

The recovery process follows in exactly the same way as for Lenstra's algorithm-2 by applying the formula (3.7) in page 55.

Comparing the timing, Roblot in [ROB 2], shows that his algorithm implemented in PARI is faster than Pohst's algorithm implemented in KANT. There seems to be a remarkable difference in the time consumed by each, but we are not sure whether Pohst's algorithm in [POH 2] is an improved version of that used for this comparison. We have chosen to present only Roblot's algorithm as they are very similar. Pohst's approach will be presented for function fields.

3.3.4 Van Hoeij's factorization method of polynomials over a number field

Van Hoeij's algorithm for factorization of polynomials over the rationals and its generalization by Belabas to polynomials over a number field, are based on the Zassenhaus-Hensel factorization algorithm, but proceed differently for the recombination phase to make it more efficient and hopefully in a polynomial-time. This new method due to van Hoeij, relies on two main ideas:

1. The possibility to linearise the combinatoric problem.
2. The use of lattice techniques to determine the irreducible factors, as it turns out that they also correspond to particularly small vectors in some naturally defined lattice.

Comparing with Lenstra's et al. algorithms, van Hoeij's algorithm has the following advantages that make it superior.

- It gives all the irreducible factors at once.
- It uses lattices with smaller dimensions.
- It uses vectors that are already small since they belong to $\{0,1\}^d$. This makes the computations faster and enables finding smallest vectors for a lower value of $\mathtt{k}$.

In this subsection, we will present van Hoeij's method for a number field $\mathbb{K} \neq \mathbb{Q}$. This will include all the major ideas for the rational case. We will focus on the so called *all-traces* version of this algorithm, one of the series of variants that were given in the original paper [HOE 2], as well as in [BEL 1].

We will apply the generic algorithm following Roblot, so we assume all the previous notations and results. Whatever other necessary changes that are needed will be specified.

By Hensel's lemma (Theorem 1.2), considering f as element of $\mathcal{O}_{\mathbb{K}_\mathfrak{p}}[\mathtt{X}]$, we can lift the factorization of $f \mod \mathfrak{p}$ to a factorization in $\mathcal{O}_{\mathbb{K}_\mathfrak{p}}[\mathtt{X}]$, that is,

$$f = \prod_{j=1}^{r} f_j \qquad f_j \in \mathcal{O}_{\mathbb{K}_\mathfrak{p}}[\mathtt{X}] \quad \text{irreducible,}$$

such that

$$f \mod \mathfrak{p} = \prod_{j=1}^{r} (f_j \mod \mathfrak{p}) \quad \text{in } \mathcal{O}_{\mathbb{K}_\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{\mathbb{K}_\mathfrak{p}}[\mathtt{X}] \simeq \mathcal{O}_{\mathbb{K}}/\mathfrak{p}[\mathtt{X}]$$

The polynomials f_j, called *local factors* of f, having $\mathfrak{p}$-adic coefficients, can not be determined with infinite accuracy, but for any given accuracy $\mathtt{k}$, their reductions $\mod \mathfrak{p}^{\mathtt{k}}$ can be calculated and correspond to the factors of $f \mod \mathfrak{p}^{\mathtt{k}}$ obtained by Hensel lifting those factors of $f \mod \mathfrak{p}$.

Let's denote by $g_1, \cdots, g_s$ the irreducible factors of f over $\mathbb{K}$.

From the Zassenhaus-Hensel factorization technique, we know that: $0 < s \leq r \leq n$, and, the g_i's are combinations of the f_j's, moreover since f is squarefree, we can characterise the monic factors of f as those polynomials $g \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ of the form:

$$g = \prod_{j=1}^{r} f_j^{v_j} \qquad \text{where } v_j \in \{0,1\} \tag{3.10}$$

This defines a correspondence between vectors $\boldsymbol{v} = (v_1, \cdots, v_r)^{tr} \in \{0,1\}^r$ and monic factors of f.

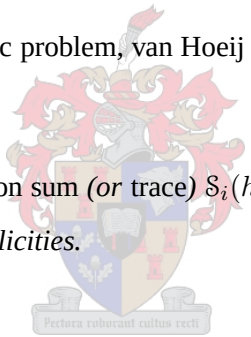
The combinatoric search of the Berlekamp-Zassenhaus algorithm checks all such combinations by trial divisions without knowing -before hand- whether they have integral coefficients or not. Van Hoeij's algorithm proceeds differently: it checks the necessary condition of having integral coefficients instead, by looking for the set of vectors $\boldsymbol{v}$ for which the polynomial g has integral coefficients.

The Knapsack problem

In order to linearise the combinatoric problem, van Hoeij used the *Newton sums* (or *traces*) defined by:

Definition 3.26

Let $h \in \mathbb{K}[\mathtt{X}]$, then the i^{th} Newton sum *(or* trace*) $\mathcal{S}_i(h)$ is the sum of the i^{th} powers of the roots of h counted with their respective multiplicities.*



It follows from the definition that:

$$\mathcal{S}_i(gh) = \mathcal{S}_i(g) + \mathcal{S}_i(h) \qquad \forall g, h \in \mathbb{K}[\mathtt{X}]$$

In particular, when g is in the form (3.10), $\mathcal{S}_i(g) = \sum_{j=1}^{r} v_j \mathcal{S}_i(f_j)$.

This formula will still hold for powers $v_j \in \mathbb{Z}$ if we extend the definition of traces as follows:

$$\mathcal{S}_i(g/h) = \mathcal{S}_i(g) - \mathcal{S}_i(h)$$

Furthermore, by writing a polynomial $h \in \mathbb{K}[\mathtt{X}]$ as $h(\mathtt{X}) = \sum_{i=0}^{d} b_i \mathtt{X}^i = lc(h) \prod_{l=1}^{d} (\mathtt{X} - \rho_l)$ so that $\mathcal{S}_i(h) = \sum_{l=1}^{d} \rho_l^i$, we see that $\mathcal{S}_i(h) \in \mathbb{K}$ as it is a symmetric function of the roots. Moreover, in case h is monic with integral coefficients, then $\mathcal{S}_i(h) \in \mathcal{O}_{\mathbb{K}}$, and we have

$$|\mathcal{S}_i(h)| \leq d B_{root}(h)^i \quad \forall i = 1, \cdots, d$$

where $B_{root}(h)$ is any bound on the roots of the polynomial h (cf page 62).

The i^{th} traces $\mathcal{S}_i(h)$ for $1 \leq i \leq d$, can be calculated from the elementary symmetric functions of the roots using the Newton identities (cf [HOE 2] or [COH]).

In particular, the Newton sums are integral combinations of the coefficients of h since these coefficients are themselves, up to sign, equal to the elementary symmetric functions of the roots and we have:

$$\mathcal{S}_1(h) = -b_{d-1}\,, \quad \mathcal{S}_i(h) = -ib_{d-i} - \sum_{l=1}^{i-1} \mathcal{S}_{i-l}(h)b_{d-l}$$

Let $G = \langle f_1, \cdots, f_r \rangle$ be the multiplicative subgroup of $\mathbb{K}_{\mathfrak{p}}(\mathtt{X})^*$ generated by the local factors of f, and let $G_{\mathbb{K}} = \langle g_1, \cdots, g_s \rangle$ be the subgroup of G generated by the irreducible true factors of f.

Proposition 3.27

Assume that 0 is not a root[5] *of* f.

Let $V_j = (\mathcal{S}_1(f_j), \cdots, \mathcal{S}_n(f_j))^{tr} \in \mathbb{K}_{\mathfrak{p}}^n$. *Then, the vectors* V_j*'s are* $\mathbb{K}_{\mathfrak{p}}-$*linearly independent. Moreover, for any* $g \in G$, *the vector* $V = \sum_{j=1}^{r} v_j V_j$ *satisfies*

$$g \in \mathbb{K}(\mathtt{X}) \Longrightarrow V \in \mathbb{K}^n \Longrightarrow V \in \mathcal{O}_{\mathbb{K}}^n$$

Proof

Denote by $\mathcal{S}_{1\cdots n}$ the operator defined by $\mathcal{S}_{1\cdots n}(h) = (\mathcal{S}_1(h), \cdots, \mathcal{S}_n(h))^{tr}$.

Let $\rho_1, \cdots, \rho_n$ be the roots of f in an algebraic closure of $\mathbb{K}_{\mathfrak{p}}$.

The vectors $\frac{1}{\rho_l}\mathcal{S}_{1\cdots n}(\mathtt{X} - \rho_l) = \frac{1}{\rho_l}(\rho_l, \rho_l^2, \cdots, \rho_l^n)^{tr}$, $1 \leq l \leq n$ form a Vandermonde matrix, and thus they are linearly independent. This means that the vectors $\mathcal{S}_{1\cdots n}(\mathtt{X} - \rho_l)$ themeselves are linearly independent. Since the local factors f_j's are disjoint products of the polynomials $(\mathtt{X} - \rho_l)$, the vectors V_j's are sums of the corresponding vectors $\mathcal{S}_{1\cdots n}(\mathtt{X} - \rho_l)$. Therefore, they are linearly independent over $\mathbb{K}_{\mathfrak{p}}$. Hence they span a lattice $\mathbb{Z}V_1 + \cdots + \mathbb{Z}V_r$ in $\mathbb{K}_{\mathfrak{p}}^n$ of rank r.

The map

$$\begin{array}{rcl} \mathcal{S}_{1\cdots n} : G & \longrightarrow & \mathbb{Z}V_1 + \cdots + \mathbb{Z}V_r \\ g = \prod_{j=1}^{r} f_j^{v_j} & \longmapsto & V = \sum_{j=1}^{r} v_j V_j \end{array}$$

is then one-to-one and we have:

$$V = \mathcal{S}_{1\cdots n}(g) = \begin{pmatrix} \mathcal{S}_1(g) \\ \cdots \\ \mathcal{S}_n(g) \end{pmatrix}$$

So if $g \in \mathbb{K}(\mathtt{X})$, then $\mathcal{S}_i(g) \in \mathbb{K}$, for all i, and hence $V \in \mathbb{K}^n$.

But since f is monic with coefficients in $\mathcal{O}_{\mathbb{K}}$, its roots ρ_l are algebraic integers.

So $\mathcal{S}_{1\cdots n}(\mathtt{X} - \rho_l) \in \mathcal{O}_{\mathbb{K}}^n$ for all l. And so is V_j for all j. □

[5] Otherwise one of the V_j's would be 0.

Corollary 3.28

If g is a monic factor of f over $\mathbb{K}_{\mathfrak{p}}$, then we have the equivalence:

$$g \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}] \Leftrightarrow V \in \mathbb{K}^n \Leftrightarrow V \in \mathcal{O}_{\mathbb{K}}^n$$

Indeed, it remains to prove that $V \in \mathbb{K}^n \Longrightarrow g \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$

From Newton identities, we deduce that $g \in \mathbb{K}[\mathtt{X}]$ whenever $V \in \mathbb{K}^n$.

Now by applying Gauss lemma, we get $g \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$. □

This means that to check whether g is a factor of f over $\mathbb{K}$, it suffices to check that $V \in \mathcal{O}_{\mathbb{K}}^n$,

i.e we check that for all i,

$$\mathcal{S}_i(g) = \sum_{j=1}^{r} v_j \mathcal{S}_i(f_j) \in \mathcal{O}_{\mathbb{K}}$$

Observe that f_j is only known up to a certain large enough precision $\mathtt{k}$.

This will also be the case for any $g \in G$.

But we are looking for irreducible factors of f over $\mathbb{K}$, i.e $g \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ monic irreducible dividing f.

The coefficients of such a polynomial g have a finite p-adic expansion[6] since they are algebraic integers. Hence, when $\mathtt{k} \to \infty$, the expansions of these coefficients remain inchanged and are much smaller than the p-adic precision $p^{\mathtt{k}}$.

Since the Newton sums $\mathcal{S}_i(g)$ are integral linear combinations of the coefficients of g, they should be much smaller than a multiple of $p^{\mathtt{k}}$, or at most close to a multiple of $p^{\mathtt{k}}$. Compared with Newton sums of other factors of f over $\mathbb{K}_{\mathfrak{p}}$, the $\mathcal{S}_i(g)$ are smaller.

Therefore, finding g means finding a $\{0,1\}$-vector $\boldsymbol{v}$ such that

$$\sum_{j=1}^{r} v_j \mathcal{S}_i(f_j) + \lambda p^{\mathtt{k}} + \mu = 0 \tag{3.11}$$

This equation is a kind of a Knaspack problem, since solving it means minimising simultaneously the linear forms $\sum_{j=1}^{r} v_j \mathcal{S}_i(f_j)$ over $\mathbb{Z}$.

Solving the Knapsack problem

In order to solve this Knapsack problem we introduce the lattice[7]:

$$W = \{\boldsymbol{v} \in \mathbb{Z}^r | g = \prod_{j=1}^{r} f_j^{v_j} \in \mathbb{K}(\mathtt{X})\}$$

[6]Note that since p is unramified, it is a prime in $\mathbb{K}_{\mathfrak{p}}$. Hence the elements of $\mathbb{K}_{\mathfrak{p}}$ can be written as Laurent series $\sum_{i=n_0}^{\infty} \lambda_i p^i$, where the λ_i belong to a set of representatives of the residue field.

[7]Observe that, in contrast to the LLL factorization algorithms, the rank of the lattice, W in this case, doesn't depend on the degree of the extension $\mathbb{K}/\mathbb{Q}$. It is equal to the number of modular factors whether we are working over $\mathbb{Q}$ or over $\mathbb{K}/\mathbb{Q}$.

Then W is in a one-to-one correspondence with $G_{\mathbb{K}}$. The irreducible factors of f over $\mathbb{K}$ provide a basis to W that, up to a permutation of the vectors, is in *row-reduced-echelon form*. This is due to the squarefreeness of f and the irreducibility of the g_i. Since well known algorithms that reduce a basis of W to one in row-reduced-echelon form, are available, knowing any basis of W would solve the problem.

Furthermore, as the elements of the basis $g_1, \cdots, g_s$ of $G_{\mathbb{K}}$ should satisfy Equation (3.11) and are irreducible, their Newton sums are not only small compared to Newton sums of any other non-integral combination of the f_j's, but they are the smallest even amongest Newton sums of elements of $G_{\mathbb{K}}$.
This brings us to the idea of reducing the basis of W via the LLL algorithm which will reveal these polynomials as those corresponding to the smallest elements in the lattice W.

As for the LLL factorization algorithms, an iterative process defining lattices approximating the lattice W would help determining this lattice. This relies on the following result due to van Hoeij.

Theorem 3.29

Let L be a lattice such that $W \subset L \subset \mathbb{Z}^r$. Let R be the row-reduced-echelon form of the matrix of a basis of L. Then $L = W$ if and only if the following two conditions hold.

(A) Each column of R contains precisely one 1, all other entries are 0.

(B) If $(v_1, \cdots, v_r)$ is a row of R, then $g = \prod_{j=1}^{r} f_j^{v_j} \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$.

Proof: See [HOE 2].

The iterative process is initialised by taking $L_0 = \mathbb{Z}^r$, and constructing a decreasing sequence of lattices $W \subset \cdots L_2 \subset L_1 \subset \mathbb{Z}^r$ where at each step, the conditions (A) and (B) are checked. W is found when both these two conditions hold. At this very moment, a complete factorization of f is obtained since the irreducible factors are the columns of R, the basis of W in row-reduced-echelon form.

It remains to show that effectively it is possible to construct this decreasing sequence of lattices.
More precisely, given the lattice L as in Theorem (3.29), we need to construct a lattice L', hopefully of smaller rank, such that

$$W \subset L' \subset L$$

For that recall that, in Step 2 of the generic algorithm, we have already chosen the precision $\mathtt{k}$ necessary for the Hensel lifting and which enables the reconstruction of the algebraic numbers from their $\mathfrak{p}$-adic approximations.
The algebraic numbers can be written in terms of the integral basis $\omega_1, \cdots, \omega_m$.
A basis of the ideal $\mathfrak{p}^{\mathtt{k}}$ is then obtained by: $(\omega_i)M$, where M is an $m \times m$ integral matrix.

Recall also that for $x = \sum_i x_i \omega_i \in \mathcal{O}_{\mathbb{K}}$, the element $x \bmod \mathfrak{p}^{\mathtt{k}}$ is obtained by the formula in Lemma (1.17) when the basis (ω_i) is LLL reduced for the T_2-norm.

We can now define the so-called *Knapsack lattice* Λ given by

$$M^* = \begin{pmatrix} CI_r & 0 \\ \mathbb{S} & Q \end{pmatrix}$$

where $C \geq 1$ is a suitably chosen integer constant to be made precise, I_r is the identity matrix of order r, Q is a $nm \times nm$ block diagonal matrix, with diagonal blocks equal to M, and

$$\mathbb{S} = \begin{pmatrix} \mathbb{S}_{i_1}(f_1) & \dots & \mathbb{S}_{i_1}(f_r) \\ \vdots & \vdots & \vdots \\ \mathbb{S}_{i_n}(f_1) & \dots & \mathbb{S}_{i_n}(f_r) \end{pmatrix}$$

This means that the lattice Λ is the image of the multiplication by the matrix above.
The quadratic form defined on Λ has Gram matrix $M^{*\,tr} M^*$.
Observe that $\Lambda \subset \mathbb{Z}^{nm+r}$ and the lattice L can be obtained from Λ by projeting some how on $\mathbb{Z}^r$.

In order to bound the Newton sums, we need the following two lemmata.

Lemma 3.30 *(cf [BEL 1])*

Let $g = \sum_{l=0}^{d} b_l \mathtt{X}^l$ be a monic factor of f. Then for all i,

$$T_2(\mathbb{S}_i(g)) \leq n^2 \sum_{\sigma} B_{root}(\sigma(f))^{2i}$$

where $B_{root}(\sigma(f))$ is any bound on the roots of the polynomial $\sigma(f)$ (cf page 62).

In his generalisation of van Hoeij's method, Belabas has chosen to work with the norm $|x|' := (\sum_i x_i^2)^{1/2}$. This norm is related to the natural norm over $\mathbb{K}$, T_2, by

Lemma 3.31 *(cf [BEL 1])*

Let $\mathtt{T}$ be the transition matrix from the basis $\{1, \alpha, \cdots, \alpha^{m-1}\}$ to the basis $\omega_1, \cdots, \omega_m$, and let V be the Vandermonde matrix associated with the complex conjugates of α. Then

$$|x|'^2 \leq C_{T_2} T_2(x) \qquad \text{where } C_{T_2} = \|\mathtt{T}^{-1} V^{-1}\|^2$$

and where the norm $\|(a_{ij})\| := \left(\sum_i |a_{ij}|^2 \right)^{1/2}$

Proof: See [BEL 1].

The problem now is to find a vector $\binom{\boldsymbol{v}}{\epsilon}$, where $\boldsymbol{v} \in \{0,1\}^r$ and $\epsilon \in \mathbb{Z}^{nm}$, whose image $\begin{pmatrix} C\boldsymbol{v} \\ \mathcal{S}\boldsymbol{v} + Q\epsilon \end{pmatrix}$ in Λ has bounded norm $\|.\|$.
In such a case, we have:

$$\| \begin{pmatrix} C\boldsymbol{v} \\ \mathcal{S}\boldsymbol{v} + Q\epsilon \end{pmatrix} \|^2 = C^2\|\boldsymbol{v}\|^2 + \|\mathcal{S}\boldsymbol{v} + Q\epsilon\|^2 \leq C^2 r + \|\mathcal{S}\boldsymbol{v} + Q\epsilon\|^2$$

We can bound the Newton sums using the two lemmas above, obtaining

$$\|\mathcal{S}\boldsymbol{v} + Q\epsilon\|^2 \leq C_{T_2} n^2 \sum_{l=1}^{n} \sum_{i=1}^{m} B_{root}(\sigma_i(f))^{2l} =: B_{trace}^2$$

(cf [BEL 1]).

The constant C is then chosen so that neither of the two numbers $C^2 r$ and B_{trace}^2 is much larger than the other, that is so that

$$C^2 r \approx B_{trace}^2$$

We now have sufficient tools to define the lattice L'.

We LLL reduce the basis of Λ, and using Property 6 of Lemma (1.20), we discard those LLL-basis vectors that exceed a bound given by

$$(C^2 r + B_{trace}^2)^{1/2}.$$

This defines a lattice $\Lambda' \subset \Lambda$ as the span of the first t vectors non satisfying the bound.

Then set $L' \subset L$ to be the projection of $\frac{1}{C}\Lambda$ on the first t coordinates of $\mathbb{Z}^{nm+r}$.

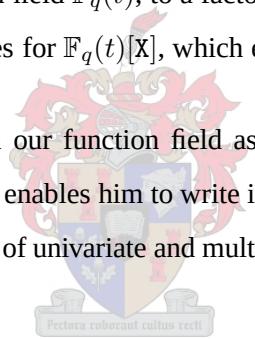
CHAPTER FOUR

DIRECT FACTORIZATION METHODS IN FUNCTION FIELDS

4.1 Introduction

In Chapter 2, we have seen how to reduce the problem of factoring a polynomial having coefficients in an extension of the rational function field $\mathbb{F}_q(t)$, to a factorization over the ground field $\mathbb{F}_q(t)$, assuming that we have some simple techniques for $\mathbb{F}_q(t)[\mathtt{X}]$, which enable us to complete the factorization .

In that chapter we only considered our function field as an algebraic extension field. This approach was used by Abbott (in [ABB]) and enables him to write interesting programs in BANP (Bath Algebraic Numbers Package) for factorization of univariate and multivariate polynomials over function fields based on Trager's method.



The drawback of this method however being the complication of computations due to the much higher degree of the new polynomial to be factored.

We turn now to the direct methods of factorization over function fields and try to apply our generic algorithm (3.11) of Chapter 3. And to do so, we will need to look more deeply to the algebraic structure of our function field and exploit its properties.

Many of the results we will introduce in this chapter are also true for a function field over a field of characteristic zero, but since we only deal with function fields that are *global fields*, we will stick to the definition of function field we gave in the Introduction, and hence consider only the positive characteristic case with finite constant field.

Let $\mathbb{K}$ be a finite separable extension of degree m of the rational function field $K = \mathbb{F}_q(t)$, where t is transcendental over the finite field $\mathbb{F}_q$. We write $\mathbb{K} = K(\alpha)$, where α is a root of its minimal polynomial

$\boldsymbol{m}_\alpha(\mathtt{Y})$, and denote by R the ring $\mathbb{F}_q[t]$ and by $\mathcal{O}_\mathbb{K}$ its integral closure in $\mathbb{K}$.

4.2 Places in a function field

Definition 4.1

A valuation ring *of the function field $\mathbb{K}$ is a ring $\mathcal{O} \subset \mathbb{K}$ such that*

$$\mathcal{O} \subsetneq \mathbb{K} \text{ and } \forall a \in \mathbb{K},\ a \in \mathcal{O} \text{ or } a^{-1} \in \mathcal{O}$$

Proposition 4.2

Let $\mathcal{O}$ be a valuation ring of the function field $\mathbb{K}$. Then

(a) *$\mathcal{O}$ is a local ring with maximal ideal $\mathfrak{p} = \mathcal{O} \setminus \mathcal{O}^*$,*
where $\mathcal{O}^*$ is the group of units of $\mathcal{O}$.

(b) *$\mathfrak{p}$ is a principal ideal, and hence $\mathcal{O}$ is a PID.*

Observe that the finite field $\mathbb{F}_q$ is contained in $\mathcal{O}$.
In the following, we will assume that $\mathbb{F}_q$ is the full constant field.

Definition 4.3

A place $\mathfrak{p}$ *of a function field $\mathbb{K}$ is the maximal ideal of some valuation ring $\mathcal{O}$ of $\mathbb{K}$. Any element $\pi \in \mathfrak{p}$ such that $\mathfrak{p} = \pi\mathcal{O}$ is called* a prime *of $\mathfrak{p}$ (or of $\mathbb{K}$).*

Remark:

$\mathcal{O}$ is uniquely determined by $\mathfrak{p}$. Indeed, it suffices to take $\mathcal{O} := \{a \in \mathbb{K} |\, a^{-1} \notin \mathfrak{p}\}$. Hence we can write $\mathcal{O} = \mathcal{O}_\mathfrak{p}$ for the valuation ring corresponding to the place $\mathfrak{p}$.

Examples:

Assume $m = 1$, i.e $\mathbb{K} = K = \mathbb{F}_q(t)$.

1. Consider a monic irreducible polynomial $p(t) \in \mathbb{F}_q[t]$.
   Set: $\mathfrak{p} = \langle p(t) \rangle$

$$\mathcal{O}_\mathfrak{p} := \left\{ \frac{a(t)}{b(t)} \in \mathbb{F}_q(t) |\ p(t) \text{ does not divide } b(t) \right\}$$

   Then $\mathfrak{p}$ is a place of $\mathbb{F}_q(t)$ and $\mathcal{O}_\mathfrak{p}$ is its valuation ring.

2. Set $\mathcal{O} := \left\{ \dfrac{a(t)}{b(t)} \in \mathbb{F}_q(t) |\ deg(a(t)) \leq deg(b(t)) \right\}$
   Then $\mathcal{O}$ is a valuation ring of $\mathbb{F}_q(t)$, whose corresponding place is called the *infinite place* and denoted by $\mathfrak{p}_\infty$.

In the following, we will call a *rational place* any place of the rational function field $\mathbb{F}_q(t)$. A place $\mathfrak{p} \neq \mathfrak{p}_\infty$ will be called a *finite place*.

These are all the places of the rational function field.

Remark:

The infinite place is the only rational place that does not come straight from a prime $p(t)$ in $\mathbb{F}_q[t]$. It is actually obtained from the prime $\pi' = t^{-1}$ of the ring $\mathbb{F}_q[t^{-1}] \subset \mathbb{F}_q(t)$, in the same way as in example (1) above.

The notion of places in a function field is also closely related to the notion of *discrete valuations* of the function field.

Indeed, let $\mathfrak{p}$ be a place of the function field $\mathbb{K}$, and let $\pi \in \mathfrak{p}$ be a prime of $\mathfrak{p}$.

Since $\mathcal{O}_\mathfrak{p}$ is local with maximal ideal $\mathfrak{p} = \pi\mathcal{O}_\mathfrak{p}$, any nonzero element $a(t) \in \mathbb{K}$ is uniquely represented in the form:

$$a(t) = \pi^r \cdot u(t) \quad \text{where} \quad r \in \mathbb{Z}, \text{ and } u(t) \in \mathcal{O}_\mathfrak{p}^* \text{ is a unit.}$$

Setting:

$$\begin{cases} \nu_\mathfrak{p}(a(t)) := r \ \text{ for } a(t) \neq 0 \\ \\ \nu_\mathfrak{p}(0) := \infty \end{cases}$$

we get a map $\nu_\mathfrak{p} : \mathbb{K} \longrightarrow \mathbb{Z} \cup \{\infty\}$ that satisfies the following properties.

Theorem 4.4

(i) *For any place $\mathfrak{p}$ of the function field $\mathbb{K}$, the function $\nu_\mathfrak{p}$ is a discrete valuation of $\mathbb{K}$. Moreover*

$$\mathcal{O}_\mathfrak{p} = \{a(t) \in \mathbb{K} |\ \nu_\mathfrak{p}(a(t)) \geq 0\}$$
$$\mathcal{O}_\mathfrak{p}^* = \{a(t) \in \mathbb{K} |\ \nu_\mathfrak{p}(a(t)) = 0\}$$
$$\mathfrak{p} = \{a(t) \in \mathbb{K} |\ \nu_\mathfrak{p}(a(t)) > 0\}$$

An element $z \in \mathbb{K}$ is a prime element of $\mathfrak{p}$ if and only if $\nu_\mathfrak{p}(z) = 1$.

(ii) *Conversely, suppose that ν is a discrete valuation of $\mathbb{K}$. Then the set*

$\mathfrak{p} = \{a(t) \in \mathbb{K} \mid \nu(a(t)) > 0\}$ *is a place of* $\mathbb{K}$*, and*

$\mathcal{O} = \{a(t) \in \mathbb{K} \mid \nu(a(t)) \geq 0\}$ *is the corresponding valuation ring.*

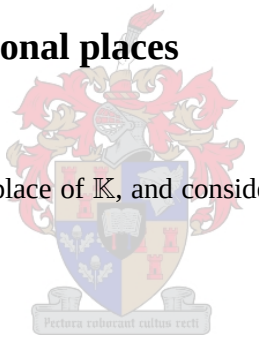
For the sake of completeness, we recall the following properties of a discrete valuation $\nu_{\mathfrak{p}}$ of $\mathbb{K}$.

1. $\nu_{\mathfrak{p}}(a) = \infty \Leftrightarrow a = 0$
2. $\nu_{\mathfrak{p}}(ab) = \nu_{\mathfrak{p}}(a) + \nu_{\mathfrak{p}}(b), \quad \forall a, b \in \mathbb{K}$
3. $\nu_{\mathfrak{p}}(a+b) \geq \min(\nu_{\mathfrak{p}}(a), \nu_{\mathfrak{p}}(b)), \quad \forall a, b \in \mathbb{K}$
   with equality whenever $\nu_{\mathfrak{p}}(a) \neq \nu_{\mathfrak{p}}(b)$
4. $\exists a \in \mathbb{K}$ with $\nu_{\mathfrak{p}}(a) = 1$
5. $\nu_{\mathfrak{p}}(a) = 0, \quad \forall a \in \mathbb{F}_q^*$

4.3 Extension of the rational places

Assume $[\mathbb{K} : K] = m > 1$

Let $\mathfrak{p}$ be a place of K, and $\mathfrak{P}$ be a place of $\mathbb{K}$, and consider the corresponding valuation rings $\mathcal{O}_{\mathfrak{p}} \subset K$ and $\mathcal{O}_{\mathfrak{P}} \subset \mathbb{K}$ respectively.



Definition 4.5

We say that $\mathcal{O}_{\mathfrak{P}}$ lies above $\mathcal{O}_{\mathfrak{p}}$ or that $\mathfrak{P}$ lies above $\mathfrak{p}$ or that $\mathfrak{P}$ divides $\mathfrak{p}$, and we write $\mathfrak{P}|\mathfrak{p}$, if:

$$\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{P}} \cap K \quad \textit{and} \quad \mathfrak{p} = \mathfrak{P} \cap K$$

In this case, the extension $\mathfrak{p}\mathcal{O}_{\mathfrak{P}}$ is a non-zero ideal of $\mathcal{O}_{\mathfrak{P}}$ contained in $\mathfrak{P}$. Thus $\mathfrak{p}\mathcal{O}_{\mathfrak{P}} = \mathfrak{P}^e$ for some integer $e = e(\mathfrak{P}|\mathfrak{p}) \geq 1$ called the *ramification index* of $\mathfrak{P}$ over $\mathfrak{p}$. And one can easily see that $\forall a \in K, \ \nu_{\mathfrak{P}}(a) = e\nu_{\mathfrak{p}}(a)$.

On the other hand, when $\mathfrak{P}|\mathfrak{p}$, there is a canonical embedding of the residue class field $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$ into $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$, and thus $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ can be considered as a field extension of $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$.

The index $[\mathcal{O}_{\mathfrak{P}}/\mathfrak{P} \ : \ \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}]$ is called the *residue class degree* of $\mathfrak{P}$ over $\mathfrak{p}$ and denoted by $f = f(\mathfrak{P}|\mathfrak{p})$.

The ramification index e is a positive integer. Moreover, we have the following result.

Proposition 4.6

Let $\mathfrak{P}$ be a place of $\mathbb{K}$ lying above the rational place $\mathfrak{p}$, we denote by $e_{\mathfrak{P}|\mathfrak{p}}$, $f_{\mathfrak{P}|\mathfrak{p}}$ the ramification index *of $\mathfrak{P}$ over $\mathfrak{p}$ and its residue class degree respectively.*
Define the local degree of $\mathfrak{P}$ over $\mathfrak{p}$ to be

$$n_{\mathfrak{P}|\mathfrak{p}} = e_{\mathfrak{P}|\mathfrak{p}} \cdot f_{\mathfrak{P}|\mathfrak{p}}.$$

Then $n_{\mathfrak{P}|\mathfrak{p}} \leq m = [\mathbb{K} : K]$

If we assume $\mathbb{K}/K$ separable, then we can construct all the $\mathfrak{P}$'s lying above a rational place $\mathfrak{p}$ by decomposing the ideal $\mathfrak{p}$ in the integral closure of $\mathcal{O}_{\mathfrak{p}}$ in $\mathbb{K}$, which is a Dedekind domain since $\mathcal{O}_{\mathfrak{p}}$ is a PID.

This shows that above any place $\mathfrak{p}$ of K, there is at least one (the maximal ideal containing the extension of $\mathfrak{p}$ in the integral closure of $\mathcal{O}_{\mathfrak{p}}$ in $\mathbb{K}$), but at most finitely many places of $\mathbb{K}$.
In particular we will be interested in the places above $\mathfrak{p}_\infty$.

Note that, the definition above implies also that for any place $\mathfrak{P}$ of $\mathbb{K}$, there is a unique place of K lying below it, namely $\mathfrak{p} = \mathfrak{P} \cap K$.

Proposition 4.7

Assume $\mathbb{K}/K$ separable, and consider the places $\mathfrak{P}_1, \cdots, \mathfrak{P}_r$ of $\mathbb{K}$ lying above a rational place $\mathfrak{p}$ with their respective ramification indexes $e_1, \cdots, e_r$, and their respective residue class degrees $f_1, \cdots, f_r$. Then we have the so called fundamental equality*:*

$$\sum_{i=1}^{r} e_i f_i = m = [\mathbb{K} : K]$$

4.4 Norms and absolute values

By $\mathcal{N}(\mathfrak{P})$, we denote the *norm* of the place $\mathfrak{P}$ of $\mathbb{K}$, that is the cardinality of the residue class field of $\mathfrak{P}$, which we know is finite as in the number field case, i.e

$$\mathcal{N}(\mathfrak{P}) = \#\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$$

where $\mathcal{O}_{\mathfrak{P}}$ is the *valuation ring* of $\mathfrak{P}$.

In particular for a finite rational place $\mathfrak{p} = \langle p(t) \rangle$, $\mathcal{N}(\mathfrak{p}) = \#\mathcal{O}_{\mathfrak{p}}/\mathfrak{p} = q^{deg(p(t))}$, and we can easily show that $\mathcal{N}(\mathfrak{p}_\infty) = q$.

Let $\mathfrak{P}$ be a place above a rational place $\mathfrak{p}$, then $\mathcal{N}(\mathfrak{P}) = \#\mathcal{O}_{\mathfrak{P}}/\mathfrak{P} = q^{[\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}:\,\mathbb{F}_q]}$.

But $[\mathcal{O}_{\mathfrak{P}}/\mathfrak{P} : \mathbb{F}_q] = [\mathcal{O}_{\mathfrak{P}}/\mathfrak{P} : \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}][\mathcal{O}_{\mathfrak{p}}/\mathfrak{p} : \mathbb{F}_q] = f_{\mathfrak{P}|\mathfrak{p}} \cdot deg(p(t))$.

Hence

$$\mathcal{N}(\mathfrak{P}) = q^{f_{\mathfrak{P}|\mathfrak{p}}\, deg(p(t))} = \mathcal{N}(\mathfrak{p})^{f_{\mathfrak{P}|\mathfrak{p}}}.$$

The $\mathfrak{p}$-adic absolute value on $\mathbb{F}_q(t)$ is defined by the real-valued functions:

$$|a|_{\mathfrak{p}} := \mathcal{N}(\mathfrak{p})^{-\nu_{\mathfrak{p}}(a)} \quad \text{for all non-zero } a \in \mathbb{F}_q(t).$$
$$|a|_{\mathfrak{p}_\infty} := q^{deg(u)-deg(v)} \quad \text{if} \quad a = \frac{u}{v} \in \mathbb{F}_q(t) \setminus \{0\} \quad \text{and} \quad deg(u) < deg(v)$$

In both cases, the absolute value of zero being zero by definition.

For every place $\mathfrak{P}|\mathfrak{p}$, we define a normalized $\mathfrak{P}$-adic absolute value corresponding to the valuation $\nu_{\mathfrak{P}}$ by setting:

$$|a|_{\mathfrak{P}} := \mathcal{N}(\mathfrak{P})^{-\nu_{\mathfrak{P}}(a)/n_{\mathfrak{P}|\mathfrak{p}}}$$

for $a \in \mathbb{K}$, $a \neq 0$, and $|0|_{\mathfrak{P}} := 0$.

This definition is motivated by the following observation.

For $0 \neq a \in K$, $|a|_{\mathfrak{p}} := \mathcal{N}(\mathfrak{p})^{-\nu_{\mathfrak{p}}(a)}$.

But $\mathcal{N}(\mathfrak{p}) = \mathcal{N}(\mathfrak{P})^{\frac{1}{f_{\mathfrak{P}|\mathfrak{p}}}}$ and $\nu_{\mathfrak{P}}(a) = e_{\mathfrak{P}|\mathfrak{p}}\nu_{\mathfrak{p}}(a)$.

Thus:

$$\begin{aligned} |a|_{\mathfrak{p}} &:= \mathcal{N}(\mathfrak{P})^{\left(-\nu_{\mathfrak{p}}(a)/f_{\mathfrak{P}|\mathfrak{p}}\right)} = \mathcal{N}(\mathfrak{P})^{\left(-\nu_{\mathfrak{P}}(a)/e_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}}\right)} \\ &= \mathcal{N}(\mathfrak{P})^{-\nu_{\mathfrak{P}}(a)/n_{\mathfrak{P}|\mathfrak{p}}} \end{aligned}$$

The normalization defined above has the effect that $|\,|_{\mathfrak{P}}$ is a prolongation of $|\,|_{\mathfrak{p}}$.

This absolute value has a unique prolongation to the completion $\mathbb{K}_{\mathfrak{P}}$ which we will also denote by $|\,|_{\mathfrak{P}}$.

Moreover, with this definition, the product formula holds.

Theorem 4.8 *Product Formula*

For each nonzero element a of the function field $\mathbb{K}$,

$$\prod_{\mathfrak{P}} |a|_{\mathfrak{P}} = 1,$$

where $\mathfrak{P}$ runs through all places of $\mathbb{K}$.

Note that Artin and Whaples (in Bull. Amer. Math. Soc. 51 (1946), pp 469-492) have proved that all global fields satisfy the Product Formula.

Definition 4.9

For an element $a \in \mathbb{K}$, we define the maximum norm by:

$$\|a\|_\infty := \max_{\mathfrak{P}|\mathfrak{p}_\infty} |a|_\mathfrak{P}$$

Then the maximum norm has the following properties of a non-archimedean norm:
For all $a, b \in \mathbb{K}$ and $\lambda \in \mathbb{F}_q(t)$,

$\|a\|_\infty = 0 \Leftrightarrow a = 0$

$\|\lambda a\|_\infty = |\lambda|_{\mathfrak{p}_\infty} \|a\|_\infty$

$\|a + b\|_\infty \leq max\{\|a\|_\infty, \|b\|_\infty\}$
with equality whenever $\|a\|_\infty \neq \|b\|_\infty$

This maximum norm will be a kind of substitute for the T_2-norm of the number fields, and will be used to obtain suitable bounds for the coefficients of a potential factor of the polynomial to be factored.

4.5 Bounds on the coefficients of a factor

For the following results, we refer to Pohst and Omaña in [POH 2] and [Om-P].

Lemma 4.10

Let $f(\mathtt{X}) = \sum_{i=0}^{n} a_i \mathtt{X}^i \in \mathcal{O}_\mathbb{K}[\mathtt{X}]$ be a monic polynomial of degree $n > 1$.
For any place $\mathfrak{P}$ of $\mathbb{K}$ lying above $\mathfrak{p}_\infty$, we define a measure *of the polynomial $f(\mathtt{X})$ by*

$$M_\mathfrak{P}(f) := \max\{\sqrt[i]{|a_{n-i}|_\mathfrak{P}}\ ;\ 1 \leq i \leq n\}$$

Then any monic polynomial $g(\mathtt{X}) = \sum_{i=0}^{r} b_i \mathtt{X}^i \in \mathbb{K}[\mathtt{X}]$ dividing $f(\mathtt{X})$ is in $\mathcal{O}_\mathbb{K}[\mathtt{X}]$, and its coefficients b_i satisfy

$$|b_{r-i}|_\mathfrak{P} \leq M^i_\mathfrak{P}(f) \ \ (1 \leq i \leq r)$$

Proof:

Since $\mathcal{O}_\mathbb{K}$ is a Dedekind domain with quotient field $\mathbb{K}$, by Gauss' lemma, any monic factor of the monic polynomial $f \in \mathcal{O}_\mathbb{K}[\mathtt{X}]$, has coefficients in $\mathcal{O}_\mathbb{K}$.

To obtain the estimate for the coefficient b_i of $g(\mathtt{X})$, we express them as elementary symmetric functions of the zeros of $g(\mathtt{X})$.

Let $\mathbb{L}$ be the splitting field of $f(\mathtt{X})$ over $\mathbb{K}$.

Let $\xi_1, \cdots, \xi_n$ be the zeros of $f(\mathtt{X})$ in $\mathbb{L}$.

Set $\tilde{M}_{\mathfrak{P}} := \max\{|\xi_i|_{\mathfrak{P}};\ 1 \leq i \leq n\}$ and $s := \#\{i \mid |\xi_i|_{\mathfrak{P}} = \tilde{M}_{\mathfrak{P}}\}$

The coefficients of $g(\mathtt{X})$ satisfy

$$\begin{aligned} |b_{r-i}|_{\mathfrak{P}} &= |\sum_{1\leq j_1<\cdots<j_i\leq r} \xi_{j_1}\cdots\xi_{j_i}\ |_{\mathfrak{P}} \leq \sum_{1\leq j_1<\cdots<j_i\leq r}\prod_{k=1}^{i}|\xi_{j_k}|_{\mathfrak{P}} \\ &\leq max\left(\prod_{k=1}^{i}|\xi_{j_k}|_{\mathfrak{P}}\right) \qquad \text{(ultra-metric property)} \\ &\leq \tilde{M}_{\mathfrak{P}}^{i} \end{aligned} \tag{4.1}$$

On the other hand, let's consider the absolute value of the coefficient a_{n-s} of $f(\mathtt{X})$:

$$|a_{n-s}|_{\mathfrak{P}} = |\sum_{1\leq j_1<\cdots<j_s\leq n} \xi_{j_1}\cdots\xi_{j_s}\ |_{\mathfrak{P}}$$

The maximum of the $|\xi_j|_{\mathfrak{P}}$ is reached exactly s times.

Taking combinations of s roots ξ_j will definitely yield a biggest element $\xi_{j_1}\cdots\xi_{j_s}$ where all the ξ_{j_k} have the maximum absolute value $\tilde{M}_{\mathfrak{P}}$.

This makes the absolute value of the sum of these combinations to equal their maximum.

Whence, assuming $s \neq n$, we get

$$|a_{n-s}|_{\mathfrak{P}} = \prod_{k=1}^{s}\tilde{M}_{\mathfrak{P}} = \tilde{M}_{\mathfrak{P}}^{s}$$

Thus $\tilde{M}_{\mathfrak{P}} \in \{\sqrt[i]{|a_{n-i}|_{\mathfrak{P}}}\ ;\ 1 \leq i \leq n\}$.

Therefore $\tilde{M}_{\mathfrak{P}} \leq M_{\mathfrak{P}}(f)$ and thus $|b_{r-i}|_{\mathfrak{P}} \leq M_{\mathfrak{P}}^{i}(f)$. □

Corollary 4.11

Let $f(\mathtt{X})$ and $g(\mathtt{X})$ be as in Lemma (4.10). Then the coefficients b_j of $g(\mathtt{X})$ satisfy

$$\|b_j\|_{\infty} \leq \max\{M_{\mathfrak{P}}^{i}(f) \mid 1 \leq i \leq r,\ \mathfrak{P}|\mathfrak{p}_{\infty}\} := M(f)$$

$(1 \leq j \leq r)$.

Indeed

For all $\mathfrak{P}|\mathfrak{p}_{\infty}$,

$$\|b_j\|_{\infty} \leq M_{\mathfrak{P}}^{r-j}(f) \leq max\{M_{\mathfrak{P}}^{i}(f)\ ;\ 1 \leq i \leq r\}$$

$$\begin{aligned} \|b_j\|_{\infty} &= \max_{\mathfrak{P}|\mathfrak{p}_{\infty}}|b_j|_{\mathfrak{P}} \\ &\leq \max\left\{M_{\mathfrak{P}}^{i}(f)\ ;\ 1 \leq i \leq r\,,\ \mathfrak{P}|\mathfrak{p}_{\infty}\right\} \end{aligned}$$

Remark 1:

The results in Lemma (4.10) and its Corolloray (4.11) are the analogous of the bound in Proposition (3.21) and Mignotte's bound in Theorem (3.22) for the function field case. The binomial term $\binom{deg(g)}{j}$ was eliminated by the ultra-metric property.

Remark 2:

The product formula yields $M(f) \geq 1$.

Indeed,

Assume $M(f) < 1$, and let's consider a coefficient b_j of a factor g of f, for some j.

By Lemma (4.10), $|b_j|_{\mathfrak{P}} \leq M_{\mathfrak{P}}(f)^{deg(g)-j}$ for all $\mathfrak{P}|\mathfrak{p}_\infty$.

But $M_{\mathfrak{P}}(f)^{deg(g)-j} \leq \max\{M^k_{\mathfrak{P}}(f) \mid 1 \leq k \leq r\} \leq M(f) < 1$.

Hence, $|b_j|_{\mathfrak{P}} < 1$ for all $\mathfrak{P}|\mathfrak{p}_\infty$, and thus, $\prod_{\mathfrak{P}|\mathfrak{p}_\infty} |b_j|_{\mathfrak{P}} < 1$.

On the other hand, since $b_j \in \mathcal{O}_{\mathbb{K}} = \bigcap_{\mathfrak{P}\, finite} \mathcal{O}_{\mathfrak{P}}$, $b_j \in \mathcal{O}_{\mathfrak{P}}$ for all finite places $\mathfrak{P}$. Hence $\nu_{\mathfrak{P}}(b_j) \geq 0$ for all $\mathfrak{P}$ finite. So

$$|b_j|_{\mathfrak{P}} \leq 1 \quad \text{for all finite places } \mathfrak{P} \tag{4.2}$$

Thus $\prod_{\mathfrak{P}\, finite} |b_j|_{\mathfrak{P}} \leq 1$, and so: $1 = \left(\prod_{\mathfrak{P}|\mathfrak{p}_\infty} |b_j|_{\mathfrak{P}}\right)\left(\prod_{\mathfrak{P}\, finite} |b_j|_{\mathfrak{P}} \leq 1\right) < 1$ Absurd. □

4.6 Application of the generic algorithm

Since the ring of integers $\mathcal{O}_{\mathbb{K}}$ of the global function field $\mathbb{K}$ is a Dedekind domain, the Henselian factorization technique can also be applied to polynomials having coefficients in $\mathcal{O}_{\mathbb{K}}$, (see subsection (3.3.1)). For that, given a monic squarefree polynomial $f(\mathtt{X}) \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$, we need to choose a suitable prime ideal of $\mathcal{O}_{\mathbb{K}}$, that is, a finite place $\mathfrak{P}$ of $\mathbb{K}$, since $\mathcal{O}_{\mathbb{K}} = \bigcap_{\mathfrak{P}\, finite} \mathcal{O}_{\mathfrak{P}}$, and then factor f over the $\mathfrak{P}$-adic completion $\mathbb{K}_{\mathfrak{P}}$ of $\mathbb{K}$, following the steps in Algorithm (1.4) and so recovering the factors of f in $\mathbb{K}[\mathtt{X}]$.
This amounts to applying the generic algorithm (3.11).

We choose a finite place $\boldsymbol{\mathfrak{P}}$ of degree 1 that doesn't contain $2 \cdot discr(f) \cdot discr(\boldsymbol{m}_\alpha)$, so that $\mathbb{K}_{\boldsymbol{\mathfrak{P}}}$ is unramified and f remains squarefree modulo $\boldsymbol{\mathfrak{P}}$. Avoiding $2 \in \boldsymbol{\mathfrak{P}}$ is not restrictive.
The number of places of degree 1 plays a crucial role in the theory of function fields. The Hasse-Weil theorem gives an estimate for this number, and in some cases this theorem yields even the value of the number of places of degree 1.

After choosing $\boldsymbol{\mathfrak{P}}$, the factorization of $f \mod \boldsymbol{\mathfrak{P}}$ and the Hensel lifting will be straightforward provided

a suitable integer $\mathtt{k}$ is also determined to limit the lifting process.

In the following, we will show how to choose $\mathtt{k}$ and the bound B on the coefficients of the factors of f over $\mathbb{K}$, in order to enable the reconstruction of these factors from their $\mathfrak{P}$-adic approximations.
We give an analogue of Proposition (3.25) for this case proving the existence of a lower bound for the maximum norm of the nonzero elements of a $\mathtt{k}^{th}$ power of $\mathfrak{P}$.

Proposition 4.12

Let a be a nonzero element of $\mathfrak{P}^{\mathtt{k}}$, where $\mathtt{k} \geq 1$. Then, for any finite place $\mathfrak{Q}$ in $\mathbb{K}$ lying above a rational place $\mathfrak{q}$,

$$\|a\|_\infty \geq |a|_{\mathfrak{Q}}^{-n_{\mathfrak{Q}|\mathfrak{q}}/m}.$$

Hence in particular,

$$\|a\|_\infty \geq \mathcal{N}(\mathfrak{P})^{\mathtt{k}/m}.$$

Proof:
We first prove for any $a \in \mathcal{O}_{\mathbb{K}}$ that $\|a\|_\infty \geq |a|_{\mathfrak{Q}}^{-n_{\mathfrak{Q}|\mathfrak{q}}/m}$.
For $\mathfrak{P}|\mathfrak{p}_\infty$, $|a|_{\mathfrak{P}} \leq \max\{|a|_{\mathfrak{P}'} \mid \mathfrak{P}'|\mathfrak{p}_\infty\} = \|a\|_\infty$. Hence, $|a|_{\mathfrak{P}}^{n_{\mathfrak{P}|\mathfrak{p}_\infty}} \leq \|a\|_\infty^{n_{\mathfrak{P}|\mathfrak{p}_\infty}}$, and thus:

$$\prod_{\mathfrak{P}|\mathfrak{p}_\infty} |a|_{\mathfrak{P}}^{n_{\mathfrak{P}|\mathfrak{p}_\infty}} \leq \|a\|_\infty^{\sum n_{\mathfrak{P}|\mathfrak{p}_\infty}} = \|a\|_\infty^m \tag{4.3}$$

by Proposition (4.7).
On the other hand, by the assertion (4.2) in Remark 2, since $a \in \mathcal{O}_{\mathbb{K}}$, $|a|_{\mathfrak{P}'} \leq 1$ for all finite places $\mathfrak{P}'$.
Moreover we should have: $\prod_{\mathfrak{P}|\mathfrak{p}_\infty} |a|_{\mathfrak{P}}^{n_{\mathfrak{P}|\mathfrak{p}_\infty}} \geq |a|_{\mathfrak{P}'}^{-n_{\mathfrak{P}'|\mathfrak{p}'}}$ for all $\mathfrak{P}'$ finite.
Indeed, if this is not the case for some finite $\mathfrak{P}'|\mathfrak{p}'$, then:

$$\left(\prod_{\mathfrak{P}|\mathfrak{p}_\infty} |a|_{\mathfrak{P}}^{n_{\mathfrak{P}|\mathfrak{p}_\infty}}\right)\left(|a|_{\mathfrak{P}'}^{n_{\mathfrak{P}'|\mathfrak{p}'}}\right) < 1$$

which contradicts the product formula, since all the remaining factors are smaller than 1.
In particular for the finite place $\mathfrak{Q}|\mathfrak{q}$,

$$\|a\|_\infty^m \geq \prod_{\mathfrak{P}|\mathfrak{p}_\infty} |a|_{\mathfrak{P}}^{n_{\mathfrak{P}|\mathfrak{p}_\infty}} \geq |a|_{\mathfrak{Q}}^{-n_{\mathfrak{Q}|\mathfrak{q}}} \tag{4.4}$$

Now when $a \in \mathfrak{Q}^{\mathtt{k}}$, $\nu_{\mathfrak{Q}}(a) \geq \mathtt{k}$, hence

$$|a|_{\mathfrak{Q}}^{-n_{\mathfrak{Q}|\mathfrak{q}}} = \mathcal{N}(\mathfrak{Q})^{+\nu_{\mathfrak{Q}}(a)} \geq \mathcal{N}(\mathfrak{Q})^{\mathtt{k}}$$

This, together with (4.3) and (4.4) yield for $\mathfrak{Q} = \mathfrak{P}$:

$$\|a\|_\infty \geq |a|_{\mathfrak{P}}^{-n_{\mathfrak{P}|\mathfrak{p}}/m} \geq \mathcal{N}(\mathfrak{P})^{\mathtt{k}/m}.$$

□

Remark:

Since for any finite place $\mathfrak{Q}|\mathfrak{q}$, $|a|_{\mathfrak{Q}} \leq 1$, and thus, $|a|_{\mathfrak{Q}}^{-n_{\mathfrak{Q}|\mathfrak{q}}/m} \geq 1$,
we conclude that: $\|a\|_\infty \geq 1\,, \qquad \forall a \in \mathcal{O}_{\mathbb{K}}$.

For the number field case, we were able, given such a lower bound, to find numbers in the fundamental domain that are congruent to the coefficients of the lifted factors of f. These numbers, when they are integers, do correspond to the actual coefficients of the true factors of f. Similarly, we did exhibit a lower bound in the case of a function field, however we can not use the same argument, nor the same formula (3.7) to determine the coefficients of f in their corresponding residue classes. In that case, an extensive use of the LLL-basis reduction algorithm helps achieve the goal. The latter algorithm being based on the existence of a scalar product over $\mathbb{K}$, can not be generalised to the function field case since these ones have only non-archimedean norms. Nevertheless, it is still possible to determine the coefficients of true factors, when they exist, as the elements of smallest maximum norm in their residue classes modulo $\mathfrak{P}^{\mathtt{k}}$, for a sufficiently large $\mathtt{k}$.

Proposition 4.13

Let $\mathfrak{Q}$ be a prime ideal of $\mathcal{O}_{\mathbb{K}}$ lying above a rational prime $\mathfrak{q}$, let $B > 1$.
For $\mathtt{k} \geq mLog(B)/Log(\mathcal{N}(\mathfrak{Q}))$, each residue class of $\mathcal{O}_{\mathbb{K}}/\mathfrak{Q}^{\mathtt{k}}$ contains at most one element a with $\|a\|_\infty < B$.

Proof:

Assume there exist two distinct elements $a, b \in \mathcal{O}_{\mathbb{K}}$ that are in the same residue class modulo $\mathfrak{Q}^{\mathtt{k}}$ and both satisfy the bound condition. Assume $\|a\|_\infty \leq \|b\|_\infty$, then we have:
$a - b \in \mathfrak{Q}^{\mathtt{k}}$ and thus, by Proposition (4.12), $\|a - b\|_\infty \geq \mathcal{N}(\mathfrak{Q})^{\frac{\mathtt{k}}{m}}$.
In addition, $\|a - b\|_\infty \leq \max\{\|a\|_\infty, \|b\|_\infty\} = \|b\|_\infty < B$.
Hence, $B > \mathcal{N}(\mathfrak{Q})^{\frac{\mathtt{k}}{m}}$ and so $\mathtt{k} < mLog(B)/Log(\mathcal{N}(\mathfrak{Q}))$. Contradiction.

□

Combining the results in Corollary (4.11) and in the Proposition above, we see that, if B is chosen such that $B \geq M(f)$, and if $\mathtt{k} \geq mLog(B)/Log(\mathcal{N}(\mathfrak{Q}))$, then the coefficients of any factor of f in $\mathbb{K}[\mathtt{X}]$ is the unique element, of its residue class of maximum norm bounded by B.

4.7 Existence of polynomial-time factorization algorithms

In this section, we will be concerned with lattice-based techniques for factorization over function fields in order to show that the results of Lenstra et al. concerning the factorization of polynomials over number fields do actually hold for function fields as well. This will prove the existence of polynomial-time algorithms for factorization of polynomials over function fields provided an algorithm for lattice bases reduction similar to the LLL algorithm can be found which has a polynomial running time.
The two following propositions are the generalisations of Propositions (3.5) and (3.6), for which the proofs apply as well. We will then consider $\mathbb{K}$ any global field.

Assume we are given a polynomial $f \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ of degree $n > 0$, a nonzero prime ideal $\mathfrak{P}$ of $\mathcal{O}_{\mathbb{K}}$, and a polynomial $h \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ satisfying the following conditions:

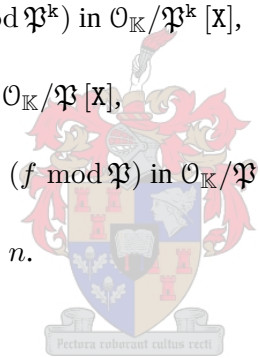
(C.1) h monic,

(C.2) $(h \bmod \mathfrak{P}^{\mathtt{k}})$ divides $(f \bmod \mathfrak{P}^{\mathtt{k}})$ in $\mathcal{O}_{\mathbb{K}}/\mathfrak{P}^{\mathtt{k}}[\mathtt{X}]$,

(C.3) $(h \bmod \mathfrak{P})$ is irreducible in $\mathcal{O}_{\mathbb{K}}/\mathfrak{P}[\mathtt{X}]$,

(C.4) $(h \bmod \mathfrak{P})^2$ does not divide $(f \bmod \mathfrak{P})$ in $\mathcal{O}_{\mathbb{K}}/\mathfrak{P}[\mathtt{X}]$.

Let $l = \deg(h(\mathtt{X}))$. Hence $0 < l \leq n$.
We can then prove the following.



Proposition 4.14

The polynomial f has a monic irreducible factor $h_0 \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ of degree $r > 0$, $l \leq r \leq n$, uniquely determined up to sign, such that $(h \bmod \mathfrak{P})$ divides $(h_0 \bmod \mathfrak{P}^{\mathtt{k}})$ in $\mathcal{O}_{\mathbb{K}}/\mathfrak{P}[\mathtt{X}]$.
Further, if $g(\mathtt{X})$ is a monic divisor of $f(\mathtt{X})$ in $\mathcal{O}_{\mathbb{K}}[\mathtt{X}]$, then the following assertions are equivalent:

(i) $(h \bmod \mathfrak{P})$ *divides* $(g \bmod \mathfrak{P})$ *in* $\mathcal{O}_{\mathbb{K}}/\mathfrak{P}[\mathtt{X}]$,

(ii) $(h \bmod \mathfrak{P}^{\mathtt{k}})$ *divides* $(g \bmod \mathfrak{P}^{\mathtt{k}})$ *in* $\mathcal{O}_{\mathbb{K}}/\mathfrak{P}^{\mathtt{k}}[\mathtt{X}]$,

(iii) $h_0(\mathtt{X})$ *divides* $g(\mathtt{X})$ *in* $\mathcal{O}_{\mathbb{K}}[\mathtt{X}]$,

In particular $(h \bmod \mathfrak{P}^{\mathtt{k}})$ *divides* $(h_0 \bmod \mathfrak{P}^{\mathtt{k}})$ *in* $\mathcal{O}_{\mathbb{K}}/\mathfrak{P}^{\mathtt{k}}[\mathtt{X}]$

Proof:

The existence of h_0 follows from (**C2**) and (**C3**) since irreducibility is preserved during the Hensel lifting by the coprimality and coherence conditions (cf section (1.2)). The uniqueness of h_0, up to sign,

comes from (**C4**). The implications (ii)⇒(i) and (iii)⇒(i) are obvious by reduction. Assuming (i) now, i.e $(h \bmod \mathfrak{P})$ divides $(g \bmod \mathfrak{P})$ in $\mathcal{O}_{\mathbb{K}}/\mathfrak{P}[\mathtt{X}]$, let's prove (ii) and then (iii).
The squarefree polynomial f is divisible by g in $\mathcal{O}_{\mathbb{K}}[\mathtt{X}]$, so $f/g \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ and is relatively prime with g. By (**C3**), (i) and (**C4**), we know $(h \bmod \mathfrak{P})$ and $(f/g \bmod \mathfrak{P})$ are coprime. So there exist polynomials $\lambda(\mathtt{X}), \mu(\mathtt{X}) \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ and $\eta(\mathtt{X}) \in \mathfrak{P}[\mathtt{X}]$ so that:

$$\lambda(\mathtt{X})\, h(\mathtt{X}) + \mu(\mathtt{X})\, f/g(\mathtt{X}) = 1 - \eta(\mathtt{X})$$

Multiplying both sides by the polynomial $g(1 + \eta + \eta^2 + \cdots + \eta^{\mathtt{k}-1})$ yields

$$\tilde{\lambda}(\mathtt{X})\, h(\mathtt{X}) + \tilde{\mu}(\mathtt{X})\, f(\mathtt{X}) = g - g\eta^{\mathtt{k}}(\mathtt{X})$$

Now reducing modulo $\mathfrak{P}^{\mathtt{k}}$ gives clearly (ii) as $(h \bmod \mathfrak{P}^{\mathtt{k}})$ divides the right hand side of this equality.
For (iii), let's note that the irreducible polynomial h_0 divides f in $\mathcal{O}_{\mathbb{K}}[\mathtt{X}]$, so if it doesn't divide g, it should divide f/g. By reducing modulo $\mathfrak{P}$, we get a contradiction with (**C4**), which proves (iii). □

Following Lenstra et al. (cf subsection (3.2.1)), we give a constructive method based on lattice techniques which determines h_0. If h divides f in $\mathcal{O}_{\mathbb{K}}[\mathtt{X}]$, then $h_0 = h$. Otherwise, we will search for h_0 as an element of a certain "*lattice*" to be defined.

So far we have used the definition of page (18) for lattices, which enables us to work with lattices in an Euclidean space $\mathbb{R}^d$, and also lattices in a polynomial ring by identifying polynomials with the vectors of their coefficients, assuming a certain ordering on these coefficients. However, the concept of *lattice* bears intrinsic properties that enable defining lattices in a more general context, as *free-$\tilde{R}$-modules of some rank* $\mathtt{k}$*, lying inside some finite dimensional vector space $\tilde{K}^d$, where $\tilde{K}$ is either the quotient field of the ring $\tilde{R}$ or any extention of it.*

In analogy to Lenstra et al. (cf [L-L-L] and page (46)), we need to consider the set L of polynomials in $\mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ of degree less than some fixed r, that when reduced $\bmod \mathfrak{P}^{\mathtt{k}}$, are divisible by $\left(h \bmod \mathfrak{P}^{\mathtt{k}}\right)$. We will choose r so that $h_0 \in L$. Observe that $L \neq \{0\}$ since $h \in L$.
Recall that, since $\mathbb{K}$ here is any global field, K will denote either $\mathbb{Q}$ or $\mathbb{F}_q(t)$. So let R denote either $\mathbb{Z}$ or $\mathbb{F}_q[t]$, and consider an integral basis of $\mathbb{K}$, $\omega_1, \cdots, \omega_m$, i.e a system of K-linearly independant integers which span $\mathcal{O}_{\mathbb{K}}$ as an R-module. Using such a basis enables us not to worry about *denominators*. It also enables us to identify an element $a = \sum_{j=1}^{m} a_j \omega_j$ of $\mathcal{O}_{\mathbb{K}}$ with the vector $\boldsymbol{a} = (a_1, \cdots, a_m)^{tr}$ of R^m.
A polynomial $g = \sum_{i=0}^{d} g_i \mathtt{X}^i = \sum_{i=0}^{d} (\sum_{j=1}^{m} a_{ij}\, \omega_j) \mathtt{X}^i \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ with degree $d \leq r$, will then be identified with the vector
$\boldsymbol{g} = (a_{01}, \cdots, a_{0m}, a_{11}, \cdots, a_{rm})^{tr} \in R^{(r+1)m}$, where $a_{ij} = 0$ if $i > d$.

To measure the size of an integer $a \in \mathcal{O}_{\mathbb{K}}$ or a polynomial $g \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ we define the following norms:

$$\text{For } a \in \mathcal{O}_{\mathbb{K}}, \quad |a|' = \begin{cases} \|\boldsymbol{a}\| = (\sum_{j=1}^{m} a_j^2)^{1/2} & \text{if } R = \mathbb{Z} \\ \begin{cases} deg_t(a) = \max\limits_{1 \le j \le m} deg(a_j) & \text{if } a \neq 0 \\ 0 \text{ otherwise} \end{cases} & \text{if } R = \mathbb{F}_q[t] \end{cases}$$

$$\text{And for } g \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}], \quad \|g\|' = \begin{cases} \|\boldsymbol{g}\| & \text{(cf page 46) if } R = \mathbb{Z} \\ \max_{0 \le i \le d} |g_i|' & \text{if } R = \mathbb{F}_q[t] \end{cases}$$

On the other hand, since R is a PID, there exists a prime $\pi \in R$ so that $\mathfrak{P} \cap R = \pi R$. Hence, examining the elements of L, we see that L is spanned over R by the K-linearly independent elements of $\mathcal{O}_{\mathbb{K}}[\mathtt{X}]$:

$$\left\{ \pi^{\mathtt{k}}\, \omega^j\, \mathtt{X}^i \;\middle|\; 1 \le j \le m\,,\ 0 \le i < l \right\} \cup \left\{ \omega^j\, h(\mathtt{X})\, \mathtt{X}^{i-l} \;\middle|\; 1 \le j \le m\,,\ l \le i \le r \right\}$$

And thus L can be viewed as an R-lattice, by identifying it with the corresponding[1] lattice in $K^{(r+1)m}$. Clearly, this lattice has determinant $d(L) = \pi^{\mathtt{k}lm}$. (Recall that $l = deg(h)$.)

Remark:

By representing the elements of $\mathbb{K}$ and $\mathcal{O}_{\mathbb{K}}$ with respect to the integral basis $\omega_1, \cdots, \omega_m$, addition and substraction of those elements are easily done coefficient-wise, which is not the case for the other arithmetical operations. For instance, to calculate a product, an already computed *multiplication table* is needed. This is a table $\Gamma \in R^{m \times m \times m}$ which represents the products $\omega_i \omega_j$ with respect to the basis itself, that is:

$$\omega_i \omega_j = \sum_{k=1}^{m} \Gamma(i,j,k)\omega_k \qquad \text{where } \Gamma(i,j,k) \in R$$

The entries of Γ can be obtained using the transition matrix from the basis $\{1, \alpha, \cdots, \alpha^{m-1}\}$ to the basis $\omega_1, \cdots, \omega_m$,

$$(\omega_1, \cdots, \omega_m)\mathtt{T} = (1, \alpha, \cdots, \alpha^{m-1})$$

Thus, if $a = \sum_{j=1}^{m} a_j \omega_j \in \mathcal{O}_{\mathbb{K}}$, and $g = \sum_{i=0}^{d} g_i \mathtt{X}^i = \sum_{i=0}^{d} (\sum_{j=1}^{m} a_{ij}\, \omega_j) \mathtt{X}^i \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$

$$a\omega_k = \sum_{j=1}^{m} a_j \omega_k \omega_j = \sum_{j=1}^{m} a_j \left(\sum_{l=1}^{m} \Gamma(j,k,l)\omega_l \right) = \sum_{l=1}^{m} \left(\sum_{j=1}^{m} a_j \Gamma(j,k,l) \right) \omega_l = \sum_{l=1}^{m} b_l \omega_l\,, \quad b_l \in R.$$

and

$$g\omega_k = \sum_{i=0}^{d} (g_i \omega_k) \mathtt{X}^i = \sum_{i=0}^{d} \sum_{l=1}^{m} \left(\sum_{j=1}^{m} a_{ij} \Gamma(j,k,l) \right) \omega_l \mathtt{X}^i$$

[1] By this identification, we will call R-lattice any subset of the polynomial ring $\mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ whose image is an R-lattice in some K^d.

Whence, if $R = \mathbb{Z}$,

$$\|g\omega_k\|'^2 = \sum_{i,l}\left(|\sum_{j=1}^{m} a_{ij}\Gamma(j,k,l)|\right)^2 \leq \sum_{i,l}\left(\sum_{j=1}^{m}|a_{ij}||\Gamma(j,k,l)|\right)^2$$

$$\leq \sum_{i,l}\left(\max_{j,k,l}|\Gamma(j,k,l)|\sum_{j=1}^{m}|a_{ij}|\right)^2$$

$$\leq (\max_{j,k,l}|\Gamma(j,k,l)|)^2\sum_{i,l}(\sum_{j=1}^{m}|a_{ij}|)^2 \leq (\max_{j,k,l}|\Gamma(j,k,l)|)^2\sum_{l=1}^{m}\left(\sum_{i,j}|a_{ij}|^2\right) = (\max_{j,k,l}|\Gamma(j,k,l)|)^2 m\|g\|'^2$$

In this case, set $C := \max_{j,k,l}|\Gamma(j,k,l)|)\sqrt{m}$ so that: $\|g\omega_k\|' \leq C\|g\|'$.

Now when $R = \mathbb{F}_q[t]$,

$$|a\omega_k|' = \max_l \deg\left(\sum_{j=1}^{m} a_j\Gamma(j,k,l)\right) \leq \max_l\left(\max_{1\leq j\leq m}\deg_t(a_j\Gamma(j,k,l))\right)$$

$$\leq \max_l\max_j(\deg_t(a_j)+\deg_t(\Gamma(j,k,l)))$$

$$\leq \max_j\deg_t(a_j)+\max_{j,k,l}\deg_t(\Gamma(j,k,l) = |a|'+\max_{j,k,l}\deg_t(\Gamma(j,k,l)$$

Set $\tilde{C} := \max_{j,k,l}\deg_t(\Gamma(j,k,l))$ and $C := \tilde{C}+1$.

If $a = 0$, then $0 = |a|' = |a\omega_k|' \leq C|a|'$.

Now, if $a \neq 0$, then $|a|' \geq 1$, thus $\tilde{C}|a|' \geq \tilde{C}$, and so

$$|a\omega_k|' \leq |a|'+\tilde{C}|a|' \leq C|a|'$$

This implies:

$$\|g\omega_k\|' = \|\sum_{i=0}^{d} g_i\omega_k\mathtt{X}^i\|' = \max_{0\leq i\leq d}|g_i\omega_k|' \leq \max_{0\leq i\leq d} C|g_i|' = C\max_{0\leq i\leq d}|g_i|' = C\|g\|'$$

Hence there is a constant C such that: $\|g\omega_k\|' \leq C\|g\|'$.

Proposition 4.15

Let a non-zero polynomial b of L satisfy:

$$d(L) = \pi^{\mathtt{k}lm} > C^{n+r}\,\|b\|'^n\|f\|'^r \tag{4.5}$$

where C is the constant defined above.

Then b is divisible by h_0 in $\mathbb{K}[\mathtt{X}]$, and in particular $GCD(f,b) \neq 1$.

Proof:

To prove that h_0 divides b in $\mathbb{K}[\mathtt{X}]$, we will actually prove that h_0 divides $g := GCD(f, b)$ in $\mathbb{K}[\mathtt{X}]$, and for that it suffices, by Proposition (4.14), to show that $(h \bmod \mathfrak{P})$ divides $(g \bmod \mathfrak{P})$ in $\mathcal{O}_{\mathbb{K}}/\mathfrak{P}\,[\mathtt{X}]$.[2]
Assume this is not the case. So by **(C.3)**, there exist polynomials $\lambda_0(\mathtt{X}), \mu_0(\mathtt{X}) \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}]$ and $\eta_0(\mathtt{X}) \in \mathfrak{P}[\mathtt{X}]$ satisfying:

$$\lambda_0(\mathtt{X})\, h(\mathtt{X}) + \mu_0(\mathtt{X})\, g(\mathtt{X}) = 1 - \eta_0(\mathtt{X}) \tag{4.6}$$

Set $M := \{\lambda\, f + \mu\, b \in \mathcal{O}_{\mathbb{K}}[\mathtt{X}] \mid deg(\lambda) < deg(b) - deg(g)\ \&\ deg(\mu) < n - deg(g)\}$.
The nonzero elements of M are multiples of g and have degrees:

$$deg(g) \le deg(\lambda f + \mu b) \le \max\{deg(\lambda) + n,\, deg(\mu) + deg(b)\} < n + deg(b) - deg(g)$$

Note that: $deg(g) \le deg(b) \le r$ and thus $0 \le deg(b) - deg(g) \le r - deg(g) \le r$.

In addition, M is generated over R by the polynomials:

$$\left\{\omega^j\, \mathtt{X}^i f \mid\ 1 \le j \le m\,,\ 0 \le i < deg(b) - deg(g)\right\} \cup \left\{\omega^j\, \mathtt{X}^i b \mid\ 1 \le j \le m\,,\ 0 \le i < n - deg(g)\right\} \tag{4.7}$$

which we identify with the $m(n + deg(b) - 2deg(g))$-dimensional vectors of their coefficients.
So their projections on $\oplus_{i,j}\omega_j \mathtt{X}^i\, R$, where $1 \le j \le m$ and $deg(g) \le i \le n + deg(b) - deg(g)$, form a basis of an R-lattice $\tilde{M}$ of rank $m(n + deg(b) - 2deg(g))$.
Indeed, it suffices to show that they are K-linearly independent.
Suppose an R-linear combination of the polynomials in (4.7), i.e an element $\lambda\, f + \mu\, b$ of M, projects to zero in $\tilde{M}$. So $deg(\lambda f + \mu b) < deg(g)$ which implies that $\lambda f + \mu b = 0$ because it is a multiple of g. Hence, $\lambda\, f/g = -\mu\, b/g$, where $GCD(f/g,\, b/g) = 1$. This implies that f/g divides μ. But $deg(\mu) < n - deg(g) = deg(f/g)$, and thus $\mu = 0$. Therefore $\lambda = \mu = 0$. And so, the projections of the polynomials in (4.7) effectively form a basis of the lattice $\tilde{M}$.

By Hadamard inequality we get,

$$d(M) = d(\tilde{M}) \le \prod_{i,j} \|\omega^j\, \mathtt{X}^i f\|' \prod_{i,j} \omega^j\, \mathtt{X}^i b\|' \le C^{n+deg(b)}\, \|f\|'^{deg(b)}\, \|b\|'^n \le C^{n+r}\, \|f\|'^r\, \|b\|'^n < \pi^{\mathbf{k}lm}$$

from our hypothesis.

On the other hand, we can prove that the subset: $M' = \{\gamma \in M \mid deg(\gamma) < deg(g) + deg(h)\}$[3]

[2] Note that Proposition (4.14) can not be applied to b because b is not necessarily a factor of f.

[3] Note that since $(h \bmod \mathfrak{P})$ divides $(f \bmod \mathfrak{P})$ and not $(g \bmod \mathfrak{P})$ it then divides $(f/g \bmod \mathfrak{P})$, so we get
$$deg(g) + deg(h) \le deg(b) + deg(f/g) = n + deg(b) - deg(g).$$

of M is contained in $\mathfrak{P}^{\mathtt{k}}[\mathtt{X}]$. Indeed, let $\gamma \in M$, then $g|\gamma$ and from Equation (4.6) we deduce that:

$$(\lambda_0\, h + \mu_0\, g)\gamma/g = (1-\eta_0)\gamma/g$$
$$(\lambda_0\gamma/g)h + \mu_0\gamma = (1-\eta_0)\gamma/g$$

Multiplying both sides by the polynomial $(1+\eta_0+\cdots+\eta_0^{\mathtt{k}-1})$ we get:

$$\tilde{\lambda}\, h + \tilde{\mu}\, \gamma = \gamma/g - \eta_0^{\mathtt{k}}\, \gamma/g$$

Then, since $b \in L$, $(h \bmod \mathfrak{P}^{\mathtt{k}})$ divides $(b \bmod \mathfrak{P}^{\mathtt{k}})$ in $\mathcal{O}_{\mathbb{K}}/\mathfrak{P}^{\mathtt{k}}[\mathtt{X}]$, and so it also divides $(g \bmod \mathfrak{P}^{\mathtt{k}})$. This implies that $(h \bmod \mathfrak{P}^{\mathtt{k}})$ divides $(\gamma \bmod \mathfrak{P}^{\mathtt{k}})$ since $g|\gamma$. Whence, $(h \bmod \mathfrak{P}^{\mathtt{k}})$ divides $(\gamma/g \bmod \mathfrak{P}^{\mathtt{k}})$. But then,

$$deg(h) \leq deg(\gamma/g) = deg(\gamma) - deg(g) < deg(h)$$

by definition of M'. Contradiction.
Therefore γ/g belongs to $\mathfrak{P}^{\mathtt{k}}[\mathtt{X}]$ and so does γ itself.

Knowing that $M' \subset \mathfrak{P}^{\mathtt{k}}[\mathtt{X}]$, we will derive a contradiction which concludes the proof of Proposition(4.15).

Let $b_1, \cdots, b_t$ be a basis of M' is Hermite Normal Form, given in terms of the basis $\omega_j \mathtt{X}^i$ of $\mathcal{O}_{\mathbb{K}}[\mathtt{X}]$. Hence, the matrix of the b_j's is triangular and so $d(M')$ equals the product of the norms of the diagonal elements of this matrix, i.e, the product of the norms of the leading coefficients of the b_j's. Since $b_j \in \mathfrak{P}^{\mathtt{k}}[\mathtt{X}]$, $lc(b_j) \in \mathfrak{P}^{\mathtt{k}} \cap R = \pi^{\mathtt{k}} R$ and so $d(M')$ is a power of $\pi^{\mathtt{k}}$.
Moreover we know since $b_j \in M'$ that $deg(b_j) \leq l + deg(g) \leq n + deg(b) - deg(g) \leq n + r$.
Considering among the b_j those with $deg(b_j) \leq l$ (there are $m \times l$ of them) yields: $d(M') \geq \pi^{kml}$.
Thus $\pi^{kml} \leq d(M') \leq d(M) < \pi^{kml}$. Contradiction. □

This, unfortunately remains a theoretical result, but is good as it shows that the problem studied is no longer difficult. However the large dimensions of the lattices involved in this case make this approach impractical.

Bibliography

[ABB] **J. A. Abbott,** *On the Factorization of Polynomials over Algebraic Fields.* PhD thesis, School of Math. Sciences, University of Bath, England (1988)

[A-S-Z] **J. A. Abbott, V. Shoup & P. Zimmermann**, *Factorization in $\mathbb{Z}[x]$: The Searching Phase.* to appear in ISSAC 2000

[A-M] **M.F. Atiyah & I.G. Macdonald,** *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company (1969)

[ART] **E. Artin,** *Algebraic numbers and algebraic functions*. Gordon and Breach, New York, (1967)

[BEL 1] **K. Belabas,** *A Relative van Hoeij Algorithm over Number Fields.* to appear in Journal of Symbolic Computation,

[BEL 2] **K. Belabas,** *Topics in Computational Algebraic Number Theory* . Available from the Internet.

[B-H-K-S] **K. Belabas, M. van Hoeij, J. Kluners & A. Steel** *Factoring Polynomials over Globel Fields.* ArXiv: math NT/0409510v1 27 Sept (2004)

[B-H-Z] **K. Belabas, G. Hanrot & P. Zimmermann,** *Tuning and Generalizing van Hoeij's Algorithm.* Rapport de Recherche N^o 4124, INRIA, France, February (2001)

[BER] **E. R. Berlekamp,** *Factoring Polynomials Over Large Finite Fields.* Mathematics of Computation, Vol 24 N^o 111, July (1970), pp 713-735,

[C-G] **D. G. Cantor & D. Gordon,** *Factoring Polynomials over p-adic Fields.* Proceedings of ANTS IV, LNCS 1838, (2000), pp. 185-208 .

[C-Z] **D. G. Cantor & H. Zassenhaus ,** *A New Algorithm for Factoring Polynomials Over Finite Fields.* Mathematics of Computation, Vol 36 N^0 154, April (1981), pp 587-592,

[COH] **H. Cohen,** *A Course in Computational Algebraic Number Theory.* Springer-Verlag, Berlin Heidelberg (1993)

[EIC] **M. Eichler** *Introduction to the theory of algebraic numbers and functions* . Translated by G. Striker, Academic Press, New York, (1966)

[ENC] **M.J. Encarnación ,** *Factoring Polynomials over Algebraic Number Fields via Norms.* Proceeding of the ISSAC'97, Hawaii, (1997), pp 265-270, ACM Press, USA

[F-G-P] **P. Flajolet, X. Gordon & D. Panario,** *The Complete Analysis of a Polynomial Factorization Algorithm over Finite Fields.* Journal of Algorithms (2001), Academic Press

[Fr-T] **A. Fröhlich & M.J. Taylor,** *Algebraic number theory*. Cambridge University Press, England, (1991)

[G-P] **J. von zur Gathen & D. Panario,** *Factoring Polynomials Over Finite Fields: A Survey.* Journal of Symbolic Computation , Vol 31 (2001), pp 3-17

[G-G] **J. von zur Gathen & J. Gerhard ,** *Modern Computer Algebra*. Cambridge University Press, 1^{st} edition (1999).

[G-C-L] **K. O. Geddes, S. R. Czapor, G. Labahn,** *Algorithms for computer algebra*. Kluwer Academic Publishers, 1992, 6^{th} printing (1999)

[G-A] **H. Gunji & D. Arnon,** *On Polynomial Factorization Over Finite Fields.* Mathematics of Computation, Vol 36 N^o 153, January (1981), pp 281-287

[HOE 1] **M. van Hoeij,** *An Algorithm for Computing an Integral Basis Reduction in an Algebraic Function Field.* Journal of Symbolic Computation, Vol 18 (1994), pp 353 - 363

[HOE 2] **M. van Hoeij,** *Factoring Polynomials and the Knapsack Problem.* Journal of Number theory, Vol 95, (2002), pp 167-189

[KAL 1] **E. Kaltofen,** *Factorization of Polynomials.* in Computer Algebra Symbolic and Algebraic Computation, by B. Buchberger et al. pp 95-113, 2nd Edition (1982)

[KAL 2] **E. Kaltofen,** *On The Complexity of Factoring Polynomials with Integer Coefficients.* PhD Thesis, University of Delaware, Newark USA (1982)

[K-M-S] **E. Kaltofen, D. R. Musser, B. D. Saunders,**
A Generalized Class of Polynomials that are Hard to Factor. SIAM Journal of Computation, Vol 12 N^{o}3, August (1983), pp 473-483

[KNU] **D. Knuth,** *The Art of Computer Programming, Vol2: Seminumerical Algorithms.* 3^{rd} edition, Addison-Wesley, Reading MA (1997)

[LAD] **S. Landau ,** *Factoring Polynomials Over Algebraic Number Fields.* SIAM Journal of Computation, Vol 14 N^{o}2, February (1985), pp 184-195

[LAG] **S. Lang**, *Algebra*, Addison-Wesley series in Mathematics, N 4177, (1971)

[LEN 1] **A. K. Lenstra**, *Factorization of Polynomials.* in Computational Methods in Number Theory, Part I, Mathematical Centre Tracts 154, Mathematisch Centrum, Amsterdam, pp 168-198 (1982)

[LEN 2] **A. K. Lenstra**, *Lattices and Factorization of Polynomials over Algebraic Number Fields.* Proceeding Eurocam'82, LNCS vol 144, (1982), pp 32-39

[LEN 3] **A. K. Lenstra**, *Factoring Polynomials over Algebraic Number Fields.* LNCS, vol 162, (1983), pp 245-254

[L-L-L] **A. K. Lenstra, H. W. Lenstra, & L.Lovasz** , *Factoring Polynomials with Rational Coefficients,* Math. Ann. Vol 261 N^o 4 (1982), pp 515-534

[LOR] **D. Lorenzini** *An invitation to arithmetic geometry* . Graduate series in mathematics, American Mathematical Society, (1996)

[MIG] **M. Mignotte** *An Inequality About Factors of Polynomials*. Mathematics of Computation, Vol 28 N^o 128, October (1974), pp 1153-1157

[M-S] **M. Mignotte & D. Stefãnescu** *La Première Méthode de Factorisation des Polynômes.* Preprint IRMA Strasbourg N 2001-010, (2001) Available on the Internet at:
http://www-irma.u-strasbg.fr/irma/publications/2001/01010.shtml

[MOE] **R. Moenck,** *On the Efficiency of Algorithms for Polynomial Factoring.* Mathematics of Computation, Vol 31 N^o 137, January (1977), pp 235-250

[NAR] **W. Narkiewicz,** *Elementary and Analytic Theory of Algebraic Numbers.* Springer-Verlag & Polish Scientific Publishers, Second edition (1990)

[Om-P] **J. M. Omaña & M. E. Pohst,** *Factoring Polynomials over Global Fields II* to appear in Journal of Symbolic Computation

[POH 1] **M. E. Pohst,** *Computational Algebraic Number Theory.* DMV Seminar, Band 21 Birkhauser Verlag (1993)

[POH 2] **M. E. Pohst,** *Factoring Polynomials over Global Fields I* Journal of Symbolic Computation , Vol 39 (2005), pp 617-630

[P-Sc] **M. E. Pohst & & M. Schörnig,** *On Integral Basis Reduction in Global Function Fields.* LNCS, vol 1122, (1996), pp 273-282

[P-Z] **M. E. Pohst & H. Zassenhaus,** *Algorithmic Algebraic Number Theory* Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge (1989)

[Pr-D] **A. Prestel & C. N. Delzell,** *Positive Polynomials.* Springer-Verlag, Berlin - Heidelberg (2001)

[PRA] **V. V. Prasolov** *Polynomials.*, series Algorithms & Computation in Mathematics, Vol 11, Springer-Verlag, Berlin - Heidelberg (2004)

[REI] **I. Reiner,** *Maximal Orders.* Academic Press Inc. (London) Ltd, (1975)

[ROB 1] **X. F. Roblot,** *Algorithmes de Factorization dans les Extensions Relatives et Applications de la Conjecture de Stark à la construction des corps de Classes de Rayon.* Thèse de Doctorat, Université de Bordeaux (1997)

[ROB 2] **X. F. Roblot,** *Polynomial Factorization Algorithms over Number Fields.* Journal of Symbolic Computation, Vol 11 (2002), pp 1-14

[ROS] **M. Rosen** *Number Theory in Function Fields* . GTM, Springer-Verlag, (2002)

[SCH] **W.M. Schmidt,** *Construction and Estimation of Bases in Function Fields.* Journal of Number Theory, Vol 39, (1996), pp 181 - 224

[SHO] **V. Shoup,** *A New Polynomial Factorization Algorithm and its Implementation.* Journal of Symbolic Computation, Vol 20 Issue 4, October (1996), pp 363 - 397

[STI] **H. Stichtenoth,** *Algebraic Function Fields and Codes.* Springer-Verlag (1993)

[W-R] **P.I. Weinberger & L.P. Rothschild,** *Factoring Polynomials over Algebraic Number Fields.* ACM Transactions on Mathematical Software (TOMS), Vol 2 Issue 4, December (1976), pp 335-350

[WIN] **F. Winkler,** *Polynomial Algorithms in Computer Algebra.* Series Texts& Monographs in Symbolic Computatio. Springer-Verlag, (1996)

[ZAS 1] **H. Zassenhaus,** *On Hensel factorization I.* Journal of Number Theory, Vol 1, (1969), pp 291-311

[ZAS 2] **H. Zassenhaus,** *A Remark on the Hensel Factorization Method.* Mathematics of Computation, Vol 32 N^o 141, January (1978), pp 287-292

[ZAS 3] **H. Zassenhaus,** *On Polynomial Factorization.* Rocky Mountain Journal of Mathematics, Vol 15 N^o 2, Spring (1985), pp 657-665

[Z-S] **O.Zariski & P. Samuel,** *Commutative Algebra.* Vol I Springer Verlag, 2nd printing, USA (1979)

Index